



**Júlio Battisti**

**Aprovado em 30 Exames de Certificação Microsoft:**

MCP 2000 e 2003, MCP+I, MCSE +I,  
MCSE 2000, MCSE 2003, MCSA 2000,  
MCSA 2003, MCSD, MCDBA e MCDST

Guia de  
Estudos Para o

**MCSE 70-290**

**Site: [www.juliobattisti.com.br](http://www.juliobattisti.com.br)**  
**e-mail: [webmaster@juliobattisti.com.br](mailto:webmaster@juliobattisti.com.br)**

## **Nota sobre direitos autorais:**

Este ebook é de autoria de Júlio Battisti, sendo comercializado diretamente através do site [www.juliobattisti.com.br](http://www.juliobattisti.com.br) ou através do site de leilões Mercado Livre: [www.mercadolivre.com.br](http://www.mercadolivre.com.br), pelo usuário GROZA. **Nenhum outro usuário, pessoa ou site está autorizado a vender este ebook.**

Ao adquirir este ebook você tem o direito de lê-lo na tela do seu computador e de imprimir quantas cópias desejar. É vedada a distribuição deste arquivo, mediante cópia ou qualquer outro meio de reprodução, para outras pessoas. **Se você recebeu este ebook através do e-mail ou via ftp de algum site da Internet, ou através de um CD de Revista, saiba que você está com uma cópia pirata, não autorizada. A utilização de uma cópia pirata, não autorizada, é crime de Violação de Direitos Autorais, sujeita a pena de Cadeia.**

O valor cobrado por este arquivo é praticamente simbólico, pelas horas e horas de trabalho que ele representa. Novos e-books somente poderão ser desenvolvidos pela honestidade de pessoas que adquirem o arquivo do e-book e não o distribuem livremente para outras pessoas. Se você recebeu uma cópia deste arquivo sem tê-la adquirido diretamente com o autor, seja honesto, entre em contato com o autor, através do e-mail [webmaster@juliobattisti.com.br](mailto:webmaster@juliobattisti.com.br), para regularizar esta cópia.

Ao regularizar a sua cópia você estará remunerando, mediante uma pequena quantia, o trabalho do autor e incentivando que novos trabalhos sejam disponibilizados.

Se você tiver sugestões sobre novos cursos que gostaria de ver disponibilizados, entre em contato pelo e-mail: [webmaster@juliobattisti.com.br](mailto:webmaster@juliobattisti.com.br).

Visite periodicamente o site [www.juliobattisti.com.br](http://www.juliobattisti.com.br) para ficar por dentro das novidades:

- ◆ Cursos de informática.
- ◆ Artigos e dicas sobre Certificações da Microsoft.
- ◆ Artigos sobre Carreira e Trabalho.
- ◆ Dicas de livros e sites sobre diversos assuntos.
- ◆ Simulados gratuitos, em português, para os exames da Microsoft.

**PIRATARIA É CRIME, COM PENA DE CADEIA. EU AGRADEÇO PELA SUA HONESTIDADE. SE VOCÊ COMPROU UMA CÓPIA DESTE CURSO, DIRETAMENTE COM O AUTOR, NÃO DISTRIBUA CÓPIAS PARA OUTRAS PESSOAS. SE VOCÊ RECEBEU UMA CÓPIA ILEGAL DESTE ARQUIVO, NÃO ADQUIRIDA DIRETAMENTE COM O AUTOR JÚLIO BATTISTI, ENTRE EM CONTATO E REGULARIZE A SUA CÓPIA.**

# Agradecimentos

Escrever um manual detalhado para o Exame 70-290 parece fácil diante do momento de parar e escrever algumas palavras de agradecimento. Sempre fica o medo de ter esquecido de alguém, já que são tantas as pessoas que, direta ou indiretamente, contribuem para que um trabalho como este se torne realidade.

Ninguém conseguiria concluir um trabalho deste porte sem a ajuda, o incentivo e, principalmente, a confiança de muitas pessoas. Inicialmente queria registrar o meu agradecimento pelo convite e pela confiança do amigo e editor Ricardo. Principalmente pela sua insistência e confiança no meu trabalho, em momentos em que eu estive não tão animado como de costume. Em seguida a equipe da Axcel que mais uma vez apostou em um trabalho de minha autoria, passando pelos colegas de produção, edição, arte gráfica, revisão, enfim, uma equipe trabalhando muito para que mais este livro chegue às mãos do amigo leitor.

A minha esposa Lu, pelo carinho, amor, dedicação, companheirismo e tolerância. Por tantas e tantas horas que ela teve que passar sozinha e eu, em frente ao computador. Pelos domingos em que ficamos em casa ao invés de sairmos. Mas ela sabe que isso tudo faz parte de um projeto de vida de longo prazo e que muitos resultados já estão presentes em nosso dia-a-dia.. Dividir o marido com os livros, com o trabalho na Receita Federal, com dois sites na Internet e com uma rede de computadores em casa realmente não é uma tarefa fácil. Apenas com muito, mas muito mesmo, Amor e carinho. Querida Lu, o teu Amor e carinho apenas me dão mais e mais força para seguir na luta, sempre na busca de um trabalho melhor, mais simples e mais útil para o amigo leitor. Que Deus te ilumine e ajude a realizar todos os teus sonhos. Cada vez admiro mais a tua coragem diante dos obstáculos da vida, sei que não foram e não estão sendo fáceis os momentos que passastes após a tua cirurgia para recuperação da tua saúde. Que Deus te dê toda a saúde do mundo para que possamos criar nossos filhos que em breve virão a este mundo.

A dona Lucy, minha mãe, por sempre me apoiar e ser uma grande admiradora e incentivadora de tudo o que faço. Por ter me dado como primeiro presente um livro, despertando em mim uma paixão ardente de leitor, daqueles que sempre compra mais livros do que realmente pode ler. Por ter muito orgulho do meu trabalho e por entender as vezes em que fica algumas semanas sem poder visitá-la em minha terra natal, o nosso bom e velho Boqueirão do Leão.

Aos amigos lá do Boqueirão do Leão, minha querida terra Natal. Não cito nomes para não cometer a injustiça de esquecer de alguém. Agradeço imensamente pelos momentos de lazer, de calma e serenidade, quando nos reunimos para jogar um Bocha, tomar uma cerveja ou simplesmente para conversar. Saibam que estão todos em meu coração. Está muito perto o dia em que poderemos passar mais tempo juntos, simplesmente conversando e tomando um chimarrão.

A meu Pai, em memória, pelo jeito simples e pacato, que me ensinou a parar e refletir nos momentos difíceis. Aos meus irmãos agradeço pelos bons momentos que juntos passamos.

Aos leitores que leram os outros livros de minha autoria e sempre entram em contato via email, para solucionar dúvidas, enviar sugestões, críticas e elogios. Agradeço a todos. Este retorno é muito importante é um grande motivador. Aos leitores que enviam email com dúvidas e sugestões sobre o meu e sobre Certificações. A todos o meu mais sincero agradecimento.

A Deus por nos dar a inteligência e a determinação na busca de cada vez fazer as coisas de uma maneira melhor e mais simples, com o objetivo de ajudar mais e mais pessoas. E que o grande criador e arquiteto de tudo o que existe, permita-me ainda muitos trabalhos, permita-me sempre ajudar mais e mais pessoas a alcançar seus objetivos e a aprender um pouco mais sobre cada um dos assuntos sobre os quais escrevo.

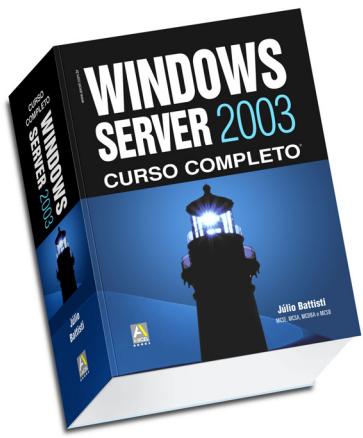
# Conheça Outros Livros do Autor Júlio Battisti



## Manual de Estudos Para o Exame 70-217 – 752 páginas

Chega ao mercado editorial mais um aguardado lançamento da Axcel Books Editora - Certificação Microsoft - Guia de Estudos Para o MCSE - Exame 70-217, onde o autor Júlio Battisti descreve, de forma detalhada e com exemplos passo-a-passo, todos os tópicos que fazem parte do programa oficial da Microsoft para o exame de certificação 70-217. A obra apresenta e explica desde os princípios básicos, incluindo os fundamentos do Active Directory; passando por serviços tais como DNS, gerenciamento de compartilhamentos, Master Operations, permissões NTFS, Grupos de Usuários, Unidades Organizacionais e Group Policy Objects, os GPOs; além de ainda tratar de questões como a configuração de Auditoria de Objetos, o gerenciamento do Schema, entre outros.

Um curso completo de Active Directory para o Windows 2000 Server



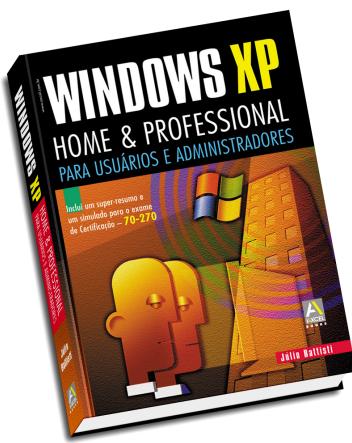
## Windows Server 2003 – Curso Completo – 1568 páginas

O livro ensina desde os fundamentos básicos do Active Directory, passando pela instalação do Windows Server 2003 e por dicas sobre o projeto, implementação e migração do Windows 2000 Server para o Windows Server 2003. Você aprenderá, em detalhes, sobre os serviços de compartilhamento de arquivos e impressoras, segurança, como tornar o Windows Server 2003 um servidor Web, aprenderá sobre os serviços de rede: DNS, DHCP, WINS, RRAS, IPSec, Análise de Segurança, Group Policy Objects e muito mais. Confira, vale a pena.



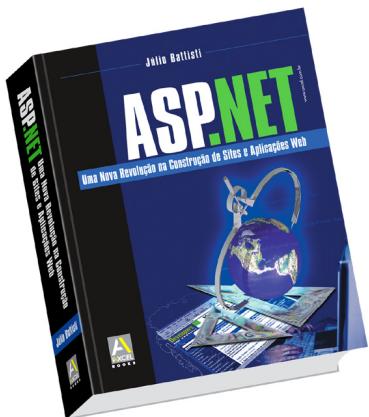
## Manual de Estudos Para o Exame 70-216 – 712 páginas

Neste aguardado lançamento da Axcel Books Editora - Certificação Microsoft - Guia de Estudos Para o MCSE - Exame 70-216, o autor Júlio Battisti descreve, de forma detalhada e com exemplos passo-a-passo, todos os tópicos que fazem parte do programa oficial da Microsoft para o exame de certificação. A obra apresenta e explica desde os princípios básicos, incluindo os fundamentos do protocolo TCP/IP; passando por instalação, configuração e administração do DNS, DHCP, WINS e RRAS; além de ainda tratar de questões quanto ao roteamento, NAT, Certificados Digitais, IPSec, entre outros.



## Windows XP Home & Professional – 840 páginas

O novo mundo do Windows XP, que representa a nova era do sistema operacional para usuários e administradores está reunido nesta obra. Júlio Battisti apresenta a nova interface do sistema, completamente redesenhada e com a experiência de um profissional certificado da Microsoft. Na obra, os leitores irão aprender a implementar, configurar e utilizar o Windows XP, desvendando as funcionalidades, além das configurações de segurança, de desempenho e de estabilidade do sistema. O livro aborda ainda toda a parte de Internet do Windows XP - conectando e usando a Internet; configurando o firewall de conexão; além dos novos recursos do correio eletrônico. Veja também os detalhes sobre o Active Directory, as configurações de rede e protocolo TCP/IP, criptografia, registry do Windows, entre tantos outros assuntos. O leitor ainda vai poder contar com um capítulo exclusivo e um simulado com 100 questões/respostas destinados aos interessados no exame de Certificação 70-270 da Microsoft.



## ASP.NET: Uma Nova Revolução Na Criação de Sites e Aplicações Web – 730 páginas

Conheça o ASP.NET, a mais nova versão do ASP, que representa uma mudança no modelo de desenvolvimento de aplicações Web. O livro traz todas as informações necessárias sobre o assunto, inclusive os detalhes da iniciativa .NET, o CLR, o MSIL e o C#, a nova linguagem da Microsoft. Aprenda os novos controles do ASP.NET e como utilizar o Visual Studio.NET para criar páginas ASP.NET. Veja ainda como criar formulários avançados para edição de dados, configurar as opções de segurança do Windows 2000, do IIS e do ASP.NET, além de aprender como criar páginas ASP.NET para as mais diversas funções.



## SQL Server 2000: Administração & Desenvolvimento – Curso Completo - 816 páginas

O lançamento é destinado aos usuários/leitores da versão anterior do SQL Server, o SQL 7, além de redes de computadores em geral, Windows 2000 Server, TCP/IP, Bancos de Dados em geral, do Microsoft Access e do Visual Basic. O leitor aprenderá na obra destinada ao iniciante ao avançado detalhes sobre o modelo de dados relacional, como instalar o SQL Server 2000 em diferentes plataformas, além da criação e administração de bancos de dados, tabelas e outros objetos. Aprenda ainda Como criar páginas ASP que acessam os dados do SQL Server 2000.

# Sumário

|   |           |
|---|-----------|
| <b>Capítulo 1: Redes Baseadas no Windows 2003 Server</b>                        | <b>21</b> |
| Introdução  | 21        |
| Uma Nova Versão de Servidor Para o Windows?                                     | 23        |
| Uma Breve História "dos Windows"  | 24        |
| Os "Windows" Para Estações de Trabalho e Computadores de Uso Residencial:       | 24        |
| Os "Windows" Para Servidores:   | 26        |
| A Quem se Destina Este Livro?   | 28        |
| Equipamento e Software Necessários  | 28        |
| É Hora de Começar   | 29        |
| Introdução ao Windows Server 2003   | 29        |
| Um Sistema Operacional – Quatro Edições   | 32        |
| Windows Server 2003 Standard Edition  | 32        |
| Serviços e/ou recursos não disponíveis no Windows Server 2003 Standard Edition: | 33        |
| Windows Server 2003 Enterprise Edition  | 33        |
| Windows Server 2003 Data Center Edition   | 34        |
| Windows Server 2003 Web Edition   | 35        |
| Comparação Entre as Diferentes Edições  | 35        |
| Novidades do Windows Server 2003  | 37        |
| Novidades no Active Directory   | 37        |
| Novidades nos Serviços de Compartilhamento de Arquivos e Impressão              | 39        |
| Novidades na área de segurança no Windows Server 2003                           | 41        |
| Novidades nos serviços de rede e comunicação                                    | 41        |
| Novidades nos serviços de gerenciamento do Windows Server 2003                  | 42        |
| Novidades no suporte ao desenvolvimento de Aplicativos                          | 44        |
| Novidades em outras áreas do Windows Server 2003:                               | 45        |
| Redes de computadores   | 45        |
| No princípio, um modelo Centralizado baseado no Mainframe                       | 45        |
| Morte ao Mainframe, viva a descentralização!!!                                  | 47        |
| Modelo em 2 camadas   | 49        |
| Aplicações em 3 camadas.  | 51        |
| Aplicações em quatro camadas.   | 52        |
| O Júlio ficou louco ou estamos voltando ao Mainframe?                           | 53        |
| Papel do Windows Server 2003 na rede da sua empresa                             | 54        |
| Onde entra o Windows Server 2003 neste história?                                | 54        |
| O Protocolo TCP/IP  | 57        |
| Uma visão geral do protocolo TCP/IP   | 57        |
| Configurações do protocolo TCP/IP para um computador em rede                    | 58        |

|  |    |
|--|----|
| Configuração de IP do Windows  | 62 |
| Configuração de IP do Windows  | 62 |
| Sistema de numeração binário   | 64 |
| Como converter decimal para binário:   | 66 |
| Operador E:  | 67 |
| Como o TCP/IP usa a máscara de sub-rede:   | 67 |
| Como o TCP/IP usa a máscara de sub-rede e o roteador:  | 68 |
| Endereçamento IP – Classes de Endereços  | 71 |
| Redes Classe A:  | 71 |
| Redes Classe B:  | 72 |
| Redes Classe C:  | 73 |
| Redes Classe D:  | 74 |
| Redes Classe E:  | 74 |
| Endereços Especiais:   | 75 |
| O papel do Roteador em uma rede de computadores:   | 75 |
| Como eu sei qual o Default Gateway que está configurado no meu computador com o Windows Server 2003 instalado? | 76 |
| Configuração de IP do Windows  | 77 |
| Explicando Roteamento – um exemplo prático:  | 78 |
| Executar um teste de compatibilidade antes da instalação do Windows Server 2003                                | 80 |
| Itens a serem verificados e/ou considerados antes de iniciar a instalação:                                     | 86 |
| Instalando o Windows Server 2003   | 87 |
| Instalando o Windows Server 2003 a partir do zero – boot a partir do CD-ROM                                    | 88 |
| Instalação não assistida e arquivo de respostas  | 93 |
| O arquivo de respostas   | 94 |
| Como utilizar o arquivo de respostas durante a instalação?   | 96 |
| Conclusão  | 97 |

|  |            |
|--|------------|
| <b>Capítulo 2: Active Directory – Conceitos, Estrutura Lógica e Física e Componentes</b> | <b>101</b> |
| Introdução   | 101        |
| Conceito de Diretório e Exemplos.  | 103        |
| Senhas demais, por favor alguém me ajude!  | 104        |
| Um diretório único para todas as aplicações.   | 105        |
| Entendendo o conceito de Diretórios e Workgroups.  | 106        |
| Domínios e Grupos de Trabalho (Workgroups):  | 106        |
| Entendendo o funcionamento de uma rede baseada no modelo de Workgroups:                  | 106        |
| Entendendo o funcionamento de uma rede baseada no conceito de Diretório – Domínio:       | 107        |
| Domínios, Árvores de domínios e Unidades Organizacionais – Conceitos.                    | 109        |
| Active Directory   | 110        |
| Árvore de domínios:  | 112        |
| Unidades Organizacionais   | 113        |
| Conhecendo os principais Objetos de um domínio.  | 113        |

|  |     |
|--|-----|
| <b>Contas de usuários, computadores e grupos de usuários</b>   | 114 |
| <b>Contas de usuários</b>  | 114 |
| <b>Contas de Computador</b>  | 115 |
| <b>Grupos de usuários</b>  | 115 |
| <b>Atribuição de permissões em múltiplos domínios.</b>   | 119 |
| <b>Uma árvore com sete domínios:</b>   | 120 |
| Um pouco sobre nomenclaturas de objetos no domínio, LDAP e caminhos UNC:                             | 121 |
| <b>Estudo de caso 01: Exemplo de uso de Grupos Universais:</b>                                       | 122 |
| <b>Estudo de caso 02: Analisando o escopo de grupos em relação a membros e permissões de acesso:</b> | 124 |
| <b>Entendendo as Unidades organizacionais.</b>   | 125 |
| <b>Relações de confiança e florestas.</b>  | 127 |
| <b>Como eram as relações de confiança na época do NT Server 4.0?</b>                                 | 127 |
| E como são as relações de confiança no Windows Server 2003?  | 129 |
| <b>Outros tipos de relações de confiança:</b>  | 129 |
| <b>Tipos padrão de relações de confiança:</b>  | 129 |
| <b>Outros tipos de relações de confiança:</b>  | 130 |
| <b>Servidores de Catálogo Global (Global Catalogs)</b>   | 132 |
| <b>Principais funções desempenhadas por um Servidor de Catálogo Global:</b>                          | 133 |
| <b>Replicação de informações entre os Servidor de Catálogo Global:</b>                               | 134 |
| <b>Sites, replicação do Active Directory e estrutura física da rede.</b>                             | 135 |
| <b>Introdução e definição de sites.</b>  | 135 |
| <b>Para que o Active Directory utiliza sites:</b>  | 135 |
| <b>Definição de sites utilizando sub-redes:</b>  | 136 |
| A relação entre sites e domínios:  | 136 |
| <b>Replicação no Active Directory:</b>   | 137 |
| <b>Replicação dentro do mesmo site – Intrasite Replication</b>                                       | 138 |
| <b>Replicação entre sites:</b>   | 139 |
| <b>O Schema do Active Directory</b>  | 139 |
| <b>Como os objetos do Active Directory são definidos no Schema:</b>                                  | 140 |
| <b>Como o Schema é armazenado no Active Directory:</b>   | 140 |
| <b>Cache do Schema.</b>  | 140 |
| <b>Níveis de funcionalidade de um domínio.</b>   | 140 |
| <b>Fundamentos em: Preparação para a instalação do Active Directory.</b>                             | 141 |
| <b>Uma visão geral do DNS e de espaço de nomes de um domínio.</b>                                    | 142 |
| <b>Instalação do Active Directory – Criação de um Novo Domínio</b>                                   | 145 |
| <b>Modificações feitas com a instalação do Active Directory.</b>                                     | 152 |
| <b>Como rebaixar um DC de volta a Member Server.</b>   | 154 |
| <b>Criar um novo DC em um domínio já existente.</b>  | 158 |
| <b>Preparando um domínio do Windows 2000 Server para migração.</b>                                   | 163 |
| <b>Operações diversas com o Active Directory.</b>  | 163 |
| <b>Modos de funcionalidade do domínio e da floresta.</b>   | 163 |

|  |     |
|--|-----|
| Como configurar o nível de funcionalidade de um domínio e de uma floresta: | 165 |
| Gerenciando relações de confiança entre domínios.                          | 167 |
| Configurando um DC como Servidor de Catálogo Global.                       | 168 |
| Conclusão  | 169 |

## **Capítulo 3: Consoles de Administração e Snap-in – interface padrão para Administração do Windows Server 2003**

|  |     |
|--|-----|
| Introdução   | 173 |
| Microsoft Management Console (MMC) e Snap-in – Conceitos | 174 |
| Criando consoles personalizados                          | 177 |
| Consoles instalados com o Windows Server 2003.           | 183 |
| Conclusão  | 189 |

## **Capítulo 4: Administração de contas de usuários e grupos do Active Directory**

|  |     |
|--|-----|
| Introdução   | 190 |
| Contas de Usuários   | 191 |
| Definindo um padrão de nomes para as contas de usuários.                           | 193 |
| Observações Sobre o Nome das Contas de Usuários                                    | 193 |
| Questões relacionadas com a definição da senha do usuário                          | 194 |
| Criação e administração de contas de usuários.                                     | 195 |
| Criando uma nova conta de usuário no domínio:                                      | 195 |
| Configurando uma conta de usuário  | 199 |
| Configurando informações gerais e de endereço para a conta do usuário:             | 199 |
| Configurando informações sobre a conta do usuário:                                 | 202 |
| Definindo o horário de logon e os computadores na qual a conta pode fazer o logon. | 206 |
| Limitando os computadores nos quais o usuário pode fazer o logon.                  | 207 |
| Criando e utilizando uma conta modelo  | 209 |
| Comandos para trabalhar com contas de usuários.                                    | 211 |
| O comando CSVDE:   | 211 |
| O comando DSADD:   | 213 |
| dsadd computer   | 213 |
| dsadd group  | 214 |
| dsadd ou   | 215 |
| dsadd user   | 215 |
| dsget user   | 217 |
| Outros commandos disponíveis:  | 220 |
| O Conceito de Profiles   | 220 |
| Vantagens de se Utilizar Profiles:   | 221 |
| Tipos de User Profile:   | 221 |
| Entendendo o conteúdo de uma User profile  | 223 |

|  |     |
|--|-----|
| A pasta All Users  | 224 |
| Criando um Profile a ser aplicada a vários usuários  | 226 |
| Configurando uma profile no Perfil do usuário:   | 228 |
| Conhecendo as chamadas “Contas Built-in”   | 230 |
| Demais operações com contas de usuários  | 232 |
| Grupos de usuários: Conceitos, tipos e utilização.   | 235 |
| Classificação dos grupos quanto ao tipo:   | 236 |
| Classificação dos grupos quanto ao Escopo:   | 237 |
| Ações práticas com grupos de usuários.   | 239 |
| Built-in Groups.   | 239 |
| Criando novos grupos e adicionando novos membros a um grupo.   | 244 |
| Fundamentos em: Conceito e utilização de Unidades Organizacionais.   | 252 |
| Ações práticas com Unidades Organizacionais (OUs).   | 253 |
| Delegando tarefas administrativas a nível de OU:   | 257 |
| Propriedades e Permissões de Segurança em Unidades Organizacionais.  | 261 |
| Contas de computadores – Conceito e Prática  | 262 |
| Criando uma conta de computador no Active Directory.   | 264 |
| Criando uma conta de computador com o console  | 264 |
| Usuários e computadores do Active Directory:   | 264 |
| Criando uma conta de computador usando o comando dsadd computer:   | 265 |
| Configurando uma estação de trabalho, para fazer parte de um domínio   | 265 |
| Políticas de Senha para o Domínio  | 271 |
| Descrição das diretivas do grupo Diretivas de senha: No Windows Server 2003, por padrão, são definidas as seguintes políticas de segurança em relação as senhas de usuários: | 273 |
| Descrição das diretivas do grupo Diretivas de bloqueio de conta  | 276 |
| Administração do “Schema” do Active Directory.   | 278 |
| Conclusão  | 282 |

|   |            |
|---|------------|
| <b>Capítulo 5: Administrando discos e volumes no Windows Server 2003</b>                  | <b>283</b> |
| Conceitos que Você Precisa Conhecer   | 284        |
| Disco físico  | 284        |
| Volumes lógicos   | 284        |
| Armazenamento Básico e Armazenamento Dinâmico   | 285        |
| Armazenamento básico  | 285        |
| Armazenamento dinâmico  | 287        |
| Operações Práticas no Gerenciamento   | 289        |
| de Discos e Volumes   | 289        |
| Criando um console personalizado para gerenciamento de discos e volumes                   | 289        |
| Reativando discos que ainda não foram completamente reconhecidos pelo Windows Server 2003 | 292        |
| Acessando informações sobre os discos do seu servidor                                     | 296        |

|   |            |
|---|------------|
| Trabalhando com partições em um disco de armazenamento básico   | 298        |
| Eliminando um volume set, disk mirror, stripe set e stripe set com paridade em discos de armazenamento básico | 302        |
| Convertendo um disco de Armazenamento básico para Armazenamento dinâmico                                      | 302        |
| Criando e expandindo um Volume simples  | 305        |
| Criando um volume estendido   | 309        |
| Criando um striped volume (volume distribuído)  | 311        |
| Criando um volume RAID-5  | 314        |
| Criando um volume espelhado   | 317        |
| Restabelecendo um volume do tipo mirror (espelhado)   | 318        |
| Restabelecendo um volume do tipo RAID-5   | 318        |
| Configurações e personalizações do snap-in gerenciamento de discos  | 319        |
| Ferramentas Para Manutenção de Discos e Volumes   | 321        |
| O conceito de fragmentação  | 321        |
| O utilitário de desfragmentação   | 322        |
| Algumas recomendações sobre o processo de desfragmentação   | 324        |
| O comando defrag  | 325        |
| Verificando e reparando erros no sistema de arquivos e no disco rígido  | 326        |
| Comandos para a verificação e correção de erros   | 327        |
| O comando chkdsk  | 327        |
| Usando chkdsk com arquivos abertos  | 330        |
| O comando chkntfs   | 330        |
| Outros comandos importantes para trabalhar com discos e volumes   | 331        |
| O comando convert   | 331        |
| O utilitário DiskPart   | 332        |
| O comando Fsutil: file  | 333        |
| Criptografia de Arquivos em Partições NTFS  | 335        |
| Criptografia – definições e conceitos   | 335        |
| Garantindo a recuperação dos dados  | 337        |
| Criptografando arquivos e pastas  | 342        |
| Operações com Arquivos Criptografados (para o exame, não esqueça destes detalhes)                             | 345        |
| Permitindo que outros usuários tenham acesso a arquivos e pastas que você criptografou                        | 346        |
| Alterando a diretiva de recuperação do Computador local   | 347        |
| Recomendações sobre a criptografia de pastas e arquivos   | 348        |
| O comando cipher  | 349        |
| Conclusão   | 350        |
| <b>Capítulo 6: Criando e Administrando Pastas Compartilhadas e Permissões de acesso</b>                       | <b>352</b> |
| Introdução  | 352        |
| Pastas compartilhadas, Permissões de Compartilhamento e Permissões NTFS.                                      | 353        |
| Restringindo o acesso às pastas compartilhadas.   | 354        |

|   |     |
|---|-----|
| <b>Entendendo as permissões de compartilhamento.</b>  | 355 |
| <b>Quando um usuário pertence a mais de um grupo, como é que fica a permissão efetiva do usuário??</b>        | 356 |
| <b>Orientações para a criação de pastas compartilhadas:</b>   | 358 |
| <b>Sistemas de arquivos e permissões NTFS – conceito.</b>   | 358 |
| <b>Compartilhando pastas, definindo permissões de compartilhamento e NTFS</b>                                 | 363 |
| <b>O console para monitoração de compartilhamentos.</b>   | 369 |
| <b>Criando e gerenciando compartilhamentos local e remotamente</b>  | 370 |
| <b>Permissões NTFS.</b>   | 374 |
| <b>Combinando permissões de compartilhamento e permissões NTFS – estudo de casos.</b>                         | 382 |
| <b>Mapeando unidades de rede.</b>   | 384 |
| <b>Distributed File System - DFS</b>  | 386 |
| <b>Entendendo o que é o Distributed File System - DFS.</b>  | 386 |
| <b>DFS – Conceito e utilizações</b>   | 387 |
| <b>DFS: Modelo proposto e benefícios</b>  | 388 |
| <b>Limitações no Cliente e no Servidor</b>  | 390 |
| <b>Implementando o DFS – um exemplo prático</b>   | 391 |
| <b>O ambiente em uso nos exemplos</b>   | 391 |
| <b>O Console DFS</b>  | 392 |
| <b>Criando um root de domínio</b>   | 393 |
| <b>Criando links para as pastas compartilhadas na rede:</b>   | 395 |
| <b>Acessando a raiz DFS no cliente:</b>   | 399 |
| <b>Definição de cotas em volumes e partições.</b>   | 400 |
| <b>Configurando cotas de disco no Windows Server 2003.</b>  | 400 |
| <b>Configurando cotas de disco em um volume NTFS.</b>   | 401 |
| <b>Recomendações sobre o uso de cotas de disco:</b>   | 404 |
| <b>O comando fsutil quota.</b>  | 405 |
| <b>Entendendo e Utilizando Pastas off-line</b>  | 407 |
| <b>Pastas Off-line: conceito e utilizações.</b>   | 407 |
| <b>Configurando o computador dos usuários para que ele esteja apto a usar o recurso de arquivos off-line.</b> | 408 |
| <b>Configurando um compartilhamento para que os seus arquivos possam ser acessados off-line.</b>              | 410 |
| <b>Definindo quais arquivos serão armazenados no cache, para acesso off-line.</b>                             | 411 |
| <b>O gerenciador de sincronização.</b>  | 412 |
| <b>Compactação de pastas e arquivos.</b>  | 413 |
| <b>Compactação de arquivos e pastas.</b>  | 413 |
| <b>Compactando e descompactando pastas e arquivos em volumes NTFS.</b>  | 414 |
| <b>Arquivos compactados no padrão .ZIP.</b>   | 415 |
| <b>Trabalhando com pastas e arquivos compactados no padrão .ZIP.</b>  | 415 |
| <b>Gerando um arquivo compactado no padrão .zip.</b>  | 415 |
| <b>Conclusão.</b>   | 417 |

|  |            |
|--|------------|
| <b>Capítulo 7: Instalação, Configuração e Administração de Impressoras</b>                 | <b>418</b> |
| Introdução   | 418        |
| O Sistema de Impressão do Windows Server 2003 – Conceitos Teóricos                         | 419        |
| Uma bela confusão de termos  | 420        |
| Entendendo o serviço de impressão no Windows Server 2003.                                  | 421        |
| Alguns detalhes sobre o processo de impressão do Windows Server 2003                       | 422        |
| Padronização de nomes e outros detalhes importantes para o uso de impressoras em rede.     | 424        |
| Considerações sobre o “custo da impressora” e o “custo de impressão”.                      | 424        |
| Instalação e Configuração de Impressoras - Prática   | 426        |
| Instalando uma nova impressora (instalando o driver da impressora)                         | 426        |
| Compartilhando uma impressora para uso através da rede.                                    | 432        |
| net view \\srv-win2003   | 434        |
| Atribuindo permissões de acesso para a impressora.   | 435        |
| Acessando uma impressora compartilhada através da rede.                                    | 440        |
| Administrando trabalhos enviados para uma impressora.                                      | 444        |
| Configurando propriedades importantes e outras ações.                                      | 448        |
| Administrando a impressora através do navegador.   | 450        |
| Utilizando impressoras de rede.  | 451        |
| Diferentes prioridades para diferentes grupos.   | 457        |
| Criando um “pool” de impressão.  | 459        |
| Comandos para o gerenciamento e administração de compartilhamento de impressoras e pastas. | 461        |
| O comando net share  | 462        |
| Compartilhando uma pasta usando o comando net share.                                       | 463        |
| Modificando um compartilhamento usando o comando net share.                                | 464        |
| Excluindo um compartilhamento usando o comando net share.                                  | 464        |
| O comando net use.   | 464        |
| O comando net statistics   | 466        |
| Pesquisando impressoras no Active Directory  | 467        |
| Conclusão  | 470        |
| <b>Capítulo 8: Fazendo o Backup dos Dados e Agendando Tarefas</b>                          | <b>472</b> |
| Introdução   | 472        |
| O conceito de Tarefas agendadas  | 473        |
| Questões de segurança, relacionadas com tarefas agendadas.                                 | 474        |
| Criação e Administração de Tarefas agendadas.  | 476        |
| Exemplo: Criando e agendando uma tarefa para execução automática.                          | 476        |
| Alterando uma tarefa agendada.   | 481        |
| Para executar uma tarefa imediatamente siga os passos indicados a seguir:                  | 482        |
| Para renomear uma tarefa agendada, siga os passos indicados a seguir:                      | 482        |
| Alterar a conta com a qual a tarefa é executada.   | 482        |

|  |            |
|--|------------|
| Alterar o agendamento da tarefa.   | 483        |
| Alterar opções avançadas do agendamento.   | 484        |
| Criar múltiplos agendamentos.  | 486        |
| Verificar o log do Agendador de tarefas.   | 487        |
| Comandos at para agendamento de comandos.  | 489        |
| Estratégias de backup e restore.   | 490        |
| Definindo o tipo de Backup a ser utilizado.                                      | 491        |
| Exemplos de estratégias de backup/restore.                                       | 493        |
| Questões de segurança relacionadas ao Backup                                     | 494        |
| Fazendo o backup e o restore de pastas e arquivos com o Windows Server 2003.     | 495        |
| Introdução   | 495        |
| Fazendo o backup de pastas e arquivos utilizando o modo assistente de backup.    | 497        |
| Fazendo o backup de pastas e arquivos utilizando a interface completa.           | 505        |
| Fazendo o restore das informações a partir do backup.                            | 508        |
| O log do backup.   | 512        |
| Definindo opções padrão de backup e restore.                                     | 513        |
| Fazendo o Backup e o Restore do Active Directory..                               | 516        |
| Backup do Active Directory:  | 517        |
| Restore do Active Directory  | 517        |
| Fazendo o backup do Active Directory.  | 518        |
| Fazendo o restore do Active Directory.   | 522        |
| Efetuando um restore nonauthoritative, usando o utilitário de backup.            | 523        |
| Efetuando um authoritative restore.  | 524        |
| Os comandos Ldifde e Dsadd.  | 526        |
| Conclusão  | 528        |
| <b>Capítulo 9: Manutenção do Windows 2003 Server e Gerenciamento de Hardware</b> | <b>530</b> |
| Introdução   | 530        |
| Uma Introdução ao Terminal Services.   | 531        |
| Como funciona o Terminal Services.   | 532        |
| Recursos de hardware necessários para o funcionamento do Terminal Services.      | 536        |
| Implementação e Administração do Terminal Services.                              | 537        |
| Utilizando o Terminal Services no modo de Compartilhamento de Aplicações:        | 543        |
| Instalando o serviço Terminal Services.  | 543        |
| Configurando o licenciamento para o Terminal Services.                           | 546        |
| Instalando aplicações para uso no modo compartilhado.                            | 548        |
| Instalando o Office 2000 para uso através do Terminal Sevices.                   | 551        |
| Administração do Terminal Services.  | 551        |
| Gerenciando as conexões com o Gerenciador dos serviços de terminal.              | 552        |
| Configurações do Terminal Server.  | 557        |

|   |     |
|---|-----|
| O Recurso de Assistência Remota.  | 568 |
| Tipos de conexões de assistência remota   | 569 |
| Questões de segurança   | 569 |
| Habilitando o recurso de Assistência Remota   | 569 |
| Enviando um convite de assistência remota   | 571 |
| O novo recurso de Shadow Copies.  | 572 |
| Mais algumas observações sobre o recurso de shadow copies.  | 573 |
| O agendamento do recursos de shadow copies.   | 574 |
| Habilitando o recurso de shadow copies em um volume:  | 574 |
| Instalando o cliente de shadow copies.  | 576 |
| Acessando as shadow copies:   | 577 |
| Desabilitando o recurso de shadow copies em um volume:  | 578 |
| Gerenciando shadow copies com o comando vssadmin.   | 579 |
| Group Police Objects – GPOs.  | 580 |
| Introdução  | 580 |
| Group Policy Objects – Fundamentação Teórica  | 581 |
| Políticas de usuários e políticas de computador:  | 583 |
| Novidades no Windows Server 2003.   | 584 |
| Entendendo como é feito o processamento e aplicação das GPOs.   | 585 |
| Detalhando a ordem de processamento das GPOs.   | 588 |
| O recurso de loopback.  | 589 |
| Ordem de eventos quando o computador é inicializado e o usuário faz o logon:  | 589 |
| Entendendo como funciona o mecanismo de herança – Policy inheritance  | 590 |
| Exemplos práticos de uso das opções “No Override (Não substituir)” e “Block Policy inheritance (Bloquear herança de diretiva)”: 592 | 592 |
| Situação 01:  | 592 |
| Situação 02:  | 592 |
| Implementação e Administração de GPOs.  | 592 |
| O console de administração das GPOs.  | 593 |
| Usando o console de configuração das GPOs.  | 594 |
| Criando uma nova GPO e associando-a com uma unidade organizacional:   | 598 |
| Configurando as Propriedades de uma GPO.  | 601 |
| Gerenciamento de Hardware e de Drivers.   | 605 |
| Adicionando, removendo e gerenciando o Hardware do computador.  | 605 |
| O Gerenciador de Dispositivos   | 607 |
| Assinatura de drivers   | 612 |
| Conclusão.  | 613 |

|  |            |
|--|------------|
| <b>Capítulo 10: Auditoria, Log de Eventos e Serviços</b> | <b>614</b> |
| Introdução   | 614        |
| Log de Eventos e de Auditoria – Conceito.                | 615        |

|  |     |
|--|-----|
| Trabalhando com o Log de Eventos.  | 618 |
| Exemplo: Visualizando eventos e detalhes dos eventos.  | 618 |
| Habilitando/configurando os eventos do log de segurança.   | 622 |
| Recomendações da Microsoft, para configurações de auditoria.   | 630 |
| Filtrando eventos nos logs de auditoria.   | 631 |
| Exemplo - Para filtrar os eventos do log do sistema, pelo tipo de evento, siga os passos indicados a seguir: | 631 |
| Configurando as propriedades do log.   | 635 |
| Exemplo - Para definir o tamanho máximo e o local onde o Log é gravado, siga os passos indicados a seguir:   | 636 |
| Definindo as propriedades dos logs de auditoria, usando as diretivas de segurança do domínio:                | 637 |
| Mais configurações do log e exportação dos eventos do log de auditoria.                                      | 640 |
| Configurando a auditoria de acesso a arquivos, pastas e impressoras.   | 642 |
| Gerenciando Serviços no Windows Server 2003.   | 646 |
| Acessando informações sobre serviços e administrando os serviços instalados.                                 | 646 |
| Conclusão.   | 654 |

|   |            |
|---|------------|
| <b>Capítulo 11: Monitoração de Desempenho e Logs de Alerta</b>              | <b>656</b> |
| Introdução  | 656        |
| Monitoração de desempenho – conceitos básicos.                              | 657        |
| Utilização do console Desempenho  | 659        |
| Monitorando o Processador e a Memória do seu Servidor.                      | 659        |
| Monitorando o acesso ao sistema de discos.                                  | 663        |
| Contadores a serem monitorados em servidores.                               | 665        |
| Valores indicativos de limites de desempenho para contadores                | 667        |
| Configurando o console Desempenho para capturar dados automaticamente.      | 670        |
| Montando gráficos de desempenho a partir de informações de arquivos de log. | 679        |
| Utilizando Alertas para monitorar situações limite.                         | 683        |
| Conclusão   | 686        |
| Não tenho essa figura   | 686        |

|  |            |
|--|------------|
| <b>Capítulo 12: Ferramentas de recuperação a desastres</b>             | <b>687</b> |
| Introdução   | 687        |
| Entendendo o processo de boot do Windows Server 2003                   | 688        |
| O arquivo Boot.ini e caminhos ARC                                      | 691        |
| Entendendo a sintaxe dos caminhos ARC.                                 | 692        |
| As chaves que podem ser utilizadas no arquivo Boot.ini.                | 693        |
| Configurações de inicialização através do utilitário System (Sistema). | 694        |
| A Registry do Windows Server 2003.                                     | 701        |
| Acessando e alterando informações na Registry do Windows Server 2003.  | 702        |
| O Modo Seguro, Last Known Good Configuration e Control Sets..          | 709        |
| Opções de inicialização do Windows Server 2003 e o Modo seguro.        | 709        |

|  |     |
|--|-----|
| Entendendo o Modo seguro de inicialização – Safe mode.               | 710 |
| Last know good configuration e Control Sets.                         | 711 |
| Outras opções de configuração do Menu de opções avançadas do Windows | 712 |
| Diversas ferramentas de recuperação a desastres.                     | 712 |
| O recurso ASR – Automated System Recovery Disks                      | 712 |
| Criando um disquete de boot.   | 716 |
| O Console de Recuperação.  | 717 |
| A opção Roll Back Driver.  | 720 |
| Conclusão  | 721 |

## **Capítulo 13: Internet Information Services 6.0 – IIS 6.0 e Software Update Services – SUS** 722

|  |     |
|--|-----|
| Introdução   | 722 |
| Instalação do IIS 6.0.   | 723 |
| Preparando o seu computador para acompanhar os exemplos práticos de utilização do IIS. | 727 |
| Criando a estrutura de pastas e subpastas.   | 728 |
| Tornando a pasta exemplos parte dos servidor IIS – criando uma pasta virtual.          | 728 |
| Como são formados os endereços de acesso à páginas do IIS?                             | 732 |
| Configurando opções do servidor de páginas e do servidor ftp.                          | 734 |
| Questões e configurações de segurança com o IIS.                                       | 743 |
| Porque devo me preocupar com segurança?  | 743 |
| Autenticação de usuários com o IIS.  | 744 |
| O acesso anônimo.  | 745 |
| Como definir a conta para acesso anônimo no IIS.                                       | 746 |
| SUS – Software Update Services   | 748 |
| Introdução ao SUS  | 748 |
| Componentes do SUS:  | 749 |
| Instalando o SUS   | 750 |
| Administrando o SUS  | 755 |
| Configurar os clientes para utilizar o SUS.  | 759 |
| Configurando os clientes via GOP:  | 760 |
| Opções da Registry relacionadas com o SUS:   | 765 |
| Conclusão  | 765 |

## **Capítulo 14: Resumo Final – O que você não pode esquecer para o Exame** 767

|   |     |
|---|-----|
| Introdução  | 767 |
| Resumo para o exame 70-290.   | 767 |
| Redes Baseadas no Windows 2003 Server                                     | 768 |
| Uma breve história “dos Windows”  | 768 |
| Os “Windows” para estações de trabalho e computadores de uso residencial: | 768 |
| Os “Windows” para Servidores:   | 771 |

|   |     |
|---|-----|
| Definindo exatamente o papel do Windows Server 2003   | 772 |
| O Protocolo TCP/IP  | 775 |
| O papel do Roteador em uma rede de computadores:  | 775 |
| Executar um teste de compatibilidade antes da instalação do Windows Server 2003               | 776 |
| Itens a serem verificados e/ou considerados antes de iniciar a instalação:                    | 776 |
| Modos de Licenciamento do Windows Server 2003   | 778 |
| Active Directory – Conceitos, Estrutura Lógica e Física e Componentes                         | 778 |
| Entendendo o conceito de Diretórios e Workgroups  | 778 |
| Domínios e Grupos de Trabalho (Workgroups):   | 778 |
| Entendendo o funcionamento de uma rede baseada no modelo de Workgroups:                       | 779 |
| Entendendo o funcionamento de uma rede baseada no conceito de Diretório – Domínio:            | 780 |
| Domínios, Árvores de domínios e Unidades Organizacionais – Conceitos.                         | 781 |
| Active Directory  | 783 |
| Árvore de domínios:   | 785 |
| Unidades Organizacionais  | 786 |
| Conhecendo os principais Objetos do Active Directory  | 786 |
| Contas de usuários  | 787 |
| Contas de Computador  | 788 |
| Grupos de usuários  | 788 |
| Atribuição de permissões em múltiplos domínios – estudos de caso.                             | 793 |
| Uma árvore com sete domínios:   | 793 |
| Um pouco sobre nomenclaturas de objetos no domínio, LDAP e caminhos UNC:                      | 794 |
| Estudo de caso 01: Exemplo de uso de Grupos Universais:                                       | 796 |
| Estudo de caso 02: Analisando o escopo de grupos em relação a membros e permissões de acesso: | 797 |
| Entendendo as Unidades organizacionais.   | 798 |
| Relações de confiança e florestas.  | 800 |
| Como eram as relações de confiança na época do NT Server 4.0?                                 | 800 |
| E como são as relações de confiança no Windows Server 2003?                                   | 802 |
| Outros tipos de relações de confiança:  | 803 |
| Tipos padrão de relações de confiança:  | 803 |
| Outros tipos de relações de confiança:  | 803 |
| Servidores de Catálogo Global (Global Catalogs)   | 805 |
| Principais funções desempenhadas por um Servidor de Catálogo Global:                          | 806 |
| Replicação de informações entre os Servidor de Catálogo Global:                               | 807 |
| O Schema do Active Directory.   | 808 |
| Como os objetos do Active Directory são definidos no Schema:                                  | 808 |
| Como o Schema é armazenado no Active Directory:   | 809 |
| Cache do Schema.  | 809 |
| Níveis de funcionalidade de um domínio.   | 809 |
| Preparação para a instalação do Active Directory.   | 810 |
| Modificações feitas com a instalação do Active Directory.                                     | 810 |

|  |     |
|--|-----|
| Dicas de sites com mais material de estudo sobre o Active Directory:   | 812 |
| Administração de contas de usuários e grupos do Active Directory.  | 813 |
| Contas de usuários   | 814 |
| Observações sobre o nome das contas de usuários  | 816 |
| Questões relacionadas com a definição da senha do usuário  | 816 |
| Opções padrão do console Usuários e Computadores do Active Directory:  | 817 |
| Opções de configuração durante a criação de uma nova conta de usuário:   | 818 |
| Configurando opções importantes da conta do usuário  | 818 |
| Criando e utilizando uma conta modelo.   | 820 |
| Comandos para trabalhar com contas de usuários.  | 821 |
| O comando CSVDE:   | 821 |
| O comando DSADD:   | 821 |
| dsget user   | 822 |
| Outros commandos disponíveis:  | 822 |
| O conceito de Profiles   | 822 |
| Vantagens de se utilizar Profiles:   | 823 |
| Tipos de User Profile:   | 823 |
| Entendendo o conteúdo de uma User profile  | 825 |
| A pasta All Users  | 827 |
| Menu Acessórios  | 828 |
| Opções de configuração da guia Perfil, das propriedades de uma conta de usuário:   | 828 |
| Mais algumas observações sobre contas de usuários:   | 829 |
| Built-in Groups.   | 830 |
| Delegando tarefas administrativas a nível de OU:   | 836 |
| Propriedades e Permissões de Segurança em Unidades Organizacionais.  | 836 |
| Contas de computadores   | 838 |
| Políticas de Senha para o Domínio  | 839 |
| Descrição das diretivas do grupo Diretivas de senha: No Windows Server 2003, por padrão, são definidas as seguintes políticas de segurança em relação as senhas de usuários: | 842 |
| Descrição das diretivas do grupo Diretivas de bloqueio de conta  | 844 |
| Gerenciamento de discos e Volumes no Windows Server 2003   | 844 |
| Disco Físico   | 844 |
| Volumes Lógicos  | 845 |
| Armazenamento Básico e Armazenamento Dinâmico  | 845 |
| Armazenamento básico   | 845 |
| Armazenamento dinâmico   | 848 |
| Reativando discos que ainda não foram completamente reconhecidos pelo Windows Server 2003.   | 849 |
| Convertendo um disco de Armazenamento básico para Armazenamento dinâmico   | 854 |
| Restabelecendo um volume do tipo Mirror (Espelhado – Raid-1):  | 855 |
| Restabelecendo um volume do tipo RAID-5:   | 855 |
| O comando Convert:   | 856 |

|  |     |
|--|-----|
| <b>Criptografia – definições e conceitos</b>   | 857 |
| Garantindo a recuperação dos dados.  | 859 |
| Operações com arquivos criptografados (para o exame, não esqueça destes detalhes).             | 860 |
| Recomendações sobre a criptografia de pastas e arquivos.                                       | 860 |
| <b>Alguns links com mais material d estudo:</b>  | 861 |
| Pastas compartilhadas, Permissões de Compartilhamento e Permissões NTFS.                       | 861 |
| Restringindo o acesso às pastas compartilhadas.  | 862 |
| Entendendo as permissões de compartilhamento.  | 863 |
| Quando um usuário pertence a mais de um grupo, como é que fica a permissão efetiva do usuário? | 865 |
| Orientações para a criação de pastas compartilhadas:   | 866 |
| Sistemas de arquivos e permissões NTFS – conceito.   | 867 |
| Combinando permissões de compartilhamento e permissões NTFS – estudo de casos.                 | 871 |
| Pastas Off-line: conceito e utilizações.   | 873 |
| Instalação, Configuração e Administração de Impressoras.                                       | 874 |
| Termos utilizados pelo sistema de impressão do Windows Server 2003:                            | 874 |
| Impressão através da Internet.   | 875 |
| Padronização de nomes e outros detalhes importantes para o uso de impressoras em rede.         | 876 |
| Atribuindo permissões de acesso para a impressora.   | 876 |
| O serviço Spooler de Impressão:  | 878 |
| Configurando propriedades importantes e outras ações.  | 879 |
| Diferentes prioridades para diferentes grupos.   | 880 |
| Tudo o que você não pode esquecer sobre Backup e Restore                                       | 883 |
| Criar múltiplos agendamentos.  | 883 |
| Estratégias de backup e restore.   | 883 |
| Definindo o tipo de Backup a ser utilizado.  | 883 |
| Exemplos de estratégias de backup/restore.   | 885 |
| Dados do estado do sistema:  | 886 |
| O log do backup  | 887 |
| Fazendo o Backup e o Restore do Active Directory..   | 887 |
| Backup do Active Directory:  | 888 |
| Restore do Active Directory  | 888 |
| Fazendo o restore do Active Directory.   | 890 |
| Efetuando um restore nonauthoritative, usando o utilitário de backup.                          | 890 |
| Terminal Services (Serviços de Terminal):  | 891 |
| Introdução   | 891 |
| Como funciona o Terminal Services.   | 891 |
| Algumas considerações importantes sobre o Terminal Services:                                   | 895 |
| Administração do Terminal Services.  | 897 |
| Configurações do Terminal Services:  | 897 |
| O novo recurso de Shadow Copies.   | 901 |
| Mais algumas observações sobre o recurso de shadow copies.                                     | 902 |

|  |            |
|--|------------|
| O agendamento do recursos de shadow copies.                                  | 902        |
| Instalando o cliente de shadow copies.                                       | 902        |
| Log de Eventos e de Auditoria – Conceito.                                    | 902        |
| Habilitando eventos de auditoria.  | 905        |
| Configurando a auditoria de acesso a arquivos, pastas e impressoras.         | 911        |
| Monitoração de desempenho  | 911        |
| Monitoração de desempenho – conceitos básicos.                               | 911        |
| Contadores a serem monitorados em servidores.                                | 913        |
| Valores indicativos de limites de desempenho para contadores.                | 914        |
| Configurando o console Desempenho para capturar dados automaticamente.       | 917        |
| Mais um resumo de contadores, para você não esquecer:                        | 918        |
| Ferramentas de recuperação a desastres.                                      | 919        |
| O Modo Seguro, Last Know Good Configuration e Control Sets..                 | 919        |
| Opções de inicialização do Windows Server 2003 e o Modo seguro.              | 920        |
| Entendendo o Modo seguro de inicialização – Safe mode.                       | 920        |
| Last know good configuration e Control Sets.                                 | 922        |
| Outras opções de configuração do Menu de opções avançadas do Windows.        | 923        |
| O recurso ASR – Automated System Recovery Disks                              | 923        |
| Criando um disquete de boot.   | 925        |
| O Console de Recuperação.  | 926        |
| Internet Information Services 6.0 – IIS 6.0 e Software Update Services – SUS | 928        |
| Pontos importantes sobre o IIS, a serem lembrados para o exame:              | 928        |
| SUS – Software Update Services   | 929        |
| Introdução ao SUS  | 929        |
| Componentes do SUS:  | 930        |
| Instalando o SUS   | 931        |
| Administrando o SUS  | 936        |
| Configurar os clientes para utilizar o SUS.                                  | 940        |
| Configurando os clientes via GOP:  | 941        |
| Opções da Registry relacionadas com o SUS:                                   | 946        |
| Conclusões finais e uma proposta de Plano de Estudos.                        | 946        |
| <b>Capítulo 15: Simulado para o Exame 70-290 – 60 Questões</b>               | <b>948</b> |
| Simulado para o Exame 70-290 – 60 questões – respostas – comentários:        | 948        |
| Conclusão  | 1000       |

# Introdução

# INTRODUÇÃO

Prezado leitor, este é o terceiro livro, de uma série de livros de minha autoria sobre os exames de Certificação da Microsoft. Após alguns anos trabalhando com Certificações Microsoft e após a aprovação em 27 exames, sinto-me muito à vontade para escrever sobre este assunto e a orientá-lo na obtenção da tão sonhada aprovação nos Exames de Certificação. Meu principal objetivo é passar uma série de dicas e um pouco da minha experiência prática, para ajudar o amigo leitor a obter sucesso nos exames de Certificação da Microsoft.

Este é um livro específico para o Exame 70-290: Managing and Maintaining a Windows Server 2003 Environment (Mantendo e Gerenciando um Ambiente baseado no Windows Server 2003). Neste livro abordarei os tópicos do exame, de acordo com o programa oficial da Microsoft, o qual está descrito em: <http://www.microsoft.com/learning/exams/70-290.asp>

Um bom estudo a todos. Não deixem de conferir, periodicamente, novas dicas, tutoriais, simulados e artigos, diretamente no site do autor: [www.juliobattisti.com.br](http://www.juliobattisti.com.br). Você também pode acessar o fórum de discussão sobre Certificações Microsoft e trocar experiências com colegas de todo o Brasil. O endereço para acesso ao fórum é o seguinte: [www.juliobattisti.com.br/forum](http://www.juliobattisti.com.br/forum).

Um bom estudo a todos. Não deixe de enviar suas opiniões, críticas, elogios, sugestões e relato de erros encontrados no livro, diretamente para o e-mail: [webmaster@juliobattisti.com.br](mailto:webmaster@juliobattisti.com.br)

## Uma visão geral sobre Certificações Microsoft

Nesta introdução vou apresentar uma visão geral sobre o programa de Certificações da Microsoft. Vou iniciar o Capítulo falando sobre as diferentes opções de certificação para profissionais que trabalham com a administração e gerência de redes baseadas no Windows Server 2003. Em seguida vou apresentar mais detalhes sobre a certificação “Microsoft Certified Systems Engineer – MCSE”, do qual faz parte o exame 70-290 Managing and Maintaining a Windows Server 2003 Environment (objeto de estudo deste livro e obrigatório para o candidato que quer obter a certificação MCSE-2003). Também trataréi da Certificação Microsoft Certified Professional – MCP que é uma certificação, digamos, mais “light”. Para obter o MCP basta que você seja aprovado em um único exame de produto Microsoft, como por exemplo, o exame 70-210 (Windows 2000 Professional), exame 70-270 (Windows XP Professional) ou outro exame qualquer de produto Microsoft, não necessariamente um exame do Windows 2000 Server ou Windows Server 2003.

Os objetivos e conteúdos que fazem parte do exame são definidos pela própria Microsoft. O Exame 70-290 tem a seguinte denominação Oficial, em Inglês: “Exam 70-290: Managing and Maintaining a Windows Server 2003 Environment”. Eu me arriscaria a traduzir como:

“Exame 70-290: Mantendo e Gerenciando um Ambiente baseado no Windows Server 2003”

O exame inclui uma série de tópicos relacionados a Administração e Manutenção de uma rede de grande porte, com servidores baseados no Windows Server 2003 e no Active Directory. Entenda-se uma rede de grande porte, como sendo uma rede formada por escritórios em diversas localidades. Cada localidade com uma rede local e as diversas redes locais conectadas através de links de WAN. Neste cenário existe uma série de serviços e funcionalidades disponibilizadas pelo Windows Server 2003 e pelo Active Directory, tais como: Cadastro de Usuários e Grupos, Gerenciamento de Pastas e Impressoras Compartilhadas, Gerenciamento de Armazenamento de Arquivos, DNS, RIS, GPOs, Sites, replicação do Active Directory e assim por diante. Estes são justamente os tópicos a serem abordados neste livro. Por isso, segundo a Microsoft, no site oficial do exame 70-290 (<http://www.microsoft.com/learning/exams/70-290.asp>), este exame é indicado para candidatos que tem experiência de, pelo menos, um ano, na implementação/administração/gerência de redes de grande porte, baseadas em tecnologias Windows e no Active Directory, ou seja, para profissionais que já tem uma experiência com redes baseadas no Windows 2000 Server ou, preferencialmente, no Windows Server 2003.

O Exame 70-290 não é dos exames mais difíceis no caminho do candidato ao MCSE no Windows 2000. Em uma escala de um a cinco, eu diria que ele tem um nível de dificuldade três e meio. Para quem já fez o exame 70-215, para o MCSE-2000 (Administração do Windows 2000 Server), poderá comparar o nível de dificuldade dos exames, pois classifico o exame 70-215 com um nível de dificuldade três, em uma escala de um a cinco. O Exame cobra um conhecimento detalhado dos principais serviços e tarefas administrativas de um ambiente baseado no Windows Server 2003.

Este exame é recomendado para candidatos que trabalham na administração e/ou gerencia de redes de tamanho médio para grande, as quais utilizam o Windows Server 2003 nos servidores e o Windows 2000 Professional ou Windows XP Professional nas estações de trabalho da rede. É recomendado, porém não obrigatório, que você tenha, no mínimo, um ano de experiência trabalhando em uma rede com as seguintes características/serviços:

- ◆ Entre 200 e 26.000 usuários;
- ◆ Entre 5 e 500 localizações físicas: diferentes redes em diferentes localidades/escritórios da empresa;
- ◆ Cinco ou mais Controladores de Domínio (DCs);
- ◆ Compartilhamento de arquivos e impressoras;
- ◆ Infra-estrutura baseada no Active Directory.
- ◆ Servidores de banco de dados e de mensagens;
- ◆ Servidores Web baseados no IIS;
- ◆ Gerenciamento de estações de trabalho (GPOs);

Ao passar no exame 70-290 você obtém a certificação MCP, caso ainda não seja um MCP. O exame 70-290 também é um exame obrigatório (Core) para a certificação MCSE- 2003 (veja mais detalhes sobre os exames necessários ao MCSE-2003, mais adiante, nesta introdução). Este exame também pode ser utilizado obrigatório para as certificações MCDBA em SQL Server 2000 e MCSA em Windows Server 2003.

Este é um exame (como o próprio título sugere) que aborda diretamente a Administração e Gerenciamento de um ambiente de rede, baseado no Windows Server 2003. O candidato deve dominar os conceitos teóricos dos diversos serviços e funcionalidades disponibilizadas por um servidor baseado no Windows Server 2003.

**IMPORTANTE: A experiência é recomendada, não é obrigatória. Ou seja, o candidato não terá que comprovar a experiência prática para poder fazer este exame. Embora a experiência não seja obrigatória (no sentido de ter que ser comprovada), é altamente recomendada, pois somente com uma boa experiência prática, na implementação/administração/gerência de redes de grande porte, é que o candidato terá maiores chances de ser aprovado neste exame.**

Uma dúvida que muitos candidatos tem é se realmente é necessária a experiência prática. Este é um assunto que posso falar com base em uma boa experiência pessoal. Já fui aprovado em 27 Exames de Certificação da Microsoft, com o que obtive as seguintes certificações: MCP, MCP+I, MCSE, MCSE+I, MCDBA, MCSD e MCT (quando este livro for publicado já terei feito mais dois exames, para aumentar um pouco mais esta estatística). Para obter esta valiosa “sopa de letrinhas” posso garantir que a experiência prática foi de grande importância. Trabalho como Gerente do Ambiente Cliente Servidor na Delegacia da Receita Federal de Santa Maria – RS. Durante muito tempo atuei como Administrador de Rede, em um rede baseada, primeiro em clientes com Windows 9x e Servidores com NT Server 4.0; depois com clientes baseados no Windows 2000 Professional e Servidores com Windows 2000 Server. Posso garantir que a experiência prática ajuda muito na hora dos exames. Surgem questões que só a vivência prática é capaz de ajudar a resolver.

## **Uma visão geral do programa de certificação da Microsoft**

A Microsoft tem um amplo e variado programa de Certificação, do qual fazem parte certificações para diferentes perfis de profissionais. Por exemplo, existe uma certificação para Engenheiros de Sistemas – MCSE (Microsoft Certified Systems Engineer), outra para Administradores de Banco de Dados – MCDBA (Microsoft Certified Database Administrator), outras duas para desenvolvedores de aplicativos – MCSD e MCAD, outra para Administradores de Rede – MCSA, outra para Instrutores Certificados – MCT e assim por diante.

O programa de certificação é a maneira que a Microsoft tem para verificar as habilidades técnicas dos candidatos na utilização, projeto e implementação de tecnologias Microsoft nas redes das empresas e para o desenvolvimento de aplicações.

Muitos leitores me questionam sobre o real valor das certificações, para o Mercado de Trabalho. Esta é uma questão realmente difícil de responder. As certificações atestam a capacidade técnica do candidato ao emprego em uma determinada área de atuação. Porém as qualificações técnicas são apenas uma das habilidades necessárias para que o candidato se coloque bem no mercado. Hoje em dia são muitos os requisitos que se exigem de um profissional e, a maioria deles, não são técnicos.

A seguir coloco uma cópia do artigo “O Profissional Atual = Um Ser Humano Completo”, de minha autoria, o qual foi publicado no site da Revista Developers Magazine ([www.developers.com.br](http://www.developers.com.br)), e que esteve na página principal do site por quase 6 meses. Neste artigo abordo justamente as múltiplas aptidões que o profissional atual deve dominar para se colocar bem no mercado de trabalho. Leia e reflita com calma. Esta é minha modesta contribuição na área não técnica, para ajudá-lo no direcionamento e na construção de uma carreira profissional.

\*\*\*\*\*  
\*\*\*\*\*

## **Artigo: O Profissional Atual = um Ser Humano Completo**

### **Introdução**

Estamos vivendo a “era da informação, da velocidade e da orientação para resultados”. Muitas vezes, ficamos atônitos com a rapidez com que as mudanças acontecem. Já não basta mais sermos especialistas em informática. Precisamos “entender do negócio”, senão como poderemos aplicar nossos conhecimentos em benefício da empresa, ou em outras palavras: gerar resultados.

Muitos consultores e autores bem-sucedidos de livros de negócios e carreira dizem que estamos vivendo a era dos multi-especialistas. Precisamos entender de muitos assuntos: administração, finanças, informática, outros idiomas, pessoas (esta talvez seja a aptidão mais importante e mais difícil), trabalho em equipe, etc.

Como dominar tantas competências e, ao mesmo, tempo conciliar família, amigos, atividades físicas e a pressão da empresa por resultados cada vez melhores e em menor tempo? Com certeza não é fácil, mas é possível crescer profissionalmente e, principalmente, com ética, sem abrir mão de uma vida pessoal com qualidade.

## Conhecimentos técnicos são e sempre serão indispensáveis

Lembra do tempo em que era só pegar o diploma, esperar uma proposta de emprego, trabalhar por "uns trinta anos" na mesma empresa e se aposentar? Essa época simplesmente acabou. Hoje temos que nos manter em um estado de aprendizagem contínuo e o mais difícil: temos que aprender a aprender. Educação e aprendizagem não é algo que tem data para terminar em um momento determinado, como logo após a faculdade ou uma pós-graduação. Para que o profissional possa manter-se no mercado é necessário estudar sempre, mantendo-se atualizado com as mudanças tecnológicas, aprendendo a utilizar as novas ferramentas, aprimorando o conhecimento de outros idiomas e assuntos.

Precisamos conhecer uma infinidade de assuntos, dentro os quais poderia destacar os seguintes: conhecimentos sobre finanças e investimentos, noções básicas sobre contabilidade e economia, matemática financeira, um ou mais idiomas estrangeiros; preferencialmente inglês e espanhol, bom domínio da gramática e das técnicas de redação, administração, marketing, gerência de projetos, trabalho em equipe e orientação para resultados.

Somente o estudo eficaz e continuado é capaz de garantir o domínio de tantos assuntos. Por isso devemos nos preocupar, em primeiro lugar, em melhorar o nosso rendimento nos estudos.

Aliás, o princípio de educação pela vida inteira não é nenhuma novidade dos tempos modernos. Os gregos já defendiam um modelo de educação conhecido como "paideia", em que um dos pilares deste modelo era uma educação diferenciada e continuada, mesmo após a idade adulta.

Em resumo: educação e estudo durante a vida inteira.

### O primeiro dilema: mais estudo demanda mais tempo

Para exemplificar o dilema de arranjar tempo para estudar tudo o que julgamos necessário ou "que nos dizem" ser necessário, vou utilizar o exemplo da pessoa que eu melhor conheço neste mundo: "eu mesmo".

Em primeiro lugar, você precisa entender que não dá para estudar tudo o que acha ser importante ou nos dizem (jornais, revistas e sites da moda) ser indispensável para uma carreira de sucesso. Devemos ser capazes de definir prioridades e seguirlas à risca.

Durante muito tempo comprei muito mais livros do que poderia ler. Cheguei a ter mais de 30 livros esperando na fila. Constantemente, me preocupava pelo fato de não conseguir ler e estudar todos os assuntos que eu julgava importantes. Uma simples pausa para assistir a um jogo de futebol na televisão era motivo para consciência pesada por não ter aproveitado melhor meu tempo. Onde é que já se viu perder um jogo do meu Grêmio?

Neste período, acabei me afastando dos amigos, da família e até minha esposa queixava-se, com a mais absoluta razão, de que eu quase não ficava com ela. Muitas vezes eu me preocupava mais em ler um livro, do que em fazer uma análise sobre seu conteúdo e sobre o valor daquela leitura para mim como ser humano e para a minha carreira profissional. O importante era diminuir a fila de livros não lidos, mesmo que isso significasse cada vez menos horas de sono, menos horas de lazer e de atividades físicas. Pouco importava se minha qualidade de vida estava péssima e piorando dia a dia.

Talvez o amigo leitor jamais tenha chegado a esse ponto, mas não é difícil concluir que não dá pra estudar tudo. O simples fato de o estudo ter se tornado uma carga muito pesada, mais uma obrigação do que um prazer, fez com que meu rendimento e meu humor descessem a níveis preocupantes.

Não dá para aprender tudo ao mesmo tempo: Windows XP, Windows 2000, Linux, Novell, UNIX, VB, Delphi, Java, JavaScript, ASP, ASP.NET, C, C++, C#, XML, segurança, finanças, economia, administração, fazer um MBA, uma pós... e, se você ainda estiver vivo, quem sabe, uma cirurgia de ponte de safena.

Estudo e aperfeiçoamento contínuos são fundamentais sim, porém de forma organizada e, principalmente, planejada. O foco deve estar na aplicação dos conhecimentos adquiridos. Jamais no conhecimento por si só. Conhecimento não é poder, ação que é poder. Conhecimento não é o que faz a diferença, o que faz a diferença é o que você faz com o conhecimento que tem. Não se esqueça dos seguintes princípios básicos: definição de prioridades e foco na aplicação dos conhecimentos.

Parece e é o óbvio. Se cada vez temos mais assuntos para estudar, mais aptidões para desenvolver e menos tempo para tudo isso é fundamental que formemos uma base bem sólida para enfrentar os desafios atuais e os que ainda estão por vir. Como "base sólida", considero o domínio de algumas técnicas vitais para que o profissional possa manter o seu desempenho em níveis sempre elevados e ao mesmo tempo ter tempo para viver, para curtir a família, o laser e os amigos. Vamos falar um pouco sobre alguns tópicos que considero vitais:

## **Administração do tempo:**

Saber administrar de maneira racional o "escasso" tempo que dispomos é de fundamental importância. Muitas pessoas queixam-se de que não tem tempo para nada, mas se observarmos com mais atenção veremos que mesmo que o dia tivesse as "tão sonhadas 48 horas", essas pessoas não conseguiram concluir as suas tarefas, pelo simples motivo de que não administraram corretamente o tempo. Estamos sem controle do nosso tempo quando acumulamos mais informações do que podemos absorver, quando trabalhamos de olho no relógio, querendo cumprir uma carga de trabalho irreal, quando levamos uma vida sedentária com a desculpa que não temos tempo para praticar uma atividade física ou quando enchemos nossa agenda com atividades e compromissos que sabemos que não seremos capazes de cumprir.

Nos endereços a seguir você encontra uma série de artigos meus sobre Administração do Tempo:

[http://www.gabaritando.com.br/colunas/0310\\_batisti.asp](http://www.gabaritando.com.br/colunas/0310_batisti.asp)  
[http://www.gabaritando.com.br/colunas/batisti brigar\\_tempo2\\_27\\_01.asp](http://www.gabaritando.com.br/colunas/batisti brigar_tempo2_27_01.asp)  
[http://www.gabaritando.com.br/colunas/batisti brigar\\_tempo3\\_1.asp](http://www.gabaritando.com.br/colunas/batisti brigar_tempo3_1.asp)

## **Serás organizado e não procrastinarás:**

Não é um mandamento mas deve ser encarado como tal. Sabe aquele história que: "na minha bagunça eu me acho"? O profissional dos dias atuais tem que ser organizado, quer seja no trabalho, quer seja na sua vida pessoal. No final de cada ano fazer um planejamento para o ano seguinte não faz mal a ninguém. No planejamento é importante incluir quais novos conhecimentos você deseja adquirir, onde você irá aplicar estes conhecimentos (lembre sempre: conhecimento sem ação não tem valor algum), as novas aptidões que deseja desenvolver e, principalmente, quais os objetivos deseja alcançar. Parece incrível, mas muitas pessoas, no meio da correria, não tem a noção exata de quais são seus objetivos. Como diz um ditado oriental: "de que adianta correr se você está no caminho errado"? Outra "praga", que deve ser combatida com veemência é a procrastinação, o popular "empurrar com a barriga". Deixar para depois, começar amanhã ou quem sabe na semana que vem? Nada disso. Quanto antes iniciarmos nossas tarefas, com mais tranquilidade e qualidade poderemos completá-las, sem apuros e improvisações.

## **Trabalho em equipe e delegação de tarefas:**

Você é admitido na empresa e é mais do que normal que no seu primeiro emprego, seja alocado para realizar algumas tarefas operacionais. Mas como todo mundo, você quer evoluir, crescer, ser promovido. É natural que venha a ocupar, com o passar do tempo, um cargo de gerência. Quem sabe um dia será diretor, depois vice-presidente e, por que não, presidente. Não importa o cargo que você ocupa, é fundamental que saiba trabalhar em equipe, em outras palavras: "colaboração e cooperação". Isso não significa que não deva existir competição, porém em doses saudáveis. Mas o fato é que somente o trabalho em equipe é capaz de obter os resultados exigidos atualmente. Pela milionésima vez vou citar o exemplo do time de futebol formado por onze craques, porém sem espírito de equipe, onde cada um quer aparecer mais do que o outro. Com certeza este time será derrotado por uma equipe formada por onze jogadores medianos, porém com forte espírito de equipe, onde todos colaboram na busca de um objetivo comum. Na medida em que você vai ocupando cargos com características mais gerenciais do que operacionais a delegação de tarefas torna-se um instrumento indispensável. Se você chefia uma equipe é fundamental que confie nela. Com isso é possível delegar tarefas e manter um nível de acompanhamento racional; pois de nada adianta delegar uma tarefa e depois acompanhar, passo-a-passo a execução. No endereço a seguir você encontra um artigo meu sobre Delegação de Tarefas:

[http://www.timaster.com.br/revista/artigos/main\\_artigo.asp?codigo=322](http://www.timaster.com.br/revista/artigos/main_artigo.asp?codigo=322)

Não basta ser competente, os outros tem que saber que você é competente:

É importante que as pessoas saibam que você é um profissional competente, ético e em que assuntos você pode ser considerado uma referência. Não é uma questão de ser metido ou se achar o máximo. Devemos cuidar da nossa carreira da mesma maneira que cuidamos de uma empresa. Tom Peters, na excelente série de livros "Reinventando o Trabalho", editora Campus, defende que o profissional deve cuidar da divulgação do seu talento e habilidades, como se estivesse fazendo a divulgação do produto de uma empresa – ele denomina esta empresa de Você AS.. Peters ainda defende a idéia que devemos cuidar desde os aspectos básicos com uma boa aparência, boa educação, até questões mais avançadas como fazer uma auto-avaliação do tipo: "qual o valor da marca – seu nome – para o mercado de trabalho". A idéia básica é que você torne-se um profissional que as empresas necessitem e que seja capaz de fazer o seu marketing pessoal com eficiência.

Outra palavra que está bastante em moda é "networking". Esta palavra é utilizada para fazer referência à nossa rede de relacionamentos profissionais. Diversos autores são unânimes em afirmar que não devemos nos descuidar da nossa rede de relacionamentos. De preferência devemos ampliá-la para incluir contato com profissionais das mais diversas áreas. Manter nossa lista de telefones e endereços de e-mail em dia é de fundamental importância. Muitas vezes uma oportunidade surge na empresa onde um dos seus contatos/ amigos está trabalhando. É natural e ético que o seu contato/amigo indique você para ocupar a vaga. Existem empresas que dão prêmios em dinheiro, para funcionários que indicam conhecidos que sejam aprovados e admitidos para ocupar uma vaga na empresa. A simples indicação não garante o emprego, pois o candidato deverá passar pelo processo de avaliação da empresa. Além disso, se você não for competente, o seu amigo/contato não irá indicá-lo, pois ele não quer ser responsável pela admissão de uma pessoa sem as competências exigidas pela empresa ou pela indicação de um candidato que certamente será reprovado.

## **É hora de construir uma carreira de sucesso**

Agora que você já conhece os fundamentos necessários para criar uma carreira de sucesso, tais como administrar bem o tempo e a sua lista de contatos, ser organizado e ter objetivos bem claros, é hora de construir uma carreira sólida e de sucesso.

Parece óbvio, mas devo reforçar a idéia de que o profissional de TI, quer seja em nível operacional, gerencial ou executivo, deve ter sólidos conhecimentos técnicos. Um ponto importante a destacar é que "conhecimentos

técnicos" significa o domínio de algumas tecnologias essenciais e não, necessariamente, de produtos específicos. Este é um erro que tenho observado, inclusive, em diversos cursos universitários para a formação de profissionais de TI, ou seja, ao invés de ensinar tecnologia, ensinam a utilizar determinados produtos. Claro que existem alguns produtos específicos que, devido a grande aceitação pelo mercado, devem ser dominados pelo profissional de TI. A seguir coloco uma lista das tecnologias e alguns produtos específicos que considero essenciais que o profissional domine:

- ◆ Sistemas operacionais, principalmente Windows (9x, 2000, NT e XP), Linux e UNIX
- ◆ Redes de computadores (conceitos, arquiteturas, dispositivos de hardware, etc.).
- ◆ TCP/IP e tecnologias relacionadas.
- ◆ Orientação a objetos (para desenvolvedores e analistas de sistema).
- ◆ Princípios de análise e projeto de software.
- ◆ Segurança (criptografia, firewall, gerenciamento, VPN, PKI, certificados digitais, etc.).
- ◆ Banco de dados (modelo relacional, administração, integração com a Web, etc.).
- ◆ Gerência de projetos.
- ◆ No mínimo uma ferramenta/linguagem de desenvolvimento.
- ◆ Internet (arquitetura, utilização, modelo de desenvolvimento para Web em três ou mais camadas).

Pode parecer muita coisa, mas o domínio destes assuntos segue uma ordem natural e até intuitiva, mesmo nos atuais dias de correria. A maioria dos profissionais de TI iniciou sua carreira aprendendo a utilizar um sistema operacional. Em seguida, muito provavelmente, passou a estudar os princípios básicos de lógica de programação e uma linguagem para testar os conceitos aprendidos. Em seguida, chegou o momento de aprender a utilizar algumas ferramentas, como por exemplo um redator de textos e uma planilha de cálculos. E assim os conhecimentos vão sendo adquiridos um a um. O problema está na velocidade com que novas tecnologias e produtos são lançados. Não adianta nos queixarmos, a atitude correta é nos adaptarmos.

No início da Revolução Industrial, quando foram criados os primeiros teares, muitos empregados ficaram revoltados, com medo de perder o emprego. Outros procuraram entender a mudança, aprendendo a operar as novas máquinas. Estes últimos souberam se adaptar a uma situação de mudança e mantiveram seus empregos. Penso que atitude correta é exatamente esta, ou seja, o profissional de TI precisa adaptar-se ao ritmo em que vivemos. É simplesmente uma questão de adaptar-se ou ficar para trás. Aqui quero mais uma vez tocar no ponto central, o qual me levou a escrever este artigo: "é possível acompanhar o ritmo das mudanças, mantendo-se atualizado, sem perder em qualidade de vida e convívio com a família e os amigos".

Um aspecto bastante valorizado pelas empresas são as certificações oficiais. Cada empresa tem o seu próprio programa de certificação. Por exemplo, a certificação mais valorizada da Microsoft é o título de MCSE – Microsoft Certified Systems Engineer. As certificações da Cisco, IBM, Sun e Oracle também são bastante valorizadas no mercado. A certificação serve como uma espécie de atestado, o qual é um indicativo das qualificações do profissional em um determinado produto ou tecnologia.

Aquele profissional que trabalhava exclusivamente fechado na sala de processamento de dados, sem um contato mais direto com o restante da empresa, apenas realizando tarefas estritamente técnicas, não existe mais. Hoje a empresa quer um profissional completo, ou seja, um ser humano completo.

A Tecnologia da Informação é fundamental como suporte para todas as atividades de uma empresa. Para que a TI possa atender as expectativas da empresa, dos funcionários e dos clientes, é fundamental que os profissionais de TI conheçam a empresa, os funcionários, os processos, os produtos, os clientes e o mercado. Em outras

palavras: conhecer o negócio. Por isso que além dos conhecimentos técnicos são importantes os conhecimentos já citados anteriormente, tais como: finanças, administração, marketing, contabilidade, economia, etc.

A alma de uma empresa é formada por pessoas, idéias e objetivos claros e definidos. Para que as pessoas possam colocar suas idéias na busca de seus objetivos pessoais e na busca dos objetivos da empresa é fundamental que todos tenham boas capacidades de relacionamento inter e intra pessoal. A empresa espera que o profissional seja ético, honesto, que tenha espírito de equipe. Neste ponto a alta direção e os executivos da empresa desempenham um papel fundamental na criação de um bom ambiente de trabalho. A empresa tem que saber que os funcionários não ajudarão a empresa a alcançar seus objetivos se ela, a empresa, não ajudar o funcionário a realizar seus próprios sonhos.

Um bom ambiente de trabalho inclui uma estrutura sem grandes burocracias com infinitos níveis hierárquicos, com dezenas de formulários a serem preenchidos, os quais só atrapalham quem quer trabalhar e produzir. É um ambiente onde a criatividade é sempre incentivada e não sufocada por normas sem sentido; uma política de remuneração justa e transparente; desafios constantes e direitos iguais para todos. São pequenas coisas que podem começar a minar o ambiente de trabalho. Pequenas regalias para a alta administração, ineficiência na comunicação interna, etc.

Dentro deste novo ambiente, o profissional deve ser capaz de se expressar com naturalidade e eficiência. O domínio da gramática e das técnicas de redação e comunicação é fundamental, para que você possa expor suas idéias com clareza. Passamos uma parcela considerável do nosso tempo respondendo e-mails, elaborando memorandos, relatórios, notas técnicas e os mais variados tipos de documentos. O profissional que domina as técnicas de redação tem maiores chances de se destacar e ser lembrado para promoções. Além da comunicação escrita, também é de grande importância a habilidade para fazer apresentações, quer seja para um público interno (colegas de trabalho, chefes, etc.), quer seja para um público externo (clientes, fornecedores, etc.).

Todo este "arsenal" de conhecimentos e aptidões de nada adianta se você não for "orientado para resultados". Em outras palavras: a empresa não paga você para trabalhar oito horas ou para realizar determinadas tarefas ou para ter determinados conhecimentos; você é pago para obter resultados, para ação.

Para que você possa obter os resultados esperados pela empresa, são fundamentais três "Cs": Conhecimento, Contribuição e Comprometimento. Sobre a importância dos conhecimentos e do trabalho em equipe (contribuição) já falamos. Mas tudo isso não adianta se você não estiver comprometido com suas idéias, projetos e objetivos, estes alinhados com os objetivos da empresa. Comprometer-se é buscar os resultados, dando o máximo de si. Quando um projeto está com problemas, se você não estiver comprometido com o sucesso do projeto, começará a buscar desculpas que justifiquem o "possível fracasso", ao invés de trabalhar intensamente na busca de soluções. O profissional dos dias atuais tem que estar comprometido com os objetivos da empresa e também com seus objetivos pessoais, a isso chamo de ética pessoal e profissional. Esta é uma questão de postura do profissional. Para detalhes sobre este tópico consulte o meu artigo: "Vencer é uma questão de postura", disponível no endereço a seguir:

[http://www.gabaritando.com.br/colunas/Batisti\\_postura01\\_04\\_03.asp](http://www.gabaritando.com.br/colunas/Batisti_postura01_04_03.asp)

## A vida não é somente trabalho

Leia esta pequena história:

Uma vez um mestre fez uma experiência com seus alunos. Pegou um vaso e encheu-o com pedras grandes. Depois, ergueu o vaso e perguntou aos alunos: o vaso está cheio?

A turma se dividiu, com alguns dizendo que sim e outros que não. O mestre então, pegou algumas pedras pequenas e colocou-as no vaso. As pedras pequenas se encaixaram entre as grandes, e o mestre ergueu o vaso, novamente, perguntando: o vaso está cheio?

Desta vez a maioria dos alunos respondeu que sim. O mestre, então, pegou um saco de areia e despejou dentro do vaso. Depois, repetiu a pergunta.

A grande maioria respondeu que sim. O mestre, então, pegou uma jarra de água, derramou no vaso, e perguntou: o vaso está cheio?

A turma finalmente chegou a um consenso. Todos responderam que sim. Então o mestre falou: Este vaso é como a nossa vida. Se eu tivesse colocado as pedras pequenas, a areia ou a água em primeiro lugar, não haveria espaço para as pedras grandes. As pedras grandes na nossa vida são: família, amigos, carreira, trabalho, fé, lazer e saúde. É fundamental que não descuidemos delas. Não podemos perder muito tempo com coisas sem importância (as pedras pequenas), pois corremos o risco de não haver espaço para as coisas que realmente são importantes (as pedras grandes).

Para mim, foi vital entender que a carreira é importante sim, principalmente em tempos de alta rotatividade e de busca por profissionais cada vez mais qualificados. Mas ela não é tudo. Uma carreira de sucesso é sustentada por muitos pilares e, sem dúvida, família, lazer, amigos e saúde física e mental são alguns dos que têm maior importância.

Reservar um tempo para a família, programar horas de lazer ou de bate-papo com os amigos e realizar atividades físicas não podem, de maneira alguma, ser consideradas atividades que nos "roubam tempo". Às vezes, é importante uma simples parada para não fazer nada e refletir sobre a vida. A partir do momento em que conseguimos equilibrar esses aspectos, passamos a ver as coisas com mais clareza e a produzir mais e melhor.

## Planejamento e organização – mais um lembrete

Também não podemos descuidar de dois princípios básicos para uma carreira de sucesso: organização e planejamento. A cada fim de ano planejo minha carreira para os 365 dias que vão começar e sempre penso nos seguintes aspectos: novos conhecimentos que desejo adquirir e aonde vou aplicá-los, provas e exames de certificação que desejo fazer, projetos que pretendo implementar na minha empresa e projetos pessoais que quero desenvolver (como escrever livros e artigos, ministrar palestras e treinamentos).

O planejamento precisa ser feito de maneira consciente. Não adianta planejar uma carga de atividades que com certeza você não terá como cumprir. Também é importante ter consciência de que nem sempre as coisas saem conforme o planejado. É preciso ter criatividade e flexibilidade para contornar e solucionar imprevistos.

Melhorar a capacidade de organização e de gerenciamento do tempo, também é um aspecto importante. Muitas vezes me pegava navegando na Internet horas a fio, saltando de um portal para o outro, maravilhado com a quantidade de informações, mas não chegava a ler sequer um artigo. Na verdade, nem mesmo lembrava do assunto que me levou a acessar a Internet. É claro que a Internet é imprescindível, porém devemos saber utilizá-la a nosso favor, sem nos perdermos na imensidão de informações disponíveis.

Tomar café, assistir TV, ler um jornal a caminho do serviço, outro no avião, assinar um monte de revistas; são sintomas do que Richard Saul Wurman descreve como ansiedade de informação, no excelente livro com este mesmo título. Segundo o autor: "informação é aquilo que reduz a incerteza, a causa profunda da ansiedade. A ansiedade da informação acontece quando você sabe o que quer, mas não sabe como chegar lá".

No começo é difícil. Diversas vezes, em meio a uma atividade de lazer, batia aquela "dor na consciência" e eu pensava que deveria estar estudando ou terminando um trabalho qualquer. Porém com o tempo, comecei a perceber a importância dessas atividades.

Posso usar o meu exemplo pessoal para mostrar o quanto é importante não descuidar das "pedras grandes" que fazem parte da nossa vida. Em 2001, consegui publicar dois livros (SQL Server 2000 Administração

e Desenvolvimento – Curso Completo e ASP.NET, Uma Nova Revolução na Criação de Sites e Aplicações Web, ambos pela Axcel Books), em 2002 mais um livro (Windows XP Home & Professional pela Axcel Books), criei e consegui tornar conhecido o meu site ([www.juliobattisti.com.br](http://www.juliobattisti.com.br)) e viajei o Brasil inteiro ministrando treinamentos em diversas áreas, consegui estudar vários assuntos que julguei prioritários e fui aprovado em oito exames de certificação da Microsoft. Isso não significou que tive que esquecer do lazer e da família ou dos amigos.

Ainda não “zerei” a fila de livros que tenho para ler, nem dediquei todo o tempo que julgo necessário para minha vida pessoal, mas confesso que já consigo passar um domingo inteiro na beira da piscina, no clube, sem ficar com a consciência pesada. Este ano também tive momentos maravilhosos com minha família e meus amigos. Sinto-me mais leve e produzindo mais do que antes; consigo valorizar coisas que antes passavam despercebidas. Até voltei a brincar com crianças, o que antes eu achava algo irritante e sem graça. O caso era realmente sério!

Pare, viva. É possível crescer profissionalmente e obter sucesso, sem se isolar do mundo, sem sentir-se sufocado, sem perder o foco no que realmente é importante e nos faz feliz. Se você, leitor, quiser trocar idéias e sugestões, ou simplesmente contar suas experiências, é só entrar em contato comigo por e-mail ([webmaster@juliobattisti.com.br](mailto:webmaster@juliobattisti.com.br)). Será um grande prazer conversar com você.

## Referências bibliográficas:

- ◆ Dawson, Roger. 13 Segredos para o Sucesso Profissional. Editora Futura.
- ◆ Figueiredo, José Carlos. Como Anda Sua Carreira. Editora Infinito.
- ◆ Jensen, Bill. Simplicidade. Editora Campus.
- ◆ Kundtz, Dr. David. A Essencial Arte de Parar. Editora Sextante.
- ◆ Levy, Pierry. A Conexão Planetária. Editora 34.
- ◆ Minarelli, José Augusto. Empregabilidade. Editora Gente.
- ◆ Oliveira, Marco A. E Agora José? Editora SENAC.
- ◆ Peters, Tom. Série Reinventando o Trabalho. Editora Campus.
- ◆ Siegel, David. Futurize Sua Empresa. Editora Futura.
- ◆ Shinyashiki, Roberto. Você, a Alma do Negócio. Editora Gente.
- ◆ Sterneberg, Robert J. Inteligência Para o Sucesso Pessoal. Editora Campus.
- ◆ Wurman, Richard Saul. Ansiedade de Informação. Cultura Editores Associados.

Autor: Julio Battisti

**Site:** [www.juliobattisti.com.br](http://www.juliobattisti.com.br) e [www.certificacoes.com.br](http://www.certificacoes.com.br)

**E-mail:** [webmaster@juliobattisti.com.br](mailto:webmaster@juliobattisti.com.br)

\*\*\*\*\*  
\*\*\*\*\*

Este artigo reforça o meu ponto de vista de que, os conhecimentos técnicos continuam sendo importantes, porém as empresas esperam muito mais do que apenas conhecimentos técnicos. Ao obter uma ou mais certificações da Microsoft, você está comprovando os seus conhecimentos técnicos e o domínio das tecnologias relacionadas aos exames de certificação.

Conforme já descrito anteriormente, o exame 70-290 é obrigatório para quem quer obter a certificação MCSE, e também conta para as certificações MCSA e MCDBA. A seguir apresentarei alguns detalhes sobre a certificação MCSE-2003, que é a certificação indicada para profissionais que, além de administrar redes baseadas no Windows Server 2003, com clientes baseados no Windows 2000 Professional ou Windows XP Professional, também são responsáveis pelo planejamento, gerenciamento, implementação e expansão das respectivas redes.

Informações completas sobre os diversos programas de certificação da Microsoft podem ser encontradas nos seguintes endereços:

- ◆ [www.juliobattisti.com.br](http://www.juliobattisti.com.br)
- ◆ [www.microsoft.com/mcse](http://www.microsoft.com/mcse)
- ◆ [www.microsoft.com/mcsa](http://www.microsoft.com/mcsa)
- ◆ [www.microsoft.com/mcdba](http://www.microsoft.com/mcdba)
- ◆ [www.ucertify.com](http://www.ucertify.com)
- ◆ [www.certifyorsel.com](http://www.certifyorsel.com)
- ◆ [www.microsoft.com/traincert](http://www.microsoft.com/traincert)
- ◆ [www.microsoft.com/brasil/certifique](http://www.microsoft.com/brasil/certifique)
- ◆ [www.cramsession.com](http://www.cramsession.com)
- ◆ [www.examnotes.net](http://www.examnotes.net)
- ◆ [www.timaster.com.br](http://www.timaster.com.br) (coluna Certificado de Garantia, de minha autoria).
- ◆ [www.certcities.com](http://www.certcities.com)
- ◆ [www.certportal.com](http://www.certportal.com)
- ◆ [www.mcmcse.com](http://www.mcmcse.com)
- ◆ [www.2000tutor.com](http://www.2000tutor.com)
- ◆ [www.mcpmag.com](http://www.mcpmag.com)
- ◆ [www.msexpert.com](http://www.msexpert.com)

## O programa de certificação Microsoft Certified Systems Engineer – MCSE-2003:

### Introdução

Com a chegada do Windows Server 2003, em Abril de 2003, os candidatos estavam ansiosos em relação às mudanças em relação as certificações MCSA e MCSE, diretamente relacionadas com a Administração, Projeto e Implementação de Redes baseadas no Windows Server 2003. Alguns detalhes já foram revelados (conforme você poderá ver neste tópico), porém alguns itens, tais como se será e quando será descontinuada a certificação MCSE-2000, ainda não foram divulgados pela Microsoft.

A Microsoft anunciou em 19-02-2003 os requerimentos para obter o MCSE 2003, bem como as opções para quem já é MCSE no Windows 2000, obter a certificação MCSE 2003. A seguir apresento mais alguns detalhes sobre a nova certificação MCSE 2003, para que os candidatos possam já ir se planejando e preparando seus estudos.

**DÚVIDA MUITO IMPORTANTE:** Muitos leitores entram em contato comigo, via e-mail, com a seguinte pergunta:

Com a chegada do Windows Server 2003 (antes «batizado» de Windows .NET Server 2003), vale a pena continuar investindo na certificação para o Windows 2000?»

Eu diria que esta é uma resposta difícil de ser dada, neste momento (Janeiro de 2004). A migração do NT Server 4.0 para o Windows 2000 Server foi em ritmo bem lento, sendo que muitas empresas ainda não migraram ou somente agora estão iniciando projetos de migração. Isso que as vantagens do Windows 2000 em relação ao NT 4.0 são enormes. Já com o Windows Server 2003 é diferente, pois este representa apenas um conjunto de melhorias em relação ao Windows 2000 (na minha opinião), não é, nem de longe, uma mudança tecnológica e de paradigma (basta citar a introdução do Active Directory no Windows 2000) como foi do NT 4.0 para o Windows 2000. Com isso a ritmo de migração deverá ser lento (na minha opinião). Já passou a época em que as empresas seguiam os modismos e migravam só para estar em dia com a última tecnologia. Agora, as empresas vão analisar. Vale a pena migrar para o Windows Server 2003? Que vantagens eu terei em relação ao dinheiro investido? O resultado disso tudo é que o Windows 2000 continuará dominando o mercado por muito tempo e, consequentemente, continuará a haver necessidade de profissionais certificados no Windows 2000. Porém pode acontecer de daqui um mês ou dois a Microsoft anunciar a descontinuidade dos exames do MCSE-2000. Bem, pelos fatores expostos, infelizmente ainda não existe uma resposta definitiva a esta dúvida dos amigos leitores. Só nos resta aguardar.

## A quem se destina a certificação MCSE 2003:

A certificação MCSE-2003 é destinada a profissionais responsáveis pelo projeto e implementação de uma infra-estrutura de rede baseada no Windows Server 2003. Também é destinada aos profissionais responsáveis pela migração de uma rede baseada no Windows 2000 Server, Windows NT Server ou outras tecnologias, para uma rede baseada no Windows Server 2003. A idéia é que o profissional certificado com o MCSE 2003 seja capaz de planejar, projetar e coordenar a implementação de uma infra-estrutura de rede baseada no Windows Server 2003. Uma tarefa e tanto, que exige sólidos conhecimentos e domínios das tecnologias do Windows Server 2003.

O candidato à certificação MCSE 2003 terá que demonstrar os seus conhecimentos do Windows Server 2003, do Active Directory (Projeto e Implementação), dos serviços de rede (TCP/IP, DNS, DHCP, RRAS, IIS, IP-SEC e assim por diante), da parte de segurança e da parte de projeto de uma infra-estrutura de rede, baseada no Windows Server 2003.

## Quantos e quais os exames necessários ao MCSE-2003?

Para obter a certificação MCSE 2003 o candidato deve ser aprovado em sete exames, sendo seis os chamados core exames (obrigatórios) e um eletivo (que o candidato pode selecionar dentre as diversas opções disponíveis). Os exames core tem a ver diretamente com o Windows Server 2003. Desde exames mais voltados para a área de redes, outro específico para implementação e Administração do Active Directory, outro para projeto e design do Active Directory e assim por diante, conforme descreverei mais adiante. O exame eletivo pode ser selecionado entre diversas opções, conforme descreverei logo a seguir.

A seguir veremos quais as opções de exame disponíveis para obter a certificação MCSE 2003. Os exames são divididos em dois grupos: core (obrigatórios) e os eletivos. Para obter o MCSE-2003, o candidato:

- ◆ Deve ser aprovado nos seis exames obrigatórios (core).
- ◆ Deve escolher e ser aprovado em um dos diversos exames eletivos disponíveis.

## Exames Core (obrigatórios) para o MCSE - 2003 - 6 Exames:

Os seis exames obrigatórios estão divididos em três grupos, conforme descrito a seguir:

- ◆ Quatro exames de sistemas de redes.
- ◆ Um exame de Sistema Operacional Cliente.
- ◆ Um exame de Projeto (design).

## **Exames de Sistemas de redes: Você deve, obrigatoriamente, passar nos quatro exames a seguir:**

1. Exame 70-290: Managing and Maintaining a Microsoft Windows Server 2003 Environment. O Guia oficial, em inglês, com os tópicos a serem estudados para esse exame está disponível no seguinte endereço: <http://microsoft.com/traincert/exams/70-290.asp>. Este livro é um Manual de Estudos para o Exame 70-290.
2. Exame 70-291: Implementing, Managing, and Maintaining a Microsoft Windows Server 2003 Network Infrastructure. O Guia oficial, em inglês, com os tópicos a serem estudados para esse exame está disponível no seguinte endereço: <http://microsoft.com/traincert/exams/70-291.asp>. Ainda no primeiro semestre de 2004, será publicado um livro de minha autoria, específico para este exame.
3. Exame 70-293: Planning and Maintaining a Microsoft Windows Server 2003 Network Infrastructure. O Guia oficial, em inglês, com os tópicos a serem estudados para esse exame está disponível no seguinte endereço: <http://microsoft.com/traincert/exams/70-293.asp>.
4. Exame 70-294: Planning, Implementing, and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure. O Guia oficial, em inglês, com os tópicos a serem estudados para esse exame está disponível no seguinte endereço: <http://microsoft.com/traincert/exams/70-294.asp>

## **Exame de Cliente de Sistema Operacional: Dos dois exames descritos deste grupo, você deverá passar em um deles, a sua escolha:**

1. Exame 70-270: Installing, Configuring, and Administering Microsoft Windows XP Professional. Quem é MCSE 2000 talvez já tenha passado neste exame e poderá utilizá-lo para o MCSE 2003. O Guia oficial, em inglês, com os tópicos a serem estudados para esse exame está disponível no seguinte endereço: <http://microsoft.com/traincert/exams/70-270.asp>.
2. Exame 70-210: Installing, Configuring, and Administering Microsoft Windows 2000 Professional. Quem é MCSE 2000 talvez já tenha passado neste exame e poderá utilizá-lo para o MCSE 2003. O Guia oficial, em inglês, com os tópicos a serem estudados para esse exame está disponível no seguinte endereço: <http://microsoft.com/traincert/exams/70-210.asp>

## **Exame de Design: Dos dois exames descritos neste grupo, você deverá passar em um deles, a sua escolha:**

1. Exame 70-297: Designing a Microsoft Windows Server 2003 Active Directory and Network Infrastructure. O Guia oficial, em inglês, com os tópicos a serem estudados para esse exame está disponível no seguinte endereço: <http://microsoft.com/traincert/exams/70-297.asp>
2. Exame 70-298: Designing Security for a Microsoft Windows Server 2003 Network. O Guia oficial, em inglês, com os tópicos a serem estudados para esse exame está disponível no seguinte endereço: <http://microsoft.com/traincert/exams/70-298.asp>

## **Exame Eletivo para o MCSE - 2003 - 1 Exame:**

Da lista de exames a seguir você deve passar em um deles:

1. Exame 70-086: Implementing and Supporting Microsoft Systems Management Server 2.0. O Guia oficial, em inglês, com os tópicos a serem estudados para esse exame está disponível no seguinte endereço: <http://microsoft.com/traincert/exams/70-086.asp>.
2. Exame 70-227: Installing, Configuring, and Administering Microsoft Internet Security and Acceleration (ISA) Server 2000, Enterprise Edition. O Guia oficial, em inglês, com os tópicos a serem estudados para esse exame está disponível no seguinte endereço: <http://microsoft.com/traincert/exams/70-227.asp>.

3. Exame 70-228: Installing, Configuring, and Administering Microsoft SQL Server 2000 Enterprise Edition. O Guia oficial, em inglês, com os tópicos a serem estudados para esse exame está disponível no seguinte endereço: <http://microsoft.com/traincert/exams/70-228.asp>.
4. Exame 70-229: Designing and Implementing Databases with Microsoft SQL Server 2000 Enterprise Edition. O Guia oficial, em inglês, com os tópicos a serem estudados para esse exame está disponível no seguinte endereço: <http://microsoft.com/traincert/exams/70-229.asp>.
5. Exame 70-232: Implementing and Maintaining Highly Available Web Solutions with Microsoft Windows 2000 Server Technologies and Microsoft Application Center 2000. O Guia oficial, em inglês, com os tópicos a serem estudados para esse exame está disponível no seguinte endereço: <http://microsoft.com/traincert/exams/70-232.asp>.
6. Exame 70-297: Designing a Microsoft Windows Server 2003 Active Directory and Network Infrastructure. O Guia oficial, em inglês, com os tópicos a serem estudados para esse exame está disponível no seguinte endereço: <http://microsoft.com/traincert/exams/70-297.asp>.
7. Exame 70-298: Designing Security for a Microsoft Windows Server 2003 Network. O Guia oficial, em inglês, com os tópicos a serem estudados para esse exame está disponível no seguinte endereço: <http://microsoft.com/traincert/exams/70-298.asp>.

## Como fazer o Upgrade do MCSE 2000 para o MCSE 2003:

Quem já for certificado em MCSE 2000 terá que passar em apenas dois exames, para obter a certificação MCSE 2003.

Exames de Upgrade: Quem já tiver a certificação MCSE 2000, basta passar nos dois exames a seguir, para obter o MCSE 2003:

1. Exame 70-292: Managing and Maintaining a Microsoft Windows Server 2003 Environment for an MCSA Certified on Windows 2000. O Guia oficial, em inglês, com os tópicos a serem estudados para esse exame está disponível no seguinte endereço: <http://microsoft.com/traincert/exams/70-292.asp>.
2. Exame 70-296: Planning, Implementing, and Maintaining a Microsoft Windows Server 2003 Environment for an MCSE Certified on Windows 2000. O Guia oficial, em inglês, com os tópicos a serem estudados para esse exame está disponível no seguinte endereço: <http://microsoft.com/traincert/exams/70-296.asp>.

**IMPORTANTE:** Os exames 70-297 e 70-298 contam uma única vez. Por exemplo, se você for aprovado no Exame 70-297 ele é válido ou para preencher o requisito de obrigatório para Design ou como eletivo. Ele não pode contar duplamente, ou seja, como exame de Design e também como exame eletivo. O mesmo é válido em relação ao exame 70-298. Se você for aprovado nos dois, um contará como Design e outro como Eletivo.

## Resumo sobre o MCSE-2003:

Na minha opinião a Microsoft aprendeu a lição e não repetiu os mesmos erros de quando foi feita a migração do NT Server 4.0 para o Windows 2000 Server. As mudanças não são tão acentuadas e o caminho de atualização (upgrade), para quem já é certificado em Windows 2000 ficou bem mais suave. Com isso reforço a minha recomendação: Se você está estudando para os exames do Windows 2000, continue estudando e faça os exames normalmente. Depois para obter o MCSE 2003 serão apenas dois exames. Bastante razoável.

No endereço a seguir você encontra uma lista de perguntas/respostas mais freqüentes, em inglês, sobre os exames do Windows Server 2003:

<http://microsoft.com/traincert/mcp/mcse/faq.asp>

Em caso de dúvidas, sobre o MCSE-2003, entre em contato através do e-mail: [webmaster@juliobattisti.com.br](mailto:webmaster@juliobattisti.com.br).

## Algumas observações sobre os exames para o MCSE 2003:

Traduzindo a nota da Microsoft através de um exemplo: O exame 70-2297 pode ser utilizado como um exame obrigatório e também como um exame eletivo. Se você passar no exame 70-297, somente poderá utilizá-lo como core ou como eletivo e não contando para os dois casos. Se você utilizar o exame 70-297, por exemplo, como core, terá que passar em outro exame eletivo, pois ele não contará também como eletivo.

---

(\*) **NOTA DA MS:** Os exames básicos (core) que também podem ser usados como exames eletivos só podem ser computados um vez para cada certificação. Em outras palavras, se um candidato receber crédito por um exame básico não receberá crédito pelo mesmo exame como eletivo na mesma certificação.

---

## Tópicos para o exame 70-290 – Programa Oficial da Microsoft.

Vamos apresentar o programa oficial da Microsoft para o exame 70-290 - Managing and Maintaining a Windows Server 2003 Environment. Os tópicos que descrevo a seguir são baseados no programa oficial da Microsoft, constante no seguinte endereço:

<http://www.microsoft.com/learning/exams/70-290.asp>

Este livro aborda este programa, mais conceitos teóricos e exemplos práticos que julgo importantes para o candidato que está encarando o desafio do Exame 70-290. Um desafio que exige estudo e muita dedicação, mas sem dúvidas um desafio possível de ser vencido. No último capítulo do livro, apresento um simulado com 60 questões, com respostas e comentários detalhados.

## Tópicos para o exame 70-290, segundo o guia de estudos da Microsoft.

Programa Oficial para o Exame 70-290:

### 1. Managing and Maintaining Physical and Logical Devices

Manage basic disks and dynamic disks.

Monitor server hardware. Tools might include Device Manager, the Hardware Troubleshooting Wizard, and appropriate Control Panel items.

Optimize server disk performance.

Implement a RAID solution.

Defragment volumes and partitions.

Install and configure server hardware devices.

Configure driver signing options.

Configure resource settings for a device.

Configure device properties and settings.

### 2. Managing Users, Computers, and Groups

Manage local, roaming, and mandatory user profiles.

Create and manage computer accounts in an Active Directory environment.

Create and manage groups.

---

**NOTA:** Os tópicos apresentados a seguir são baseados no guia oficial para o exame 70-290, o qual pode ser acessado (em inglês), no seguinte endereço: <http://www.microsoft.com/traincert/exams/70-290.asp>. Quando você estiver se preparando para o exame, consulte este endereço regularmente, pois podem ser feitas mudanças nos tópicos que fazem parte do exame, conforme aviso contido no site da Microsoft.

---

**AVISO DA MS:** *"This preparation guide is subject to change at any time without prior notice and at Microsoft's sole discretion. Microsoft exams might include adaptive testing technology and simulation items. Microsoft does not identify the format in which exams are presented. Please use the exam objectives listed in this preparation guide to prepare for the exam, regardless of its format. Learn more, and download samples, on the Testing Innovations page (<http://www.microsoft.com/learning/mcexams/policies/innovations.asp>)."*

---

- Identify and modify the scope of a group.
  - Find domain groups in which a user is a member.
  - Manage group membership.
  - Create and modify groups by using the Active Directory Users and Computers Microsoft Management Console (MMC) snap-in.
  - Create and modify groups by using automation.
  - Create and manage user accounts.
  - Create and modify user accounts by using the Active Directory Users and Computers MMC snap-in.
  - Create and modify user accounts by using automation.
  - Import user accounts.
  - Troubleshoot computer accounts.
  - Diagnose and resolve issues related to computer accounts by using the Active Directory Users and Computers MMC snap-in.
  - Reset computer accounts.
  - Troubleshoot user accounts.
  - Diagnose and resolve account lockouts.
  - Diagnose and resolve issues related to user account properties.
  - Troubleshoot user authentication issues.
- 3. Managing and Maintaining Access to Resources**
- Configure access to shared folders.
  - Manage shared folder permissions.
  - Troubleshoot Terminal Services.
  - Diagnose and resolve issues related to Terminal Services security.
  - Diagnose and resolve issues related to client access to Terminal Services.
  - Configure file system permissions.
  - Verify effective permissions when granting permissions.
  - Change ownership of files and folders.
  - Troubleshoot access to files and shared folders.
- 4. Managing and Maintaining a Server Environment**
- Monitor and analyze events. Tools might include Event Viewer and System Monitor.
  - Manage software update infrastructure.
  - Manage software site licensing.
  - Manage servers remotely.
  - Manage a server by using Remote Assistance.
  - Manage a server by using Terminal Services remote administration mode.
  - Manage a server by using available support tools.
  - Troubleshoot print queues.
  - Monitor system performance.
  - Monitor file and print servers. Tools might include Task Manager, Event Viewer, and System Monitor.
  - Monitor disk quotas.
  - Monitor print queues.

- Monitor server hardware for bottlenecks.
  - Monitor and optimize a server environment for application performance.
  - Monitor memory performance objects.
  - Monitor network performance objects.
  - Monitor process performance objects.
  - Monitor disk performance objects.
  - Manage a Web server.
  - Manage Internet Information Services (IIS).
  - Manage security for IIS.
5. Managing and Implementing Disaster Recovery
- Perform system recovery for a server.
  - Implement Automated System Recovery (ASR).
  - Restore data from shadow copy volumes.
  - Back up files and System State data to media.
  - Configure security for backup operations.
  - Manage backup procedures.
  - Verify the successful completion of backup jobs.
  - Manage backup storage media.
  - Recover from server hardware failure.
  - Restore backup data.
  - Schedule backup jobs.

## O programa de certificação Microsoft Certified Systems Administrator - MCSA

A Microsoft no seu site define a certificação MCSA da seguinte maneira:

\*\*\*\*\*  
“A certificação de Microsoft Certified Systems Administrator (MCSA) em Microsoft Windows® 2003 foi desenvolvida para profissionais que implementam, gerenciam e solucionam problemas em sistemas baseados no Windows 2000 e Windows Server 2003.

As responsabilidades de implementação incluem a instalação e a configuração de componentes de sistemas. As responsabilidades de gerenciamento incluem a administração e o suporte a sistemas.

Como a credencial de MCSA em Microsoft Windows Server 2003 atende às suas necessidades...

A demanda por profissionais de administração de rede tem crescido de modo significativo, e os candidatos, assim como a indústria, demonstraram que é necessária uma certificação para esse tipo de função. Estudos mostram que administradores de rede/projetistas têm muito mais oportunidades de crescimento em empresas de TI que a maioria das outras categorias profissionais.

A credencial de MCSA em Windows Server 2003 oferece a profissionais de TI uma vantagem competitiva no atual ambiente empresarial em constante transformação, atestando a experiência específica necessária para a função de administrador de rede e sistemas. A certificação fornece aos empregadores um meio de identificar indivíduos qualificados com o conjunto de capacitações apropriadas para desempenhar o trabalho com êxito.

A certificação de MCSA em Windows Server 2003 é apropriada para:

- ◆ Administradores de rede
- ◆ Engenheiros de rede
- ◆ Administradores de rede
- ◆ Profissionais de tecnologia da informação
- ◆ Administradores de sistemas de informação
- ◆ Técnicos de rede
- ◆ Especialistas em suporte técnico
- ◆ Um ambiente de computação típico da credencial de MCSA...

A credencial de MCSA em Windows Server 2003 foi desenvolvida para profissionais de TI que trabalham no ambiente de computação tipicamente complexo das organizações de médio a grande porte. Um candidato à credencial de MCSA em Windows Server 2003 deve ter de seis a doze meses de experiência na administração de sistemas operacionais de clientes e de rede em ambientes com as seguintes características:

- ◆ Suporte para 200 a 26.000 ou mais usuários.
- ◆ Suporte para dois a 100 locais físicos.
- ◆ Serviços e recursos típicos de rede incluem envio e recebimento de mensagens, banco de dados, arquivos e impressão, servidor proxy ou firewall, Internet e intranet, acesso remoto e gerenciamento de computador cliente.
- ◆ A conectividade precisa incluir a conexão de filiais e usuários individuais em locais remotos com a rede corporativa e a conexão de redes corporativas com a Internet.”

\*\*\*\*\*

Eu diria que a diferença básica entre o MCSE e o MCSA é que o MCSE é um profissional responsável por planejar, projetar e também implementar uma infra-estrutura de rede baseada no Windows Server 2003. Já o MCSA trabalha somente com a parte de implementação/administração da infra-estrutura de rede projetada pelo MCSE. Quem já tem a certificação MCSE, pode obter a certificação MCSA apenas passando em mais um exame eletivo. Caso você já tenha sido aprovado em um dos exames eletivos aceitos para o MCSA 2003, ao obter o MCSE – 2003, você estará obtendo, também, o MCSA – 2003.

## Requisitos para obter a Certificação MCSA:

Candidatos a certificação MCSA em Windows 2000 têm que passar em 3 exames obrigatórios e 1 exame eletivo. A seguir descrevo os exames que fazem parte de cada grupo.

Exames obrigatórios para a certificação MCSA:

1. Um exame de Sistema Operacional Cliente. Você deve selecionar um dos dois exames indicados a seguir:
  - Exame 70-210: Installing, Configuring, and Administering Microsoft Windows 2000 Professional
  - Exame 70-270: Installing, Configuring, and Administering Microsoft Windows XP Professional
2. Dois exames de Sistema Operacional de Rede. Os dois exames a seguir são obrigatórios, isto é, o candidato a MCSA deve passar nos dois:
  - Exame 70-290: Managing and Maintaining a Microsoft Windows Server 2003 Environment
  - Exame 70-291: Implementing, Managing, and Maintaining a Microsoft Windows Server 2003 Network Infrastructure

3. Um exame eletivo. Selecione um dos exames da lista a seguir:

Exam 70-086: Implementing and Supporting Microsoft Systems Management Server 2.0

Exam 70-227: Installing, Configuring, and Administering Microsoft Internet Security and Acceleration (ISA) Server 2000, Enterprise Edition

Exam 70-228: Installing, Configuring, and Administering Microsoft SQL Server™ 2000 Enterprise Edition

Exam 70-284: Implementing and Managing Microsoft Exchange Server 2003

Exam 70-299: Implementing and Administering Security in a Microsoft Windows Server 2003 Network

Alternativa aos exames eletivos citados acima: a seguinte combinação de certificações podem substituir um exame eletivo MCSA:

CompTIA A+ and CompTIA Network+

OU

CompTIA A+ and CompTIA Server+

OU

CompTIA Security+

**IMPORTANTE:** Se você já é um MCSE-2000 ou um MCSA-2000, você não precisará fazer um dos exames eletivos descritos anteriormente, pois estas certificações contam como um exame eletivo para o MCSA-2003.

## Upgrade para quem já é um MCSA – 2000:

O candidato que já tem a certificação MCSA-2000, terá que fazer um único exame, para obter o MCSE-2003. Para estes candidatos, basta passar no seguinte exame de atualização:

- ◆ Exam 70-292: Managing and Maintaining a Microsoft Windows Server 2003 Environment for an MCSA Certified on Windows 2000

## A quem se destina este livro?

Este é um manual de estudos para os candidatos ao Exame de Certificação 70-290: Managing and Maintaining a Microsoft Windows Server 2003 Environment. Este é o foco deste livro, ser um manual de estudo para os candidatos que irão fazer o exame 70-290.

Usuários interessados nos assuntos abordados também poderão se beneficiar do texto deste livro, mesmo que não tenham a intenção de fazer o exame 70-290. Conceitos como a definição de diretório, a definição dos elementos do Active Directory, a divisão lógica do Active Directory, a divisão física do Active Directory, conceito de sites, links, instalação do Windows Server 2003, administração de recursos, pastas compartilhadas, permissões de segurança, gerenciamento de volumes e impressoras e assim por diante.

## Pré-requisitos para o livro.

Neste manual não serão apresentados conceitos básicos de utilização da interface gráfica do Windows e nem serão apresentados conceitos básicos tais como o que é um ícone ou o que é uma pasta. Estes são conceitos básicos que o candidato a um exame de Certificação, já deve dominar, de longa data.

# Ordem dos exames para obter o MCSE-2003

Os candidatos me perguntam se existe uma ordem obrigatória para passar nos sete exames do MCSE-2003. Não, não existe uma ordem obrigatória. Existe uma seqüência que é a mais aconselhada, e que indico logo a seguir. Esta é uma seqüência, natural, ou seja, o candidato ao MCSE deve fazer os exames na seguinte ordem (esta ordem não é obrigatória, mas é altamente recomendada):

1. Exame 70-210 ou 70-270
2. Exame 70-290
3. Exame 70-291
4. Exame 70-293
5. Exame 70-294
6. Um dos exames de Design
7. Um exame eletivo

## É hora de começar

Feitas as devidas apresentações e esclarecimentos é hora de iniciar o estudo para o exame 70-290. Embora este seja um exame com um nível de dificuldade um pouco maior do que os exames 70-210 e 70-215 (o equivalente ao 70-290, só que para o Windows 2000 Server) é perfeitamente possível passar neste exame. Sugiro que você estude este manual, além dos materiais que indicarei ao longo dos capítulos do livro. Não deixe de consultar as referências indicadas nos endereços da Internet, que apresentarei ao longo do livro. Em cada Capítulo você encontra questões práticas, comentadas e no final do livro um simulado completo, com 60 questões.

## Sugestão de plano de estudo

Vamos supor que você disponha de três semanas para se preparar para o exame 70-290. Você precisa passar neste exame para obter a certificação MCSE (contando que você já passou nos demais exames necessários para essa certificação).

Para isso você está disposto a estudar quatro horas por dia, durante 20 dias. Com isso você terá um total de 80 horas de estudo. A questão é a seguinte: “Com o tempo disponível é possível passar neste exame”? A resposta é um sonoro sim. Eu até diria que você tem tempo de sobra. Para tal sugiro o seguinte programa de estudo:

- ◆ Material: Este livro. Tempo de estudo. Entre 30 horas e 35 horas.
- Resumos: Disponíveis nos sites [www.cramsession.com](http://www.cramsession.com) e [www.examnotes.net](http://www.examnotes.net): 5 horas
- Simulado dos sites indicados ao longo do livro: 10 horas.
- Simulados da Transcender – [www.transcender.com](http://www.transcender.com): 15 horas
- Revisão do livro e dos resumos. 10 horas
- Revisão final: Principalmente dos simulados, dos resumos, para ser feita na véspera do exame. 5 horas
- Total 80 horas

Para enviar as suas críticas e sugestões, basta entrar em contato através do e-mail: [webmaster@juliobattisti.com.br](mailto:webmaster@juliobattisti.com.br). Desejo a todos uma boa leitura e sucesso no exame 70-290.

Júlio Battisti,

[www.juliobattisti.com.br](http://www.juliobattisti.com.br)

MCP, MCP+I, MCSE NT 4, MCSE 2000, MCSE+I, MCSA, MCDBA e MCSD

# Introdução

O objetivo deste capítulo é mostrar exatamente qual o papel do Windows Server 2003, como sistema operacional de servidores em uma rede. Este é um capítulo que você encontrará em todos os livros de minha autoria, sobre certificações do MCSE-2003. O objetivo é fazer com que o candidato entenda, exatamente o que é o Windows Server 2003 e como utilizá-lo em uma rede.

Neste capítulo apresentarei ao amigo leitor o Windows Server 2003. Ao terminar este capítulo você terá uma visão geral do Windows Server 2003 e já poderá começar a formar a sua opinião sobre os novos recursos disponíveis e a melhoria nos recursos já existentes, em relação ao Windows 2000 Server.

Iniciarei o capítulo fazendo uma breve introdução ao Windows Server 2003, falando sobre o seu papel em uma rede de computadores. Em seguida falarei sobre as diferentes edições do Windows Server 2003.

A exemplo do que ocorre com o Windows 2000 Server, o Windows Server 2003 também é fornecido em diferentes edições. O que caracteriza cada edição são os recursos disponíveis e os limites de Hardware, tais como quantidade máxima de memória RAM e número de processadores, além do preço, é claro. Vou iniciar o capítulo apresentando as diferentes edições do Windows Server 2003 e as características de cada uma. Logo em seguida apresento uma tabela (baseada em artigo publicado no site oficial do Windows Server 2003):

<http://www.microsoft.com/windowsserver2003>.

Conforme mostrarei neste capítulo, estão disponíveis quatro diferentes edições do Windows Server 2003:

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

Para que a equipe de Tecnologia da Informação – TI, de uma empresa resolva investir e fazer a atualização do Windows 2000 Server para o Windows Server 2003, é preciso que esta equipe esteja convencida (e após estar convencida, seja capaz de convencer a Administração a fazer os investimentos necessários) de que os benefícios oferecidos pelo Windows Server 2003, compensem o dinheiro a ser investido. Em resumo, nada mais é do que uma análise baseada em uma relação custos x benefícios.

Na seqüência vou apresentar um resumo das principais novidades e melhorias do Windows Server 2003 em relação ao Windows 2000 Server. Com base nestas informações você já pode começar a formar idéias para tomar uma decisão se vale a pena ou não a migração do Windows 2000 Server para o Windows Server 2003.

Apresentarei as novidades de uma maneira resumida, salientando as novas características e as melhorias disponíveis. Ao longo dos demais capítulos deste livro irei detalhar as novidades diretamente relacionadas com o Exame 70-290.

# CAPÍTULO

## 1

### Redes Baseadas no Windows 2003 Server

No endereço a seguir, você encontra uma descrição detalhada de todas as novidades do Windows Server 2003:

<http://www.microsoft.com/windowsserver2003/evaluation/overview/technologies/default.mspx>

Neste endereço você encontra descrição completa de todas as novidades, divididas em categorias: Active Directory, Serviços de Aplicações, Tecnologias de Cluster, Serviços de impressão e arquivos, Serviços Web, Segurança, Gerenciamento, Serviços de Mídia e assim por diante.

Em seguida será a vez de apresentar os fundamentos teóricos sobre os quais serão desenvolvidos os capítulos restantes do livro. Nesta parte mostrarei como é formada uma infra-estrutura de rede baseada no Windows Server 2003.

Seguindo a exposição teórica falarei com um pouco mais de detalhes sobre o conceito de uma rede baseada no modelo Cliente/Servidor. Aqui é importante não confundirmos o conceito de uma rede Cliente/Servidor, com os modelos de desenvolvimento de aplicações, onde temos os modelos em 2 camadas, conhecido como Cliente/Servidor e o modelo Web, baseado em 3 ou mais camadas, embora estes conceitos tenha estreitos laços de ligação.

Uma vez apresentados os conceitos básicos sobre redes de computadores, você aprenderá qual o papel do Windows Server 2003 em uma rede, que diferentes funções um servidor baseado no Windows Server 2003 pode exercer e quais os serviços mais comuns que o Windows Server 2003 pode prestar na rede.

O entendimento dos diferentes papéis que um servidor baseado no Windows Server 2003 pode exercer é de fundamental importância, para que você possa planejar e implementar uma infra-estrutura de rede baseada no Windows Server 2003, a qual atenda a requisitos de desempenho, disponibilidade e segurança. Este entendimento também é de grande importância para responder questões do tipo cenário, onde é apresentado um problema prático e você deve apontar um conjunto de ações, dentre várias ações disponíveis, capaz de solucionar o problema apresentado.

Nesta parte do capítulo você também aprenderá os conceitos básicos sobre Grupos de Trabalho (Workgroups), Diretórios e Domínios, conceitos estes (principalmente o conceito de Diretório), que serão detalhados no Capítulo 2, onde você aprenderá mais sobre o Active Directory, seus componentes e a divisão lógica e física do Active Directory.

Seguindo nossa exposição neste capítulo (que repito, apresenta conceitos teóricos fundamentais para o acompanhamento do restante do livro), vou apresentar os aspectos básicos do protocolo TCP/IP. Você entenderá exatamente o que é um protocolo e porque o TCP/IP é o protocolo padrão do Windows Server 2003.

Nos tópicos sobre TCP/IP, você aprenderá verá detalhes tais como a definição de número IP, máscara de sub-rede, cálculos binários envolvendo o número IP e a máscara de sub-rede, o conceito de endereçamento IP, classes de endereçamento, roteamento e os utilitários básicos para trabalhar com o protocolo TCP/IP.

Você verá como através de cálculos binários o protocolo TCP/IP consegue determinar se dois computadores estão na mesma rede ou não. E também verá o que o TCP/IP faz, caso os dois computadores estejam em redes diferentes, para permitir que as informações possam ser transmitidas entre os dois computadores, mesmo estando eles em redes diferentes.

Na parte final do capítulo você aprenderá a instalar o Windows Server 2003. Conforme mostrarei no exercício prático sobre a instalação do Windows Server 2003, o processo de instalação é muito semelhante ao processo de instalação do Windows XP e também do Windows 2000 Server.

Você pode fazer a instalação do Windows Server 2003 de diferentes maneiras:

---

**NOTA:** Para uma descrição detalhada dos modelos de desenvolvimento de aplicações em 2, 3 ou n camadas, consulte o livro: **ASP.NET: Uma Nova Revolução na Criação de Sites e Aplicações Web.**

---

- ◆ Instalando o Windows Server 2003 em um servidor novo, no qual não existe nenhum sistema operacional instalado: Neste caso basta ligar o servidor com o CD do Windows Server 2003 no drive de CD. O processo de instalação inicia automaticamente, conforme descreverei neste capítulo.
- ◆ 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 de CD 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 e neste caso pode ocorrer de o respectivo dispositivo de Hardware não funcionar após a instalação do Windows Server 2003. Por exemplo, você pode ter instalado uma placa de fax modem, para a qual não está disponível um driver no Windows Server 2003. Neste caso, a placa de fax modem deixará de funcionar após a instalação do Windows Server 2003. Caso algum dos programas instalados (no caso de você fazer uma atualização de um servidor já existente) não seja compatível com o Windows Server 2003, você terá uma incompatibilidade de software. O programa (ou os programas) não compatível poderão não executar ou executar incorretamente no Windows Server 2003.

Para ajudá-lo a identificar incompatibilidades de hardware e software, o Windows Server 2003 oferece um assistente que faz a verificação de todos os componentes do computador e no final apresenta um relatório de possíveis incompatibilidades.

Você também pode fazer a instalação usando o comando winnt32.exe que está na pasta i386 do cd de instalação. Ao utilizar este comando você tem à disposição uma série de opções de linha de comando, as quais controlam diferentes aspectos da instalação. Você aprenderá a utilizar o comando winnt32 e as opções de linha de comando.

Existem outras formas de instalação do Windows Server 2003, tais como instalação não assistida, usando um arquivo de respostas. Neste capítulo você aprenderá os conceitos básicos sobre uma instalação não assistida e o uso de um arquivo de respostas.

Novas ferramentas de suporte para o Windows Server 2003 são disponibilizadas periodicamente pela Microsoft. Consulte regularmente o site oficial do Windows Server 2003 para fazer o download de novas ferramentas: <http://www.microsoft.com/brasil/windowsserver2003>

Muito bem. Pode parecer um pouco chato, toda esta teoria. Mas posso garantir ao amigo leitor, que o entendimento destes fundamentos teóricos é fundamental para que você possa entender todos os demais tópicos práticos, que serão abordados nos capítulos subsequentes. A teoria apresentada neste capítulo e no Capítulo 2, é a base sobre a qual todos os demais capítulos do livro irão se basear. Então, mãos a obra.

## **Uma Nova Versão de Servidor Para o Windows?**

Sim, o Windows Server 2003 é uma evolução do Windows 2000 Server. Eu utilizo o termo evolução ao invés de revolução, pois o Windows Server 2003 traz muitas melhorias em relação ao Windows 2000 Server, porém não representa uma mudança tão grande como a que ocorreu quando da migração do NT Server 4.0 para o Windows 2000 Server. São novidades em termos de desempenho, novos recursos e funcionalidades, novas ferramentas e comandos, enfim, uma série de melhorias.

Você aprenderá a utilizar os novos recursos do Windows Server 2003, aprenderá a utilizar os principais recursos disponíveis para administração de uma rede empresarial baseada em servidores com o Windows Server 2003.

Neste capítulo também vou apresentar as diferentes versões do Windows Server 2003. Farei uma descrição das principais novidades desta versão, em relação ao Windows 2000 Server.

## Uma Breve História “dos Windows”

Observe bem o título deste item – “dos Windows”. Não é um erro de português que o autor cometeu e que a equipe de revisão deixou passar. Com o termo “dos Windows” estou fazendo referência as inúmeras versões do Windows que foram lançadas na última década.

Vou apresentar um histórico destas versões, de tal maneira que fique claro onde o Windows Server 2003 se encaixa nesta história. Vou iniciar apresentando o histórico das versões do Windows utilizadas em estações de trabalho e nos computadores pessoais residenciais. Uma história que teve início com o nosso bom e velho MS-DOS.

### Os “Windows” Para Estações de Trabalho e Computadores de Uso Residencial:

Neste tópico vou mostrar a evolução que teve início com o MS-DOS e tem como seu mais novo representante o Windows XP (Home ou Professional). Uma nova versão do Windows, para estações de trabalho, já está sendo desenvolvida. Por enquanto ela tem o codinome de Longhorn e deverá ser lançada, provavelmente, em 2005. Considere o diagrama da Figura 1.1:

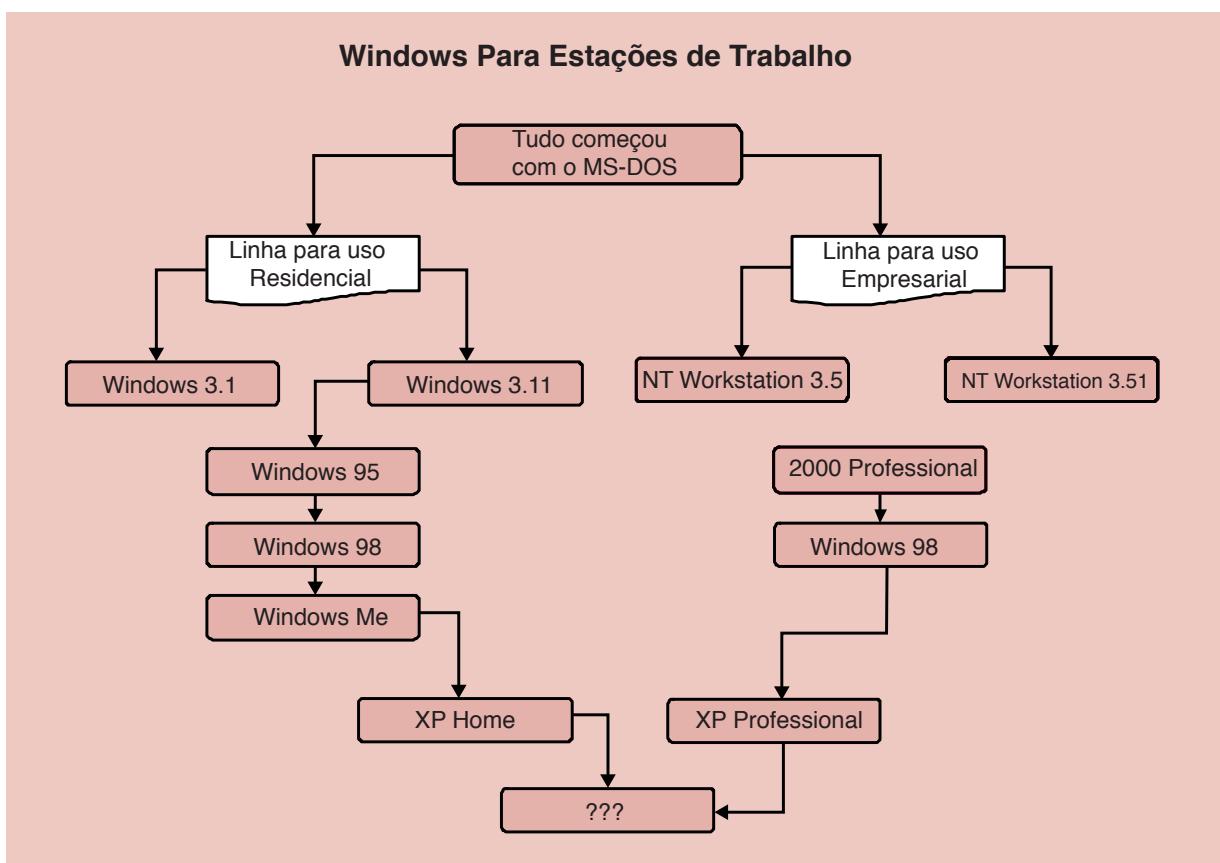


Figura 1.1 A Família Windows para estações de trabalho.

Farei alguns comentários sobre o diagrama da Figura 1.1.

O início de tudo foi o MS-DOS. Sem nenhuma dúvida, independentemente das qualidades/méritos do produto, foi o produto que transformou a Microsoft de uma empresa de garagem em uma empresa rumo a tornar-se a gigante dos dias atuais. Muita gente, inclusive este que escreve este texto, tem saudade de algumas das características do bom e velho MS-DOS. Para instalar programas, uma simplicidade: bastava copiar o diretório do programa de uma máquina para a outra e pronto. Uma interface a caractere, porém bastante rápida. Claro que “gastávamos” o teclado digitando comandos e mais comandos: dir, type, copy, etc.

Como sucessor do MS-DOS, porém ainda dependente do MS-DOS, surge o Windows. As versões iniciais do Windows pouco foram utilizadas no Brasil. Embora você possa não acreditar (ou não possa imaginar como era), existiu um Windows 1.0, um Windows 2.0 e assim por diante. A primeira versão a tornar-se popular no Brasil foi o Windows 3.1. O Sistema apresentava uma interface gráfica onde tínhamos novidades como ícones, atalhos e outros “enfeites” mais. Muitos classificavam o Windows 3.1 como sendo apenas um Ambiente Operacional e não um Sistema Operacional, por ser este dependente do MS-DOS para realizar uma série de tarefas básicas.

Com a disseminação das redes e a necessidade de compartilhamento de periféricos e de 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 for Workgroups, conforme o próprio nome sugere, 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. Uma revolução estava prestes a acontecer.

Em 25 de Agosto de 1995 deu-se a referida revolução: Foi 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 e tantos 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 (logo a seguir apresentarei o histórico das versões do Windows para Servidores, onde se encaixa o Windows Server 2003). Segundo recomendações da própria Microsoft o NT Workstation era indicado para uso empresarial, isto é, nas estações de trabalho das redes das empresas. O NT Workstation 3.5 e 3.51 tinham uma interface idêntica a do Windows 3.1/Windows 3.11 e também eram baseados na tecnologia de 16 bits.

Nesta época iniciava-se a confusão. Por que ter duas linhas diferentes do Windows? Drivers que funcionavam no Windows 3.1 ou 95 não funcionavam no NT. Instalar determinados dispositivos de Hardware no NT (Workstation ou Server) era um verdadeiro suplício. A linha Workstation, segundo a Microsoft, foi criada tendo como fundamentos, a criação de um sistema mais estável, com configurações de segurança mais avançadas e com suporte às tecnologias de rede existentes. Sem dúvida um sistema para uso em redes empresariais. Já para o usuário doméstico, a Microsoft não recomendava o uso do NT Workstation, principalmente pelo fato do NT precisar de Hardware mais potente do que o Windows 3.11 ou 95. Outro motivo é que muitos dispositivos de Hardware não tinham driver para NT. Além disso, muitos aplicativos que rodavam no Windows 3.11 ou 95 não rodavam no NT, principalmente jogos.

Neste momento a Microsoft já falava em unificar, quem sabe um dia, as duas linhas do Windows, porém este era uma promessa ainda distante. Uma nova versão do NT foi lançada: NT Workstation 4.0 e NT Server 4.0 (para servidores de rede). Esta era a versão do NT baseada na tecnologia de 32 Bits e com cara de Windows 95. Melhorias substanciais forma feitas em relação a versão anterior do NT. Neste momento muitas empresas começam a adotar o NT Workstation 4.0 como Sistema Operacional para as estações da rede. Embora o preço da licença do NT Workstation fosse um pouco mais caro, os benefícios em termos de estabilidade e segurança compensavam. Cabe aqui ressaltar que o NT Workstation 4.0 é muitíssimo mais estável do que o Windows 95, 98 ou Me.

Logo após o lançamento do NT 4.0 a Microsoft já começava a falar no lançamento do NT 5.0. Muita expectativa havia em relação a esta versão do NT. Porém uma série de fatores fez com que o lançamento do NT 5.0 fosse atrasando mais e mais. Na introdução do meu primeiro livro, “Série Curso Básico & Rápido Microsoft Windows 2000 Server”, eu escrevi o seguinte:

“Bem vindo ao Windows 2000 Server. Sem a menor sombra de dúvidas o Sistema Operacional mais aguardado de toda a história da indústria da Informática. Nunca falou-se e até mesmo especulou-se tanto sobre um Sistema Operacional, como se fez a respeito do Windows 2000 Server. No início do projeto este era chamado de Windows NT Server 5.0. Após diversos atrasos e adiamentos, o sistema foi “rebatizado” para Windows 2000 Server. Finalmente a data oficial do lançamento está confirmada para o dia 17 de Fevereiro do ano 2000. O código final do produto foi enviado para produção no dia 15 de Dezembro de 1999, após diversas versões de avaliação. Atrasos e especulações a parte, o fato é que o Windows 2000 Server representa um grande esforço da Microsoft em melhorar o seu Sistema Operacional para servidores de rede. Inúmeros recursos novos foram acrescentados, além da melhoria dos recursos já existentes.”

Conforme descrito no parágrafo anterior, o que seria o NT 5.0, devido a sucessivos atrasos, foi lançado somente em Fevereiro de 2000, com o nome de Windows 2000. Neste meio tempo foi lançado o Windows 98, idêntico ao Windows 95 apenas com algumas melhorias e um número muito pequeno de novidades. O Windows 2000, a exemplo do NT 4.0 tem a versão para servidor – Windows 2000 Server e a versão para estação de trabalho – Windows 2000 Professional. 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 e muitas ainda estão em processo de migração.

Observe que neste momento ainda temos duas linhas bem distintas. Uma com o Windows 9x/Me e outra com o Windows 2000. 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.

Durante o ano de 2000 ainda foi lançado o Windows Me, que deveria ser o substituto do Windows 98. Como esta nova versão apresentava poucas diferenças, com apenas algumas inovações não muito significativas, o ritmo de adoção do Windows Me foi e continua um pouco lento. Acredito que o sucesso do Windows 2000 também colaborou para a adoção lenta do Windows Me.

Finalmente, em Outubro de 2001 foi lançado o Windows XP. Segundo a Microsoft XP de Experience. O Windows XP, conforme visto na Figura 1.1, foi lançado em duas versões: Home e Professional. O Windows XP representa, agora sim, um passo 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, confiabilidade e segurança do Windows 2000.

## Os “Windows” Para Servidores:

Neste tópico vou mostrar a evolução que teve início com as primeiras versões do Windows NT Server até a última versão do Windows para Servidores: Windows Server 2003.

Considere o diagrama da Figura 1.2:

# Windows Para Servidores de Rede

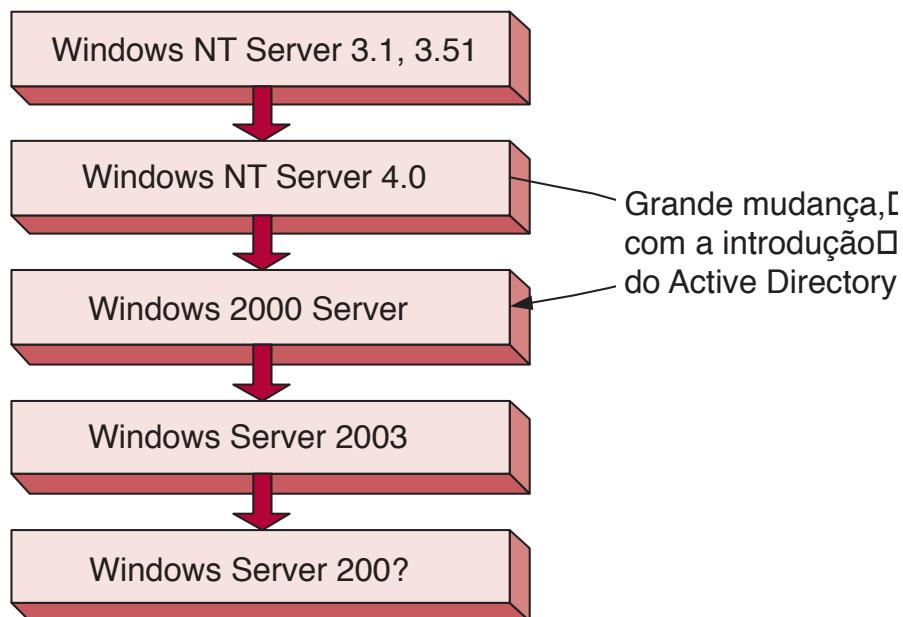


Figura 1.2 A Família Windows para servidores.

Farei alguns comentários sobre o diagrama da Figura 1.2.

A Microsoft entrou na “briga” dos servidores de rede no início dos anos 90, com o lançamento do NT Server. NT de New Tecnology. No início, na minha opinião, as versões do NT não tinham os mesmos recursos e nível de desempenho/segurança do que concorrentes mais antigos, como Novell e as versões do UNIX. 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.

Porém a realidade é que o NT Server teve uma boa aceitação. Até a versão 3.51 o NT tinha a mesma interface do Windows 3.11. A partir do NT Server 4.0, a interface era a do Windows 95. Com o NT Server 4.0, a participação da Microsoft no mercado de servidores realmente decolou. Muitas empresas passaram a adotar o NT Server 4.0 como Sistema Operacional para os seus servidores de rede.

Mas com tudo na vida tem dois lados, mais usuários significa mais exigências, ou seja, rapidamente as deficiências do NT Server 4.0 passaram a ser questionadas pelos usuários. A Microsoft em resposta começou a anunciar o NT 5.0, o qual conteria uma série de novos recursos para solucionar os problemas do NT 4.0. Porém o projeto do NT 5.0 começou a atrasar, conforme já descrito anteriormente (o que fez com que a concorrência começasse a chamar o NT 5.0 de “Vaporware”, em uma alusão a um sistema que não existe).

Finalmente em 17 de Fevereiro de 2000 a Microsoft lança a nova versão, agora “rebatizada” como Windows 2000 Server. A nova versão representou uma verdadeira revolução em relação ao NT Server 4.0. Basta citar o Active Directory para exemplificar esta revolução, esta verdadeira mudança de paradigma. Apesar das dúvidas e da apostila da concorrência de que não haveria uma aceitação do Windows 2000 Server, o fato é que este foi e continua sendo amplamente adotado por empresas do mundo inteiro.

Hoje, a maioria dos servidores Intel que rodam alguma versão do Windows, são baseados no Windows 2000 Server. Existem profissionais capacitados, farta literatura e fontes de referência na Internet e o Windows 2000 Server tem-se mostrado bastante estável e seguro.

Se o Windows 2000 Server está tão bom, então porque uma nova versão? Porque, como sempre, com a utilização por milhões de usuários, novas demandas e funcionalidades são solicitadas. Em resposta a estas demandas e necessidades de melhoria, a Microsoft apresenta o Windows Server 2003, lançado no dia 24 de Abril de 2003.

Neste Capítulo farei uma breve apresentação sobre as novidades e melhorias do Windows Server 2003 em relação ao Windows 2000 Server. Nos demais capítulos do livro apresentarei os principais recursos de Administração do Windows Server 2003, recursos estes cobrados no Exame 70-290.

E o futuro? Bem, ainda é cedo para especular. Mas provavelmente em 2005 saia uma nova versão do Windows para estações de trabalho, ou seja, o sucessor do Windows XP. E em 3 ou 4 anos, saia o sucessor do Windows Server 2003. Mas são apenas especulações que podem ou não se confirmar.

## A Quem se Destina Este Livro?

O Windows Server 2003 é a nova versão do Sistema Operacional para servidores de rede. Qualquer usuário interessado em aprender a utilizar esta versão, quer já conheça o Windows 2000 Server ou seja iniciante na área, poderá utilizar os assuntos apresentados neste livro para aprender a utilizar os principais recursos do Windows Server 2003.

Neste livro você aprenderá exatamente qual o papel do Windows Server 2003 em uma rede de computadores e aprenderá a Administrar os recursos que fazem parte do programa oficial do Exame 70-290. Em resumo, é um Manual de Estudos para o candidato que está se preparando para prestar o Exame 70-290.

## Equipamento e Software Necessários

Para acompanhar todos os exemplos propostos no livro, você precisará de um computador onde está instalado uma das seguintes versões do Windows Server 2003.

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

Para determinar uma configuração mínima para instalar o Windows Server 2003, temos que levar em consideração uma série de fatores, sendo o principal deles, a lista de aplicativos e serviços que serão utilizados. A seguir vou apresentar a configuração mínima, recomendada, para você utilizar em um computador para estudo. Para um servidor de rede, o hardware mínimo depende do papel que o servidor desempenha da rede, do número de usuários e de uma série de outros fatores.

Como equipamento para ser utilizado em casa, ou em um laboratório de teste na sua empresa, aconselho a seguinte configuração mínima:

- ◆ Processador Pentium 900 ou superior.
- ◆ 382 MB de RAM, sendo 512 MB, altamente recomendáveis.
- ◆ 10 GB de espaço livre no Disco rígido.
- ◆ Unidade de CD-ROM com capacidade de Boot pela unidade de CD.

---

**NOTA:** Neste capítulo você aprenderá sobre as características e os recursos disponíveis em cada uma das diferentes edições do Windows Server 2003.

---

Em cada um dos capítulos, apresentarei uma série de exemplos práticos. Com o uso destes exemplos, você poderá entender melhor a aplicação dos conceitos teóricos apresentados. Em muitas situações, a melhor maneira de entender um determinado assunto, é através da utilização deste para resolução de um problema prático do dia-a-dia. Muitos dos exemplos apresentados, principalmente na parte relacionada com o uso do Windows Server 2003 em uma rede de computadores, são baseados na minha experiência prática como Administrador e depois como Gerente de redes. São situações que surgem no dia-a-dia da Administração, gerência e suporte aos usuários da rede.

---

**NOTA:** Com menos de 256 MB de RAM, o desempenho, mesmo para uma máquina de testes fica muito comprometido, principalmente depois que você instala o Active Directory.

---

## É Hora de Começar

Ao escrever este livro procurei imaginar a seqüência lógica, iniciando pela instalação do Windows Server 2003 e pela implementação da rede, passando pela administração das tarefas mais comuns e finalizando com configurações sofisticadas de segurança e como os serviços de Internet. Coloquei tópicos que vão da execução de tarefas básicas do dia-a-dia, até a utilização de ferramentas administrativas avançadas. É o meu mais sincero desejo que este livro possa ser seu “companheiro inseparável”, enquanto se prepara para o Exame 70-290.

Caso você tenha sugestões sobre tópicos que gostaria de ver incluídos em futuras edições deste livro, ou queira relatar algum erro encontrado no livro, basta entrar em contato através do e-mail: [webmaster@juliobattisti.com.br](mailto:webmaster@juliobattisti.com.br).

Desejo a todos uma boa leitura e tenho certeza que este trabalho irá ajudá-los no entendimento e na utilização do Windows Server 2003. Uma boa leitura a todos.

## Introdução ao Windows Server 2003

Neste item farei uma apresentação do Windows Server 2003. Os conceitos apresentados neste item, fornecem uma visão geral dos elementos que compõem uma rede baseada no Windows Server 2003.

O Windows Server 2003 é um sistema operacional para ser instalado em servidores de uma rede. Em uma rede de computadores temos, basicamente, dois tipos de equipamentos conectados (além dos equipamentos responsáveis pela conectividade da rede, tais como hubs, switchs, roteadores, etc):

- ◆ Estações de trabalho
- ◆ Servidores

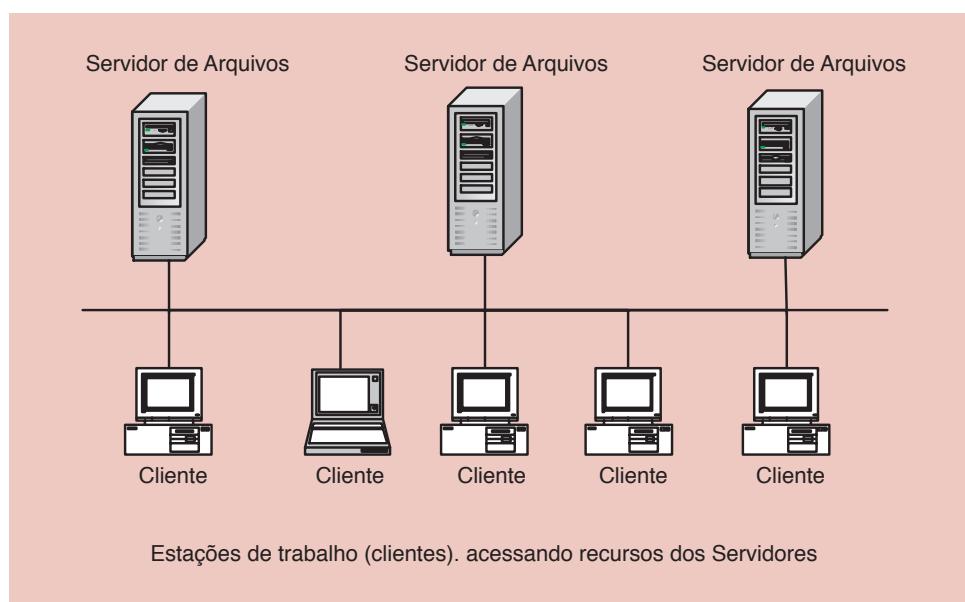
Como o próprio nome sugere, um Servidor fornece serviços para vários clientes. Por exemplo, podemos ter um servidor de arquivos onde ficam gravados arquivos, os quais podem ser acessados através da rede, por todos as estações da rede (estações de trabalho), as quais são conhecidas como Clientes. Outro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

Com base na explicação acima, podemos apresentar um outro conceito, que certamente a maioria dos leitores já conhece: O conceito da Arquitetura Cliente-Servidor. A Arquitetura Cliente-Servidor, de uma maneira simples, nada mais é do que uma rede 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.

Um exemplo típico, que com certeza utilizamos diariamente, é o acesso à Internet. Por exemplo, 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 dezenas ou até centenas de milhões de clientes acessando os mais variados recursos e serviços disponibilizados pelos servidores.

Na Figura 1.3, apresento um diagrama de exemplo de uma rede Cliente-servidor, onde serviços de Compartilhamento de arquivos e de Impressão são oferecidos por dois servidores com o Windows Server 2003 instalado, recursos estes que são acessados pelos Clientes da rede.



**Figura 1.3 Um exemplo simples de uma rede Cliente-servidor.**

Em uma rede de computadores (onde temos Servidores e Clientes, conforme descrito anteriormente), todos os computadores precisam “Falar a mesma língua”, para que possam ser trocadas informações entre os computadores da rede. Este “Falar a mesma língua”, em termos de redes, significa que todos os computadores de uma rede precisam ter o mesmo Protocolo de comunicação instalado e corretamente configurado.

Um protocolo de comunicação, nada mais é do que um conjunto de regras e normas para que os computadores possam trocar informações. Dois computadores que não possuem um protocolo em comum, não conseguirão trocar informações. É como um brasileiro que não sabe Chinês, tentando falar com um Chinês que não sabe Português. O diálogo (ou troca de informações), fica simplesmente impossível.

Existem vários protocolos de comunicação entre computadores e outros dispositivos de uma rede. O Windows Server 2003 fornece suporte a uma série de protocolos, porém o mais utilizado é o TCP-IP – Transmission Control Protocol – Internet Protocol. Vários são os motivos que tornaram o TCP-IP, o protocolo mais adotado, e por isso mesmo o protocolo padrão do Windows Server 2003, isto é, o protocolo que é adicionado durante a instalação do Windows Server 2003. Um dos principais motivos para a ampla aceitação é que o TCP-IP é o protocolo utilizado na Internet, isto

é, para que um computador possa ter acesso a Internet ele precisa ter o protocolo TCP-IP instalado e corretamente configurado. Outro motivo é a forte aceitação do Mercado em relação ao TCP-IP, uma vez que grande maioria dos Sistemas Operacionais adota o TCP-IP como protocolo padrão.

No diagrama da Figura 1.3 foram apresentados apenas exemplos de servidores baseados no Windows Server 2003 atuando nos serviços de compartilhamento de arquivos e de impressoras. Porém o Windows Server 2003 podem desempenhar diversos outros papéis, tais como:

- ◆ Servidor de Internet/Intranet, prestando serviços de hospedagem de sites (http), cópia de arquivos (ftp), envio de mensagens (SMTP), servidor de aplicativos Web, hospedando páginas ASP ou ASP.NET, etc. No Capítulo 13 você aprenderá um pouco mais sobre a utilização do IIS, que é o servidor Web disponibilizado com o Windows Server 2003.
- ◆ Controlador de domínio – DC (Domain Controller): Um servidor onde está instalado o Active Directory, que é o banco de dados onde ficam gravados as contas de usuários e as senhas dos usuários, contas dos computadores da rede, nome dos grupos de usuários e a lista de membros de cada grupo e uma série de outras informações necessárias ao funcionamento da rede. Um servidor com o Active Directory instalado é conhecido como DC – Domain Controller. Neste capítulo você aprenderá a transformar um servidor em DC, usando o comando depromo.
- ◆ Serviços de rede: Oferecendo serviços de resolução de nomes, tais como o DNS e WINS, serviço de configuração automática do protocolo TCP/IP (DHCP), roteamento e acesso remoto (RRAS) e assim por diante.
- ◆ Servidor de banco de dados: Um servidor com o Windows Server 2003 instalado e com o SQL Server 2000 (ou versão posterior) instalado. O SQL Server 2000 é o banco de dados para uso empresarial, com suporte a grande volume de acesso.
- ◆ Servidor de correio eletrônico e de ferramentas de colaboração: Um servidor como Windows Server 2003 instalado e com o Exchange 2000 (ou posterior) 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, uma aplicativo para aprovação de despesas de viagem. O funcionário que vai viajar preenche um formulário solicitando recursos para a viagem. O formulário é enviado, 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, Firewall, roteamento, etc. São muitas as funções que um servidor baseado no Windows Server 2003 pode exercer.

Para resumir este item posso dizer o seguinte: “O Windows Server 2003 é um Sistema Operacional para uso em servidores de rede. Ele pode ser configurado para oferecer uma série de serviços aos clientes da rede. Possui novas funcionalidades e características em relação ao Windows 2000 Server.”

**DICA: No Windows Server 2003 o protocolo TCP/IP é automaticamente adicionado durante a instalação do Sistema Operacional e não pode ser desinstalado. Esta é uma das novidades do Windows Server 2003. Fique atente a este ponto, principalmente ao prestar os exames de Certificação para o MCSE – 2003 (Microsoft Certified Systems Engineer no Windows Server 2003). Para todos os detalhes sobre os exames necessários para obter o MCSE-2003, consulte o endereço a seguir:**

[www.juliobattisti.com.br/  
artigosw2k/mcse2003.asp](http://www.juliobattisti.com.br/artigosw2k/mcse2003.asp)

No próximo tópico você aprenderá sobre as diferentes edições do Windows Server 2003 e sobre as características de cada uma das edições.

## Um Sistema Operacional – Quatro Edições

O Windows Server 2003 é disponibilizado em quatro diferentes edições:

- ◆ 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 da 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, número de processadores, número máximo de servidores em um Cluster e assim por diante. Logo em seguida apresento uma descrição de cada uma das quatro edições do Windows Server 2003.

### Windows Server 2003 Standard Edition

Esta edição é indicada para ser utilizada em servidores de pequenas e médias organizações ou servidores departamentais com um número médio de usuários (10 a 100 usuários). Normalmente utilizado para serviços tais como o compartilhamento de arquivos e impressoras, gerenciamento centralizado das estações de trabalho, servidor de Intranet e servidor de conectividade com a Internet.

Se você precisa de um servidor para uma rede com um número de pequeno a médio de usuários (eu diria até 100 usuários), para serviços básicos, tais como autenticação de usuários, compartilhamento de arquivos e impressão e servidor de Intranet, eu recomendo esta edição do Windows Server 2003.

O Windows Server 2003 Standard Edition apresenta as seguintes limitações, quanto ao Hardware:

- ◆ Até quatro processadores
- ◆ 4 GB de memória RAM

Se você precisa de um servidor com maior capacidade, que possa suportar mais do que 4 processadores e/ou mais do que 4 GB de memória RAM, você deve utilizar o Windows Server 2003 Enterprise Edition ou o Windows Server 2003 Data Center Edition.

Ao final deste item apresentarei uma tabela comparativa entre as quatro edições do Windows Server 2003. Esta tabela é baseada nas informações do site da Microsoft, no seguinte endereço:

<http://www.microsoft.com/windowsserver2003/evaluation/features/compareeditions.mspx>

Além dos limites de hardware apresentados anteriormente, o Windows Server 2003 Standard Edition também não tem suporte ao serviço de Cluster – Cluster Services. Com o serviço de Cluster é possível configurar dois ou mais servidores para atuar como se fossem um único servidor. Para o usuário (cliente da rede) é como se fosse um único servidor. Se um dos servidores do Cluster falhar, os outros continuam atendendo aos clientes normalmente. Caso você necessite de serviços de Cluster, deve utilizar o Windows Server 2003 Enterprise Edition ou Windows Server 2003 Data Center Edition.

Você pode estar perguntando: Se o Windows Server 2003 Enterprise Edition e Windows Server 2003 Data Center Edition são as edições com o maior número de recursos, então porque não utilizar diretamente estas edições. Obviamente que maior número de recursos implica em preço mais elevado. Desta maneira é importante que você faça uma análise cuidadosa das suas necessidades e opte pela edição que atende estas necessidades, sem ter que pagar mais por isso. Por exemplo, se as características do Windows Server 2003 Standard Edition atendem todas as necessidades da sua rede, porque pagar mais por uma das edições com mais recursos, sendo que você não irá utilizar estes recursos.

### **Serviços e/ou recursos não disponíveis no Windows Server 2003 Standard Edition:**

- ◆ Suporte a mais do que 4 processadores.
- ◆ Suporte a mais do que 4 GB de memória RAM.
- ◆ Suporte a serviço de Cluster.
- ◆ Versão de 64 Bits para processadores Intel Itanium
- ◆ Troca de memória sem desligar o servidor (somente disponível nas edições Enterprise e Data Center e depende de suporte do fabricante do Hardware do servidor).
- ◆ Suporte a serviços de Metadiretório
- ◆ Windows System Resource Manager (WSRM): Este recurso permite a alocação de recursos de Hardware para processos específicos. Por exemplo, em um servidor Web você pode alocar mais recursos de hardware para os processos do IIS (Internet Information Services), dando prioridade para estes processos em relação aos demais.

---

**NOTA: A maioria destes recursos estão disponíveis nas edições Enterprise Edition e Data Center Edition.**

---

## **Windows Server 2003 Enterprise Edition**

Esta é uma edição mais robusta, com mais recursos do que a Standard Edition. É recomendada para redes de porte de médio tendendo para grande. Eu diria que a partir de 100 usuários já é preciso uma análise mais detalhada para decidir entre o Windows Server 2003 Standard Edition e o Windows Server 2003 Enterprise Edition. É recomendado para servidores que fornecem serviços como: Roteamento, servidor de Banco de dados (SQL Server 2000, ORACLE, etc), correio eletrônico e aplicativos de colaboração (Microsoft Exchange, Lotus Notes, etc), Sites de comércio eletrônico e outros aplicativos utilizados em redes de grande porte.

O Windows Server 2003 Enterprise Edition apresenta as seguintes limitações, quanto ao Hardware:

- ◆ Oito processadores na versão de 32 bits.
- ◆ 32 GB de memória RAM na versão de 32 bits.
- ◆ Cluster com até oito servidores.

Com certeza o Windows Server 2003 Enterprise Edition atende às necessidades da maioria dos servidores de rede. As funcionalidades a seguir, que não estão disponíveis no Windows Server 2003 Standard Edition, estão disponíveis no Windows Server 2003 Enterprise Edition:

- ◆ Suporte a serviço de Cluster.
- ◆ Versão de 64 Bits para processadores Intel Itanium
- ◆ Troca de memória sem desligar o servidor (somente disponível nas edições Enterprise e Data Center e depende de suporte do fabricante do Hardware do servidor).
- ◆ Suporte a serviços de Metadiretório

- ◆ Windows System Resource Manager (WSRM): Este recurso permite a alocação de recursos de Hardware para processos específicos. Por exemplo, em um servidor Web você pode alocar mais recursos de hardware para os processos do IIS (Internet Information Services), dando prioridade para estes processos em relação aos demais.

## Windows Server 2003 Data Center Edition

Esta é a edição “peso-pesado”, ou seja, aquela que apresenta o maior número de recursos e a maior capacidade para atender aplicações com um grande número de usuários e com elevadas exigências de desempenho. O Windows Server 2003 Data Center Edition é indicado para as chamadas aplicações de missão-crítica, ou seja, aquelas aplicações que não podem falhar em hipóteses alguma. Quer alguns exemplos de aplicações de missão crítica? Fácil:

- ◆ As aplicações que mantém em funcionamento uma bolsa de valores.
- ◆ As aplicações Web que mantém um site de comércio eletrônico em funcionamento.
- ◆ As aplicações que mantêm um banco em funcionamento.

Existem inúmeros outros exemplos de aplicações que são vitais para o funcionamento de uma empresa. Por exemplo, nos últimos anos, houve uma grande adoção dos chamados softwares de ERP – Enterprise Resource Planning. Estes softwares disponibilizam as mais variadas funcionalidades, desde um simples controle de estoque, passando por contas a pagar e a receber, até o controle da produção na fábrica. Este é um exemplo típico de aplicação que precisa estar em funcionamento sempre, que tem que atender a um grande número de usuários, que trata com um grande volume de dados e assim por diante. O Windows Server 2003 Data Center Edition é o Sistema Operacional indicado para ser utilizado em servidores que irão hospedar as chamadas aplicações de missão crítica.

O Windows Server 2003 Data Center Edition apresenta as seguintes limitações, quanto ao 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 seguinte 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 queriam 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.

## Windows Server 2003 Web Edition

Esta edição do Windows Server 2003 é especificamente projetada para servidores que prestarão serviço de hospedagem de sites, de aplicações Web, e aplicações baseadas na plataforma .NET, utilizando tecnologias como ASP.NET, XML e Web Services.

O Windows Server 2003 Web Edition é para o uso específico em servidores Web ou servidores da Intranet da empresa, na qual estarão hospedadas páginas e aplicações Web. Esta é realmente uma edição com uma finalidade específica. Para você ter uma idéia, não é possível instalar o Active Directory no Windows Server 2003 Web Edition, transformando-o em um Controlador de Domínio, ou seja, ele foi especificamente projetado para ser utilizado como um servidor de Internet/Intranet.

O Windows Server 2003 Web Edition apresenta os seguintes limites de Hardware:

- ◆ Suporta, no máximo, dois processadores.
- ◆ Suporta, no máximo, 2 GB de memória RAM.

Uma série de serviços e recursos disponíveis nas outras edições, não estão disponíveis no Windows Server 2003 Web Edition, conforme você poderá conferir na tabela de comparação entre as edições, no final deste item.

## Comparação Entre as Diferentes Edições

A seguir apresento uma tabela comparativa entre as diferentes versões. Na tabela 1.1 apresento uma comparação entre os recursos de hardware mínimos, exigidos por cada uma das diferentes edições. Claro que 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 e assim por diante. Na tabela 1.2 apresento uma comparação exibida no site da Microsoft, onde são listados os recursos disponíveis em cada uma das edições.

**Tabela 1.1 Recursos mínimos de Hardware para as diferentes edições do Windows Server 2003.**

| Recurso                    | Web     | Standard | Enterprise                               | Data Center                              |
|----------------------------|---------|----------|--|--|
| CPU mínima                 | 133 MHZ | 133 MHZ  | 133 MHZ p/x86<br>733 MHZ p/Intel Itanium | 400 MHZ p/X86<br>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                                   |

**NOTA:** Para maiores detalhes sobre a plataforma .NET, a criação de aplicações Web com ASP.NET e uma introdução aos Web Services, consulte o livro “ASP.NET: Uma Nova Revolução na Criação de Sites e Aplicações Web”, de minha autoria e publicado pela editora Axcel Books ([www.axcel.com.br](http://www.axcel.com.br)).

**DICA:** Para o exame, não esqueça de que não é possível instalar o Active Directory no Windows Server 2003 Web Edition.

Para você ter uma idéia um pouco melhor sobre esta questão de desempenho, o computador que eu estou utilizando para escrever este livro, tem as seguintes configurações de Hardware:

- ◆ Processador Pentium de 1 GHZ
- ◆ 512 MB de RAM
- ◆ 30 GB de disco rígido

A minha rede doméstica tem dois computadores. O servidor onde está instalado o Windows Server 2003 e mais uma estação de trabalho com o Windows 2000 Professional. O sistema está com um bom desempenho. Após a instalação do Active Directory já houve uma queda de desempenho. A questão agora é: “Quantos usuários em rede neste servidor seria capaz de atender, por exemplo, com serviços de compartilhamento de arquivos e impressão, mais serviços Web (http, ftp, etc.)?”. Só simulando um ambiente onde o número de usuários é aumentado pouco a pouco, para determinar com precisão o limite de capacidade desta configuração.

No endereço a seguir, você encontra uma comparação entre as diferentes edições do Windows Server 2003 em termos dos recursos disponíveis em cada edição. A tabela apresentada no site da Microsoft Brasil, as funcionalidades estão divididas por categorias, tais como: Tecnologias de Cluster, serviços de diretório, Serviços de arquivo e impressão e assim por diante.

Tabela comparativa entre as quatro edições do Windows Server 2003:

<http://www.microsoft.com/brasil/windowsserver2003/compare.mspx>

Na Figura 1.4 exibo um trecho da tabela disponível no endereço informado, com a comparação entre as diferentes edições.

| Recurso   | Servidores Web | Standard Server | Enterprise Server | Datacenter Server |
|---|----------------|-----------------|-------------------|-------------------|
| <b>Tecnologias de cluster</b>                     |                |                 |                   |                   |
| Balanceamento de carga da rede                    | ●              | ●               | ●                 | ●                 |
| Cluster de falhas                                 | ○              | ○               | ●                 | ●                 |
| <b>Comunicações e serviços de rede</b>            |                |                 |                   |                   |
| 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 (ICCS) | ○              | ●               | ●                 | ○                 |
| <b>Serviços de diretório</b>                      |                |                 |                   |                   |
| Active Directory™                                 | ○              | ●               | ●                 | ●                 |
| Supporte para serviços de metadiretório (MMS)     | ○              | ○               | ●                 | ●                 |
| <b>Serviços de arquivo e impressão</b>            |                |                 |                   |                   |
| 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                           | ○              | ○               | ●                 | ●                 |
| <b>Serviços de gerenciamento</b>                  |                |                 |                   |                   |
| IntelliMirror                                     | ○              | ●               | ●                 | ●                 |
| Conjunto de diretrivas resultante (RSOP)          | ○              | ●               | ●                 | ●                 |
| Windows Management Instrumentation (WMI)          | ○              | ●               | ●                 | ●                 |
| Servidor de instalação remota (RIS)               | ○              | ●               | ●                 | ●                 |
| <b>Serviços de segurança</b>                      |                |                 |                   |                   |
| Firewall de conexão com a Internet                | ○              | ●               | ●                 | ○                 |
| Serviços de certificado                           | ○              | ●               | ●                 | ●                 |
| Serviços de terminal                              | ●              | ●               | ●                 | ●                 |
| Área de trabalho remota para administração        | ●              | ●               | ●                 | ●                 |

Figura 1.4 Tabela comparativa entre as diferentes edições.

**NOTA:** Obviamente que estes são valores mínimos para tirar o CD do Windows Server 2003 da caixa e instalar o sistema. A quantidade de memória e processamento necessária varia com diversos fatores, conforme descrito anteriormente. Agora vamos ser sinceros, mesmo sendo apontado como valor mínimo, você consegue imaginar o Windows Server 2003 Enterprise Edition, rodando em um Pentium 133 com 128 MB de RAM? Nem o Windows 2000 Professional rodaria bem em um equipamento destes. Ao invés de rodar eu gosto de utilizar o termo “girar lentamente”. Na empresa onde eu trabalho, sempre que algum aplicativo apresenta problemas de desempenho e alguém pergunta: “Júlio, como está rodando o aplicativo xyz?”. Eu respondo: “Não está rodando, está girando lentamente”. Com isso os colegas já sabem que eu estou querendo dizer que o aplicativo está com sérios problemas de desempenho.

# Novidades do Windows Server 2003

Neste tópico apresentarei uma breve descrição das novidades e novas funcionalidades do Windows Server 2003, em relação ao Windows 2000 Server.

Vou fazer uma apresentação das novas funcionalidades, dividindo-as em categorias. Por exemplo, quais as novidades do Active Directory, quais as novidades nos serviços de compartilhamento de arquivos e impressão, quais as novidades de segurança e assim por diante.

## Novidades no Active Directory

O Active Directory é o componente principal do Windows Server 2003 (a exemplo do que acontece no Windows 2000 Server). O Active Directory é um banco de dados no qual ficam armazenadas informações sobre todos os componentes da rede, tais como nomes de computadores, nomes de usuários e grupos e assim por diante. No Capítulo 2 você estudará o Active Directory em detalhes.

No Windows Server 2003 ficou mais fácil administrar o Active Directory. Novas ferramentas e funcionalidades facilitam a vida do Administrador. No Windows Server 2003 estão disponíveis as seguintes novidades no Active Directory:

- ◆ **Active Directory Migration Tool - ADMT 2.0:** Esta ferramenta ajuda na migração das versões anteriores do Windows (NT Server 4.0 e Windows 2000 Server) para uma estrutura baseada no Active Directory no Windows Server 2003. Por exemplo, esta ferramenta permite fazer a migração de todas as contas de usuários e as respectivas senhas, de uma rede baseada no NT Server 4.0 para o Windows Server 2003 ou em uma rede baseada no Windows 2000 Server para o Windows Server 2003.
- ◆ **Renomear um domínio:** Com o Windows Server 2003 é possível renomear um domínio, o que não era possível no NT Server 4.0 ou no Windows 2000 Server. Para que seja possível renomear um domínio, algumas condições devem ser atendidas, conforme mostrarei no Capítulo 2, onde falarei sobre o Active Directory.
- ◆ **Maior flexibilidade para o gerenciamento do Schema:** O Schema (conforme detalharei no Capítulo 2) é a definição da estrutura do banco de dados do Active Directory. Por exemplo, é no esquema que está a definição de quais campos formam um objeto do tipo usuário, qual o tipo de cada campo, quais campos são de preenchimento obrigatório e quais não são e assim por diante.
- ◆ **Active Directory in Application Mode (AD/AM):** Esta é uma novidade realmente interessante. É possível instalar e configurar o Active Directory em um servidor, para que ele seja executado no modo de aplicação. Quando configurado para rodar no modo de aplicação, o Active Directory roda como se não fosse um serviço do próprio sistema operacional e com isso não é obrigatório que o servidor seja um DC (Domain Controller – Controlador de domínio). Ao não rodar como um serviço do Sistema Operacional, é possível ter múltiplas instâncias do Active Directory instaladas no mesmo servidor, cada uma sendo independente da outra, ou seja, cada instância contém o seu próprio conjunto de objetos. Esta funcionalidade está prevista para ser disponibilizada como um componente separadamente do Windows Server 2003, ou seja, não será lançado juntamente com o Windows Server 2003. Não existe ainda informação se será um componente pago ou estará disponível para Download gratuito através do site da Microsoft na Internet.
- ◆ **Microsoft Group Policy Management Console (GPMC):** Este é um console para administração de tarefas relacionadas com a configuração e aplicação de Group Policies Objects (GPOs). Com este console será possível fazer o gerenciamento da aplicação de GPOs em múltiplos domínios, você poderá arrastar polices de um

**IMPORTANTE:** Existe uma incompatibilidade do Windows Server 2003 em trabalhar em sistemas com multiprocessadores que utilizam algumas versões do Pentium Pro e do Pentium II. Para um descrição completa deste problema e da lista de processadores incompatíveis, consulte o seguinte endereço:

<http://support.microsoft.com/default.aspx?scid=kb;en-us;319091>

domínios para aplica-las em outro domínio. Você poderá fazer o backup, restore, cópia e relatório das GPOs. Com este console ficará muito mais fácil fazer o gerenciamento das GPOs. Esta funcionalidade está prevista para ser disponibilizada como um componente separadamente do Windows Server 2003, ou seja, não será lançado juntamente com o Windows Server 2003. Segundo informações da Microsoft este componente estará disponível para Download gratuito, através do site da Microsoft.

- ◆ **Melhorias nos consoles de administração do Active Directory:** No Windows Server 2003 estão disponíveis novas funcionalidades nos consoles de administração do Active Directory, tais como: capacidade de arrastar-e-soltar, seleção de múltiplos objetos e a capacidade de salvar e utilizar novamente pesquisas efetuadas no Active Directory. Por exemplo, com a capacidade de arrastar-e-soltar, você pode mover uma conta de usuário de uma Unidade Organizacional para outra, simplesmente arrastando, a exemplo do que você faz com arquivos e pastas no Windows Explorer.
- ◆ **Melhorias na segurança do Active Directory:** Em relação a segurança foram implementadas as seguintes melhorias:
  - ◆ **Cross-forest authentication:** Este tipo de autenticação permite um acesso seguro aos recursos disponíveis na rede, quando a conta do usuário pertence a um domínio que está em uma floresta e a conta do computador onde o usuário esta fazendo o logon, está em um domínio em uma outra floresta. Com esta funcionalidade os usuários podem, de uma maneira segura, acessar recursos localizados em servidores de outras florestas, sem a necessidade de ter uma conta de usuário em um domínio da floresta de destino.
  - ◆ **Cross-forest authorization:** Este recurso permite ao Administrador selecionar usuários e grupos de outra floresta (com a qual existe uma relação de confiança), para inclusão em grupos locais ou em uma lista de permissão de acesso para arquivos, pastas ou impressoras.
- ◆ **Políticas para restrição de Software:** Esta é uma das novidades que eu mais aprecio. Com o uso desta funcionalidade, o Administrador pode criar uma lista de Softwares permitidos, ou seja, de programas que são autorizados a serem executados nas estações de trabalho da rede da empresa. Os programas que fazem parte da lista de software autorizado funcionarão normalmente. Se o usuário instalar um programa não autorizado, as políticas de restrição de Software farão com que o programa não possa ser executado. Como Administrador você poderá criar exceções à política de restrição de Software. Por exemplo, você poderia configurar as políticas de restrição para permitir que o DOOM fosse executado na sua estação de trabalho. Brincadeiras à parte, está é uma funcionalidade realmente importante.
- ◆ **Facilidade de logon para usuários remotos:** As informações de logon de um usuário remoto são mantidas em um cache, no controlador de domínio da rede onde o usuário está. Com isso, não existe a necessidade de conexão com um servidor de Catálogo Global do domínio de origem do usuário. Assim, se por exemplo, a conexão com a WAN da empresa for perdida, o usuário poderá fazer o logon, utilizando as informações que estão no cache do servidor, sem a necessidade de conexão com um servidor de catálogo global do seu domínio de origem. Isso reduz o tráfego de rede e permite que o usuário faça o logon, mesmo quando não houver conectividade com o seu domínio de origem.
- ◆ **Melhoria na replicação das alterações feitas em grupos de usuários:** No Windows 2000 Server, sempre que um grupo for alterado (um novo usuário é adicionado ou removido, ou o grupo for renomeado), todas as informações do grupo serão replicadas para os demais DCs do domínio. Com isso é gerada uma boa quantidade de tráfego de rede, sempre que um ou mais grupos são alterados. No Windows Server 2003, sempre que um grupo for alterado, somente as modificações serão replicadas, o que reduz o tráfego de rede e facilita a propagação das alterações feitas em um DC para todos os demais DCs do domínio.
- ◆ **Application Directory Partitions:** Algumas informações armazenadas no Active Directory não precisam estar disponíveis em todos os DCs do domínio. Por exemplo, você pode armazenar informações sobre o

DNS apenas nos servidores que estão atuando como servidores de DNS e não para todos os DCs do domínio. Você pode incluir as informações sobre o DNS em uma Application Directory Partitions (Partição de Aplicação do Active Directory) e configurar para quais servidores estas informações devem ser replicadas. Com isso você reduz o tráfego na rede e tem um controle maior sobre a replicação destas informações.

- ◆ **Instalar uma réplica do Active Directory a partir de um CD, fita de backup ou HD:** Esta é uma das novidades que eu mais gosto. Com o Windows 2000 Server quando você instalava um novo DC, este precisava copiar a base de dados completa do Active Directory, através da replicação. Em domínios grandes, com um grande número de usuários e computadores, a base do Active Directory chega facilmente a tamanhos como 2 GB ou mais. Imagine replicar (ou seja transmitir) esta informação através de um link de WAN de 64 kbps. São dias e dias até que a base do novo DC fique completa e funcional. Com o Windows Server 2003 você pode fazer uma cópia do Active Directory em CD, fita de backup ou HD. Quando você instala um novo DC, você carrega a cópia do Active Directory que você levou gravada e depois só é preciso replicar as alterações desde o momento em que você gerou a cópia até a instalação do novo DC. O que com certeza é um volume de informações bem menor do que ter que replicar uma cópia completa do Active Directory. Esta funcionalidade é especialmente útil quando você tem que instalar um novo DC em escritórios da empresa, conectados com links de baixa velocidade, tais como 64 kbps ou 128 kbps.
- ◆ **Novas ferramentas para o gerenciamento da replicação entre os DCs do domínio:** Para o gerenciamento da atualização dos servidores de Catálogo Global e uma ferramenta para gerenciar e implementar uma topologia de replicação entre sites, mais eficiente, o que permite um número maior de sites por domínio, do que no Windows 2000 Server.

**NOTA:** Os conceitos de Controladores de Domínio (DCs), servidores de Catálogo Global e sites serão detalhados no Capítulo 2, onde o Active Directory será descrito em detalhes.

## Novidades nos Serviços de Compartilhamento de Arquivos e Impressão

Sem dúvidas os serviços mais utilizados são o compartilhamento de arquivos e de impressoras. Foi para prestar este tipo de serviço que os primeiros servidores foram projetados. O Windows Server 2003 fornece diversas novidades e melhorias nos serviços de compartilhamento de arquivos e de impressoras, conforme descrito a seguir:

- ◆ **Remote Document Sharing (WebDAV):** Este é um recurso que facilita o acesso a arquivos armazenados em servidores HTTP, utilizando os mesmos comandos utilizados para acessar arquivos locais, do disco rígido, do CD-ROM ou de um driver de rede. Esta funcionalidade facilita a criação de aplicativos que acessam dados em servidores HTTP. Com o redirecionador WebDav, o programa “enxerga” os arquivos remotos como se fossem arquivos locais.
- ◆ **Automated System Recovery (ASR):** Esta é uma das funcionalidades que eu mais aprecio. Foi introduzida (de maneira tímida) no Windows Me, está disponível no Windows XP e agora no Windows Server 2003. Com este recurso você pode fazer um ou mais backups do “estado do sistema” – configurações de software e de hardware do sistema. Quando houver algum problema, você pode utilizar um determinado backup, para restaurar o sistema ao estado em que ele estava, quando o respectivo backup foi efetuado. Por exemplo, você faz um backup (criando um Ponto de Restauração) as 9:00 hs da manhã. Logo após você instala uma nova versão do driver da placa de rede. Ao reiniciar o servidor o sistema fica extremamente instável. Você pode utilizar o ponto de restauração criado as nove horas, para restaurar o sistema ao estado em que se encontrava as 9:00, ou seja, com a versão antiga do driver e estável. Eu considero uma ferramenta realmente de grande valor para o Administrador.

- ◆ **Novos comandos para gerenciamento de discos e volumes:** O Windows Server 2003 fornece uma série de novos comandos para o gerenciamento de discos e volumes no Windows Server 2003. Com estes comandos fica bem mais fácil criar scripts para fazer o gerenciamento de discos e volumes no Windows Server 2003.
- ◆ **GUID Partition Table (GPT):** As versões de 64 bits do Windows Server 2003 suportam um novo formato de particionamento de disco conhecido como GPT. Neste novo formato, as informações necessárias ao funcionamento do disco são gravadas na própria partição, ao invés de gravadas em setores ocultos ou espaço não particionado do disco, a exemplo do que ocorre com o padrão MBR – Master Boot Record. Com isso, ao fazer o backup da partição, também é feito o backup das informações necessárias ao seu funcionamento. As partições GPT também fornecem redundância em relação a tabela de arquivos da partição, o que minimiza o risco de perda de dados.
- ◆ **Utilitário de desfragmentação:** O utilitário de desfragmentação do Windows Server 2003 é mais rápido e eficiente do que nas versões anteriores. No Windows 2000 Server é aconselhável que você utilize um software de terceiros para fazer a desfragmentação dos volumes. No Windows Server 2003 isso não é necessário, já que o utilitário de desfragmentação fornecido com o sistema operacional é bem eficiente.
- ◆ **Enhanced Distributed File System (DFS):** O DFS facilita a consolidação das diversas pastas compartilhadas da rede em um único ponto lógico de acesso. Também permite que sejam configuradas réplicas de uma pasta compartilhada para prover redundância no caso de falha de um servidor. Uma das principais melhorias do DFS no Windows Server 2003 é a possibilidade de criar mais de um DFS Root por servidor. No Capítulo 5 você aprenderá a configurar e a administrar o DFS.
- ◆ **DFS File Replication Services (FRS):** Este serviço trabalha em conjunto com o DFS para fornecer os serviços de replicação de conteúdo. No Windows Server 2003 você pode configurar a topologia de replicação, o que não era permitido no Windows 2000 Server. Esta facilidade permite que você configure uma tecnologia levando em conta as velocidades dos links de comunicação, definindo desta maneira, horários de replicação que não venham a sobrecarregar os links de comunicação durante o horário de expediente.
- ◆ **Melhorias no sistema de criptografia de arquivos – EFS:** Também foram disponibilizadas novas APIs – Application Program Interfaces para facilitar a criação de software anti-vírus mais eficientes, os quais não interferem no desempenho do servidor. Também foram introduzidas melhorias de performance no utilitário CHKDSK.
- ◆ **Shadow Copies for Users:** Esta é uma funcionalidade que pode ser habilitada em cada pasta compartilhada. Ao habilitar esta funcionalidade o Windows Server 2003 faz cópias das versões anteriores dos arquivos. Ou seja, sempre que você altera um arquivo e salva no disco, o Windows Server 2003 mantém uma cópia de um determinado número de versões anteriores do arquivo. O usuário pode acessar, facilmente, qualquer uma das versões anteriores disponíveis. Para isso basta clicar com o botão direito do mouse no arquivo e utilizar as opções do menu para acessar as versões anteriores. No endereço a seguir você encontra uma demonstração de como funciona este recurso. Para acessar esta demonstração você precisa do Internet Explorer e do Player do Flash instalados. Se você não tiver o Player do Flash, este será automaticamente copiado e instalado pela Internet.

<http://www.microsoft.com/windowsserver2003/docs/VolumeShadowCopyService.swf>

A seguir descrevo as novidades em relação ao sistema de impressão no Windows Server 2003:

- ◆ Novos utilitários de linha de comando para a execução das principais tarefas de administração de impressoras e compartilhamento de impressoras.
- ◆ **Print Cluster Support (Enterprise Edition & Datacenter Edition only):** Impressão em um cluster de servidores. Quando você instala um driver de impressora em um dos servidores do cluster, o Windows Server 2003 automaticamente instala este driver em todos os demais servidores que fazem parte do cluster. Esta característica facilita bastante a administração de impressoras instaladas em um cluster.

- ◆ **Suporte a um grande número de novos drivers de impressoras:** Para ser mais preciso, segundo a documentação oficial do Windows Server 2003, é fornecido suporte para cerca de 3800 novas impressoras.
- ◆ **Melhorias na performance da impressão e na detecção de dispositivos Plug and Play:** Melhorias na performance da impressão através da rede. As ferramentas de gerenciamento também ficaram mais fáceis de utilizar, bem como o gerenciamento de impressão através do navegador apresenta novas funcionalidades. Estão disponíveis uma série de objetos e contadores para acompanhar os trabalhos de impressão através da rede, tais como o número de páginas impressas por usuário, por impressora e assim por diante.

## Novidades na área de segurança no Windows Server 2003

Segurança é um dos pontos mais importantes quando você decide sobre qual sistema operacional utilizar nos servidores da sua rede. No Windows Server 2003 foram feitas diversas melhorias para tornar o sistema ainda mais seguro.

- ◆ **Firewall de Conexão com a Internet (IFC - Internet Connection Firewall):** Com o Windows XP Professional é fornecido um Firewall de Conexão com a Internet, o qual também é disponibilizado com o Windows Server 2003. Este Firewall permite um primeiro nível de proteção contra ataques vindos da Internet.
- ◆ **Suporte ao protocolo IEEE 802.1X:** Este protocolo é utilizado para a conexão de dispositivos Wireless (sem fio) à redes Ethernet. Com o suporte ao protocolo IEEE 802.1X, os dispositivos Wireless podem se conectar e autenticar com um domínio baseado no Windows Server 2003.
- ◆ **Políticas para restrição de Software:** Esta é uma das novidades que eu mais aprecio, conforme já descrevi anteriormente. Com o uso desta funcionalidade, o Administrador pode criar uma lista de Softwares permitidos, ou seja, de programas que são autorizados a serem executados nas estações de trabalho da rede da empresa. Os programas que fazem parte da lista de software autorizado funcionarão normalmente. Se o usuário instalar um programa não autorizado, as políticas de restrição de Software farão com que o programa não possa ser executado. Como Administrador você poderá criar exceções à política de restrição de Software. Por exemplo, você poderia configurar as políticas de restrição para permitir que o DOOM fosse executado na sua estação de trabalho. Brincadeiras à parte, está é uma funcionalidade realmente importante.
- ◆ **Configurações padrão de segurança do IIS 6.0:** O IIS 6.0 é instalado com as configurações de segurança para proteção máxima. Ou seja, a maioria dos recursos são restritos e protegidos. A medida que for necessário o Administrador vai alterando as configurações de segurança para atender as necessidades do servidor. Desta maneira a política utilizada é “tudo bloqueado”, a medida que forem necessários, os recursos vão sendo liberados.
- ◆ **O IIS não é instalado por padrão, quando o Sistema Operacional é instalado:** Com o Windows 2000 Server, o IIS era instalado por padrão e com configurações de segurança não muito “severas”. No Windows Server 2003 o IIS não é instalado por padrão, deve ser instalado usando a opção Adicionar ou Remover Programas do Painel de controle.
- ◆ **Melhoria na performance de sites seguros que utilizam o protocolo SSL:** Com o Windows Server 2003 houve uma melhoria de até 35% na performance de aplicações Web seguras, baseadas no protocolo SSL.

No endereço a seguir, você encontra uma descrição completa das novidades na área de segurança, no Windows Server 2003:

<http://www.microsoft.com/windowsserver2003/evaluation/overview/technologies/security.mspx>

## Novidades nos serviços de rede e comunicação

Além de compartilhamento de arquivos e impressoras, um sistema operacional de rede deve fornecer uma série de outros serviços. Desde serviços para resolução de nomes, tais como o DNS, até serviços mais sofisticados de roteamento

e acesso remoto (como o RRAS). A seguir descrevo as principais novidades nos serviços de rede e comunicação, no Windows Server 2003.

- ◆ **Suporte ao IP v6:** O IP versão 6 (IP v6) é a nova versão do protocolo IP. Foi projetado para resolver problemas de desempenho do IP v4 e, principalmente, o número reduzido de números IP disponíveis na versão 4. O Windows Server 2003 fornece suporte completo ao IP v6, bem como opções para interconectar dispositivos que utilizam as diferentes versões do protocolo IP.
- ◆ **Point-to-Point Protocol over Ethernet (PPPoE):** Com o uso deste protocolo é possível a um cliente se conectar a um servidor com suporte ao protocolo PPPoE, sem o uso de nenhum software adicional.
- ◆ **Network Bridging:** Com esta funcionalidade um administrador pode conectar diferentes segmentos de rede utilizando um servidor com o Windows Server 2003 instalado. Por exemplo, você pode utilizar um computador com o Windows Server 2003 instalado e com múltiplos adaptadores de rede (Ethernet, Wireless e Dial-up), para conectar diferentes segmentos de rede.
- ◆ **Utilização do protocolo IPSec através de NAT:** Esta era uma das dificuldades encontradas no Windows 2000 Server. Não era possível utilizar o protocolo IPSec através de um servidor RRAS com o NAT (Network Address Translation) habilitado. No Windows Server 2003 esta limitação foi eliminada. Agora é possível fazer com que uma conexão Layer Two Tunneling Protocol (L2TP) sobre IPSec ou uma conexão IPSec possa ser utilizada juntamente com NAT.
- ◆ **Melhorias na Administração de Group Policies Objects, com o uso do Microsoft Group Policy Management Console (GPMC):** Também foram feitas novas adições de polices, como por exemplo polices que permitem configurar opções do DNS no cliente. Por exemplo, no Windows Server 2003 você pode configurar a lista de prefixos DNS no cliente, o que não era possível no Windows 2000 Server.

No endereço a seguir, você encontra uma descrição completa das novidades na área de redes e comunicação:

<http://www.microsoft.com/windowsserver2003/evaluation/overview/technologies/networking.mspx>

## Novidades nos serviços de gerenciamento do Windows Server 2003

Muitas melhorias foram introduzidas nas ferramentas de gerenciamento do Windows Server 2003, em relação ao Windows 2000 Server. Esta é uma área que tem que ser analisada detalhadamente, pois a melhoria nas ferramentas de administração e gerenciamento, implica em maior produtividade e maior controle por parte do Administrador, o que também contribui para uma redução do custo de administração da rede.

- ◆ **Microsoft Group Policy Management Console (GPMC):** Este é um console para administração de tarefas relacionadas com a configuração e aplicação de Group Policies Objects (GPOs). Com este console será possível fazer o gerenciamento da aplicação de GPOs em múltiplos domínios, você poderá arrastar polices de um domínio para aplicá-las em outro domínio. Você poderá fazer o backup, restore, cópia e relatório das GPOs. Com este console ficará muito mais fácil fazer o gerenciamento das GPOs. Esta funcionalidade está prevista para ser disponibilizada como um componente separadamente do Windows Server 2003, ou seja, não será lançado juntamente com o Windows Server 2003. Segundo informações da Microsoft este componente estará disponível para Download gratuito, através do site da Microsoft.
- ◆ **Resultant Set of Policy (RSoP):** Esta ferramenta facilita o planejamento e a implementação das políticas de segurança. Com o uso desta ferramenta o Administrador pode analisar os efeitos das alterações nas políticas de segurança, antes de aplicá-las efetivamente. Com esta ferramenta o Administrador pode determinar qual será o conjunto de políticas efetivamente aplicadas a um usuário e/ou computador, antes mesmo de aplicar as respectivas políticas. Com isso inconsistências podem ser detectadas e evitadas.

- ◆ **Novas configurações de políticas de segurança:** Com o Windows Server 2003 estão disponíveis cerca de 200 novas opções de configurações para as políticas de segurança. Um exemplo de novas opções disponíveis são as opções para definir as configurações do DNS nas estações de trabalho.
- ◆ **A interface do editor das políticas de segurança foi bem melhorada.** Por exemplo, quando você clica em uma das opções, um texto explicativo é imediatamente exibido.
- ◆ **Filtros WMI (Windows Management Instrumentation):** Você pode criar filtros WMI com base em diversas características dos computadores. Por exemplo, você pode criar um filtro WMI para selecionar apenas os computadores com processador Pentium II 350 ou superior, com 128 MB ou mais de memória RAM e com o Windows 2000 Professional instalado. Depois você pode aplicar um conjunto de políticas de segurança com base em um filtro WMI. O filtro WMI seleciona apenas os computadores que atendam os critérios definidos no filtro e as políticas serão aplicadas aos computadores selecionados.
- ◆ **Cross-Forest Support:** Por padrão GPOs somente podem ser aplicadas em um site, domínio ou unidade organizacional. Com a funcionalidade de Cross-Forest Support, é possível, por exemplo, que um usuário da floresta X, faça o logon em um computador da floresta Y, sendo que cada floresta possui um diferente conjunto de GPOs aplicadas. Outro exemplo, as configurações em uma política de distribuição de software pode fazer referência a um ponto de distribuição (pasta compartilhada com os arquivos para instalação do programa) localizado em um servidor de outra floresta.
- ◆ **Políticas para restrição de Software:** Esta é uma das novidades que eu mais aprecio. Com o uso desta funcionalidade, o Administrador pode criar uma lista de Softwares permitidos, ou seja, de programas que são autorizados a serem executados nas estações de trabalho da rede da empresa. Os programas que fazem parte da lista de software autorizado funcionarão normalmente. Se o usuário instalar um programa não autorizado, as políticas de restrição de Software farão com que o programa não possa ser executado. Como Administrador você poderá criar exceções à política de restrição de Software. Por exemplo, você poderia configurar as políticas de restrição para permitir que o DOOM fosse executado na sua estação de trabalho. Brincadeiras à parte, está é uma funcionalidade realmente importante.
- ◆ **Melhorias no serviço de instalação remota RIS – Remote Instalattion Services.** Foram feitas melhorias que melhoraram o desempenho do protocolo TFTP – Trivial FTP, utilizado para a transferência dos arquivos de instalação do servidor RIS para o computador de destino.
- ◆ **Novos utilitários de linha de comando.** Dezenas de novos utilitários de linha de comando foram disponibilizados. Isso facilita a administração e a automação de tarefas repetitivas através do uso de scripts. Os comandos apresentam uma sintaxe padronizada. Por exemplo, para obter ajuda sobre a sintaxe de um comando basta digitar o nome do comando e /?. Um arquivo de ajuda, com todos os detalhes sobre os diversos comandos: ntcmds.chm. Todos os novos comandos tem suporte a execução remota, utilizando a opção /S. Com esta opção o administrador pode fazer com que o comando seja executado em qualquer servidor da rede, simplesmente disparando o comando a partir da sua estação de trabalho e especificando o parâmetro /S, juntamente com o nome do servidor onde o comando deve ser executado.
- ◆ **Microsoft Windows Update Services Catalog Site:** O site de catálogo do Windows Update (<http://windowsupdate.microsoft.com/catalog>), permite que o Administrador faça cópia dos arquivos de atualizações do sistema e aplique estas atualizações utilizando uma ferramenta de distribuição de Software como o SMS 2.0 (System Management Server). Com isso os arquivos de atualização são baixados da Internet uma única vez e depois aplicados em todas as estações e servidores da rede. Este procedimento é bem mais racional do que baixar uma cópia dos arquivos para cada estação de trabalho e servidor onde as atualizações devam ser aplicadas.
- ◆ **Windows Update Consumer Site:** Este site é utilizado para baixar e instalar atualizações individualmente em cada computador. O Administrador da rede pode definir, com o uso de Polices (GPOs), quais os usuários estão autorizados a se conectar com o site de atualização. O endereço deste site é o seguinte: <http://windowsupdate.microsoft.com/>

- ◆ **Microsoft Software Update Services:** O Windows Update é muito prático, uma vez que o usuário pode conectar diretamente com o site do Windows Update, baixar e instalar as novas atualizações. Porém em um ambiente de rede é indicado que antes de instalar novas atualizações, estas sejam testadas em um ambiente de teste, para verificar se as atualizações não irão introduzir novos problemas ou instabilidades no Windows Server 2003. O Windows Server 2003 fornece um novo serviço chamado Microsoft Software Update Services. Com este serviço o administrador pode configurar um servidor para atuar como servidor de atualizações. As atualizações são baixadas da Internet para este servidor, são testadas e somente após aprovadas, são distribuídas para serem aplicadas nos demais computadores da rede. Via Polices (GPOs), o Administrador pode definir quando aplicar as atualizações e em quais computadores elas devem ser aplicadas. O uso de um servidor de atualizações também evita que várias cópias dos mesmos arquivos sejam feitas a partir da Internet. Com este serviço, os arquivos de atualização são copiados uma única vez – da Internet para o servidor de atualizações – e após testados, são distribuídos para os demais computadores da rede. O Microsoft Software Update Services é utilizado somente para a distribuição de atualizações de segurança e atualizações críticas. As demais categorias de atualizações são aplicadas via Windows Update. Com este serviço também é possível formar uma hierarquia de servidores de atualização. Por exemplo, o servidor da matriz copia os arquivos de atualização a partir da Internet e em seguida distribui para um servidor de atualização localizado em cada escritório da empresa. A partir do servidor de atualização de cada escritório, os computadores do escritório são atualizados.

No endereço a seguir, você encontra uma descrição completa das novidades na área de Gerenciamento no Windows Server 2003:

<http://www.microsoft.com/windowsserver2003/evaluation/overview/technologies/mgmtsrvcs.mspx>

## Novidades no suporte ao desenvolvimento de Aplicativos

A grande novidade no mundo do desenvolvimento de aplicações, baseadas em tecnologias Microsoft é a Plataforma.NET, com suas novas linguagens ASP.NET, VB.NET e C#. O Framework.NET já está disponível desde o Windows 2000 Server. Nesta seção descreverei as melhorias introduzidas no Framework.NET, pelo Windows Server 2003.

- ◆ Suporte a Web Services baseados em XML, diretamente no sistema operacional: O Windows Server 2003 oferece suporte nativo aos protocolos que permitem o funcionamento de Web Services baseados em XML, tais como: Simple Object Access Protocol (SOAP), Universal Description, Discovery and Integration (UDDI), and Web Services Description Language (WSDL).

---

**NOTA:** Para detalhes sobre o Framework.NET e os seus elementos constitutivos, consulte o livro **ASP.NET: Uma Nova Revolução na Criação de Sites e Aplicações Web**, Axcel Books, 2001.

---

- ◆ **Enterprise UDDI Services:** Com este serviço você pode implementar uma infra-estrutura interna, na Intranet da empresa, com suporte ao padrão UUDI e Web Services, sem depender de componentes externos. Com base neste serviço pode ser criado um repositório de Web Services, os quais podem ser utilizados pelas várias equipes de desenvolvimento da empresa. Com isso a reutilização de código torna-se mais fácil e integrada.
- ◆ **Framework.NET:** O Framework.NET é a base para o desenvolvimento de qualquer aplicação baseada no modelo.NET. Com o Windows Server 2003 você pode instalar o Framework.NET a partir do CD de instalação do Windows Server 2003, sem ter que baixá-lo, separadamente, a partir da Internet.
- ◆ **ASP.NET integrado com o Internet Information Services (IIS) 6.0:** Com o IIS 6.0, o suporte a aplicações ASP.NET foi grandemente melhorado, principalmente em relação a segurança e desempenho. Cada aplicação

ASP.NET é isolada das demais aplicações ASP.NET e podem se comunicar diretamente com o serviço HTTP, que no Windows Server 2003 é implementado com um driver a nível do Kernel do Sistema Operacional. Com estas novidades o número de processos que rodam no servidor IIS é reduzido, o que melhora o desempenho e evita que uma aplicação ASP.NET com problemas, interfira na execução de outras aplicações.

- ◆ **ASP.NET: Advanced Compilation:** Esta nova funcionalidade contribui para uma melhoria na performance das aplicações ASP.NET. A primeira vez que uma página ASP.NET é carregada, ela é compilada como um objeto e mantida na memória do servidor. Para atender novas solicitações, o IIS utiliza a versão compilada. O IIS fica monitorando a página para verificar se houve modificações, sempre que houver modificações, a nova versão da página substituirá a versão antiga, na memória do servidor. O resultado prático disso é uma melhoria considerável no desempenho.
- ◆ **ASP.NET: Intelligent Caching:** O modelo de programação do ASP.NET oferece classes que permitem ao programador um controle refinado sobre como será feito o cache das páginas ASP.NET no servidor. Isso permite a otimização do desempenho, através do uso de uma configuração de cache de páginas mais adequada a cada aplicação.

No endereço a seguir, você encontra uma descrição completa das novidades na área de suporte ao desenvolvimento de aplicativos no Windows Server 2003:

<http://www.microsoft.com/windowsserver2003/evaluation/overview/technologies/appsrvcs.mspx>

## Novidades em outras áreas do Windows Server 2003:

Novidades na tecnologia de Cluster:

<http://www.microsoft.com/windowsserver2003/evaluation/overview/technologies/clustering.mspx>

Novidades do Internet Information Services 6.0:

<http://www.microsoft.com/windowsserver2003/evaluation/overview/technologies/iis.mspx>

O IIS também será detalhado na Parte 3 deste livro.

Novidades na área de gerenciamento de armazenamento:

<http://www.microsoft.com/windowsserver2003/evaluation/overview/technologies/storage.mspx>

Novidades no Terminal Services:

<http://www.microsoft.com/windowsserver2003/evaluation/overview/technologies/terminalserver.mspx>

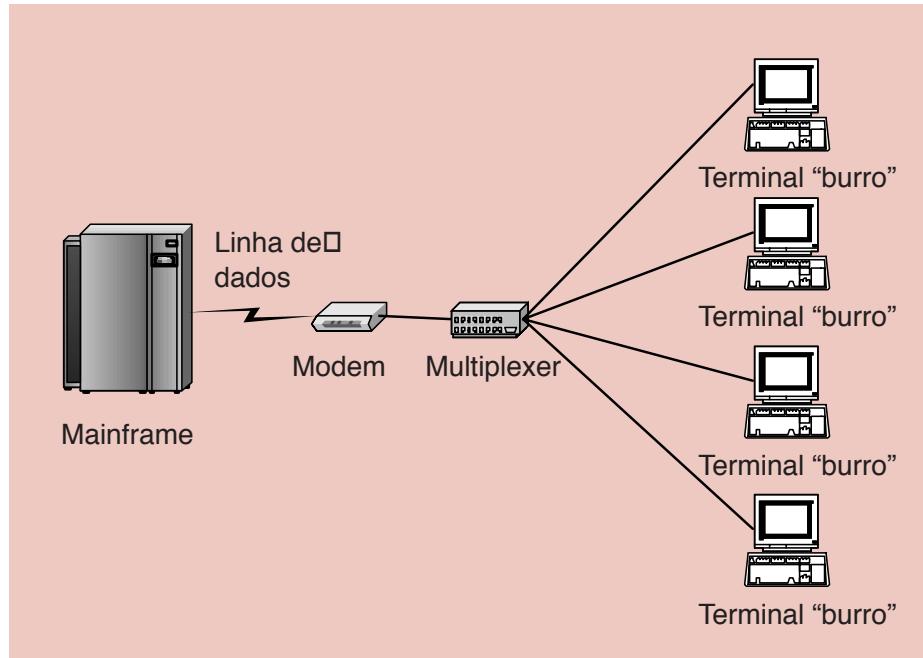
# Redes de computadores

Neste tópico apresentarei um histórico da evolução das redes de computadores, desde a época do Mainframe (o qual continua mais vivo do que nunca), passando pelas redes Cliente/Servidor clássicas, até o modelo mais atual, baseado em tecnologia de 3 ou mais camadas, como por exemplo a Internet, a maior de todas as redes.

## No princípio, um modelo Centralizado baseado no Mainframe

Todos sabem que a evolução em informática é bastante rápida. Sempre estão surgindo novos conceitos, programas e serviços. 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 Mainframe.

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 utilizados (na prática sabemos que ainda hoje este modelo é bastante utilizado, mas isso é discussão para daqui a pouco) os chamados terminais burros. Para falar um pouco mais sobre este modelo, considere o diagrama da Figura 1.4:



**Figura 1.4 O modelo baseado no Mainframe e no acesso via terminais “burros”.**

O Mainframe é um equipamento extremamente caro, na casa de milhões de dólares. Normalmente uma empresa prestadora de serviços de informática compra o Mainframe e hospeda neste equipamento, os sistemas e os dados de diversas empresas. O Mainframe é um equipamento que precisa de instalações adequadas, nas quais existe controle de temperatura, umidade do ar, alimentação elétrica estabilizada e assim por diante.

Os aplicativos e dados ficam armazenados no Mainframe. Vamos supor que a empresa X é a dona do Mainframe, no qual estão hospedados aplicativos e dados da empresa Y. Para ter acesso a estes dados, a empresa Y contrata uma linha de dados (que até o início da década de 90, aqui no Brasil, apresentava velocidades da ordem de 1 ou 2 kbps). Na sede da empresa, a linha de dados é conectada a um Modem, o qual era conectado 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 padrão para este tipo de ligação.

Com isso os terminais são, na prática, 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 no Mainframe. Pegue a lista dos dez maiores bancos brasileiros (públicos ou privados) e, no mínimo, cinco deles, ainda tem grande parte dos dados no Mainframe. Um dos bancos do qual sou correntista mantém os dados no Mainframe. Quando eu acesso meu extrato via Internet, com toda segurança, usando Certificado Digital, com uma interface gráfica (tudo muito moderno) estou na verdade acessando dados que estão no Mainframe. Tem alguma coisa de errado com isso?

Nada. Conforme você mesmo poderá concluir ao final deste tópico, o modelo baseado no Mainframe tem muitas vantagens que foram desprezadas na década de 90, mas que hoje são mais valorizadas do que nunca.

O modelo baseado no Mainframe tem inúmeras vantagens, dentre as quais destaco as listadas a seguir:

- ◆ **Gerenciamento e Administração centralizada:** Como 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 existe um único local a ser protegido.
- ◆ **Facilidade para atualização dos sistemas:** Como os sistemas são instalados em um único local, centralizadamente – no Mainframe, fica muito simplificada a tarefa de instalar novos sistemas e fazer atualizações nos sistemas já existentes. Por exemplo, quando você precisa atualizar um novo sistema, é só instalar a nova versão no Mainframe e pronto. A próxima vez que os usuários fizerem a conexão com o Mainframe, já terão acesso a versão atualizada, sem que tenha que ser atualizado software em cada um dos terminais que irão acessar a aplicação. Isso elimina grande parte do trabalho de administração, implementação e suporte a aplicações.

Claro que este modelo não era (e não é ainda hoje), somente vantagens. Pois se assim fosse, não teriam surgidos novos modelos, com propostas de descentralização como foi o caso do modelo Cliente/Servidor (o qual descreverei logo a seguir). Dentre as principais desvantagens do Mainframe, podemos destacar as seguintes:

- ◆ O custo é elevado, ou pelo menos as pessoas achavam que o custo era elevado, até descobrirem o chamado TCO – Total Cost Ownership, do modelo Cliente/Servidor. Mais adiante, quando for apresentado o modelo Cliente/Servidor, você entenderá melhor o “que” de ironia nesta frase.
- ◆ As linhas de comunicação no Brasil apresentavam problemas seríssimos de desempenho e custavam verdadeiras fortunas (não que hoje esteja uma maravilha, mas convenhamos que melhorou bastante). Além disso, a dependência da linha de comunicação era completa, ou seja, quando a linha ficasse fora do ar (o que acontecia com uma freqüência espantosa no início 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 guarda 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 de acesso aos dados. Neste momento começa surgir um movimento pró descentralização dos dados, em favor de “trazer” os dados para servidores dentro da empresa ou sob o controle da empresa. Logo a seguir descrevo este e outros motivos que foram as grandes promessas do modelo Cliente/Servidor, modelo este que “seria” o paraíso (permitam-me um sorriso irônico) comparado com o modelo centralizado, baseado no Mainframe.

## Morte ao Mainframe, viva a descentralização!!!

Normalmente quando começa a surgir um movimento de mudança, este apresenta características contrárias aos princípios do modelo vigente. Foi mais ou menos o que aconteceu com o modelo Cliente/Servidor, em relação ao modelo baseado no Mainframe.

No final da década de 80, início 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 estágio neste processo foi, naturalmente, a ligação deste computadores em rede. Desde as primeiras redes, baseadas em cabos coaxiais, até as modernas redes, baseadas em cabeamento estruturado e potentes Switchs de 100 MB ou de 1GB, 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 os dados fossem 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, que eu me atrevo a traduzir como “Redução de Tamanho”.

A seguir apresento um diagrama para ilustrar o modelo Cliente/Servidor. Depois faço alguns comentários para salientar os elementos deste modelo e em seguida comento as vantagens e desvantagens.

No diagrama da Figura 1.5 temos um exemplo de uma rede baseada no modelo Cliente/Servidor:

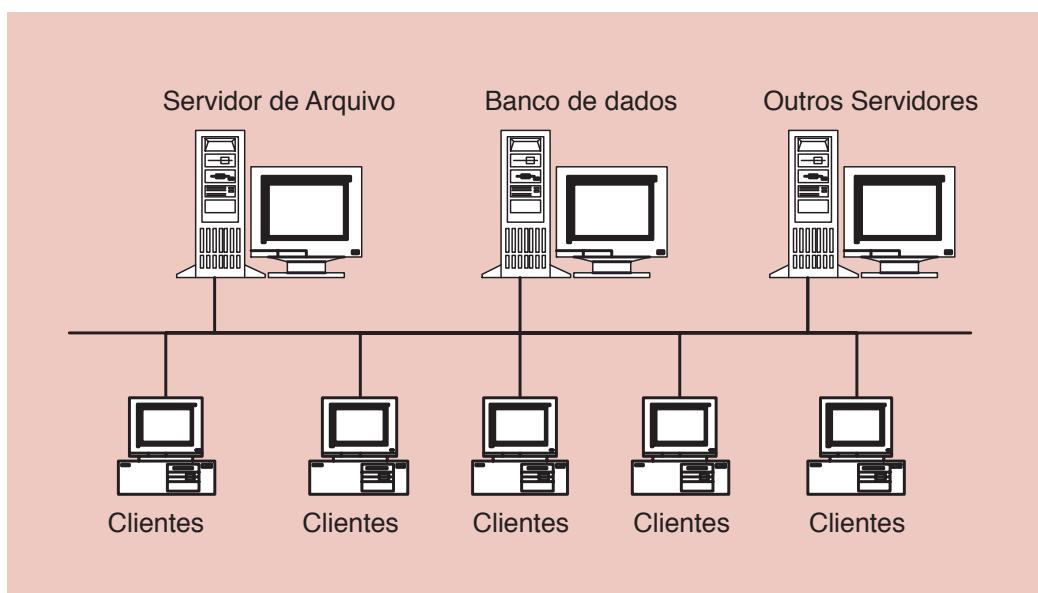


Figura 1.5 O modelo Cliente/Servidor de duas camadas.

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 dois ou mais processadores), com grande quantidade de memória RAM e grande capacidade de armazenamento em disco. Os servidores normalmente rodam um Sistema Operacional específico para servidor, como por exemplo um dos sistemas operacionais listados a seguir:

- ◆ Alguma versão do UNIX: AIX, HP-UX, SCO, etc.
- ◆ Novell
- ◆ Linux
- ◆ Windows NT Server (3.51, 4.0)
- ◆ Windows 2000 Server
- ◆ Windows Server 2003

Nos servidores ficam os recursos a serem acessados pelas estações de trabalho da rede, como por exemplo pastas compartilhadas, impressoras compartilhadas, páginas da Intranet da empresa, aplicações empresariais, bancos de

dados, etc. Como o próprio nome sugere, o servidor “Serve” recursos e serviços que serão utilizados pelas estações de trabalho da rede, as quais são chamadas de estações cliente ou simplesmente clientes.

Nas estações de trabalho dos usuários (conhecidas como clientes), são instalados programas, que fazem acesso a recursos disponibilizados pelos servidores. O exemplo mais típico de aplicação Cliente/Servidor, é uma aplicação desenvolvida em Visual Basic ou Delphi, a qual acessa dados de um servidor SQL Server 2000, instalado em um servidor da rede. No diagrama da Figura 1.5, temos um exemplo onde estão sendo utilizados três servidores:

- ◆ Servidor de arquivos
- ◆ Servidor de banco de dados
- ◆ Servidor para outras funções (autenticação de usuários, resolução de nomes, Intranet, etc).

O modelo Cliente/Servidor pareceu, no início, ser uma solução definitiva em substituição ao modelo baseado no 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, conforme descreveremos mais adiante. Para entender o porquê deste custo elevado, é preciso falar um pouco sobre o modelo de aplicações em duas camadas, também conhecido como Cliente/Servidor clássico e todos os seus problemas.

## Modelo em 2 camadas

No início 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 Power Builder, são instalados em cada estação de trabalho - Cliente. Este programa acessa dados em um servidor de banco de dados, conforme ilustrado na Figura 1.6:

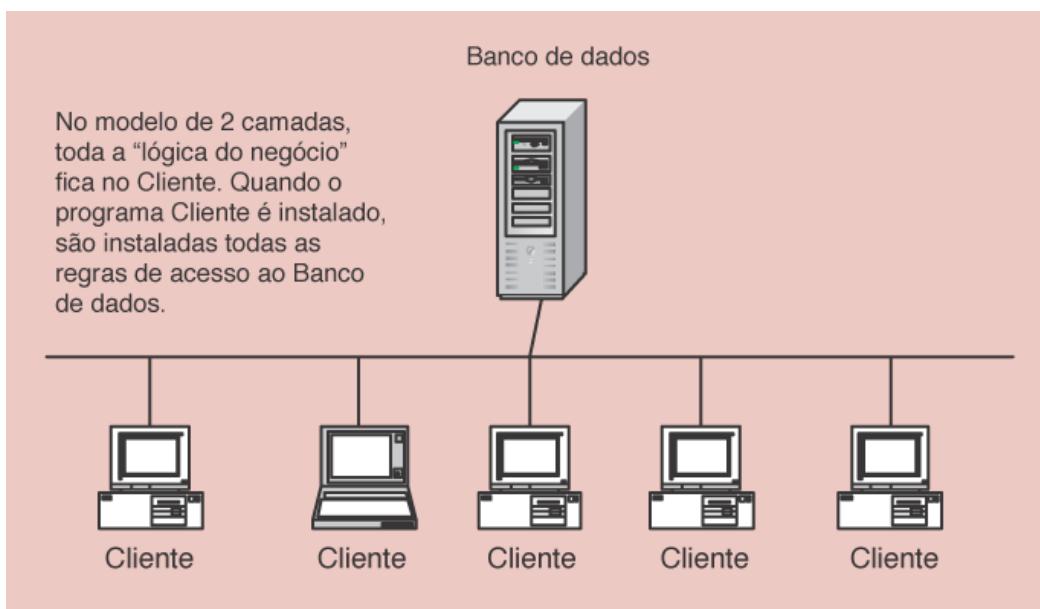


Figura 1.6 O Modelo de desenvolvimento em duas camadas.

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. Na maioria dos casos, a máquina do cliente é um PC rodando Windows, e a aplicação Cliente é desenvolvida utilizando-se um dos ambientes conhecidos, conforme citado anteriormente. Sendo a aplicação cliente, um programa para Windows (na grande maioria dos casos), esta deve ser

instalada em cada um das estações de trabalho da rede. É o processo de instalação normal, para qualquer aplicação Windows. No modelo de 2 camadas, a aplicação Cliente é responsável pelas seguintes funções:

- ◆ **Apresentação:** O Código que gera a Interface visível do programa, faz parte da aplicação 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 todos 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. Aí que começam a surgir os problemas no modelo em 2 camadas: Uma simples alteração de interface, é suficiente para gerar a necessidade de atualizar a aplicação, em centenas ou milhares de estações de trabalho, 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 da entrada de dados, como o cálculo do dígito verificador de um CPF ou CNPJ, até funções mais complexas, como descontos escalonados para os maiores clientes, de acordo com o volume da compra. Questões relativas a legislação fiscal e escrita contábil, também fazem parte da Lógica do Negócio. Por exemplo, um programa para gerência de Recursos Humanos, desenvolvido para a legislação dos EUA, não pode ser utilizado, sem modificações, por uma empresa brasileira. Isso acontece porque a legislação dos EUA é diferente da legislação brasileira. Em síntese, as regras para o sistema de Recursos humanos são diferentes. Alterações nas regras do negócio são bastante freqüentes, ainda mais com as repetidas mudanças na legislação do 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, todos as estações de trabalho que possuem a versão anterior, devem receber a nova versão, para que o usuário possa ter acesso as alterações. Agora temos mais um sério problema no modelo de 2 camadas: Qualquer alteração nas regras do negócio (o que ocorre com freqüência), é suficiente para gerar a necessidade de atualizar a aplicação, em centenas ou milhares de computadores. O que já era complicado, piorou um pouco mais.

A outra camada, no modelo de 2 camadas, é o Banco de dados, o qual fica armazenado no Servidor de banco de dados. Por exemplo, um servidor com o Windows Server 2003 e com o SQL Server 2000, no qual estão os bancos de dados utilizados pelos aplicativos Cliente/Servidor da empresa.

Com a evolução do mercado e as alterações da legislação, mudanças nas regras do negócio são bastante freqüentes. Com isso o modelo de duas camadas, demonstrou-se de difícil manutenção e gerenciamento, além de apresentar um TCO – Total Cost 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. Alguns cálculos chegaram a apontar que o custo para manter um PC em rede, por ano, fica na casa dos US\$ 10.000 (é dólares mesmo).

Na prática este custo mostrou-se impraticável. Sempre que um determinado modelo apresenta problemas, aparentemente intransponíveis, a indústria de informática parte para a criação de novos modelos. Em busca de soluções para os problemas do modelo de duas camadas, é que surgiu a proposta do modelo de 3 camadas, conforme analisaremos a seguir.

Para que você possa entender como a evolução partiu do mundo baseado no Mainframe, para uma tentativa de um mundo baseado completamente no modelo Cliente/Servidor e acabou por chegar a um modelo misto, vou detalhar o modelo de aplicações Web, baseado em 3 ou mais camadas.

## Aplicações 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 agora começam a ser centralizadas novamente nos servidores da rede), o qual é chamado de Servidor de Aplicações. O acesso ao banco de dados é feito através das regras contidas no Servidor de Aplicações. 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 1.7, nos dá uma visão geral do modelo em 3 camadas:

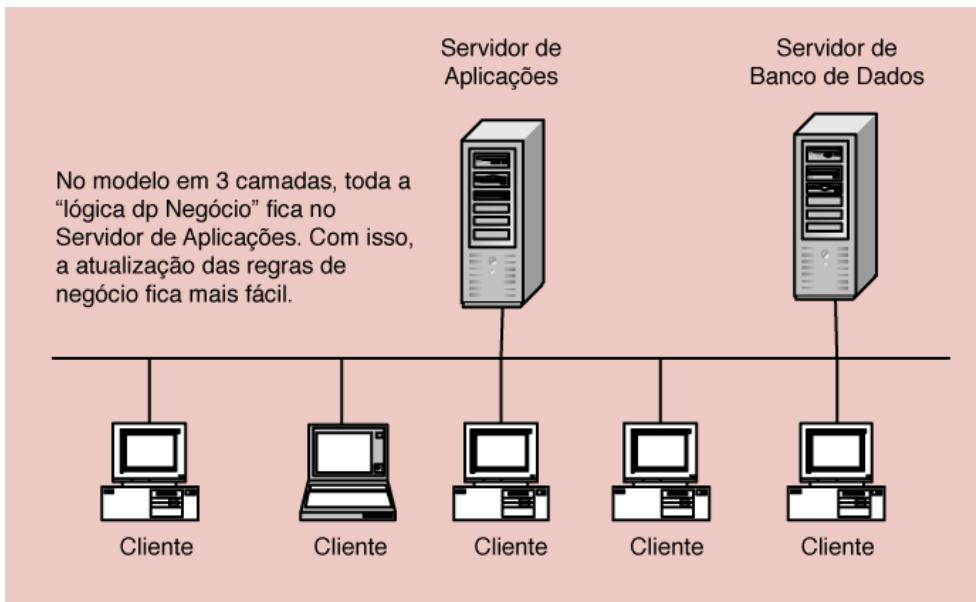


Figura 1.7 O Modelo de desenvolvimento em três camadas.

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 todos 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. Desta maneira, quando uma regra do negócio for alterada, basta atualizá-la no 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. Vejam que ao centralizar as regras do negócio em um Servidor de Aplicações, estamos facilitando a tarefa de manter a aplicação atualizada. As coisas estão começando a melhorar.
- ◆ **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 centenas ou milhares de estações de trabalho, toda vez que uma regra do negócio for alterada. Porém continuamos com o problema de atualização da interface da aplicação, cada vez que sejam necessárias mudanças na Interface. Por isso que surgiram os modelos de n-camadas.

No próximo tópico, vou falar um pouco sobre o modelo de 4 camadas.

## Aplicações em quatro camadas.

Como uma evolução do modelo de três camadas, surge o modelo de quatro camadas. A idéia básica do modelo de 4 camadas, é retirar a apresentação do cliente e centralizá-las em um determinado ponto (agora está ainda mais parecido com a época do Mainframe, onde a aplicação ficava residente no mainframe e era acessada via terminal burro), 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 ou o Netscape Navigator. A Figura 1.8, nos dá uma visão geral do modelo em quatro camadas:

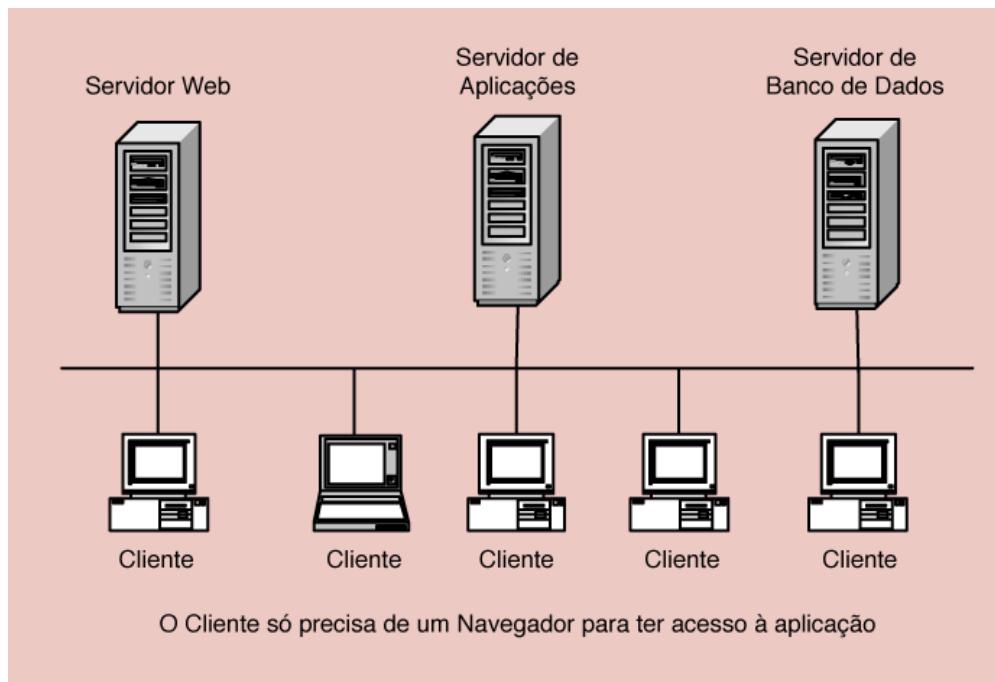


Figura 1.8 O Modelo de desenvolvimento em quatro camadas.

Para acessar a aplicação, o cliente acessa o endereço da aplicação, utilizando o seu navegador, como no exemplo a seguir:

<http://intranet.minhaempresa.com/sistemas/vendas.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:** Nesta caso o Cliente é o Navegador utilizado pelo usuário, quer seja o Internet Explorer, quer seja o Netscape Navigator, ou outro navegador qualquer.
- ◆ **Apresentação:** Passa a ser disponibilizada pelo Servidor Web. A interface pode ser composta de páginas HTML, ASP, PHP, Flash ou qualquer outra tecnologia capaz de gerar conteúdo para o navegador. Com isso alterações na interface da aplicação, são feitas diretamente no servidor Web, sendo que estas alterações estarão, automaticamente,

disponíveis para todos os Clientes (parece ou não parece Mainframe, com o Navegador fazendo o papel do terminal de acesso?). 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 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. Após a atualização, todos os usuários passarão a ter acesso a nova versão, sem que seja necessário reinstalar o programa em cada estação de trabalho da rede. Vejam que ao centralizar as regras do negócio em um Servidor de Aplicações, estamos facilitando a tarefa de manter a aplicação atualizada.
- ◆ **Dados:** Nesta camada temos o servidor de banco de dados, no qual reside toda a informação necessária para o funcionamento da aplicação.

Com o deslocamento da camada de apresentação para um Servidor Web, resolvemos o problema de termos que atualizar a aplicação, em centenas ou milhares de computadores, cada vez que uma interface precisar de alterações. Neste ponto a atualização das aplicações é uma tarefa mais gerenciável, muito diferente do que acontecia no caso do modelo em 2 camadas.

Os servidores de Aplicação, Web e banco de dados, não precisam, necessariamente ser servidores separados, isto é, uma máquina 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, um Servidor de aplicações, um servidor Web e um servidor de banco de dados. Claro que questões de desempenho devem ser levadas em consideração.

Também podemos ter a funcionalidade do Servidor de Aplicações distribuída através de vários servidores, com cada servidor tendo alguns componentes que formam parte das funcionalidades da aplicação. Este modelo onde temos componentes em diversos equipamentos, é conhecido como Modelo de Aplicações Distribuídas. Também podemos colocar os componentes em mais do que um servidor para obter um melhor desempenho, ou redundância, no caso de um servidor falhar.

## O Júlio ficou louco ou estamos voltando ao Mainframe?

Amigo leitor, nem uma, nem outra. Você deve estar utilizando os seguintes passos de raciocínio, baseado no texto que acabou de ler:

1. Na época do Mainframe os aplicativos e os dados ficavam no Mainframe. O acesso era feito através de terminais, conhecidos como terminais burros. A administração era feita centralizadamente, o que facilitava a atualização e manutenção das aplicações.
2. No modelo Cliente/Servidor clássico a aplicação e a lógica ficava no programa instalado na estação de trabalho cliente e os dados no servidor de banco de dados. Isso gera dificuldades para atualização das aplicações e um elevado custo para manter este modelo funcionando.
3. A nova tendência é portar as aplicações para um modelo de n camadas, onde as aplicações, a lógica e os dados ficam em servidores (de aplicações, Web e de banco de dados) e o acesso é feito através de um Navegador.
4. Puxa, mas o modelo em n camadas é praticamente o mesmo modelo do Mainframe, com aplicações e dados no servidor, administração centralizada e redução no custo de propriedade (TCO) em relação ao modelo Cliente/Servidor tradicional? É isso mesmo, este modelo é muito próximo do modelo do Mainframe, porém com todas as vantagens da evolução da informática nestas últimas décadas, tais como interfaces gráficas, programas mais poderosos e por aí vai.

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 da época do Mainframe.

Posso citar o exemplo de um dos bancos com os quais trabalho. Quando vou ao banco renovar um seguro ou tratar algum assunto diretamente com o gerente, vejo que ele tem na sua estação de trabalho, aplicativos de produção do dia-a-dia, tais como o Microsoft Word, Microsoft Excel, um aplicativo de cálculos e análise de crédito e assim por diante. Este mesmo gerente utiliza o site da empresa para fornecer informações. Ele também utiliza a Intranet da empresa para se manter atualizado. Além disso ele utiliza alguns sistemas que ainda residem no bom e velho mainframe. Por exemplo, quando eu peço que ele faça uma alteração no meu endereço de correspondência, ela acessa a famosa telinha verde, de um programa emulador de terminal, que acessa uma aplicação que está no Mainframe da empresa.

Este caminho me parece muito mais sensato, ou seja, não precisa ser um ou outro modelo, mas sim o melhor dos dois mundos.

Agora que você já sabe sobre os modelos de redes e de desenvolvimento de aplicações utilizados nas empresas, é hora de falar sobre o papel do Windows Server 2003 nestas redes.

## Papel do Windows Server 2003 na rede da sua empresa

### Onde entra o Windows Server 2003 neste história?

O Windows Server 2003 foi projetado para ser o sistema operacional dos servidores da rede da empresa. Como sistema operacional para servidor, ele é capaz de ser configurado para desempenhar diferentes tipos de funções, desde um simples servidor de arquivos e de impressão, até um sofisticado servidor de acesso remoto, com Firewall de proteção contra ataques vindos da Internet. O que define o papel que um servidor baseado no Windows Server 2003 irá desempenhar é, basicamente, a configuração e os serviços instalados e configurados no servidor.

A seguir descrevo os principais papéis que um servidor com o Windows Server 2003 pode desempenhar na rede da empresa:

- ◆ **Controlador de domínio:** Conhecido resumidamente como DC – Domain Controller, é um servidor onde está instalado o Active Directory. Nos DCs fica uma cópia do banco de dados com diversas informações da rede, tais como nomes de usuários, senhas, nomes de grupos, lista de membros de cada grupo, contas de computadores, políticas de segurança e assim por diante. Nos próximos capítulos você estudará, em detalhes, sobre Domínios e o Active Directory.
- ◆ **Servidor de arquivos e impressão:** Esta é um dos usos mais comuns para um servidor de rede. Os arquivos ficam gravados em pastas compartilhadas no servidor e podem ser acessados por qualquer computador da rede, desde que o usuário tenha as devidas permissões de acesso. O mesmo é válido em relação às impressoras. Posso ter, por exemplo, uma impressora laser colorida, de alto desempenho e qualidade, instalada e compartilhada em um servidor.
- ◆ **Servidor DNS, WINS e DHCP:** O DNS e o WINS são serviços para resolução de nomes em uma rede. O DNS é que faz a tradução de um endereço como por exemplo [www.juliobattisti.com.br](http://www.juliobattisti.com.br), para o respectivo endereço IP. O WINS é utilizado por questões de compatibilidades com as versões do Windows mais antigas, tais como Windows 95, 98 ou Me. O serviço DHCP é utilizado para fazer a configuração automática do protocolo TCP/IP nas estações de trabalho da rede. No Capítulo 16, do meu livro: Windows Server 2003 – Curso Completo, 1568 páginas, você aprende a instalar, configurar e administrar os serviços DNS, WINS e DHCP.

- ◆ **Servidor Web:** Com o IIS 6.0 o Windows Server 2003 pode atuar como um poderoso servidor Web, disponibilizando serviços de hospedagem de páginas (http), cópia de arquivos (ftp) e hospedagem de aplicações baseadas em tecnologias como ASP ou tecnologias mais atuais, como Web Services e ASP.NET. Você pode utilizar o Windows Server 2003 e o IIS 6.0 para criar um servidor Web para a Intranet da empresa ou para suportar o site da empresa na Internet. Com o Windows Server 2003 Data Center Edition e a tecnologia de Cluster, você pode utilizar o Windows Server 2003 para criar sites que suportam elevado número de acessos e grande número de usuários simultaneamente. Como exemplo basta citar o site da Microsoft ([www.microsoft.com](http://www.microsoft.com)), um dos mais visitados do mundo, o qual é grande parte baseado no Windows Server 2003 (algumas áreas, no momento em que escrevo este livro, ainda estão baseadas no Windows 2000 Server).
- ◆ **Servidor de banco de dados:** Neste caso temos um servidor com o Windows Server 2003 e o SQL Server 2000 instalados. O SQL Server 2000 é o servidor de banco de dados relacionais da Microsoft. Oferece funcionalidades avançadas como replicação de dados, stored procedures, acesso a diferentes fontes de dados, múltiplas instâncias em um único servidor, mecanismo de segurança refinado e integrado com o Windows Server 2003, transações distribuídas, etc. Podemos acessar os dados de um servidor SQL Server 2000, no formato XML, utilizando um navegador, através do protocolo HTTP. O SQL Server 2000 é projetado para ser instalado no Windows Server 2003, Windows 2000 Server ou NT Server 4.0.

Para maiores informações sobre o SQL Server 2000, consulte as seguintes fontes:

- ◆ <http://www.microsoft.com/sql>
- ◆ Livro: “SQL Server 2000 Administração e Desenvolvimento: Curso Completo”, de minha autoria, publicado pela editora Axcel Books ([www.axcel.com.br](http://www.axcel.com.br)).
- ◆ **Servidor de e-mail:** Neste caso além do Windows Server 2003 deve ser instalado o Exchange Server 2000. O Exchange Server 2000 É um servidor de mensagens e correio eletrônico, além de uma plataforma para desenvolvimento de aplicações do Workflow. Cada vez mais o Exchange vem ganhando mercado de concorrentes como o Lotus Notes da IBM e o Novel Groupwise da Novel. O Exchange 2000 é completamente integrado com o Active Directory do Windows 2000 Server ou Windows Server 2003, o que facilita a criação e manutenção de contas de usuários. O suporte ao padrão de dados XML também foi introduzido nesta versão do Exchange. Maiores informações sobre Exchange podem ser encontradas nos seguintes endereços:
  - ◆ <http://www.microsoft.com/exchange>
  - ◆ <http://www.swynk.com>
- ◆ **Servidor de comunicação e acesso remoto:** O Windows Server 2003 oferece o serviço RRAS – Routing and Remote Access Service, o qual permite que o Windows Server 2003 atue como um servidor de acesso remoto, para o qual usuários com notebooks ou outros dispositivos, equipados com modem, podem discar e se conectar à rede da empresa, tendo acesso aos recursos da rede, como se estivessem conectados localmente.

A seguir descrevo outros produtos da Microsoft que podem ser instalados em um servidor baseado no Windows Server 2003 e que fazem com que o servidor assuma diferentes papéis e funções na rede da empresa:

- ◆ **BizTalk Server 2000:** Este talvez seja um dos produtos da Microsoft, menos conhecidos. Porém considero um produto fundamental, principalmente para os profissionais que estão envolvidos em um projeto para a consolidação das aplicações da empresa. Com a consolidação do comércio eletrônico, principalmente do chamado B2B – Business to Business, que é o comércio entre empresas, cada vez faz-se mais necessária a integração entre sistemas de informação de diferentes empresas. Um dos maiores problemas é que estes diferentes sistemas de informação utilizam diferentes formatos de dados (a repetição da palavra “diferentes” é proposital, para enfatizar o conceito que está sendo exposto). Durante muito tempo, uma das soluções adotadas foi o EDI – Exchange Data Interchange.

Porém o EDI apresenta algumas limitações, além de um custo elevado. Com o advento da Internet e do padrão XML, a troca de informações entre empresas tem migrado para soluções onde o XML é o formato universalmente aceito, o que facilita a troca de informações. O Biztalk Server 2000 é a solução da Microsoft que facilita a criação, desde o modelo conceitual até a implementação, de aplicações baseadas em XML, para troca de informações entre diferentes empresas ou entre diferentes sistemas dentro da mesma empresa. Maiores informações e uma versão de avaliação para download podem ser encontradas no seguinte endereço:

<http://www.microsoft.com/biztalk>

- ◆ **Commerce Server 2000:** O Commerce Server trabalha em conjunto com o IIS. Na verdade o Commerce Server facilita a criação e o gerenciamento de uma site para comércio eletrônico, quer seja B2C – Business to Consumer, quer seja B2B – Business to Business. Através de uma série de modelos prontos e através da utilização de assistentes, podemos rapidamente criar um site para comércio eletrônico. Após a criação, é possível personalizar o site de acordo com as necessidades da empresa. Pode trabalhar integrado com os demais servidores.NET. Por exemplo, você pode utilizar o SQL Server 2000 para armazenar informações sobre o catálogo de produtos, preços e estoque. Maiores informações e uma versão de avaliação para download podem ser encontradas no seguinte endereço:

<http://www.microsoft.com/commerceserver>

- ◆ **Application Center 2000:** O Application Center 2000 é a ferramenta da Microsoft para a implementação e gerenciamento de Web sites que deverão suportar uma elevada carga de acesso, com um grande número de acessos simultâneos. Também oferece ferramentas para a distribuição de um site entre diversos servidores, com o objetivo de distribuir a carga entre diversos equipamentos. Com o uso do Application Center fica mais fácil realizar tarefas como por exemplo manter sincronizado o conteúdo dos diversos servidores, bem como fazer o gerenciamento e a distribuição de cargas.
- ◆ **Host Integration Server 2000:** Esta é a nova versão do antigo SNA Server da Microsoft, só que com o nome alterado. O Host Integration Server possibilita a integração de redes Windows com outros ambientes, como por exemplo, Mainframes baseados na arquitetura SNA da IBM. Esta é mais uma ferramenta que comprova que hoje as empresas procuram utilizar o melhor dos dois mundos (Mainframe e Cliente/Servidor), integrando as aplicações Cliente/Servidor com as aplicações no Mainframe. Maiores informações e uma versão de avaliação para download podem ser encontradas no seguinte endereço:

<http://www.microsoft.com/hiserver>

- ◆ **Internet Security and Acceleration Server 2000:** De certa maneira é o sucessor do Proxy Server 2.0 da Microsoft, com algumas melhorias. É utilizado para conectar a rede local da empresa, de uma maneira segura, à Internet, funcionando como um Firewall de proteção. Suas funções básicas são as seguintes:
  - ◆ Firewall
  - ◆ Cache de páginas

Maiores informações e uma versão de avaliação para download podem ser encontradas no seguinte endereço:  
<http://www.microsoft.com/isaserver>

- ◆ **Mobile Information 2001 Server:** O Framework.NET (que faz parte do Windows Server 2003) não foi concebido apenas para o desenvolvimento de aplicações que serão acessadas através de PCs ligados em rede ou computadores tradicionais. Com o Framework.NET, a Microsoft pretende fornecer uma sólida plataforma de desenvolvimento, também para os diversos dispositivos móveis existentes, tais como telefones celulares, assistentes pessoais, Palm Pilots, etc. Dentro desta estratégia, o Mobile Information 2001 Server desempenha um papel fundamental, fornecendo suporte ao protocolo WAP 1.1. Usando o Mobile Information 2001 Server

é possível, por exemplo, fazer com que as suas mensagens do Exchange sejam convertidas para o formato que possam ser lidas por um celular ou qualquer outro dispositivo habilitado ao protocolo WAP

Maiores informações e uma versão de avaliação para download podem ser encontradas no seguinte endereço:

<http://www.microsoft.com/servers/miserver/default.htm>

## O Protocolo TCP/IP

Neste capítulo você já aprendeu sobre redes, sobre o modelo Baseado no Mainframe, a evolução em direção ao Cliente/Servidor e os modernos modelos baseados em aplicações de 3 ou mais camadas. Neste item vou apresentar os princípios básicos do protocolo TCP/IP. Os conhecimentos deste item serão importantes (e necessários) em diversos capítulos deste livro e também para a resolução de questões básicas de rede, para o Exame 70-290.

### Uma visão geral do protocolo TCP/IP

Vou iniciar fazendo uma apresentação do protocolo TCP/IP, de tal maneira que o leitor possa entender exatamente o que é o TCP/IP e como é configurada uma rede baseada neste protocolo. Nos demais tópicos deste item, abordarei os seguintes tópicos:

- ◆ O Sistema Binário de Numeração.
- ◆ Conversão de Binário para Decimal.
- ◆ Endereços IP e Máscara de sub-rede.
- ◆ Classes de redes e Endereçamento no protocolo IP
- ◆ Aspectos básicos de Roteamento.

Para que os computadores de uma rede possam trocar informações é necessário que todos adotem as mesmas regras para o envio e o recebimento de informações. Este conjunto de regras é conhecido como Protocolo de comunicação. Falando de outra maneira podemos afirmar:

*“Para que os computadores de uma rede possam trocar informações entre si é necessário que todos estejam utilizando o mesmo protocolo”.*

No protocolo de comunicação estão definidas todas as regras necessárias para que o computador de destino, “entenda” as informações no formato que foram enviadas pelo computador de origem. Dois computadores com protocolos diferentes instalados, não serão capazes de estabelecer uma comunicação e trocar informações.

Antes da popularização da Internet existiam diferentes protocolos sendo utilizados nas redes das empresas. Os mais utilizados eram os seguintes:

- ◆ TCP/IP
- ◆ NETBEUI
- ◆ IPX/SPX
- ◆ Apple Talk

Se colocarmos dois computadores ligados em rede, um com um protocolo, por exemplo o TCP/IP e o outro com um protocolo diferente, por exemplo NETBEUI, estes dois computadores não serão capazes de estabelecer comunicação e trocar informações. Por exemplo, o computador com o protocolo NETBEUI instalado, não será capaz de acessar uma pasta ou uma Impressora compartilhada no computador com o protocolo TCP/IP instalado.

À medida que a Internet começou, a cada dia, tornar-se mais popular, com o aumento exponencial do número de usuários e de servidores ligados em rede, o protocolo TCP/IP passou a tornar-se um padrão de fato, utilizado não só na Internet, como também nas redes internas das empresas, redes estas que começavam a ser conectadas à Internet. Como as redes internas precisavam conectar-se à Internet, tinham que usar o mesmo protocolo da Internet, ou seja: TCP/IP.

Dos principais Sistemas Operacionais do mercado, o UNIX sempre utilizou o protocolo TCP/IP como padrão. O Windows dá suporte ao protocolo TCP/IP desde as primeiras versões, porém o TCP/IP somente tornou-se o protocolo padrão a partir do Windows 2000. No Windows Server 2003 o TCP/IP é instalado automaticamente e não pode ser desinstalado (esta é uma das novidades do Windows Server 2003).

Ser o protocolo padrão significa que o TCP/IP será instalado durante a instalação do Sistema Operacional, a não ser que um protocolo diferente seja selecionado. Até

mesmo o Sistema Operacional Novell, que sempre foi baseado no IPX/SPX como protocolo padrão, passou a adotar o TCP/IP como padrão a partir da versão 5.0.

O que temos hoje, na prática, é a utilização do protocolo TCP/IP na esmagadora maioria das redes. Sendo a sua adoção cada vez maior. Como não poderia deixar de ser, o TCP/IP é o protocolo padrão do Windows 2000, do Windows XP e também do Windows Server 2003.

Agora passaremos a estudar algumas características do protocolo TCP/IP. Veremos que cada equipamento que faz parte de uma rede baseada no TCP/IP tem alguns parâmetros de configuração que devem ser definidos, para que o equipamento possa comunicar-se com sucesso na rede e trocar informações com os demais equipamentos da rede.

## Configurações do protocolo TCP/IP para um computador em rede

Quando utilizamos o protocolo TCP/IP como protocolo de comunicação em uma rede de computadores, temos alguns parâmetros que devem ser configurados em todos os equipamentos (computadores, servidores, hubs, switchs, impressoras de rede, etc) que fazem parte da rede. Na Figura 1.9 temos uma visão geral de uma pequena rede baseada no protocolo TCP/IP:

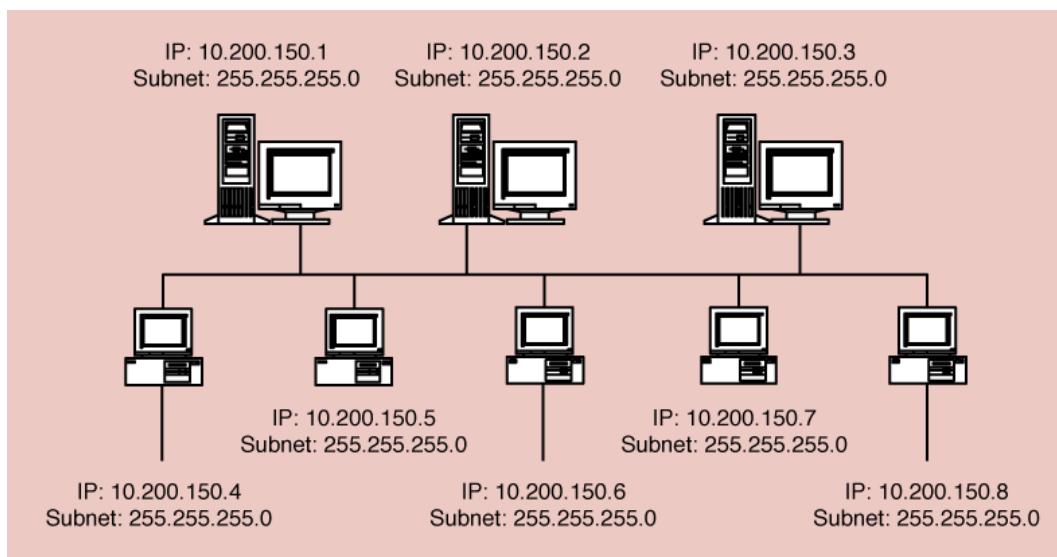


Figura 1.9 Uma rede baseada no protocolo TCP/IP.

**NOTA:** Para pequenas redes, não conectadas à Internet, é recomendada a adoção do protocolo NETBEUI, devido a sua simplicidade de configuração e facilidade de administração. Porém esta é uma situação muito rara, pois dificilmente teremos uma rede isolada, sem conexão com a Internet ou com parceiros de negócios, como clientes e fornecedores.

No exemplo da Figura 1.9 temos uma rede local para uma pequena empresa. Esta rede local não está conectada a outras redes ou à Internet. Neste caso cada computador da rede precisa de, pelo menos, dois parâmetros do protocolo TCP/IP, configurados:

- ◆ Número IP
- ◆ Máscara de sub-rede.

O Número IP é um número no seguinte formato:

**x.y.z.w**

ou seja, são quatro números separados por ponto. Não podem existir duas máquinas, com o mesmo número IP, dentro da mesma rede. Caso você configure, por engano, um novo equipamento com o mesmo número IP de uma máquina já existente, será gerado um conflito de Número IP e um dos equipamentos, muito provavelmente o novo equipamento que está sendo configurado, não conseguirá se comunicar com a rede. O valor máximo para cada um dos números (x, y, z ou w) é 255.

---

**NOTA:** Você entenderá o porquê deste valor máximo, mais adiante quando for explicado o sistema de numeração binário.

---

Uma parte do Número IP (1, 2 ou 3 dos 4 números) é a identificação da rede, a outra parte é a identificação da máquina dentro da rede. O que define quantos dos quatro números fazem parte da identificação da rede e quantos fazem parte da identificação da máquina é a máscara de sub-rede (subnet mask). Vamos considerar o exemplo de um dos computadores da rede da Figura 2.6:

**Número IP:** 10.200.150.1  
**Subrede:** 255.255.255.0

As três primeiras partes da máscara de sub-rede (subnet) iguais a 255 indicam que os três primeiros números representam a identificação da rede e o último número é a identificação do equipamento dentro da rede. Para o nosso exemplo teríamos a rede: 10.200.150, ou seja, todos os equipamentos do nosso exemplo fazem parte da rede 10.200.150 ou, em outras palavras, o número IP de todos os equipamentos da rede começam com 10.200.150.

Neste exemplo, onde estou utilizando os três primeiros números para identificar a rede e somente o quarto número para identificar o equipamento, temos um limite de 254 equipamentos que podem ser ligados neste rede. Observe que são 254 e não 256, pois o primeiro número – 10.200.150.0 e o último – 10.200.150.255 não podem ser utilizados como números IP de equipamentos da rede. O primeiro é o próprio número da rede: 10.200.150.0 e o último é o endereço de Broadcast: 10.200.150.255. Ao enviar uma mensagem para o endereço de Broadcast, todas as máquinas da rede receberão a mensagem.

Com base no exposto é possível apresentar a seguinte definição:

Para se comunicar em uma rede baseada no protocolo TCP/IP, todo equipamento deve ter, pelo menos, um número IP e uma máscara de sub-rede, sendo que todos os equipamentos da rede devem ter a mesma máscara de sub-rede.

No exemplo da figura 1.9 observe que o computador com o IP 10.200.150.7 está com uma máscara de sub-rede diferente dos demais: 255.255.0.0. Neste caso é como se o computador com o IP 10.200.150.7 pertencesse a outra rede. Na prática o que irá acontecer é que este computador não conseguirá se comunicar com os demais computadores da rede, por ter uma máscara de sub-rede diferente dos demais. Este é um dos erros de configuração mais comuns. Se a máscara de sub-rede estiver incorreta, ou seja, diferente da máscara dos demais computadores da rede, o computador com a máscara de sub-rede incorreta não conseguirá comunicar-se na rede.

Na Tabela 1.3, a seguir temos alguns exemplos de máscaras de sub-rede e do número máximo de equipamentos em cada uma das respectivas redes.

**Tabela 1.3 Exemplos de máscara de sub-rede.**

| Máscara       | Número de equipamentos na rede |
|---------------|--------------------------------|
| 255.255.255.0 | 254                            |
| 255.255.0.0   | 65.534                         |
| 255.0.0.0     | 16.777.214                     |

Quando a rede está isolada, ou seja, não está conectada à Internet ou a outras redes externas, através de links de comunicação de dados, apenas o número IP e a máscara de sub-rede são suficientes para que os computadores possam se comunicar e trocar informações.

A conexão da rede local com outras redes é feita através de linhas de comunicação de dados. Para que essa comunicação seja possível é necessário um equipamento capaz de enviar informações para outras redes e receber informações destas redes. O equipamento utilizado para este fim é o Roteador. Todo pacote de informações que deve ser enviado para outras redes deve, obrigatoriamente, passar pelo Roteador. Todo pacote de informação que vem de outras redes também deve, obrigatoriamente, passar pelo Roteador. Como o Roteador é um equipamento de rede, este também terá um número IP. O número IP do roteador deve ser informado em todos os demais equipamentos que fazem parte da rede, para que estes equipamentos possam se comunicar com as redes externas. O número IP do Roteador é informado no parâmetro conhecido como Default Gateway (Gateway Padrão). Na prática quando configuramos o parâmetro Default Gateway, estamos informando o número IP do Roteador.

Quando um computador da rede tenta se comunicar com outros computadores/servidores, o protocolo TCP/IP faz alguns cálculos utilizando o número IP do computador de origem, a máscara de sub-rede e o número IP do computador de destino (veremos estes cálculos em detalhes, mais adiante neste capítulo). Se, após feitas as contas, for concluído que os dois computadores fazem parte da mesma rede, os pacotes de informação são enviados para o barramento da rede local e o computador de destino captura e processa as informações que lhe foram enviadas. Se, após feitas as contas, for concluído que o computador de origem e o computador de destino, fazem parte de redes diferentes, os pacotes de informação são enviados para o Roteador (número IP configurado como Default Gateway) e o Roteador é o responsável por achar o caminho (a rota) para a rede de destino.

Com isso, para equipamentos que fazem parte de uma rede, baseada no protocolo TCP/IP e conectada a outras redes ou à Internet, devemos configurar, no mínimo, os seguintes parâmetros:

- ◆ Número IP
- ◆ Máscara de sub-rede
- ◆ Default Gateway

Em redes empresariais existem outros parâmetros que precisam ser configurados. Um dos parâmetros que deve ser informado é o número IP de um ou mais servidores DNS – Domain Name System. O DNS é o serviço responsável pela resolução de nomes. Toda a comunicação, em redes baseadas no protocolo TCP/IP é feita através do número IP. Por exemplo, quando vamos acessar um site: <http://www.juliobattisti.com.br/>, tem que haver uma maneira de encontrar

o número IP do servidor onde fica hospedado o site. O serviço que localiza o número IP associado a um nome é o DNS. Por isso a necessidade de informarmos o número IP de pelo menos um servidor DNS, pois sem este serviço de resolução de nomes, muitos recursos da rede estarão indisponíveis.

Existem aplicativos antigos que são baseados em um outro serviço de resolução de nomes conhecido como WINS – Windows Internet Name System. O Windows NT Server 4.0 utilizava intensamente o serviço WINS para a resolução de nomes. A partir do Windows 2000 Server, o serviço utilizado é o DNS, porém podem existir aplicações que ainda dependam do WINS. Nestes casos você terá que instalar e configurar um servidor WINS na sua rede e configurar o IP deste servidor em todos os equipamentos da rede. No Windows Server 2003 o DNS também é o serviço padrão para a resolução de nomes.

As configurações do protocolo TCP/IP podem ser definidas manualmente, isto é, configurando cada um dos equipamentos necessários. Esta é uma solução razoável para pequenas redes, porém pode ser um problema para redes maiores, com um grande número de equipamentos conectados. Para redes maiores é recomendado o uso do serviço DHCP – Dynamic Host Configuration Protocol. O serviço DHCP pode ser instalado em um servidor com o Windows NT Server 4.0, Windows 2000 Server ou Windows Server 2003. Uma vez disponível e configurado, o serviço DHCP fornece todos os parâmetros de configuração do protocolo TCP/IP para os equipamentos conectados à rede. Os parâmetros são fornecidos quando o equipamento é inicializado e podem ser renovados em períodos definidos pelo Administrador. Com o uso do DHCP uma série de procedimentos de configuração podem ser automatizados, o que facilita a vida do Administrador e elimina uma série de erros.

O uso do DHCP também é muito vantajoso quando são necessárias alterações no número IP dos servidores DNS ou WINS. Vamos imaginar uma rede com 1000 computadores e que não utiliza o DHCP, ou seja, os diversos parâmetros do protocolo TCP/IP são configurados manualmente em cada computador. Agora vamos imaginar que o número IP do servidor DNS foi alterado. Neste caso o Administrador e a sua equipe técnica terão que fazer a alteração do número IP do servidor DNS em todas as estações de trabalho da rede. Um serviço e tanto. Se esta mesma rede estiver utilizando o serviço DHCP, bastará alterar o número do servidor DNS, nas configurações do servidor DHCP. O novo número será fornecido para todas as estações da rede, na próxima vez que a estação for reinicializada. Muito mais simples e prático e, principalmente, com menor probabilidade de erros.

Você pode verificar, facilmente, as configurações do protocolo TCP/IP que estão definidas para o seu computador (Windows 2000, Windows XP ou Windows Server 2003). Para isso siga os seguintes passos:

1. Faça o logon.
2. Abra o Prompt de comando: Iniciar -> Todos os Programas -> Acessórios -> Prompt de comando.
3. Na janela do Prompt de comando digite o seguinte comando:  
**ipconfig/all**  
e pressione Enter
4. Serão exibidas as diversas configurações do protocolo TCP/IP, conforme indicado a seguir, no exemplo obtido a partir de um dos meus computadores da rede que eu utilizo em casa:

---

**NOTA: No Capítulo 16 do livro: Windows Server 2003 – Curso Completo, 1568 páginas, você aprende a instalar, configurar e administrar o DNS.**

---

---

**NOTA: No Capítulo 16 do livro: Windows Server 2003 – Curso Completo, 1568 páginas, você aprende a instalar, configurar e administrar o DHCP.**

---

## Configuração de IP do Windows

```
Nome do host.....: servidor01      Sufixo DNS primário.....: groza.com      Tipo
de nó.....: híbrido            Roteamento de IP ativado.....: não       Proxy WINS
ativado.....: não              Lista de pesquisa de sufixo DNS..: groza.com
Adaptador Ethernet Conexão local:
Sufixo DNS específico de conexão.: Descrição.....: Realtek RTL8139
Family PCI Fast Ethernet NIC      Endereço físico.....: 00-E0-7D-9F-6B-7C
DHCP ativado.....: Não           Endereço IP.....: 10.204.123.2
Máscara de sub-rede.....: 255.255.255.0   Gateway padrão.....:
10.204.123.100
Servidores DNS.....: 10.204.123.1      10.204.123.3      Servidor WINS
primário.....: 10.204.123.1
```

O comando ipconfig exibe informações para as diversas interfaces de rede instaladas – placa de rede, modem, etc. No exemplo anterior temos uma única interface de rede instalada, a qual é relacionada com uma placa de rede Realtek RTL8139 Family PCI Fast Ethernet NIC. Observe que temos o número IP para dois servidores DNS e para um servidor WINS. Outra informação importante é o Endereço físico, mais conhecido como MAC-Address ou endereço da placa. O MAC-Address é um número que identifica a placa de rede. Os seis primeiros números/letras são uma identificação do fabricante e os seis últimos uma identificação da placa. Não existem duas placas com o mesmo MAC-Address, ou seja, este endereço é único para cada placa de rede.

No exemplo da listagem a seguir, temos um computador com duas interfaces de rede. Uma das interfaces é ligada a placa de rede (Realtek RTL8029(AS) PCI Ethernet Adapter), a qual conecta o computador a rede local. A outra interface é ligada ao fax-modem (WAN (PPP/SLIP) Interface), o qual conecta o computador à Internet. Para o protocolo TCP/IP a conexão via Fax modem aparece como se fosse mais uma interface de rede, conforme pode ser conferido na listagem a seguir:

## Configuração de IP do Windows

```
Nome do host.....: servidor
Sufixo DNS primário.....: groza.com
Tipo de nó.....: Híbrida

Roteamento de IP ativado.....: Não
Proxy WINS ativado.....: Não
Lista de pesquisa de sufixo DNS..: groza.com

Ethernet adaptador Conexão de rede local:
Sufixo DNS específico de conexão.: groza.com
Descrição.....: Realtek RTL8029(AS) PCI Ethernet Adapter
Endereço físico.....: 00-00-21-CE-01-11
DHCP ativado.....: Não
Endereço IP.....: 10.204.123.1
Máscara de sub-rede.....: 255.255.255.0
Gateway padrão.....:
Servidores DNS.....: 10.204.123.1
Servidor WINS primário.....: 10.204.123.1

PPP adaptador TERRAPREMIUM:
Sufixo DNS específico de conexão. :
Descrição.....: WAN (PPP/SLIP) Interface
Endereço físico.....: 00-53-45-00-00-00
DHCP ativado.....: Não
Endereço IP.....: 200.176.166.146
Máscara de sub-rede.....: 255.255.255.255
Gateway padrão.....: 200.176.166.146
Servidores DNS.....: 200.176.2.10
                                         200.177.250.10
NetBIOS por Tcpip.....: Desativado
```

Bem, estes são os aspectos básicos do TCP/IP. Nos endereços a seguir, você encontra tutoriais, em português, onde você poderá aprofundar os seus estudos sobre o protocolo TCP/IP:

<http://www.juliobattisti.com.br/tcpip.asp>

[http://www.guiadohardware.info/tutoriais/enderecamento\\_ip/index.asp](http://www.guiadohardware.info/tutoriais/enderecamento_ip/index.asp)

[http://www.guiadohardware.info/curso/redes\\_guia\\_completo/22.asp](http://www.guiadohardware.info/curso/redes_guia_completo/22.asp)

[http://www.guiadohardware.info/curso/redes\\_guia\\_completo/23.asp](http://www.guiadohardware.info/curso/redes_guia_completo/23.asp)

[http://www.guiadohardware.info/curso/redes\\_guia\\_completo/28.asp](http://www.guiadohardware.info/curso/redes_guia_completo/28.asp)

<http://www.aprendaemcasa.com.br/tcpip1.htm>

<http://www.aprendaemcasa.com.br/tcpip2.htm> (estes endereços vão até o `tcpip46.htm`, sendo um curso gratuito OnLine sobre TCP/IP no Windows 2000).

<http://www.vanquish.com.br/site/020608>

[http://unsekurity.virtualave.net/texto1/texto\\_tcpip\\_basico.txt](http://unsekurity.virtualave.net/texto1/texto_tcpip_basico.txt)

<http://unsekurity.virtualave.net/texto1/tcpipI.txt>

[http://www.rota67.hpg.ig.com.br/tutorial/protocolos/amfhp\\_tcpip\\_basico001.htm](http://www.rota67.hpg.ig.com.br/tutorial/protocolos/amfhp_tcpip_basico001.htm)

[http://www.rota67.hpg.ig.com.br/tutorial/protocolos/amfhp\\_tcpip\\_av001.htm](http://www.rota67.hpg.ig.com.br/tutorial/protocolos/amfhp_tcpip_av001.htm)

<http://www.geocities.com/ResearchTriangle/Thinktank/4203/doc/tcpip.zip>

A seguir coloco um exemplo de questão típica, envolvendo os conhecimentos básicos do protocolo TCP/IP, que cai em exames de Certificação da Microsoft e de outros fabricantes:

Questão de exemplo para os exames de Certificação:

Questão: A seguir estão as configurações básicas do TCP/IP de três estações de trabalho: micro01, micro02 e micro03.

◆ Configurações do micro01:

Número IP: 100.100.100.3

Máscara de sub-rede: 255.255.255.0

Gateway: 100.100.100.1

◆ Configurações do micro02:

Número IP: 100.100.100.4

Máscara de sub-rede: 255.255.240.0

Gateway: 100.100.100.1

◆ Configurações do micro03:

Número IP: 100.100.100.5

Máscara de sub-rede: 255.255.255.0

Gateway: 100.100.100.2

O micro 02 não está conseguindo comunicar com os demais computadores da rede. Já o micro03 consegue comunicar-se na rede local, porém não consegue se comunicar com nenhum recurso de outras redes, como por exemplo a Internet. Quais alterações você deve fazer para que todos os computadores possam se comunicar normalmente, tanto na rede local quanto com as redes externas?

- a) Altere a máscara de sub-rede do micro02 para 255.255.255.0

Altere o Gateway do micro03 para 100.100.100.1

- b) Altere a máscara de sub-rede do micro01 para 255.255.240.0  
Altere a máscara de sub-rede do micro03 para 255.255.240.0
- c) Altere o Gateway do micro01 para 100.100.100.2  
Altere o Gateway do micro02 para 100.100.100.2
- d) Altere o Gateway do micro03 para 100.100.100.1
- e) Altere a máscara de sub-rede do micro02 para 255.255.255.0

Resposta certa: a

Comentários: Pelo enunciado o computador micro02 não consegue comunicar com nenhum outro computador da rede. Este é um sintoma típico de problema na máscara de sub-rede. É exatamente o caso, o micro02 está com uma máscara de sub-rede 255.255.240.0, diferente da máscara dos demais computadores. Por isso ele está isolado na rede. Já o micro03 não consegue comunicar-se com outras redes, mas consegue comunicar-se na rede local. Este é um sintoma de que a configuração do Default Gateway está incorreta. Por isso a necessidade de alterar a configuração do Gateway do micro03, para que este utilize a mesma configuração dos demais computadores da rede. Observe como esta questão testa apenas conhecimentos básicos do TCP/IP, tais como Máscara de sub-rede e Default Gateway.

## Sistema de numeração binário

Neste tópico apresentarei os princípios básicos do sistema de numeração binário. Também mostrarei como realizar cálculos simples e conversões de Binário para Decimal e vice-versa. Feita a apresentação das operações básicas com números binários, mostrarei como o TCP/IP através de cálculos binários e, com base na máscara de sub-rede (subnet mask), determina se dois computadores estão na mesma rede ou fazem parte de redes diferentes.

Vou iniciar falando do sistema de numeração decimal, para depois fazer uma analogia ao apresentar o sistema de numeração binário. Todos nós conhecemos o sistema de numeração decimal, no qual são baseados os números que usamos no nosso dia-a-dia, como por exemplo: 100, 259, 1450 e assim por diante. Você já parou para pensar porque este sistema de numeração é chamado de sistema de numeração decimal?

Não? Bem, a resposta é bastante simples: este sistema é baseado em dez dígitos diferentes, por isso é chamado de sistema de numeração decimal. Todos os números do sistema de numeração decimal são escritos usando-se uma combinação dos seguintes dez dígitos:

0    1    2    3    4    5    6    7    8    9

Dez dígitos = Sistema de numeração decimal.

Vamos analisar como é determinado o valor de um número do sistema de numeração decimal. Por exemplo, considere o seguinte número:

**4538**

O valor deste número é formado, multiplicando-se os dígitos do número, de trás para frente (da direita para a esquerda), por potências de 10, começando com  $10^0$ . O último dígito (bem à direita) é multiplicado por  $10^0$ , o penúltimo por  $10^1$ , o próximo por  $10^2$  e assim por diante. o valor real do número é a soma destas multiplicações. Observe o esquema indicado na Figura 1.10 que será bem mais fácil de entender este conceito:

|                 |                       |                |               |              |
|-----------------|-----------------------|----------------|---------------|--------------|
|                 | 4                     | 5              | 3             | 8            |
| Multiplica por: | $10^3$                | $10^2$         | $10^1$        | $10^0$       |
| ou seja:        | 1000                  | 100            | 10            | 1            |
| Resultado:      | $4 \times 1000$       | $5 \times 100$ | $3 \times 10$ | $8 \times 1$ |
| Igual a:        | 4000                  | 500            | 30            | 8            |
| Somando tudo:   | $4000 + 500 + 30 + 8$ |                |               |              |
| E igual a:      | 4538                  |                |               |              |

Figura 1.10 Como é obtido o valor de um número no sistema decimal.

Observe que 4538 significa exatamente:

$$\begin{aligned} & 4 \text{ milhares } (10^3) \\ & + 5 \text{ centenas } (10^2) \\ & + 3 \text{ dezenas } (10^1) \\ & + 8 \text{ unidades } (10^0) \end{aligned}$$

E assim para números com mais dígitos teríamos potências  $10^4$ ,  $10^5$  e assim por diante. Observe que multiplicando cada dígito por potências de 10, obtemos o número original. Este princípio aplicado ao sistema de numeração decimal é válido para qualquer sistema de numeração. Se for o sistema de numeração Octal (baseado em 8 dígitos), multiplica-se por potências de 8:  $8^0$ ,  $8^1$ ,  $8^2$  e assim por diante. Se for o sistema Hexadecimal (baseado em 10 dígitos e 6 letras) multiplica-se por potências de 16, só que a letra A equivale a 10, já que não tem sentido multiplicar por uma letra, a letra B equivale a 11 e assim por diante.

Bem, por analogia, se o sistema decimal é baseado em dez dígitos, então o sistema binário deve ser baseado em dois dígitos? Exatamente. Números no sistema binários são escritos usando-se apenas os dois seguintes dígitos:

0            1

Isso mesmo, números no sistema binário são escritos usando-se apenas zeros e uns, como nos exemplos a seguir:

**01011100**  
**11011110**  
**00011111**

Também por analogia, se, no sistema decimal, para obter o valor do número, multiplicamos os seus dígitos, de trás para frente, por potências de 10, no sistema binário fizemos esta mesma operação, só que baseada em potências de 2, ou seja:  $2^0$ ,  $2^1$ ,  $2^2$ ,  $2^3$ ,  $2^4$  e assim por diante.

Vamos considerar alguns exemplos práticos. Como faço para saber o valor decimal do seguinte número binário:

**11001110**

Vamos utilizar a tabelinha indicada na Figura 1.11 para facilitar os nossos cálculos:

|                 |                      |       |       |       |       |       |       |       |
|-----------------|----------------------|-------|-------|-------|-------|-------|-------|-------|
|                 | 1                    | 1     | 0     | 0     | 1     | 1     | 1     | 0     |
| Multiplica por: | $2^7$                | $2^6$ | $2^5$ | $2^4$ | $2^3$ | $2^2$ | $2^1$ | $2^0$ |
| Equivale a:     | 128                  | 64    | 32    | 16    | 8     | 4     | 2     | 1     |
| Multiplicação:  | 1x128                | 1x64  | 0x32  | 0x16  | 1x8   | 1x4   | 1x2   | 0x1   |
| Resulta em:     | 128                  | 64    | 0     | 0     | 8     | 4     | 2     | 0     |
| Somando tudo:   | $128+64+0+0+8+4+2+0$ |       |       |       |       |       |       |       |
| Resulta em:     | 206                  |       |       |       |       |       |       |       |

Figura 1.11 Determinando o valor decimal do número binário: 11001110

Ou seja, o número binário 11001110 equivale ao decimal 206. Observe que onde temos 1 a respectiva potência de 2 é somada e onde temos o zero a respectiva potência de 2 é anulada por ser multiplicada por zero. Apenas para fixar um pouco mais este conceito, vamos fazer mais um exemplo de conversão de binário para decimal.

Converter o número 11100010 para decimal. A resolução está indicada na Figura 1.12:

|                 |                       |       |       |       |       |       |       |       |
|-----------------|-----------------------|-------|-------|-------|-------|-------|-------|-------|
|                 | 1                     | 1     | 1     | 0     | 0     | 0     | 1     | 0     |
| Multiplica por: | $2^7$                 | $2^6$ | $2^5$ | $2^4$ | $2^3$ | $2^2$ | $2^1$ | $2^0$ |
| equivale a:     | 128                   | 64    | 32    | 16    | 8     | 4     | 2     | 1     |
| Multiplicação:  | 1x128                 | 1x64  | 1x32  | 0x16  | 0x8   | 0x4   | 1x2   | 0x1   |
| Resulta em:     | 128                   | 64    | 32    | 0     | 0     | 0     | 2     | 0     |
| Somando tudo:   | $128+64+32+0+0+0+2+0$ |       |       |       |       |       |       |       |
| Resulta em:     | 226                   |       |       |       |       |       |       |       |

Figura 1.12 Determinando o valor decimal do número binário: 11100010

### Como converter decimal para binário:

Bem, e se tivéssemos que fazer o contrário, converter o número 234 de decimal para binário, qual seria o binário equivalente??

Existem muitas regras para fazer esta conversão, eu prefiro utilizar uma bem simples, que descreverei a seguir e que serve perfeitamente para o propósito deste tópico.

Vamos voltar ao nosso exemplo, como converter 234 para um binário de 8 dígitos?

Eu começo o raciocínio assim. Primeiro vamos lembrar o valor de cada dígito:

128    64    32    16    8    4    2    1

Lembrando que estes números representam potências de 2, começando, de trás para frente, com  $2^0$ ,  $2^1$ ,  $2^2$  e assim por diante, conforme indicado logo a seguir:

128    64    32    16    8    4    2    1  
 $2^7$      $2^6$      $2^5$      $2^4$      $2^3$      $2^2$      $2^1$      $2^0$

Pergunto: 128 cabe em 234? Sim, então o primeiro dígito é 1. Somando 64 a 128 passa de 234? Não, dá 192, então o segundo dígito também é 1. Somando 32 a 192 passa de 234? Não, dá 224, então o terceiro dígito também é 1. Somando 16 a 224 passa de 234? Passa, então o quarto dígito é zero. Somando 8 a 224 passa de 234? Não, da 232, então o quinto dígito é 1. Somando 4 a 232 passa de 234?

**NOTA:** Nos exemplos deste tópico vou trabalhar com valores de, no máximo, 255, que são valores que podem ser representados por 8 dígitos binários, ou na linguagem do computador 8 bits, o que equivale exatamente a um byte. Por isso que cada um dos quatro números que fazem parte do número IP, somente podem ter um valor máximo de 255, que é um valor que cabe em um byte, ou seja, 8 bits.

Passa, então o sexto dígito é zero. Somando 2 a 232 passa de 234? Não, dá exatamente 234, então o sétimo dígito é 1. Já cheguei ao valor desejado, então todos os demais dígitos são zero. Com isso, o valor 234 em binário é igual a:

**11101010**

Para exercitar vamos converter mais um número de decimal para binário. Vamos converter o número 144 para decimal.

Pergunto: 128 cabe em 144? Sim, então o primeiro dígito é 1. Somando 64 a 128 passa de 144? Sim, dá 192, então o segundo dígito é 0. Somando 32 a 128 passa de 144? Sim, dá 160, então o terceiro dígito também é 0. Somando 16 a 128 passa de 144? Não, dá exatamente 144, então o quarto dígito é 1. Já cheguei ao valor desejado, então todos os demais dígitos são zero. Com isso, o valor 144 em binário é igual a:

**10010000**

Bem, agora que você já sabe como converter de decimal para binário, está em condições de aprender sobre o operador “E” e como o TCP/IP usa a máscara de sub-rede (subnet mask) e uma operação “E”, para verificar se duas máquinas estão na mesma rede ou não.

## Operador E:

Existem diversas operações lógicas que podem ser feitas entre dois dígitos binários, sendo as mais conhecidas as seguintes: “E”, “OU”, “XOR” e “NOT”.

Para o nosso estudo interessa o operador E. Quando realizamos um “E” entre dois bits, o resultado somente será 1, se os dois bits forem iguais a 1. Se pelo menos um dos bits for igual a zero, o resultado será zero. Na figura 1.13 temos todos os valores possíveis da operação E entre dois bits:

| bit-1 | bit-2 | (bit-1) E (bit-2) |
|-------|-------|-------------------|
| 1     | 1     | 1                 |
| 1     | 0     | 0                 |
| 0     | 1     | 0                 |
| 0     | 0     | 0                 |

Figura 1.13 Operador lógico E.

## Como o TCP/IP usa a máscara de sub-rede:

Considere a Figura 1.14, onde mostro a representação de uma rede local, ligada a uma outras redes através de um roteador.

É apresentada uma rede que usa como máscara de sub-rede 255.255.255.0 (uma rede classe C. Ainda não abordamos as classes de redes, o que será feito mais adiante). A rede é a 10.200.150, ou seja, todos os equipamentos da rede tem os três primeiras partes do número IP como sendo: 10.200.150. Veja que existe uma relação direta entre a máscara de sub-rede a quantas das partes do número IP são fixas, ou seja, que definem a rede, conforme foi descrito anteriormente.

A rede da Figura 1.14 é uma rede bastante usual, onde existe um roteador ligado à rede e o roteador está conectado a um Modem, através do qual é feita a conexão da rede local com a rede WAN da empresa, utilizando uma linha de dados (link de comunicação).

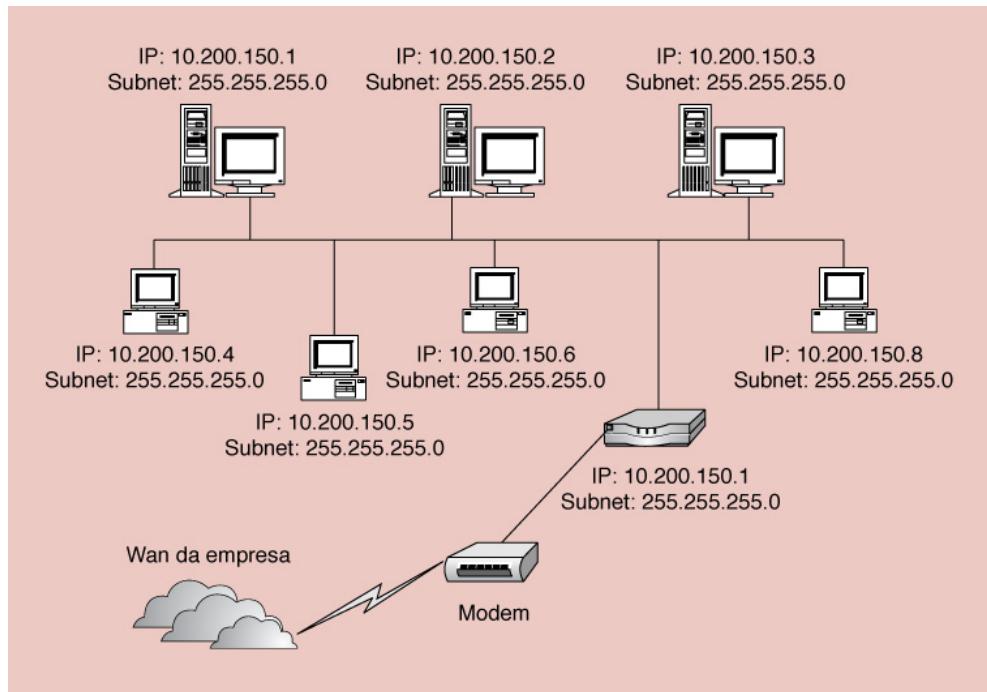


Figura 1.14 Roteador ligando duas ou mais redes locais.

## Como o TCP/IP usa a máscara de sub-rede e o roteador:

Quando dois computadores tentam trocar informações em uma rede, o TCP/IP precisa, primeiro, calcular se os dois computadores pertencem a mesma rede ou a redes diferentes. Neste caso podemos ter duas situações distintas:

- ◆ **Situação 1:** Os dois computadores pertencem a mesma rede: Neste caso o TCP/IP envia o pacote para o barramento da rede local. Todos os computadores recebem o pacote, mas somente o destinatário do pacote (o destinatário é identificado pelo campo IP de destino, contido no pacote de informações) é que o captura e passa para processamento pelo Windows e pelo programa de destino. Como é que o computador sabe se ele é ou não o destinatário do pacote? Muito simples, no pacote de informações está contido o endereço IP do destinatário. Em cada computador, o TCP/IP compara o IP de destinatário do pacote com o IP do computador, para saber se o pacote é ou não para o respectivo computador.
- ◆ **Situação 2:** Os dois computadores não pertencem a mesma rede: Neste caso o TCP/IP envia o pacote para o Roteador (endereço do Default Gateway configurado nas propriedades do TCP/IP) e o Roteador se encarrega de fazer o pacote chegar à rede de destino. Mais adiante mostrarei detalhes sobre como o Roteador é capaz de rotear pacotes de informações até redes distantes.

Agora a pergunta que tem a ver com este tópico:

*“Como é que o TCP/IP faz para saber se o computador de origem e o computador de destino pertencem a mesma rede?”*

Vou usar alguns exemplos práticos para explicar como o TCP/IP faz isso:

Exemplo 1: Com base na Figura 1.14, suponha que o computador cujo IP é 10.200.150.5 (origem) queira enviar pacotes de informações para o computador cujo IP é 10.200.150.8 (destino), ambos com máscara de sub-rede igual a 255.255.255.0.

O primeiro passo é converter o número IP das duas máquinas e da máscara de sub-rede para binário. Com base nas regras que vimos anteriormente, teríamos as conversões indicadas na Figura 1.15:

|                        |     |     |   |
|------------------------|-----|-----|---|
| Computador de origem:  |     |     |   |
| 10                     | 200 | 150 | 5 |
| <b>00001010</b>        |     |     |   |
| 10                     | 200 | 150 | 8 |
| <b>00001010</b>        |     |     |   |
| Computador de destino: |     |     |   |
| 10                     | 200 | 150 | 8 |
| <b>00001010</b>        |     |     |   |
| Máscara de sub-rede:   |     |     |   |
| 255                    | 255 | 255 | 0 |
| <b>11111111</b>        |     |     |   |
| 255                    | 255 | 255 | 0 |
| <b>11111111</b>        |     |     |   |
| 255                    | 255 | 255 | 0 |
| <b>00000000</b>        |     |     |   |

**Figura 1.15 Convertendo o IP de destino, IP de Origem e máscara de sub-rede para binário.**

Feitas as conversões para binário, vou mostrar que tipo de cálculos o TCP/IP faz, para determinar se o computador de origem e o computador de destino estão na mesma rede.

Em primeiro lugar é feita uma operação “E”, bit a bit, entre o Número IP e a máscara de Sub-rede do computador de origem, conforme indicado na Figura 1.16.

|               |          |          |          |          |           |
|---------------|----------|----------|----------|----------|-----------|
| 10.200.150.5  | 00001010 | 11001000 | 10010110 | 00000101 | E         |
| 255.255.255.0 | 11111111 | 11111111 | 11111111 | 00000000 |           |
| 10.200.150.0  | 00001010 | 11001000 | 10010110 | 00000000 | Resultado |

**Figura 1.16 Operação “E” entre o número IP de origem e a máscara de sub-rede.**

Em seguida é feita uma operação “E”, bit a bit, entre o Número IP e a máscara de sub-rede do computador de destino, conforme indicado na Figura 1.17.

|               |          |          |          |          |           |
|---------------|----------|----------|----------|----------|-----------|
| 10.200.150.8  | 00001010 | 11001000 | 10010110 | 00001000 | E         |
| 255.255.255.0 | 11111111 | 11111111 | 11111111 | 00000000 |           |
| 10.200.150.0  | 00001010 | 11001000 | 10010110 | 00000000 | Resultado |

**Figura 1.17 Operação “E” entre o número IP de destino e a máscara de sub-rede.**

Agora o TCP/IP compara os resultados das duas operações. Se os dois resultados forem iguais, isto significa que os dois computadores, origem e destino, pertencem a mesma rede local. Neste caso o TCP/IP envia o pacote para o barramento da rede local. Todos os computadores recebem o pacote, mas somente o destinatário do pacote é que o captura e passa para processamento pelo Windows e pelo programa de destino. Como é que o computador sabe se ele é ou não o destinatário do pacote? Muito simples, no pacote de informações está contido o endereço IP do destinatário. Em cada computador, o TCP/IP compara o IP de destinatário do pacote com o IP do computador, para saber se o pacote é ou não para o respectivo computador.

É o que acontece neste exemplo, pois o resultado das duas operações “E” é igual: 10.200.150.0, ou seja, os dois computadores pertencem a rede: 10.200.150.0

Como você já deve ter adivinhado, agora vamos a um exemplo, onde os dois computadores não pertencem a mesma rede, pelo menos devido às configurações do TCP/IP.

Exemplo 2: Suponha que o computador cujo IP é 10.200.150.5 (origem) queira enviar um pacote de informações para o computador cujo IP é 10.204.150.8 (destino), ambos com máscara de sub-rede igual a 255.255.255.0.

O primeiro passo é converter o número IP das duas máquinas e da máscara de sub-rede para binário. Com base nas regras que vimos anteriormente, teríamos as conversões indicadas na Figura 1.18:

| Computador de origem:  |          |          |          |  |
|------------------------|----------|----------|----------|--|
| 10                     | 200      | 150      | 5        |  |
| 00001010               | 11001000 | 10010110 | 00000101 |  |
| Computador de destino: |          |          |          |  |
| 10                     | 204      | 150      | 8        |  |
| 00001010               | 11001100 | 10010110 | 00001000 |  |
| Máscara de sub-rede:   |          |          |          |  |
| 255                    | 255      | 255      | 0        |  |
| 11111111               | 11111111 | 11111111 | 00000000 |  |

Figura 1.18 Convertendo o IP de destino, IP de Origem e máscara de sub-rede para binário.

Feitas as conversões para binário, vamos ver que tipo de cálculos o TCP/IP faz, para determinar se o computador de origem e o computador de destino estão na mesma rede.

Em primeiro lugar é feita uma operação “E”, bit a bit, entre o Número IP e a máscara de Sub-rede do computador de origem, conforme indicado na Figura 1.19

|               |          |          |          |          |           |
|---------------|----------|----------|----------|----------|-----------|
| 10.200.150.5  | 00001010 | 11001000 | 10010110 | 00000101 | E         |
| 255.255.255.0 | 11111111 | 11111111 | 11111111 | 00000000 |           |
| 10.200.150.0  | 00001010 | 11001000 | 10010110 | 00000000 | Resultado |

Figura 1.19 Operação “E” entre o número IP de origem e a máscara de sub-rede.

Agora é feita uma operação “E”, bit a bit, entre o Número IP e a máscara de sub-rede do computador de destino, conforme indicado na Figura 1.20

Agora o TCP/IP compara os resultados das duas operações. Neste exemplo, os dois resultados são diferentes: 10.200.150.0 e 10.204.150.0. Nesta situação o TCP/IP envia o pacote para o Roteador (endereço do Default Gateway configurado nas propriedades do TCP/IP) e o Roteador se encarrega de fazer o pacote chegar através do destino. Em outras palavras o Roteador sabe entregar o pacote para a rede 10.204.150.0 ou sabe para quem enviar (um outro roteador), para que este próximo roteador possa encaminhar o pacote. Este processo continua até que o pacote seja entregue na rede de destino.

Observe que, na Figura 1.20, temos dois computadores que, apesar de estarem fisicamente na mesma rede, não conseguirão se comunicar devido a um erro de configuração na máscara de sub-rede de um dos computadores. É o caso dos computador 10.200.150.4 (com máscara de sub-rede 255.255.250.0). Como este computador está com uma máscara de sub-rede diferente dos demais computadores da rede (os quais estão com máscara: 255.255.255.0), ao fazer os cálculos, o TCP/IP chega a conclusão que este computador pertence a uma rede diferente, o que faz com que ele não consiga se comunicar com os demais computadores da rede local.

|               |          |          |          |          |           |
|---------------|----------|----------|----------|----------|-----------|
| 10.204.150.8  | 00001010 | 11001100 | 10010110 | 00001000 | E         |
| 255.255.255.0 | 11111111 | 11111111 | 11111111 | 00000000 |           |
| 10.204.150.0  | 00001010 | 11001100 | 10010110 | 00000000 | Resultado |

Figura 1.20 Operação “E” entre o número IP de origem e a máscara de sub-rede.

## Endereçamento IP – Classes de Endereços

Neste item vou falar sobre o endereçamento IP. Mostrarei que, inicialmente, foram definidas classes de endereços IP. Porém, devido a uma possível falta de endereços, por causa do grande crescimento da Internet, novas alternativas tiveram que ser buscadas, sendo uma delas a criação de uma nova versão do protocolo IP, o IP v6 (versão 6). O Windows Server 2003 dá suporte completo ao IP v6.

Mostrei anteriormente que a máscara de sub-rede é utilizada para determinar qual “parte” do endereço IP representa o número da Rede e qual parte representa o número da máquina dentro da rede. A máscara de sub-rede também foi utilizada na definição original das classes de endereço IP. Em cada classe existe um determinado número de redes possíveis e, em cada rede, um número máximo de máquinas.

Foram definidas cinco classes de endereços, identificadas pelas letras: A, B, C, D e E. Vou iniciar com uma descrição detalhada de cada Classe de Endereços e, em seguida apresento um quadro resumo.

### Redes Classe A:

Esta classe foi definida com tendo o primeiro bit do número IP (dos 32 bits, ou seja, quatro números de 8 bits) como sendo igual a zero. Com isso o primeiro número IP somente poderá variar de 1 até 126 (na prática até 127, mas o número 127 é um número reservado, conforme detalharei mais adiante). Observe, no esquema da Figura 1.21 (explicado anteriormente), que o primeiro bit sendo 0, o valor máximo (quando todos os demais bits são iguais a 1) a que se chega é de 127:

|                 |                      |       |       |       |       |       |       |       |
|-----------------|----------------------|-------|-------|-------|-------|-------|-------|-------|
|                 | 0                    | 1     | 1     | 1     | 1     | 1     | 1     | 1     |
| Multiplica por: | $2^7$                | $2^6$ | $2^5$ | $2^4$ | $2^3$ | $2^2$ | $2^1$ | $2^0$ |
| equivale a:     | 128                  | 64    | 32    | 16    | 8     | 4     | 2     | 1     |
| Multiplicação:  | 0x128                | 1x64  | 1x32  | 1x16  | 1x8   | 1x4   | 1x2   | 1x1   |
| Resulta em:     | 0                    | 64    | 32    | 16    | 8     | 4     | 2     | 1     |
| Somando tudo:   | $0+64+32+16+8+4+2+1$ |       |       |       |       |       |       |       |
| Resulta em:     | 127                  |       |       |       |       |       |       |       |

**Figura 1.21 Redes classe A – primeiro bit é sempre igual a 0.**

O número 127 não é utilizado como rede Classe A, pois é um número especial, reservado para fazer referência ao próprio computador. O número 127.0.0.1 é um número especial, conhecido como localhost. Ou seja, sempre que um programa fizer referência a localhost ou ao número 127.0.0.1, estará fazendo referência a si mesmo.

Por padrão, para a Classe A, foi definida a seguinte máscara de sub-rede: 255.0.0.0. Com esta máscara de subrede observe que temos 8 bits para o endereço da rede e 24 bits para o endereço das máquinas dentro da rede. Com base no número de bits para a rede e para as máquinas, podemos determinar quantas redes Classe A podem existir e qual o número máximo de máquinas por rede. Para isso utilizamos a fórmula a seguir:

$$2^{n-2}$$

, onde “n” representa o número de bits utilizado para a rede ou para a identificação da máquina dentro da rede. Vamos aos cálculos:

Número de redes Classe A:

Número de bits para a rede: 7. Como o primeiro bit sempre é zero, este não varia. Por isso sobram 7 bits (8-1) para formar diferentes redes:

$$2^7-2 \rightarrow 128-2 \rightarrow 126 \text{ redes Classe A}$$

Número de máquinas (hosts) em uma rede Classe A:

Número de bits para identificar a máquina: 24.

$$2^{24}-2 \rightarrow 128-2 \rightarrow 16.777.214 \text{ máquinas em cada rede classe A.}$$

Na Classe A temos apenas um pequeno número de redes disponíveis - 126, porém um grande número de máquinas em cada rede – 16.777.214.

Com isso você pode concluir que este número de máquinas, na prática, jamais será instalado em uma única rede. Com isso observe que, com este esquema de endereçamento, teríamos poucas redes Classe A (apenas 126) e com um número muito grande de máquinas em cada rede. Isso causaria desperdício de endereços, pois se o endereço de uma rede Classe A fosse disponibilizado para um empresa, esta utilizaria apenas uma pequena parcela dos endereços disponíveis e todos os demais endereços ficariam sem uso.

## Redes Classe B:

Esta classe de rede foi definida com tendo os dois primeiros bits do número IP como sendo sempre iguais a 1 e 0. Com isso o primeiro número do endereço IP somente poderá variar de 128 até 191. Como o segundo bit é sempre 0, o valor do segundo bit que é 64 nunca é somado para o primeiro número IP, com isso o valor máximo fica em: 255-64, que é o 191. Observe, no esquema da Figura 1.22, explicado anteriormente, que o primeiro bit sendo 1 e o segundo sendo 0, o valor máximo (quando todos os demais bits são iguais a 1) a que se chega é de 191:

|                 |                       |       |       |       |       |       |       |       |
|-----------------|-----------------------|-------|-------|-------|-------|-------|-------|-------|
|                 | 1                     | 0     | 1     | 1     | 1     | 1     | 1     | 1     |
| Multiplica por: | $2^7$                 | $2^6$ | $2^5$ | $2^4$ | $2^3$ | $2^2$ | $2^1$ | $2^0$ |
| equivale a:     | 128                   | 64    | 32    | 16    | 8     | 4     | 2     | 1     |
| Multiplicação:  | 1x128                 | 0x64  | 1x32  | 1x16  | 1x8   | 1x4   | 1x2   | 1x1   |
| Resulta em:     | 128                   | 0     | 32    | 16    | 8     | 4     | 2     | 1     |
| Somando tudo:   | $128+0+32+16+8+4+2+1$ |       |       |       |       |       |       |       |
| Resulta em:     | 191                   |       |       |       |       |       |       |       |

Figura 1.22 Redes classe B – segundo bit é sempre igual a 0.

Por padrão, para a Classe B, foi definida a seguinte máscara de sub-rede: 255.255.0.0. Com esta máscara de sub-rede observe que temos 16 bits para o endereço da rede e 16 bits para o endereço das máquinas dentro da rede. Com base no número de bits para a rede e para as máquinas, podemos determinar quantas redes Classe B podem existir e qual o número máximo de máquinas por rede. Para isso utilizamos a fórmula a seguir:

$$2^{n-2}$$

, onde “n” representa o número de bits utilizado para a rede ou para a identificação da máquina dentro da rede. Vamos aos cálculos:

Número de redes Classe B:

Número de bits para a rede: 14. Como o primeiro e o segundo bit são sempre 10, fixos, não variam, sobram 14 bits (16-2) para formar diferentes redes:

$$2^{14-2} \rightarrow 16.384-2 \rightarrow 16.382 \text{ redes Classe B}$$

Número de máquinas (hosts) em uma rede Classe B:

Número de bits para identificar a máquina: 16.

$$2^{16-2} \rightarrow 65.536-2 \rightarrow 65.534 \text{ máquinas em cada rede classe B}$$

Na Classe B temos um número razoável de redes Classe B, com um bom número de máquinas em cada rede.

O número máximo de máquinas, por rede Classe B já está mais próximo da realidade para as redes de algumas grandes empresas tais como Microsoft, IBM, HP, GM, etc. Mesmo assim, para muitas empresas menores, a utilização de um endereço Classe B, representa um grande desperdício de números IP.

## Redes Classe C:

Esta classe foi definida com tendo os três primeiros bits do número IP como sendo sempre iguais a 1, 1 e 0. Com isso o primeiro número do endereço IP somente poderá variar de 192 até 223. Como o terceiro bit é sempre 0, o valor do terceiro bit que é 32 nunca é somado para o primeiro número IP, com isso o valor máximo fica em: 255-32, que é 223. Observe, no esquema indicado na Figura 1.23, explicado anteriormente, que o primeiro bit sendo 1, o segundo bit sendo 1 e o terceiro bit sendo 0, o valor máximo (quando todos os demais bits são iguais a 1) a que se chega é de 223.

Por padrão, para a Classe C, foi definida a seguinte máscara de sub-rede: 255.255.255.0. Com esta máscara de sub-rede observe que temos 24 bits para o endereço da rede e apenas 8 bits para o endereço da máquina dentro da rede. Com base no número de bits para a rede e para as máquinas, podemos determinar quantas redes Classe C podem existir e qual o número máximo de máquinas por rede. Para isso utilizamos a fórmula a seguir:

$$2^{n-2}$$

, onde “n” representa o número de bits utilizado para a rede ou para a identificação da máquina dentro da rede. Vamos aos cálculos:

Número de redes Classe C:

Número de bits para a rede: 21. Como o primeiro, o segundo e o terceiro bit são sempre 110, ou seja:fixos, não variam, sobram 21 bits (24-3) para formar diferentes redes:

$$2^{21-2} \rightarrow 2.097.152-2 \rightarrow 2.097.150 \text{ redes Classe C}$$

Número de máquinas (hosts) em uma rede Classe C:

Número de bits para identificar a máquina: 8

$$2^8-2 \rightarrow 256-2 \rightarrow 254 \text{ máquinas em cada rede classe C}$$

Observe que na Classe C temos um grande número de redes disponível, com, no máximo, 254 máquinas em cada rede. É o ideal para empresas de pequeno e médio porte. Mesmo com a Classe C, pode existir um grande desperdício de endereços. Imagine uma pequena empresa com apenas 20 máquinas em rede. Usando um endereço Classe C, estariam sendo desperdiçados 234 endereços.

|                 |                       |       |       |       |       |       |       |       |
|-----------------|-----------------------|-------|-------|-------|-------|-------|-------|-------|
|                 | 1                     | 1     | 0     | 1     | 1     | 1     | 1     | 1     |
| Multiplica por: | $2^7$                 | $2^6$ | $2^5$ | $2^4$ | $2^3$ | $2^2$ | $2^1$ | $2^0$ |
| equivale a:     | 128                   | 64    | 32    | 16    | 8     | 4     | 2     | 1     |
| Multiplicação:  | 1x128                 | 1x64  | 0x32  | 1x16  | 1x8   | 1x4   | 1x2   | 1x1   |
| Resulta em:     | 128                   | 64    | 0     | 16    | 8     | 4     | 2     | 1     |
| Somando tudo:   | $128+64+0+16+8+4+2+1$ |       |       |       |       |       |       |       |
| Resulta em:     | 223                   |       |       |       |       |       |       |       |

Figura 1.23 Redes classe C – terceiro bit é sempre igual a 0.

## Redes Classe D:

Esta classe foi definida com tendo os quatro primeiros bits do número IP como sendo sempre iguais a 1, 1, 1 e 0. A classe D é uma classe especial, reservada para os chamados endereços de Multicast.

## Redes Classe E:

Esta classe foi definida com tendo os quatro primeiros bits do número IP como sendo sempre iguais a 1, 1, 1 e 1. A classe E é uma classe especial e está reservada para uso futuro.

Na Figura 1.24, é apresentado um quadro resumo das Classes de Endereço IP:

| Classe | Primeiros bits | Número de redes                  | Número de hosts | Máscara padrão |
|--------|----------------|----------------------------------|-----------------|----------------|
| A      | 0              | 126                              | 16.777.214      | 255.0.0.0      |
| B      | 10             | 16.382                           | 65.534          | 255.255.0.0    |
| C      | 110            | 2.097.150                        | 254             | 255.255.255.0  |
| D      | 1110           | Utilizado para tráfego Multicast |                 |                |
| E      | 1111           | Reservado para uso futuro        |                 |                |

Figura 1.24 Quadro resumo das classes de redes.

## **Endereços Especiais:**

Existem alguns endereços IP especiais, reservados para funções específicas e que não podem ser utilizados como endereços de uma máquina da rede. A seguir descrevo estes endereços.

B= Endereços da rede 127.0.0.0: Este endereço é utilizado como um alias (apelido), para fazer referência a própria máquina. Normalmente é utilizado o endereço 127.0.0.1, o qual é associado ao nome localhost. Esta associação é feita através do arquivo hosts. No Windows 95/98/Me o arquivo hosts está na pasta onde o Windows foi instalado e no Windows NT/2000/XP/2003, o arquivo hosts está no seguinte caminho: system32/drivers/etc, sendo que este caminho fica dentro da pasta onde o Windows foi instalado.

- ◆ **Endereço com todos os bits destinados à identificação da máquina, iguais a 0:** Um endereço com zeros em todos os bits de identificação da máquina, representa o endereço da rede. Por exemplo, vamos supor que você tenha uma rede Classe C. A máquina a seguir é uma máquina desta rede: 200.220.150.3. Neste caso o endereço da rede é: 200.220.150.0, ou seja, zero na parte destinada a identificação da máquina. Sendo uma rede classe C, a máscara de sub-rede é 255.255.255.0.
- ◆ **Endereço com todos os bits destinados à identificação da máquina, iguais a 1:** Um endereço com valor 1 em todos os bits de identificação da máquina, representa o endereço de broadcast. Por exemplo, vamos supor que você tenha uma rede Classe C. A máquina a seguir é uma máquina desta rede: 200.220.150.3. Neste caso o endereço de broadcast desta rede é o seguinte: 200.220.150.255, ou seja, todos os bits da parte destinada à identificação da máquina, iguais a 1. Sendo uma rede classe C, a máscara de sub-rede é 255.255.255.0. Ao enviar uma mensagem para o endereço de broadcast, a mensagem é endereçada para todos as máquinas da rede.

## **O papel do Roteador em uma rede de computadores:**

Neste item vou falar sobre Roteamento. Falarei sobre o papel dos roteadores na ligação entre redes locais (LANs) para formar uma WAN. Mostrarei um exemplo básico de roteamento.

Mostrei anteriormente que a máscara de sub-rede é utilizada para determinar qual “parte” do endereço IP representa o número da Rede e qual parte representa o número da máquina dentro da rede. A máscara de sub-rede também foi utilizada na definição original das classes de endereço IP. Em cada classe existe um determinado número de redes possíveis e, em cada rede, um número máximo de máquinas. Com base na máscara de sub-rede o protocolo TCP/IP determina se o computador de origem e o de destino estão na mesma rede local. Com base em cálculos binários, o TCP/IP pode chegar a dois resultados distintos:

- ◆ **O computador de origem e de destino estão na mesma rede local:** Neste caso os dados são enviados para o barramento da rede local. Todos os computadores da rede recebem os dados. Ao receber os dados cada computador analisa o campo Número IP do destinatário. Se o IP do destinatário for igual ao IP do computador, os dados são capturados e processados pelo sistema, caso contrário são simplesmente descartados. Observe que com este procedimento, apenas o computador de destino é que efetivamente processa os dados para ele enviados, os demais computadores simplesmente descartam os dados.
- ◆ **O computador de origem e de destino não estão na mesma rede local:** Neste caso os dados são enviados o equipamento com o número IP configurado no parâmetro Default Gateway (Gateway Padrão). Ou seja, se após os cálculos baseados na máscara de sub-rede, o TCP/IP chegar a conclusão que o computador de destino e o computador de origem não fazem parte da mesma rede local, os dados são enviados para o Default Gateway, o qual será encarregado de encontrar um caminho para enviar os dados até o computador de destino. Esse “encontrar o caminho“ é tecnicamente conhecido como Rotear os dados até o destino. O responsável por

“Rotear” os dados é o equipamento que atua como Default Gateway o qual é conhecido como Roteador. Com isso fica fácil entender o papel do Roteador:

*“É o responsável por encontrar um caminho entre a rede onde está o computador que enviou os dados e a rede onde está o computador que irá receber os dados.”*

Quando ocorre um problema com o Roteador, tornando-o indisponível, você consegue se comunicar normalmente com os demais computadores da rede local, porém não conseguirá comunicação com outras redes de computadores, como por exemplo a Internet.

## Como eu sei qual o Default Gateway que está configurado no meu computador com o Windows Server 2003 instalado?

Você pode verificar as configurações do TCP/IP de um computador com o Windows Server 2003 de duas maneiras: com as propriedades da interface de rede ou com o comando ipconfig. A seguir descrevo estas duas maneiras:

Verificando as configurações do TCP/IP usando a interface gráfica:

1. Selecione Iniciar -> Painel de Controle -> Conexões de Rede. Clique com o botão direito do mouse na opção Conexão de rede local.
2. No menu que é exibido clique na opção Propriedades.
3. Será exibida a janela de Propriedades da conexão de rede local, conforme indicado na Figura 1.25:

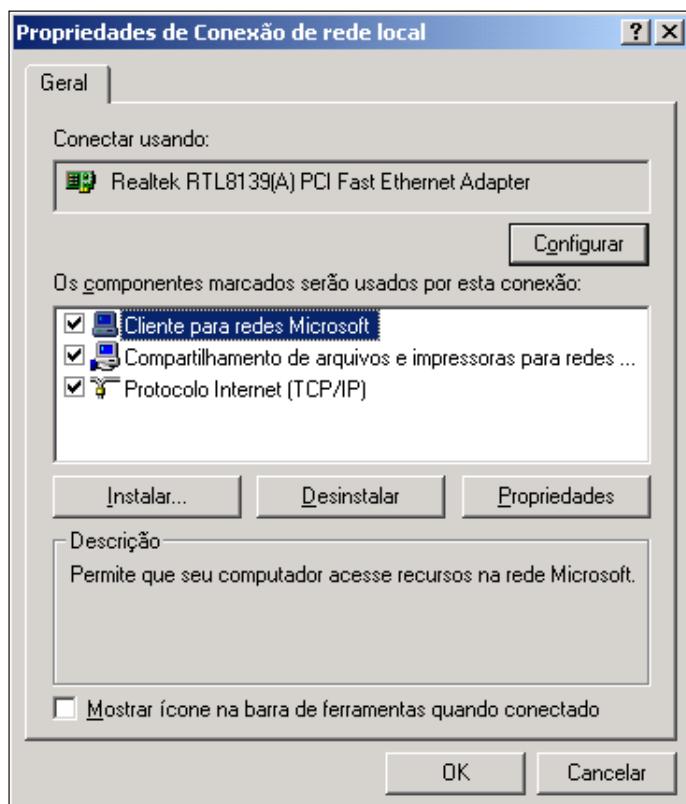
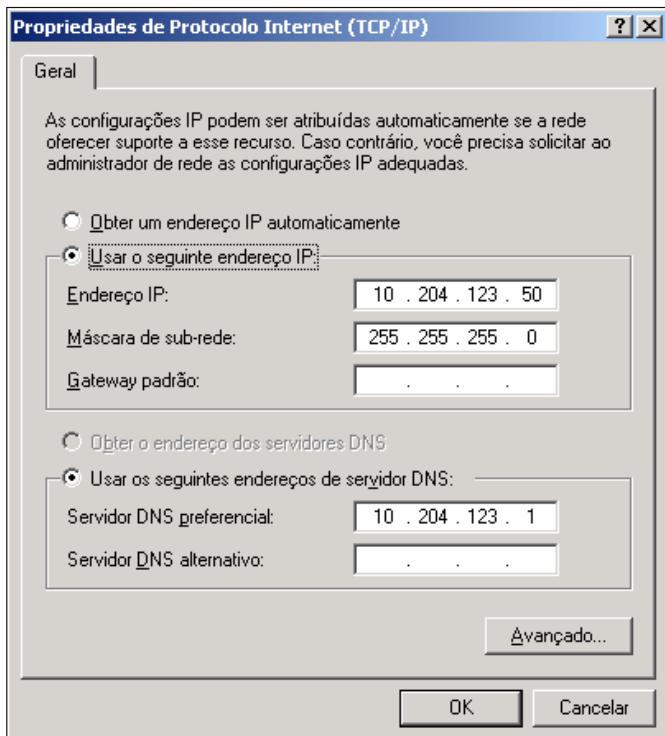


Figura 1.25 Janela de Propriedades da conexão de rede local.

4. Clique na opção Protocolo Internet (TCP/IP) e depois clique no botão Propriedades.

5. A janela de propriedades do TCP/IP será exibida, conforme indicado na Figura 1.26. Nesta janela são exibidas informações sobre o número IP do computador, a máscara de sub-rede, o Gateway padrão e o número IP dos servidores DNS primário e secundário. Se a opção obter um endereço IP automaticamente estiver marcada, o computador tentará obter todas estas configurações a partir de um servidor DHCP, durante a inicialização. Neste caso as informações sobre as configurações TCP/IP, inclusive o número IP do Roteador (Gateway Padrão), somente poderão ser obtidas através do comando ipconfig, conforme descrevo logo a seguir.
6. Clique em OK para fechar a janela de Propriedades do protocolo TCP/IP.



**Figura 1.26 Informações sobre a configuração do TCP/IP.**

Verificando as configurações do TCP/IP usando o comando ipconfig:

Para verificar as configurações do TCP/IP, utilizando o comando ipconfig, siga os seguintes passos:

1. Abra o Prompt de comando: Iniciar -> Todos os Programas -> Acessórios -> Prompt de comando.
2. Digite o comando ipconfig/all
3. Serão listadas as configurações do TCP/IP, conforme exemplo da listagem a seguir:

### Configuração de IP do Windows

```

Nome do host.....: MICRO080
Sufixo DNS primário.....: abc.com.br
Tipo de nó.....: Híbrida
Roteamento de IP ativado.....: Não
Proxy WINS ativado.....: Não
Lista de pesquisa de sufixo DNS...: abc.com.br
                                vendas.abc.com.br
                                finan.abc.com.br
Ethernet adaptador Conexão de rede local:
Sufixo DNS específico de conexão.: abc.com.br
Descrição.....: 3COM - AX 25

```

```

Endereço físico.....: 04-02-B3-92-82-CA
DHCP ativado.....: Sim
Configuração automática ativada...: Sim
Endereço IP.....: 10.10.10.222
Máscara de sub-rede.....: 255.255.0.0
Gateway padrão.....: 10.10.10.1
Servidor DHCP.....: 10.10.10.2
Servidores DNS.....: 10.10.10.2
Servidor WINS primário.....: 10.10.10.2

```

## Explicando Roteamento – um exemplo prático:

Vou apresentar a explicação sobre como o roteamento funciona, através da análise de um exemplo simples. Vamos imaginar a situação de uma empresa que tem a matriz em SP e uma filial no RJ. O objetivo é conectar a rede local da matriz em SP com a rede local da filial no RJ, para permitir a troca de mensagens e documentos entre os dois escritórios. Nesta situação o primeiro passo é contratar um link de comunicação entre os dois escritórios. Em cada escritório deve ser instalado um Roteador. E finalmente os roteadores devem ser configurados para que seja possível a troca de informações entre as duas redes. Na Figura 1.27, apresento a ilustração desta pequena rede de longa distância (WAN). Em seguida vou explicar como funciona o roteamento entre as duas redes:

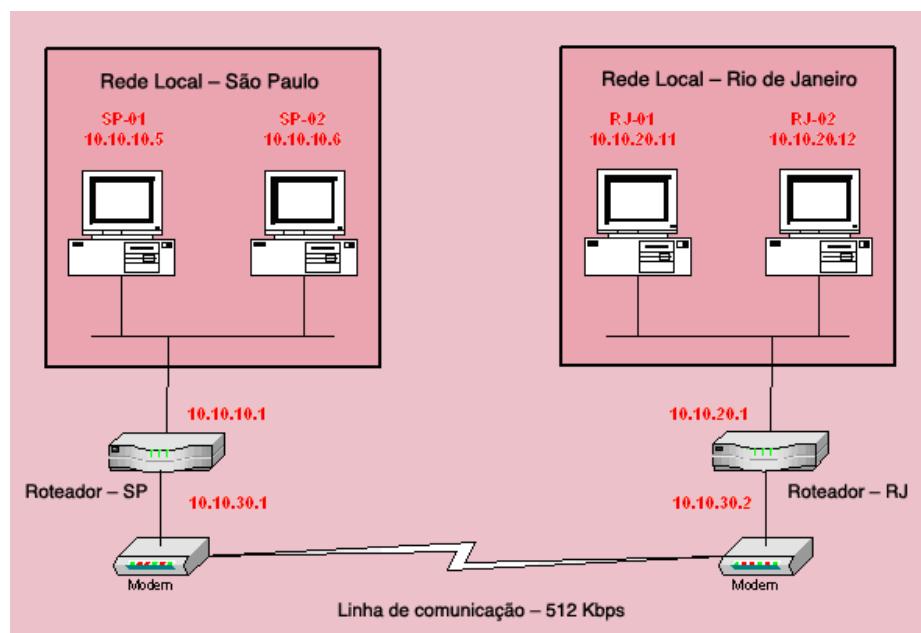


Figura 1.27 Interligando duas redes locais para formar a WAN da empresa.

Nesta pequena rede temos um exemplo simples de roteamento, mas muito a explicar. Então vamos lá.

Como está configurado o endereçamento das redes locais e dos roteadores?

- ◆ **Rede de SP:** Esta rede utiliza um esquema de endereçamento 10.10.10.0, com máscara de sub-rede 255.255.255.0. Observe que embora, teoricamente, seria uma rede Classe A (primeiro número na faixa de 1 a 126), está sendo utilizada uma máscara de sub-rede classe C.
- ◆ **Rede de RJ:** Esta rede utiliza um esquema de endereçamento 10.10.20.0, com máscara de sub-rede 255.255.255.0. Observe que embora, teoricamente, seria uma rede Classe A, está sendo utilizada uma máscara de sub-rede classe C.
- ◆ **Roteadores:** Cada roteador possui duas interfaces. Uma é a chamada interface de LAN (rede local), a qual conecta o roteador com a rede local. A outra é a interface de WAN (rede de longa distância), a qual conecta o roteador com o link de dados. Na interface de rede local, o roteador deve ter um endereço IP da rede interna.

No roteador de SP, o endereço é 10.10.10.1. Não é obrigatório, mas é um padrão normalmente adotado, utilizar o primeiro endereço da rede para o Roteador. No roteador do RJ, o endereço é 10.10.20.1

◆ **Rede dos roteadores:** Para que as interfaces externas dos roteadores possam se comunicar, eles devem fazer parte de uma mesma rede, isto é, devem compartilhar um esquema de endereçamento comum. As interfaces externas dos roteadores (interfaces WAN), fazem parte da rede 10.10.30.0, com máscara de sub-rede 255.255.255.0.

◆ **Na verdade – 3 redes:** Com isso temos, na prática três redes, conforme resumido a seguir:

**SP:** 10.10.10.0/255.255.255.0

**RJ:** 10.10.20.0/255.255.255.0

**Interfaces WAN dos Roteadores:** 10.10.30.0/255.255.255.0

◆ Na prática é como se a rede 10.10.30.0 fosse uma “ponte” entre as duas outras redes.

Como é feita a interligação entre as duas redes?

Vou utilizar um exemplo prático, para mostrar como é feito o roteamento entre as duas redes.

Exemplo: Vou analisar como é feito o roteamento, quando um computador da rede em SP, precisa acessar informações de um computador da rede no RJ. O computador SP-01 (10.10.10.5), precisa acessar um arquivo que está em uma pasta compartilhada do computador RJ-02 (10.10.20.12). Como é feito o roteamento, de tal maneira que estes dois computadores possam trocar informações?

Acompanhe os passos descritos a seguir:

1. O computador SP-01 é o computador de origem e o computador RJ-02 é o computador de destino. A primeira ação do TCP/IP é fazer os cálculos para verificar se os dois computadores estão na mesma rede, conforme explicado anteriormente. Os seguintes dados são utilizados para realização destes cálculos:

**SP-01:** 10.10.10.5/255.255.255.0

**RJ-02:** 10.10.20.12/255.255.255.0

2. Feitos os cálculos, o TCP/IP chega a conclusão de que os dois computadores pertencem a redes diferentes: SP-01 pertence a rede 10.10.10.0 e RJ-02 pertence a rede 10.10.20.0.

3. Como os computadores pertencem a redes diferentes, os dados devem ser enviados para o Roteador da rede 10.10.10.0, que é a rede do computador de origem.

4. No roteador de SP chega o pacote de informações com o IP de destino: 10.10.20.12. O roteador precisa consultar a sua tabela de roteamento e verificar se ele conhece um caminho para a rede 10.10.20.0, ou seja, se ele sabe para quem enviar um pacote de informações, destinado a rede 10.10.20.0.

5. O roteador de SP tem, em sua tabela de roteamento, a informação de que pacotes para a rede 10.10.20.0 devem ser encaminhados pela interface 10.10.30.1. É isso que ele faz, ou seja, encaminha os pacotes através da interface de WAN: 10.10.30.1.

6. Os pacotes de dados chegam na interface 10.10.30.1 e são enviados, através do link de comunicação, para a interface 10.10.30.2, do roteador do RJ.

7. No roteador do RJ chega o pacote de informações com o IP de destino: 10.10.20.12. O roteador precisa consultar a sua tabela de roteamento e verificar se ele conhece um caminho para a rede 10.10.20.0.

8. O roteador do RJ tem, em sua tabela de roteamento, a informação de que pacotes para a rede 10.10.20.0 devem ser encaminhados pela interface 10.10.20.1, que é a interface que conecta o roteador a rede local 10.10.20.0. O pacote é enviado, através da interface 10.10.20.1, para o barramento da rede local. Todos os computadores recebem os pacotes de dados e os descartam, com exceção do computador 10.10.20.12 que é o computador de destino.

9. Para que a resposta possa ir do computador RJ-02 para o computador SP-01, um caminho precisa ser encontrado, para que os pacotes de dados possam ser roteados do RJ para SP (o caminho de volta no nosso exemplo). Para tal todo o processo é executado novamente, até que a resposta chegue ao computador SP-01.
10. A chave toda para o processo de roteamento é o software presente nos roteadores, o qual atua com base em tabelas de roteamento.

O exemplo mostrado na Figura 1.27 é um exemplo simples, onde mostrei como é feito o roteamento entre duas redes ligadas através de um link de WAN. O princípio básico é o mesmo, para redes maiores até para a maior das redes que é a Internet.

## Executar um teste de compatibilidade antes da instalação do Windows Server 2003

Antes de fazer a instalação do Windows Server 2003 é recomendável que você faça execute um teste de verificação de compatibilidade, para detectar se existe alguma incompatibilidade de Hardware ou de Software.

Se você for instalar o Windows Server 2003 em um servidor novo, basta ligar o servidor com o cd do Windows Server 2003 já no drive de CD. Em uma das primeiras telas do processo de instalação, será exibida uma opção para você executar um teste de compatibilidade.

A seguir mostro os passos para que você execute um teste de compatibilidade em um servidor que já está com o Windows 2000 Server instalado e que você pretende atualizar para o Windows Server 2003:

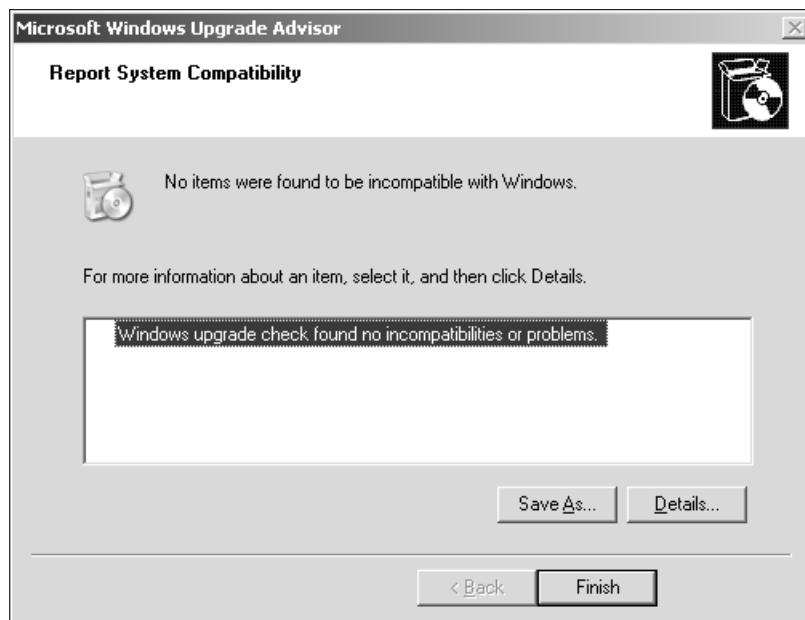
1. Inicialize o servidor e faça o logon com uma conta com permissão de Administrador.
2. Insira o CD do Windows Server 2003 no drive de CD.
3. Será exibida a tela inicial do assistente de instalação do Windows Server 2003, conforme indicado na Figura 1.28:



Figura 1.28 A tela inicial do assistente de instalação

**NOTA:** Você encontra um curso bem detalhado sobre TCP/IP, com mais detalhes sobre endereçamento IP, tabelas de roteamento e classes de redes, nos livros "TCP/IP Internet Protocols & Tecnologias 3ª Edição. Número de páginas: 362. ISBN: 85-7323-150-5"; "InternetWorking Manual de Tecnologias, diversos autores, Editora Campus"; "Interligação em Rede com TCP/IP, Douglas E. Comer, Editora Campus." e "TCP/IP: a Bíblia MRIDULA PARIHAR PAUL LASALLE ROB CRIMGER ET AL., Editora Campus".

4. Clique na opção Checar compatibilidade do sistema (Check System Compatibility).
5. Será exibida uma segunda tela com três opções: Checar o sistema automaticamente (Check my system automatically), Visitar o Web site de compatibilidade (Visit Web site compatibility) ou voltar. Clique na opção Checar o sistema automaticamente.
6. Ao final é exibido um tela com informações resumidas. No exemplo da Figura 1.29, nenhuma incompatibilidade foi verificada.



**Figura 1.29 Nenhuma incompatibilidade foi verificada.**

7. Clique em Concluir (Finish) para fechar o teste de compatibilidade.
8. Caso alguma incompatibilidade tenha sido detectada, a lista de incompatibilidades será exibida na tela final do sistema. Você pode clicar em uma das incompatibilidades e depois no botão Detalhes (Details), para ver uma explicação sobre a incompatibilidade selecionada e recomendações para solucionar a incompatibilidade.
9. Clique no botão Salvar como (Save As), para salvar o relatório de incompatibilidades em um arquivo.txt. Por padrão o assistente sugere o nome upgrade.txt. Selecione a pasta e o nome do arquivo e clique em salvar.
10. Na listagem 1.1, você encontra um exemplo do relatório de incompatibilidades gerado em um computador com o Windows 2000 Server e o Active Directory Instalados. A avaliação foi feita em um computador com o Windows 2000 Server em Inglês e o Active Directory instalados.:

#### **Listagem 1.1 – Exemplo de um relatório de incompatibilidades, gerado com o comando winnt32/checkupgradeonly**

```
*****
Windows Upgrade Compatibility
*****
The Windows 2000 Active Directory forest and domain need to be prepared for Windows.NET
=====
Setup has detected that the Active Directory forest and domain need to be prepared for
Windows.NET Server 2003.
```

**Description:**

- The forest and domains are prepared by using the adprep command on the schema operations master and infrastructure operations master, respectively.
- This domain controller is the schema operations master.
- To prepare the Active Directory forest and domains, perform the following procedures in the order provided.

To prepare an Active Directory forest for Windows.NET Server 2003:

1. To exit Setup, click Next, click Finish, and then click Exit.
2. At a command prompt, change to the \I386 directory on the installation media and then type:

```
adprep /forestprep
```

When prompted, type 'C', and then press ENTER to begin forest preparation, or type any other key, and then press ENTER to cancel.

3. After the forest preparation data has replicated throughout the forest, prepare the domains for Windows.NET Server 2003 as described below. The domain preparation operation must be performed on the infrastructure operations master of each domain in the forest.

To prepare an Active Directory domain for Windows.NET Server 2003:

1. On the domain controller holding the infrastructure operations master role, insert or connect to the installation media.
2. If the splash screen opens, click Exit.
3. At a command prompt, change to the \I386 directory on the installation media, and then type:

```
adprep /domainprep
```

If the command is run on a domain controller other than the current operations master, the name of the current operations master is displayed. In this case, repeat steps 1 through 3 on the current operations master.

4. After the domain preparation data has replicated throughout the domain, upgrade the domain controller by running Windows.NET Server 2003 Setup (I386\winnt32.exe on the installation media).

**Notes:**

- You cannot upgrade domain controllers in a forest without first preparing the forest and domains by using adprep on the schema and infrastructure operations masters, respectively.
- Depending on the replication schedule for your organization, the time it takes to propagate preparation data will vary.

IIS World Wide Web Publishing Service (W3SVC) will be disabled during upgrade

IIS World Wide Web Publishing Service (WWW service) Is Disabled During Upgrade

To protect your server from attacks by malicious users, the World Wide Web Publishing Service (WWW service) will be disabled during upgrade. Microsoft® Windows® 2000 Server installs Internet Information Services (IIS) by default, and requires administrators to secure IIS to prevent attacks.

The IIS Lockdown Wizard has not been run on this Windows 2000 server. If you do not want to allow the WWW service to be disabled, you must download and run the IIS Lockdown Wizard, or add the override registry key. Otherwise, you may continue with the upgrade and re-enable the WWW service after the upgrade has completed.

**Important:** If you use the World Wide Web Publishing Service (WWW service), we strongly recommend that you run the IIS Lockdown Wizard before upgrading to a product in the Windows.NET Server 2003 family. The IIS lockdown Wizard will help secure your computer by disabling or removing unnecessary features that are present in your Windows 2000 Server installation. These features would otherwise have remained on your machine after upgrading, leaving your server vulnerable to attacks. Using the IIS Lockdown Wizard instead of using the override registry key or re-enabling the WWW service after installation allows you to fine-tune the level of security to your particular needs.

When upgrading to a member of the Windows.Net Server 2003 family, the WWW service will NOT be disabled if any of the following conditions are present:

- You have already run the IIS Lockdown Wizard on your Windows 2000 server before starting the upgrade process. The IIS Lockdown Wizard reduces surface attack by disabling unnecessary features, and it allows you to decide which features to enable for your site. The IIS Lockdown Wizard is available at IIS Lockdown Tool (<http://go.microsoft.com/fwlink/?LinkId=8599>).
- The registry key RetainW3SVCStatus has been added to the registry under HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\W3SVC. Under RetainW3SVCStatus you can add any value and then assign a DWORD value to it. For example, you can create the key HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\W3SVC\RetainW3SVCStatus\do\_not\_disable with the DWORD value of 1.
- In the unattended install case, an entry "DisableWebServiceOnUpgrade = false" exists in the unattended install script.

After the upgrade is completed, you can enable the WWW service using either IIS Manager or the Services snap-in.

To start the World Wide Web Publishing Service after upgrade

In IIS Manager:

From the Start menu, point to Administrative Tools, and click Internet Information Services (IIS) Manager.

Expand the local computer, and then expand the Web Sites folder.

Right-click the Web site you want to start, and click Start.

Click Yes to enable the WWW service and start the Web site.

In the Services snap-in:

Click Start, point to Administrative Tools, and click Services.

In the list of services, right-click World Wide Web Publishing Service, and then click Properties.

On the General tab, in the Startup type list, click Automatic, and then click OK.

In the list of services, right-click World Wide Web Publishing Service, and then click Start.

Windows 2000 Administration Tools

=====

Setup has detected Windows 2000 Administration Tools on your computer. Windows 2000 Administration Tools are incompatible with Windows.NET Server 2003 family operating systems. Do one of the following:

\*) Cancel this upgrade, uninstall Windows 2000 Administration Tools, and then restart the upgrade.

\*) Complete this upgrade, and then install Windows.NET 2003 Administration Tools Pack by running the adminpak.msi Windows Installer package file. Adminpak.msi is located in the \i386 directory of your Windows.NET Server 2003 compact disc.

For more information about Windows.NET 2003 Administration Tools Pack installation requirements, see Microsoft Knowledge Base article Q304718 or visit <http://www.microsoft.com>

To remotely administer Server Services and Applications from a computer running Windows XP Professional or Windows.NET Server 2003, use Remote Desktop.

For a list of software supported by the Windows.NET Server 2003 family operating systems or Windows XP, see the list of compatible software on the Microsoft Web site at <http://go.microsoft.com/fwlink/?LinkId=9946>.

## Fax Services

=====

This version of Windows Fax will be installed as part of this upgrade, since an existing operating system Fax component is currently installed on this computer.

If you do not plan to use Fax, then for best security practice it is recommended that you uninstall it after the upgrade. You can remove the Fax component using Add or Remove Programs, Add\Remove Windows Components in the Control Panel.

For a list of software supported by this version of Windows, see the Microsoft Windows Compatibility List at <http://go.microsoft.com/fwlink/?LinkId=9946>.

Windows 95 and Windows NT 4.0 interoperability issues (Read Details!)

=====

Windows 95 and Windows NT 4.0 interoperability issues.

### SUMMARY

Windows.NET Server 2003 Domain Controllers implement default security settings that help prevent Domain Controller communications from being hijacked or otherwise tampered with. Certain downlevel machines are not capable of meeting these security requirements and thus cannot communicate with.NET Domain Controllers without administrative intervention.

Affected machines include Windows for Workgroups, Windows 95 machines that do not have the DS client pack installed, and Windows NT 4.0 machines prior to Service Pack 4.

### SMB SIGNING

By default, Windows.NET Server 2003 Domain Controllers require that all clients digitally sign SMB-based communications. The SMB protocol is used to provide file sharing, print sharing, various remote administration functions, and logon authentication for some downlevel clients. Windows for Workgroups, Windows 95 machines without the DS Client Pack, and Windows NT 4.0 machines prior to Service Pack 3 are not capable of performing SMB signing and therefore cannot connect to.NET Domain Controllers by default. If such clients cannot be upgraded to a current operating system or upgraded to meet the minimum requirements described above, then the SMB signing requirement can be removed by disabling the following security policy in the Default Domain Controller GPO on the domain controllers OU:

Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Microsoft Network Server: Digitally sign communications (always)  
Detailed instructions on how to modify this setting are provided below.

Warning: Disabling this security setting exposes all of your Domain Controller communications to "man in the middle" types of attacks. Therefore it is highly recommended that you upgrade your clients rather than disabling this security setting. The DS Client Pack, necessary for Windows 95 clients to perform SMB signing, can be obtained from the \clients\win9x sub-directory of the Windows 2000 Server CD.

### SECURE CHANNEL SIGNING

By default, Windows.NET Server 2003 Domain Controllers require that all secure channel communications be either signed or encrypted. Secure channels are used by Windows NT-based machines for communications between domain members and domain controllers as well as between domain controllers that have a trust relationship. Windows NT 4.0 machines prior to Service Pack 4 are not capable of signing or encrypting secure channel communications. If Windows NT 4.0 machines prior to SP4 must join this domain, or this domain must trust other domains that contain pre-SP4 Domain Controllers, then the secure channel signing requirement can be removed by disabling the following security policy in the Default Domain Controller GPO:

Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Domain Member: Digitally encrypt or sign secure channel data (always)

Detailed instructions on how to modify this setting are provided below.

**Warning: Disabling this security setting exposes secure channel communications to "man in the middle" types of attacks. Therefore it is highly recommended that you upgrade your Windows NT 4.0 machines rather than disabling this security setting.**

#### **MODIFYING THE DEFAULT DOMAIN CONTROLLER GPO**

To ensure all domain controllers are enforcing the same SMB and secure channel signing requirements, define the corresponding security settings in the Default Domain Controller GPO as follows:

1. Log on to a machine that has the Active Directory Users and Computers Snap-in installed.
2. Start → Run → DSA.MSC
3. Expand the Domain that contains your.NET Domain Controllers.
4. Right-click on the Domain Controllers OU and then click Properties.
5. Click the Group Policy tab, select the "Default Domain Controller Policy", and then click Edit.
6. Expand Computer Configuration, Windows Settings, Security Settings, Local Policies, Security Options
7. In the result pane, double click the security option you want to modify. For example, Microsoft Network Server: Digitally sign communications (always) or Domain Member: Digitally encrypt or sign secure channel data (always).
8. Check the "Define this policy setting" box.
9. Disable or Enable the security setting as desired and select OK.

#### **WinZip 6.3-8.0**

=====

WinZip 6.3-8.0 has a known compatibility issue with this version of Windows. For an update that is compatible with this version of Windows, contact Nico Mak Computing.

WinZip Computing, Inc. Web site: <http://www.winzip.com>

#### **WinZip 6.3-8.0**

=====

WinZip 6.3-8.0 has a known compatibility issue with this version of Windows. For an update that is compatible with this version of Windows, contact Nico Mak Computing.

WinZip Computing, Inc. Web site: <http://www.winzip.com>

\*\*\*\*\*

Observe que além da lista de incompatibilidades, o relatório aponta soluções, inclusive indicando o que deve ser feito passo-a-passo. Por exemplo, no início do relatório é informado que o Active Directory precisa ser preparado para a migração, conforme exemplificado no trecho inicial do relatório:

The Windows 2000 Active Directory forest and domain need to be prepared for Windows.NET

=====

Setup has detected that the Active Directory forest and domain need to be prepared for Windows.NET Server 2003.

#### **Description:**

- The forest and domains are prepared by using the adprep command on the schema operations master and infrastructure operations master, respectively.
- This domain controller is the schema operations master.
- To prepare the Active Directory forest and domains, perform the following procedures in the order provided.

To prepare an Active Directory forest for Windows.NET Server 2003:

1. To exit Setup, click Next, click Finish, and then click Exit.

...

**NOTA:** Você também pode executar o teste de compatibilidade, utilizando o comando winnt32.exe, da pasta i386 do CD de instalação do Windows Server 2003, com a opção /chekupgradeonly, conforme exemplo a seguir: winnt32/checkupgradeonly

## **Itens a serem verificados e/ou considerados antes de iniciar a instalação:**

Antes de iniciar a instalação do Windows Server 2003 você deve fazer uma espécie de inventário de alguns fatores. O primeiro deles é o teste de compatibilidade explicado anteriormente. Em seguida você deve verificar se o hardware atende os requisitos mínimos para o servidor onde será instalado o Windows Server 2003. Os requisitos mínimos dependem de uma série de fatores, tais como aplicações e serviços que serão executados no servidor, número de usuários simultâneos, volume de informações que será acessada e assim por diante.

Os requisitos mínimos de hardware foram apresentados no início deste capítulo. Mas lembre que estes são requisitos mínimos e não requisitos reais, que levam em conta a carga de trabalho a qual será submetida o servidor, uma vez que este seja colocado em operação.

Em seguida você deve decidir se será feita uma nova instalação ou se será feita a atualização de uma versão anterior do Windows já instalada, como o Windows 2000 Server ou o NT Server 4.0.

A vantagem de uma nova instalação é que você tem a certeza de partir com uma instalação sem problemas, sem arquivos corrompidos, sem comportamentos imprevistos e tantos outros problemas que podem surgir em uma instalação já existente. Ao fazer uma nova instalação é recomendado que você formate o Disco Rígido onde será feita a instalação (sempre lembrando de fazer um backup dos dados, se houver dados importantes no disco rígido que será formatado, pois este processo exclui toda a informação existente no disco rígido). Isso para o caso de você fazer uma nova instalação em um servidor já existente.

A desvantagem de fazer uma nova instalação é que todos os programas instalados e configurações serão perdidas. Você terá que reinstalar todos os programas e fazer as configurações novamente. Se você estiver fazendo a instalação de um novo servidor, esta é a única opção disponível.

Para servidores que já tem o Windows 2000 Server 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 vá fazer um upgrade, sempre é recomendável (eu diria até 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 2000 Server, das versões de servidor do Windows. Por exemplo, não é possível fazer um upgrade do Windows 2000 Professional ou do Windows XP Professional para o Windows Server 2003. Na Tabela 1.4, você tem uma relação dos caminhos de atualização de outras versões do Windows para o Windows Server 2003.

**Tabela 1.4 Caminhos para a atualização para o Windows Server 2003**

| <b>Versão anterior</b>      | <b>Pode atualizar para o Windows Server 2003?</b>  |
|-----------------------------|--|
| 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 Adv. Server    | Sim  |

| Versão anterior           | Pode atualizar para o Windows Server 2003? |
|---------------------------|--|
| Windows 2000 Professional | Não  |
| Windows XP Professional   | Não  |

Outra decisão que você deve tomar é se o servidor que está sendo instalado será um controlador de domínio ou um servidor para prestar outros serviços, como compartilhamento de arquivos, servidor Web, servidor de banco de dados e assim por diante. No caso de você estar fazendo uma atualização, é provável que o servidor continue a exercer as funções que estava exercendo antes.

Também é recomendado que você reuna as informações sobre as configurações de rede que serão utilizadas no servidor. Por exemplo:

- ◆ **O servidor fará parte de um domínio ou de um Workgroup?** (maiores detalhes sobre domínios e workgroups no Capítulo 2)
- ◆ **Qual o nome do servidor?** Sempre lembrando que não pode haver dois servidores com o mesmo nome, no mesmo domínio.
- ◆ **Configurações do protocolo TCP/IP.** Serão automáticas, obtidas a partir de um servidor DHCP? Ou serão configuradas manualmente. No caso de serem configuradas manualmente, você deve obter as seguintes informações com o administrador da rede: Número IP, máscara de sub-rede, número IP do Default Gateway, número IP de um ou mais servidores DNS, número IP de um ou mais servidores WINS (se existir servidores WINS na sua rede), nome de host e domínio DNS.

Eu também poderia iniciar uma discussão sobre o sistema de arquivos que deve ser utilizado na partição onde o Windows Server 2003 será instalado. Estão disponíveis os sistemas de arquivo FAT32 e NTFS, os quais serão detalhadamente esplícados no Capítulo 5. Porém são tantas as vantagens do sistema de arquivos NTFS, que nem vale a pena discutir. Servidor com o Windows Server 2003? Utilize NTFS. No Capítulo 5 você verá o porquê desta recomendação.

Antes de iniciar a instalação você também deve estar de posse do número de licença, o qual normalmente vem impresso em uma etiqueta colada na caixa do CD de instalação do Windows Server 2003.

Levantadas as informações necessárias e feito o teste de compatibilidade, você já está pronto para fazer a instalação do Windows Server 2003. No próximo item você acompanhará, passo-a-passo, a instalação do Windows Server 2003 Standard Edition em um novo computador, ou seja, uma instalação feita a partir do zero.

## Instalando o Windows Server 2003

Neste item você acompanhará todas as etapas da instalação do Windows Server 2003 em um novo servidor. O computador que estou utilizando, para este exemplo (e para a maioria dos exemplos deste livro), tem as seguintes características:

- ◆ Pentium de 1 GHz
- ◆ 512 MB de RAM
- ◆ Disco Rígido de 20 GB

**NOTA:** Para maiores detalhes sobre a instalação do Active Directory, domínios e a criação de Controladores de Domínio, consulte o Capítulo 2.

- ◆ Número IP: 10.10.100.50 (informado manualmente durante a instalação. Você deve utilizar as configurações do TCP/IP de acordo com o padrão da rede onde o servidor está sendo instalado. Para mais detalhes sobre os padrões de TCP/IP da sua rede, entre em contato com o Administrador da rede)
- ◆ Nome: MCSE70-290

## Instalando o Windows Server 2003 a partir do zero – boot a partir do CD-ROM

Agora vou fazer uma instalação do Windows Server 2003 Standard Edition a partir do zero, em um computador novo, onde ainda não existe nenhuma versão do Windows instalada. Utilizarei um dos métodos de instalação mais simples, que consiste em inicializar o sistema a partir do CD-ROM. Hoje em dia praticamente todos os computadores tem a capacidade de inicializar o sistema (ou, utilizando um termo popular na informática: “dar o boot”) a partir do CD-ROM, somente computadores mais antigos de quatro ou cinco anos atrás que não tem a capacidade de inicializar pelo CD-ROM.

Dependendo da quantidade de memória e da velocidade do processador a instalação pode demorar entre trinta e noventa minutos. Estou utilizando um computador com 512 MB de RAM, com um processador Pentium III de 1 GHZ.

Agora vamos aprender, passo –a passo, a fazer a instalação do Windows Server 2003.

Para instalar o Windows Server 2003 Standard Edition, em um computador novo, faça o seguinte:

1. Ligue o computador, insira o CD-ROM do Windows Server 2003 no drive e desligue o computador.
2. Agora ligue novamente o computador, desta vez o CD-ROM do Windows Server 2003 já deve estar no drive.
3. 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 inicialização a partir do CD-ROM. Fique atento a esta mensagem e se necessário pressione qualquer tecla para iniciar o boot a partir do CD-ROM.
4. O Windows Server 2003 começa a ser carregado a partir do CD-ROM.
5. Surge 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.
6. Aguarde alguns instantes até que os arquivos necessários à instalação sejam lidos do CD-ROM e copiados para uma pasta temporária no disco rígido do computador.
7. Surge uma tela com o título “Instalação do Windows Server 2003, Versão do Windows”. No computador que estou utilizando, vou instalar o Windows Server 2003 Standard Edition, com isso é exibido o seguinte título: “Windows Server 2003, Standard Edition”.
8. Nesta tela temos a opção de pressionar ENTER para continuar a instalação ou pressionar F3 para cancelar o processo de instalação.
9. Pressione ENTER para continuar com a instalação. É apresentada uma tela com três Opções: Enter para continuar, pressionar ‘R’ para Reparar uma instalação com problemas ou pressionar F3 para cancelar a instalação. Pressione Enter.

---

**NOTA:** O procedimento para fazer a instalação das demais edições do Windows Server 2003 é praticamente o mesmo.

---

**NOTA:** Em alguns computadores, a opção para dar o boot a partir CD-ROM não está automaticamente habilitada. Nestes casos você precisa entrar no Setup do sistema e configurar a opção para habilitar o boot pelo CD-ROM. Para entrar no Setup do sistema, basta pressionar várias vezes a tecla Del, logo após ter ligado o computador. Para orientações sobre a configuração do Setup, consulte o manual da placa mãe do seu equipamento, pois a configuração do Setup é diferente para cada tipo/modelo de placa mãe.

---

10. O programa de instalação faz algumas verificações e em seguida exibe uma tela com o “Contrato de Licença de Usuário Final”. Neste contrato estão os direitos e deveres do usuário, definidos pela licença do Windows Server 2003 que você adquiriu.
11. Para ler todo o contrato você pode utilizar a tecla Page Down para rolar o texto na tela.
12. Pressione a tecla F8 para aceitar o Contrato de Licença e seguir com a instalação.
13. Em seguida será exibida uma relação com todas as partições disponíveis no seu computador. Se for um computador novo será exibido apenas uma Partição ainda não formatada, com o espaço total do disco rígido. Nesta etapa temos as seguintes opções:
  - ◆ Você pode selecionar uma das partições que está sendo exibida e pressionar ENTER para instalar o Windows Server 2003 nesta partição.
  - ◆ Selecionar uma partição não formatada (aparece com a descrição “espaço não particionado – Unpartitioned Space) e pressionar a letra C para criar uma partição nova, onde será instalado o Windows Server 2003.
  - ◆ Selecionar uma partição e pressionar a letra D para excluir a partição. Fique atento, pois ao excluir uma partição, todos os dados desta partição serão excluídos.
14. Como estou instalando o Windows Server 2003 em um computador novo, o qual tem somente uma partição, a qual ocupa o tamanho total do disco rígido, basta selecionar esta partição e pressionar Enter.
15. O Windows Server 2003 será instalado na partição selecionada na pasta \WinNT, normalmente é no drive C:, na pasta C:\WinNT.
16. Se a partição escolhida ainda não estiver formatada você tem a opção de formatá-la. Neste momento você tem quatro opções:
  - ◆ NTFS (Rápido)
  - ◆ FAT (Rápido)
  - ◆ NTFS
  - ◆ FAT
17. O sistema de arquivos FAT vem desde a época do MS-DOS e somente é aconselhável caso você queira utilizar versões antigas do Windows, em conjunto com o Windows Server 2003, em uma máquina Multi-boot. Em equipamentos servidores não é recomendado o uso do sistema de arquivos FAT. No Capítulo 5 você aprenderá sobre as diversas vantagens do sistema de arquivos NTFS, em relação ao sistema de arquivos FAT.
18. Para poder utilizar as configurações de segurança do Windows Server 2003, tais como permissões de acesso e criptografia, você precisa do sistema de arquivos NTFS.
19. A diferença entre (Rápido) e sem o Rápido é quanto a maneira que o disco é formatado. A opção (Rápido), como era de se esperar, demora bem menos do que a outra opção.
20. Selecione a opção NTFS (Rápido) e pressione Enter.
21. Inicia o processo de formatação da partição escolhida. Aguarde alguns instantes, pois dependendo do tamanho do disco rígido pode demorar alguns minutos.
22. Após a formatação é feita uma análise da partição para verificar se não existem problemas com ela, tais como danos físicos no disco rígido.
23. Após a análise inicia um processo de cópia de arquivos do CD-ROM para o disco rígido. Neste momento são copiados os arquivos que darão suporte a próxima fase da instalação, a qual será iniciada após o encerramento da fase atual, quando o computador é inicializado novamente e então inicia a fase gráfica da instalação.

24. Ao final do processo de cópia surge uma mensagem avisando que o computador será reinicializado em 15 segundos. Se você não quiser aguardar os 15 segundos, basta pressionar Enter que o Computador será reinicializado imediatamente.
25. Após a reinicialização começa a parte gráfica do processo de instalação.
26. O processo de instalação continua trabalhando por conta.
27. A janela é dividida em duas partes. No painel da esquerda são exibidas as etapas da instalação já cumpridas (Coletando informações, Atualização dinâmica, Preparando a instalação) e as etapas restantes (Instalando o Windows, Finalizando a instalação), bem como uma estimativa do tempo restante para finalizar a instalação.
28. No painel da direita são exibidas mensagens sobre as novas características/funcionalidades do Windows Server 2003.
29. Durante esta fase são detectados e instalados os vários dispositivos de Hardware, e efetuadas as diversas configurações necessárias para o funcionamento do Windows Server 2003.
30. Aguarde até que as etapas sejam executadas até que surja a janela Opções regionais e de idiomas. Nesta tela definimos as configurações de idioma do Windows Server 2003. As configurações do idioma definem uma série de aspectos do Windows Server 2003. Por exemplo, o símbolo da moeda, o formato da data, se o relógio do sistema é de 12 ou de 24 horas e assim por diante. Estas configurações podem ser alteradas após a instalação do Windows Server 2003, utilizando o ícone Opções regionais e de idioma, do Painel de controle.
31. Defina as configurações Regionais e de Teclado adequadas ao equipamento e ao idioma que será utilizado.
32. Dê um clique no botão Avançar, seguindo para a próxima etapa da instalação.
33. Surge a janela Personalizar o software, pedindo que você digite o seu Nome e o nome da sua empresa.
34. Preencha os campos Nome e Organização e dê um clique no botão Avançar, seguindo para a próxima etapa da instalação.
35. Em seguida é exibida a janela Chave do produto (Product Key), na qual você deve digitar a chave de 25 dígitos que aparece na etiqueta do CD de instalação do Windows Server 2003.
36. Digite a chave solicitada e dê um clique no botão Avançar, seguindo para a próxima etapa da instalação.
37. Será exibida a janela Modo de Licenciamento, na qual você deve informar o modo de Licenciamento, a qual pode ser: Por servidor (Per Server) ou Por dispositivo ou por usuário (Per Device or Per User), de acordo com as licenças que você adquiriu.

A seguir descrevo as diferenças entre os dois modos de licenciamento:

- ◆ **Por Servidor:** Esta forma de licenciamento é mais indicado para pequenas empresas, nas quais existe um único servidor com o Windows Server 2003 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 no servidor, este último usuário 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, independentemente 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 CALs, uma para cada estação de trabalho. O preço de uma CAL para este modo de

licenciamento é maior do que para o Per Server, mas em compensação com uma única CAL, a estação de trabalho pode acessar recursos em qualquer servidor que esteja utilizando o licenciamento Per Device

38. Informe o modo de licenciamento e o número de licenças e dê um clique no botão Avançar, seguindo para a próxima etapa da instalação.
39. Surge a janela Nome do computador e senha do administrador.
40. Se você estiver instalando o Windows Server 2003 em um computador residencial ou em uma pequena rede que você mesmo administra, você pode selecionar o nome do computador sem maiores problemas. Se você está instalando o Windows Server 2003 em uma estação de trabalho de uma rede corporativa, consulte o Administrador da rede para saber se existe algum padrão de nomes para as estações de trabalho e para os servidores da rede. O nome do computador é importante pois é através do nome que acessamos os recursos compartilhados, tais como pastas e impressoras, do computador.
41. Para nome digite MCSE70-290 (ou outro nome que você irá utilizar em sua rede).
42. Também é solicitada uma senha para o usuário Administrador. Ao instalar o Windows Server 2003, automaticamente, é criada uma conta chamada Administrador (na versão em Português, Administrator na versão em Inglês). Esta conta tem permissão para realizar qualquer operação no computador: instalar e desinstalar dispositivos de Hardware, instalar e desinstalar programas e até mesmo formatar o disco rígido. Por isso é importante a definição de uma senha para a conta Administrador, pois se deixarmos a senha em branco, qualquer usuário poderá fazer o logon como Administrador e ter acesso a todos os recursos do computador.
43. Digite a seguinte senha: senhaXYZ ou outra senha qualquer que você for utilizar. É importante definir uma senha que não seja fácil de ser descoberta. Falarei mais sobre a definição de senhas no Capítulo 4.
44. Digite novamente a senha escolhida no campo Confirmar senha.
45. Dê um clique no botão Avançar seguindo para a próxima etapa da instalação. Pode ser exibida uma janela informando que a senha selecionada não atende a critérios de segurança. O Windows Server 2003 sugere que você utilize uma senha de, no mínimo, 6 caracteres, que sejam utilizados caracteres não alfanuméricos (;, / \* e assim por diante). Clique em Sim para aceitar a senha digitada anteriormente.
46. Se você tiver um modem conectado ao computador, o Windows Server 2003 detecta o modem e abre uma janela para que você selecione em qual país região você está, qual o código DDI do seu país, se é necessário digitar um número para ter acesso a uma linha externa e o tipo de discagem: De tom ou de pulso.
47. Preencha as informações sobre discagem, caso você tenha um modem conectado.
48. Dê um clique no botão Avançar seguindo para a próxima etapa da instalação.
49. Surge uma janela para que você confira a data, a hora e o fuso horário. Verifique se as informações estão corretas e altere o que for necessário.
50. Dê um clique no botão Avançar seguindo para a próxima etapa da instalação.
51. Caso exista uma placa de rede conectada ao micro, será iniciado o processo de instalação da rede.
52. Temos duas opções para a configuração de rede:
  - ◆ **Configurações típicas:** Esta opção é utilizada quando você instala o Windows Server 2003 em uma estação de trabalho de uma rede corporativa. Com esta opção as configurações de rede são carregadas, a partir de um servidor DHCP (veja Capítulo 16 do livro Windows Server 2003 – Curso Completo, 1568 páginas), toda vez que o computador é ligado. Não é utilizada em redes que não tenham servidores de rede. Se o Servidor que você está instalando deve ser um controlador de domínio (DC), ele deverá ter um número IP fixo. Neste caso ele não poderá utilizar esta opção.

- ◆ **Configurações personalizadas:** Com esta opção é aberta uma janela para que sejam informados diversos parâmetros para configuração da rede. Por padrão, é instalado o protocolo TCP/IP. Para que dois computadores possam trocar informações, ambos devem ter instalado o mesmo protocolo para comunicação na rede. O protocolo mais utilizado, que é o padrão no Windows Server 2003 é o protocolo TCP/IP, o qual também é utilizado na Internet.
53. Selecione a opção Configurações personalizadas.
54. Dê um clique no botão Avançar seguindo para a próxima etapa da instalação.
55. Nesta etapa é exibida a marca/modelo da placa de rede que foi detectada pelo Windows Server 2003. Vamos alterar alguns parâmetros do protocolo TCP/IP.
56. Dê um clique na opção Protocolo TCP/IP e depois dê um clique no botão Propriedades.
57. Surge a janela de propriedades do protocolo TCP/IP. Marque a opção Usar o seguinte endereço IP.
58. Preencha os seguintes campos com os seguintes valores (ou substitua por valores que você estiver utilizando em sua rede):
- ◆ Endereço IP: 10.100.100.50
  - ◆ Máscara de rede: 255.255.255.0
  - ◆ Default Gateway: 10.100.100.1
  - ◆ Preferred DNS Server: 10.100.100.5
59. Dê um clique no botão OK.
60. Dê um clique no botão Avançar seguindo para a próxima etapa da instalação.
61. Surge uma janela perguntando se o computador fará parte de um grupo de trabalho (Workgroup) ou de um domínio. Grupos de trabalhos são utilizados para pequenas redes, de até 5 computadores, onde não existem servidores com o Windows 2000 Server ou Windows Server 2003 instalado. Domínios são utilizados em redes empresariais, com um grande número de equipamentos, onde existem servidores com o Windows 2000 Server ou Windows Server 2003 instalado. Falaremos mais sobre Workgroup e Domínios no Capítulo 2.
62. Selecione a opção “Não, o computador não está em uma rede ou está em uma rede sem um domínio. Tornar este computador um membro do seguinte grupo de trabalho:”.
63. No campo para digitação do nome do grupo de trabalho digite GROZA ou outro nome qualquer que você for utilizar para a sua instalação.
64. Dê um clique no botão Avançar seguindo para a próxima etapa da instalação.
65. A instalação do Windows Server 2003 continua, automaticamente com mais algumas etapas: cópia de arquivos, registro de componentes, configurações do menu Iniciar e assim por diante.
66. Ao final desta etapa o computador é automaticamente reinicializado.
67. O computador reinicia, a nova tela do Windows Server 2003 já é exibida. A primeira inicialização demora um pouco mais do que o normal, pois são feitas diversas configurações necessárias para o funcionamento do Windows Server 2003.
68. Uma pequena animação com o logotipo do Windows Server 2003 é exibida e logo em seguida é exibida a tela de Logon. Pressione Ctrl+Alt+Del e faça o logon com a conta Administrador e a senha definida durante a instalação. Pronto, o Windows Server 2003 está instalado e você já fez o primeiro logon. Ao fazer o primeiro logon o aplicativo Configure o seu Servidor (Manage Your Server) será exibido. Feche este aplicativo. Agora vamos ativar o Windows.

---

**NOTA:** Estes são valores que utilize em uma rede residencial. Consulte o Administrador de rede sobre os valores que você deve utilizar para as configurações do protocolo TCP/IP

---

69. Selecione o comando Iniciar -> Todos os programas -> Acessórios -> Ferramentas do sistema -> Ativar o Windows. Se você tiver conectado à Internet a ativação pode ser feita automaticamente, caso contrário você terá que fazer a ativação por telefone. Se você não fizer a ativação o Windows Server 2003 somente funcionará por 14 dias, ao final deste período o sistema deixa de funcionar.
70. Será exibido o Assistente para Ativação. Marque a primeira opção “Sim, Ativar o Windows Através da Internet Agora”. Clique no botão Avançar, seguindo para a próxima etapa do assistente de ativação.
71. Nesta etapa marque a segunda opção, indicando que você quer somente ativar o Windows, sem fazer o registro junto à Microsoft, neste instante e clique no botão Avançar, seguindo para a próxima etapa do assistente.
72. Surge uma tela para configuração da sua conexão com a Internet. Nesta tela informamos se a conexão será feita por Modem, por um serviço baseado em DSL (assinante de linha digital) ou através de uma rede local.
73. Vamos fazer uma conexão via Modem/linha discada.
74. Selecione a opção Discagem usando um Modem. Dê um clique no botão Avançar, seguindo para a próxima etapa da configuração.
75. Surge uma tela informando que o Windows Server 2003 fará uma discagem para ativar o Windows. Clique em Avançar para iniciar a discagem.
76. O Windows Server 2003 disca para um servidor de ativação da Microsoft, conecta e faz a ativação do Windows. Ao final uma mensagem de que a ativação foi efetuada com sucesso é exibida.
77. Clique em OK e pronto, o Windows Server 2003 foi ativado, a Área de trabalho do Windows Server 2003 é exibida e estamos pronto para utilizá-lo.

## Instalação não assistida e arquivo de respostas

Você pode automatizar a instalação do Windows Server 2003 utilizando um arquivo de respostas. O arquivo de respostas é um arquivo.txt, com um padrão bem definido. No arquivo de respostas estão contidas as respostas às telas de instalação do Windows Server 2003. Com o uso do arquivo de respostas, a instalação do Windows Server 2003 segue, passo-a-passo, sem a necessidade de intervenção do usuário (por isso que é chamada de instalação não assistida). As informações necessárias em cada etapa da instalação são lidas a partir do arquivo de respostas, no qual podemos inserir informações tais como:

- ◆ Chave do Produto (Product Key)
- ◆ Nome da empresa
- ◆ Nome do computador
- ◆ Configurações do protocolo TCP/IP
- ◆ Quais componentes do Windows Server 2003 devem ser instalados
- ◆ Pasta de instalação
- ◆ Pasta onde estão os arquivos de instalação
- ◆ Domínio ou Workgroup do qual o servidor fará parte, dentre outros.

Uma vez criado o arquivo de respostas, você utiliza um parâmetro de linha de comando, ao iniciar a instalação, para informar o caminho e o nome do arquivo de respostas. Uma vez localizado o arquivo de respostas, a instalação inicia, todas as informações de cada etapa são lidas a partir do arquivo de respostas, sem que seja necessária a intervenção do usuário. Este processo pode ser automatizado, onde os arquivos de respostas são colocados em uma pasta compartilhada na rede e a instalação ou upgrade dos servidores pode ser automatizada através do uso de scripts. A seguir detalho os passos para fazer uma instalação não assistida do Windows Server 2003.

## O arquivo de respostas

Para facilitar o arquivo de respostas, você encontra um modelo deste tipo de arquivo, no CD de instalação do Windows Server 2003.

Para acessar o modelo de arquivo de respostas, siga os seguintes passos:

1. Insira o CD de instalação do Windows Server 2003 no drive.
2. O Assistente de instalação será aberto. Feche-o.
3. Abra o Meu computador, clique com o botão direito do mouse no drive de CD e, no menu que é exibido, clique em Explorar.
4. O Windows Explorer será aberto e as pastas do CD de instalação serão exibidas.
5. Acesse a pasta i386 do CD de instalação. Nesta pasta localize o arquivo unattended.txt e dê um clique duplo nele.

O arquivo será aberto, e o conteúdo indicado a seguir será exibido:

```
; Microsoft Windows
; (c) 1994 - 2001 Microsoft Corporation. All rights reserved.
;
; Sample Unattended Setup Answer File
;
; This file contains information about how to automate the installation
; or upgrade of Windows so the Setup program runs without requiring
; user input. You can find more information in the ref.chm found at
; CD:\support\tools\deploy.cab
;
[Unattended]
Unattendmode = FullUnattended
OemPreinstall = NO
TargetPath = *
Filesystem = LeaveAlone

[GuiUnattended]
; Sets the Timezone to the Pacific Northwest
; Sets the Admin Password to NULL
; Turn AutoLogon ON and login once
TimeZone = "004"
AdminPassword = *
AutoLogon = Yes
AutoLogonCount = 1

[LicenseFilePrintData]
; For Server installs
AutoMode = "PerServer"
AutoUsers = "5"

[GuiRunOnce]
; List the programs that you want to lauch when the machine is logged into for the first
time

[Display]
BitsPerPel = 16
XResolution = 800
YResolution = 600
VRefresh = 70

[Networking]

[Identification]
JoinWorkgroup = Workgroup

[UserData]
```

```

FullName = "Your User Name"
OrgName = "Your Organization Name"
ComputerName = *

ProductKey      = "XXXXX-YYYYY-ZZZZZ-99999-00000"
*****  

O arquivo de respostas é dividido em seções. Em cada seção estão respostas para uma etapa  

da instalação. No exemplo da seção a seguir, é definido o modo de licenciamento e o número  

de licenças:
[LicenseFilePrintData]
;For Server installs
AutoMode = "PerServer"
AutoUsers = "5"

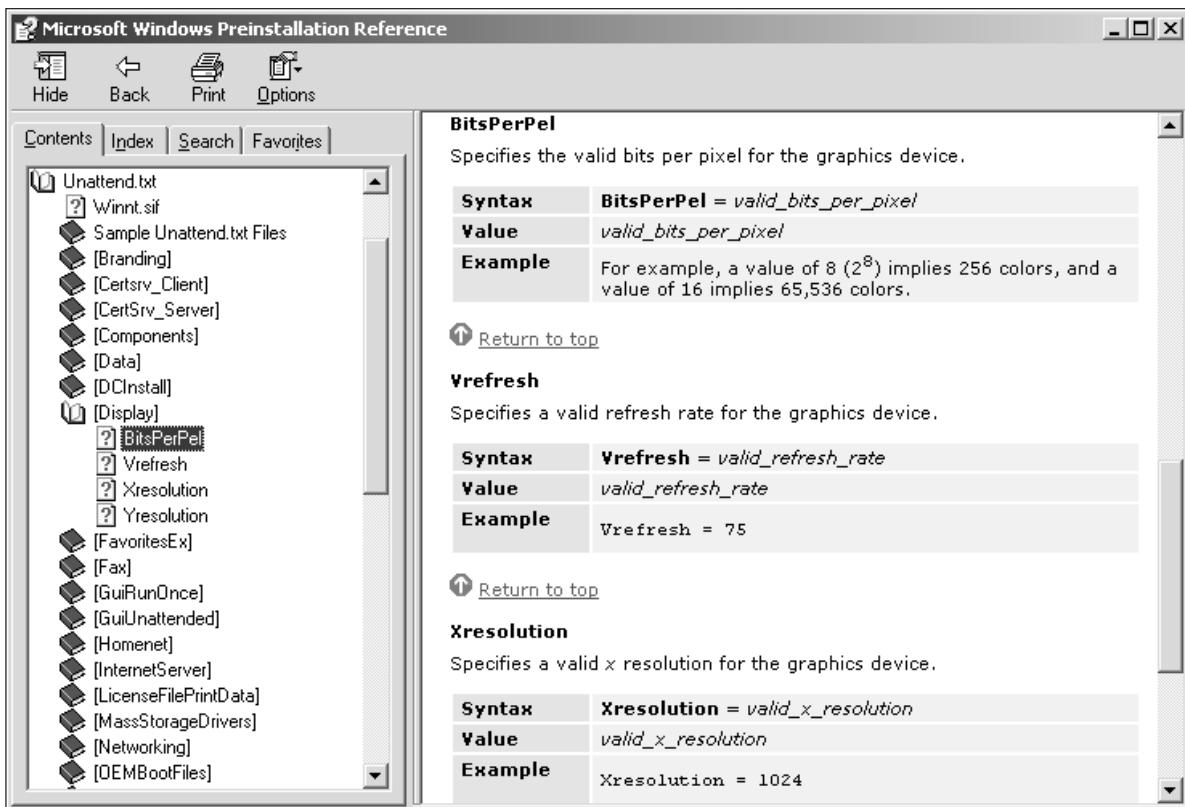
```

Esta seção serve como resposta para a etapa onde você deve informar o tipo de licença e o número de licenças adquiridas – etapa 37 do processo de instalação descrito no item anterior.

O formato do arquivo unattended.txt é bastante descritivo. Você encontra uma descrição completa sobre todas as seções e todos os parâmetros que podem ser definidos em um arquivo de respostas (arquivo este que pode ter qualquer nome, não obrigatoriamente unattended.txt), no arquivo de ajuda ref.chm, o qual está contido no arquivo compactado deploy.cab. O arquivo deploy.cab encontra-se na pasta support\tools, do CD de instalação do Windows Server 2003. A seguir descrevo como extrair o arquivo ref.chm para a pasta Meus documentos e depois abri-lo.

Para extrair o arquivo ref.chm, siga os seguintes passos:

1. Insira o CD de instalação do Windows Server 2003 no drive.
2. O Assistente de instalação será aberto. Feche-o.
3. Abra o Meu computador, clique com o botão direito do mouse no drive de CD e, no menu que é exibido, clique em Explorar.
4. O Windows Explorer será aberto e as pastas do CD de instalação serão exibidas.
5. Acesse a pasta \support\tools.
6. Dê um clique duplo no arquivo deploy.cab. O conteúdo do arquivo deploy.cab será exibido no painel da direita do Windows Explorer.
7. Clique com o botão direito do mouse no arquivo ref.chm.
8. No menu que é exibido clique na opção Extrair (Extract).
9. Na janela que é exibida clique em Meus documentos.
10. Clique em OK.
11. Clique em Extrair (Extract).
12. Abra a pasta Meus documentos.
13. Dê um clique duplo no arquivo ref.chm.
14. O arquivo de ajuda “Microsoft Windows Preinstallation Reference” será aberto. No painel da esquerda dê um clique duplo na opção Unattend.txt. Serão exibidas todas as possíveis seções de um arquivo de respostas.
15. Dê um clique duplo em uma das seções. Serão exibidos todos os possíveis parâmetros desta seção. Ao clicar em um parâmetro será exibida a sintaxe de utilização e um exemplo, conforme indicado na Figura 1.30, onde foi aberta a opção Display e estão sendo exibidas informações sobre a opção BitsPerPel (que não é difícil de concluir que é o parâmetro que define a resolução do vídeo – Bits Por Polegada).
16. Feche o arquivo ref.chm



**Figura 1.30 Utilizando o arquivo ref.chm.**

Com base no arquivo de respostas de modelo – unattended.txt e no arquivo de ajuda ref.chm, você pode criar arquivos de respostas personalizado, para fazer as instalações não assistidas, nos servidores da rede. Este método é particularmente útil se você estiver instalando ou fazendo a atualização de um grande número de servidores.

## Como utilizar o arquivo de respostas durante a instalação?

Após ter criado o arquivo de respostas, você pode utilizar o comando winnt32.exe (que está na pasta i386 do cd de instalação do Windows Server 2003), para iniciar a instalação. Para informar o caminho e o nome do arquivo de respostas, você utiliza o parâmetro /unattend:[answer\_file], como no exemplo a seguir, onde estou utilizando o arquivo de respostas respostas.txt, na pasta instala do drive C:

```
Winnt32 /unattend:C:\instala\respostas.txt
```

Este comando inicia a instalação do Windows Server 2003 e utiliza o arquivo C:\instala\respostas.txt como um arquivo de respostas, durante a instalação.

Nota: Além do arquivo de respostas de exemplo e do arquivo de ajuda ref.chm, o Windows Server 2003 também oferece um assistente para a criação de um arquivo de respostas. Você inicia o assistente e, em cada etapa vai preenchendo informações, como o nome do computador, senha do Administrador, Chave do produto, nome do domínio e assim por diante. Ao final do processo, o assistente gera um arquivo.txt, no padrão de um arquivo de respostas e utilizando as informações que você forneceu nas diversas etapas do assistente. Este assistente para criação de um arquivo de respostas, está contido no arquivo deploy.cab da pasta \support\tools do cd de instalação do Windows Server 2003. Acesse o arquivo deploy.cab, conforme descrito anteriormente e copie todos os arquivos contidos no deploy.cab para uma pasta no disco rígido. Depois vá para esta pasta e execute o arquivo Setupmgr.exe. Agora é só seguir as etapas do assistente para criar uma arquivo de respostas com base nas informações que você fornecer para o assistente.

Além da opção /unattended, o comando winnt32.exe tem várias outras opções de linha de comando, opções estas que afetam a maneira como a instalação do Windows Server 2003 é realizada. Para ver uma tela de ajuda, com a descrição completa de todas as opções do comando winnt32.exe, execute o seguinte comando: Winnt32/?

## Conclusão

Um longo capítulo, sem dúvidas. Mas necessário, igualmente, sem dúvidas. Este capítulo serviu como uma espécie de Apresentação do Windows Server 2003. Na parte inicial do Capítulo apresentei uma visão geral de uma rede baseada no Windows Server 2003. Falei sobre o conceito de uma rede Cliente/Servidor e sobre o Protocolo TCP/IP

Em seguida você foi apresentado as quatro edições do Windows Server 2003:

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

Falei sobre as principais características de cada edição, destacando as limitações de Hardware de cada uma das edições. Você aprendeu que cada uma das diferentes edições é utilizada em situações diferentes. Por exemplo, o Windows Server 2003 Standard Edition é recomendado para o uso como um servidor de arquivos e impressão ou um controlador de domínios para redes de pequenas empresas ou redes departamentais de porte de pequeno para médio. Já o Windows Server 2003 Data Center Edition é a edição peso-pesado, indicada para o uso em servidores de aplicações de missão crítica, os quais devem atender a um grande número de usuários, garantindo um desempenho, disponibilidade e um nível de segurança satisfatórios.

Apresentei uma tabela com os requisitos de Hardware mínimos e recomendados, para cada edição. Claro que os requisitos mínimos são apenas para constar nos manuais. A quantidade de memória e processamento necessária varia com diversos fatores, tais como o número de aplicativos, serviços e usuários que deverão ser atendidos pelo servidor. Agora vamos ser sinceros, mesmo sendo apontado como valor mínimo, você consegue imaginar o Windows Server 2003 Enterprise Edition, rodando em um Pentium 133 com 128 MB de RAM? Nem o Windows 2000 Professional rodaria bem em um equipamento destes.

Na seqüência apresentei uma série de novidades do Windows Server 2003. As novidades foram divididas em categorias, para facilitar o acompanhamento. Você encontra uma descrição detalhada, de todas as novidades do Windows Server 2003, em uma das seguintes fontes:

- ◆ Internet: <http://www.microsoft.com/windowsserver2003/evaluation/overview/technologies/default.mspx>
- ◆ Livro: Introducing Microsoft Windows Server 2003, Microsoft Press (<http://www.microsoft.com/mspress/books/5869.asp>)

Neste capítulo você também encontrou uma série de termos que talvez você ainda não conheça. Se você já trabalha com o Windows 2000 Server, termos como Active Directory, Group Policies Objects (GPOs), DNS, WINS, DHCP e tantos outros, já devem ser conhecidos. Se você nunca trabalhou com o NT Server 4.0 ou com o Windows 2000 Server, então a maioria destes termos provavelmente não são conhecidos para você. Mas não se preocupe, ao longo deste livro você aprenderá sobre os principais recursos do Windows Server 2003, relacionados ao Exame 70-290. Aprenderá a instalar os principais recursos, configurá-los e administrá-los.

Este foi um capítulo quase que totalmente teórico. Foram apresentados conceitos importantes para que o leitor possa entender a parte prática que será apresentada no restante do livro. Por exemplo, é impossível entender e administrar serviços como o DNS e DHCP, sem conhecer os princípios básicos do TCP/IP apresentados neste capítulo.

Iniciei com a apresentação do que vem a ser uma rede de computadores. Neste item fiz um retrospectiva desde a época em que o único modelo disponível era o modelo do Mainframe, até os modernos modelos baseados em aplicativos de n camadas.

Nesta parte apresentei com um pouco mais de detalhes o conceito de uma rede baseada no modelo Cliente/Servidor. O trecho a seguir resumo o que foi apresentado neste item:

1. Na época do Mainframe os aplicativos e os dados ficavam no Mainframe. O acesso era feito através de terminais, conhecidos como terminais burros. A administração era feita centralizadamente, o que facilitava a atualização e manutenção das aplicações.
2. No modelo Cliente/Servidor clássico a aplicação e a lógica ficava no programa instalado na estação de trabalho cliente e os dados no servidor de banco de dados. Isso gera dificuldades para atualização das aplicações e um elevado custo para manter este modelo funcionando.
3. A nova tendência é portar as aplicações para um modelo de n camadas, onde as aplicações, a lógica e os dados ficam em servidores (de aplicações, Web e de banco de dados) e o acesso é feito através de um Navegador.
4. Puxa, mas o modelo em n camadas é praticamente o mesmo modelo do Mainframe, com aplicações e dados no servidor, administração centralizada e redução no custo de propriedade (TCO) em relação ao modelo Cliente/Servidor tradicional? É isso mesmo, este modelo é muito próximo do modelo do Mainframe, porém com todas as vantagens da evolução da informática nestas últimas décadas, tais como interfaces gráficas, programas mais poderosos e por aí vai.

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 da época do Mainframe.

Posso citar o exemplo de um dos bancos com os quais trabalho. Quando vou ao banco renovar um seguro ou tratar algum assunto diretamente com o gerente, vejo que ele tem na sua estação de trabalho, aplicativos de produção do dia-a-dia, tais como o Microsoft Word, Microsoft Excel, um aplicativo de cálculos e análise de crédito e assim por diante. Este mesmo gerente utiliza o site da empresa para fornecer informações. Ele também utiliza a Internet da empresa para se manter atualizado. Além disso ele utiliza alguns sistemas que ainda residem no bom e velho mainframe. Por exemplo, quando eu peço que ele faça uma alteração no meu endereço de correspondência, ela acessa a famosa telinha verde, de um programa emulador de terminal, que acessa uma aplicação que está no Mainframe da empresa.

Este caminho me parece muito mais sensato, ou seja, não precisa ser um ou outro modelo, mas sim o melhor dos dois mundos.

Seguindo a exposição teórica, falei sobre os papéis que os servidores baseados no Windows Server 2003 podem desempenhar em uma rede. Também mostrei outros produtos da Microsoft que são projetados para trabalhar em conjunto com o Windows Server 2003, como por exemplo o SQL Server 2000 que é o servidor de banco de dados da Microsoft, o Exchange Server 2000 que é o servidor de correio eletrônico e plataforma para desenvolvimento de aplicações de colaboração e Workflow.

Seguindo, tratei de um assunto extremamente importante: O protocolo TCP/IP.

Apresentei os conceitos básicos do protocolo, iniciando pela definição de protocolo e pelo papel do TCP/IP em uma rede de computadores. Em seguida falei sobre os parâmetros do TCP/IP que devem estar configurados em um computador, tais como:

- ◆ Número IP
- ◆ Máscara de sub-rede
- ◆ Default Gateway
- ◆ Servidor DNS

Você também aprendeu um pouco sobre sistemas de numeração, mais especificamente sobre o sistema de numeração decimal e o sistema de numeração binário. Aprendeu a fazer alguns cálculos básicos. Em seguida mostrei como o TCP/IP utiliza a aritmética binária para determinar se dois computadores estão na mesma rede ou em redes diferentes.

Encerrei o tópico sobre TPC/IP apresentando os conceitos básicos sobre Roteamento e apresentando um exemplo detalhadamente explicado, com os passos envolvidos no roteamento de informações entre duas redes distantes, ligadas através de um link de WAN.

No próximo passo você aprendeu a instalar o Windows Server 2003. Antes de fazer a instalação você aprendeu sobre quais as informações que devem ser averiguadas e como fazer um teste de verificação de compatibilidade.

Antes de instalar o Windows Server 2003 você também deve decidir se fará uma instalação nova, a partir do zero ou se fará uma atualização (upgrade) de um servidor já existente. Uma nova instalação tem a vantagem de partir do zero, sem os problemas que uma instalação mais antiga pode apresentar, em compensação, após uma nova instalação, todos os programas terão que ser reinstalados e as configurações refeitas. Já uma atualização mantém todos os programas e configurações, porém pode “herdar” problemas que já existiam com a versão anterior do Windows, tais como arquivos corrompidos ou problemas de configuração.

O processo de instalação, conforme você pode conferir, é extremamente simples. Basicamente é seguir os passos de um assistente em duas etapas: uma etapa no modo caractere e outra no modo gráfico.

Também é possível fazer uma instalação sem a intervenção do usuário, conhecida como instalação não assistida. Para fazer uma instalação não assistida, você precisa de um arquivo de respostas. O arquivo de respostas é um arquivo.txt com um padrão bem definido. Para criar uma arquivo de respostas, o Windows Server 2003 fornece algumas ferramentas: um arquivo de respostas de exemplo – unattended.txt; um arquivo de referência – ref.chm e um assistente para a criação de arquivos de respostas personalizados – Setupmgr.exe. Uma vez criado o arquivo de respostas, basta iniciar a instalação usando o comando winnt32 /unattended:[caminho e nome do arquivo de respostas].

A seguir coloco alguns endereços no site da Microsoft, onde você encontra mais informações sobre a instalação do Windows Server 2003 e sobre a criação de instalações automatizadas mediante o uso de arquivos de respostas:

<http://www.microsoft.com/windows/reskits/default.asp>

<http://www.microsoft.com/windowsserver2003/techinfo/reskit/deploykit.mspx>

<http://www.microsoft.com/downloads/details.aspx?familyid=aaf0a7a4-71c1-4ee9-b974-66214651a23b&displaylang=en>

<http://download.microsoft.com/download/8/e/c/8ec3a7d8-05b4-440a-a71e-ca3ee25fe057/rktools.exe>  
(arquivo com diversas ferramentas do Resource Kit para o Windows Server 2003).

Sei que um capítulo teórico é sempre, digamos, “mais chato” de acompanhar. Porém tenha certeza amigo leitor, os conceitos apresentados neste capítulo irão ajudá-lo a entender melhor a parte prática dos demais capítulos deste livro. Caso tenha ficado alguma dúvida sobre algum conceito deste capítulo, peço que você volte ao ponto onde está a dúvida e leia novamente. É muito importante que você entenda os conceitos aqui apresentados, antes de seguir adiante.

# Introdução

O Active Directory foi, sem dúvidas, a grande novidade do Windows 2000 Server em relação ao Windows NT Server 4.0. No Windows Server 2003 o Active Directory também é o elemento central, fundamental, sobre o qual é planejada e implementada uma infra-estrutura de rede.

Neste capítulo farei um estudo teórico, detalhado do Active Directory. Desde a definição e as vantagens de se usar um serviço de diretórios, passando pela definição dos componentes do Active Directory, da estrutura lógica e física, até a apresentação de conceitos mais elaborados como por exemplo o controle de replicação entre os Controladores de Domínio (abreviados como DC).

Eu poderia, ao longo do livro, ir mostrando como trabalhar com os diversos elementos do Active Directory. Por exemplo, no Capítulo 4, quando falarei sobre usuários, eu poderia citar que usuário é um dos principais tipos de objetos do Active Directory. Porém considerei importante a colocação de um capítulo teórico como este, no qual apresento e explico os diversos elementos que compõem o Active Directory. Com isso o amigo leitor pode ter uma visão ampla e completa do que é exatamente o Active Directory, de quais os principais elementos que o compõem e da sua estrutura física e lógica.

Vou iniciar o capítulo falando sobre o conceito de diretório. Mostrarei o que exatamente é um diretório (talvez o termo mais adequado, em Português, fosse Catálogo ao invés de Diretório), porque hoje encontramos múltiplos diretórios na rede da empresa. Também mostrarei os problemas advindos do fato de se ter múltiplos diretórios e de como este fato cria problemas para o desenvolvimento de aplicações e para a integração dos sistemas informatizados de uma empresa.

Em seguida vou fazer uma introdução ao Active Directory no Windows Server 2003. Mostrarei o seu papel em uma rede com servidores baseados no Windows Server 2003 e o que deve ser feito para que o Active Directory seja instalado em um servidor, tornando o servidor um DC.

Feitas as devidas apresentações e conceituações é hora de apresentar os elementos que compõem e mantêm em funcionamento o Active Directory. Vou iniciar pelos elementos individuais, apresentando conceitos tais como:

- ◆ Domínios
- ◆ Árvores
- ◆ Florestas
- ◆ Relações de confiança
- ◆ Objetos do Active Directory
- ◆ Unidades Organizacionais
- ◆ Schema

Estes elementos compõem a chamada estrutura lógica do Active Directory, ou seja, a maneira como o Active Directory é apresentado ao Administrador e aos usuários, quando estes utilizam as ferramentas de administração e pesquisa do Active Directory.

# CAPÍTULO

## 2

### Active Directory – Conceitos, Estrutura Lógica e Física e Componentes

A estrutura lógica pode ser diferente (e normalmente é) da estrutura física. A estrutura física determina onde são armazenadas as informações do Active Directory, como as informações são sincronizadas entre os diferentes DCs do domínio (chamamos este processo de replicação). Também serão apresentados e explicados os conceitos de sites, replicação inter sites e intra sites.

Acredite amigo leitor, pode parecer um pouco “chato”, toda esta teoria sobre o Active Directory. Mas posso garantir que conhecendo os conceitos apresentados neste capítulo, será muito mais fácil planejar, implementar e administrar uma infra-estrutura de rede baseada no Windows Server 2003 e no Active Directory. Também será muito mais fácil entender a utilização das ferramentas administrativas que serão descritas nos demais capítulos do livro – aí sim, a parte prática, baseada nos conceitos teóricos, aqui apresentados.

Na seqüência do capítulo você aprenderá a instalar o Active Directory, transformando um servidor em Controlador de Domínio (DC – Domain Controller). Existem diferentes situações em que você cria um DC e todas serão discutidas neste capítulo.

Por exemplo, pode ser que você esteja instalando o primeiro DC de um domínio. Nesta situação o domínio, na verdade, nem sequer ainda existe. Ele passará a existir quando o primeiro DC for instalado. O primeiro DC de um domínio assume uma série de funções especiais, funções estas que existem em apenas um dos DCs dos domínios. Os servidores que executam esta função são conhecidos como FSMO (Flexible Single Master of Operators). Neste capítulo falarei sobre os FSMOs e suas funções.

Existem algumas ações que devem ser realizadas antes da instalação do Active Directory. Estas ações variam, dependendo se você está atualizando o Active Directory do Windows 2000 Server ou se você está criando um novo domínio. Mostrarei quais as ações de preparação necessárias em cada caso.

Também apresentarei um exemplo prático de como instalar o Active Directory e criar um novo domínio. Você verá que o assistente para instalação do Active Directory é extremamente simples de ser utilizado, desde que você conheça os conceitos apresentados no Capítulo 5, tais como: domínios, árvores de domínios e assim por diante.

Você também pode executar o assistente de instalação do Active Directory para desinstalar o Active Directory, fazendo com que um DC volte a ser um Member Server (se pertencer a um domínio) ou um Stand Alone Server, se pertencer a um workgroup. A operação de desinstalar o Active Directory é conhecida como “Rebaixar o DC” e a operação de instalar o Active Directory, é conhecida como promover o member server (ou stand alone server).

Após a instalação do Active Directory, uma série de alterações serão efetuadas no servidor. Novos arquivos serão criados (com a base de dados do Active Directory), novas ferramentas administrativas estarão disponíveis e assim por diante. Analisarei as alterações feitas pela instalação do Active Directory.

Conforme prometido no Capítulo 1, neste capítulo apresentarei mais detalhes sobre os modos de funcionalidade disponíveis para domínios e florestas, apresentando as características e limitações em cada um dos modos. Também mostrarei como alterar o modo de funcionalidade de um domínio.

Em seguida será a vez de apresentar as principais ferramentas de administração do Active Directory. Estas ferramentas são instaladas pelo assistente de instalação do Active Directory. Por exemplo, um novo console, chamado “Usuários e Computadores do Domínio” (Active Directory Users and Computers) é instalada. Este é um dos consoles que o administrador mais utiliza no seu dia-a-dia (Veja o Capítulo 4). Este console é utilizado para criar contas de usuários, grupos e computadores. També é utilizado para criar Unidades Organizacionais, incluir ou retirar usuários de grupos e para mover objetos entre diferentes OUs. Mostrarei as novas funcionalidades que estão disponíveis neste e em outros consoles de administração do Active Directory no Windows Server 2003, em relação ao Windows 2000 Server.

# Conceito de Diretório e Exemplos.

No Capítulo 1 fiz um histórico dos modelos de redes e aplicações desde a época do Mainframe (que continua mais vivo do que nunca), passando pelo modelo Cliente/Servidor tradicional, até chegar ao modelo Web, baseado no desenvolvimento de aplicações em 3 ou mais camadas.

Cada fase deixou suas características “impressas” na rede da empresa, no conjunto de aplicações que é utilizado para manter a empresa funcionando. O que ocorre na prática, é que hoje, na empresa, existem, ao mesmo tempo, aplicações rodando no Mainframe, aplicações Cliente/Servidor tradicionais e aplicações baseadas no modelo Web.

A Figura 2.1 ilustra bem este “mix” de aplicações, onde um usuário a partir da sua estação de trabalho, acessa aplicações em diferentes ambientes, para poder realizar o seu trabalho diário:

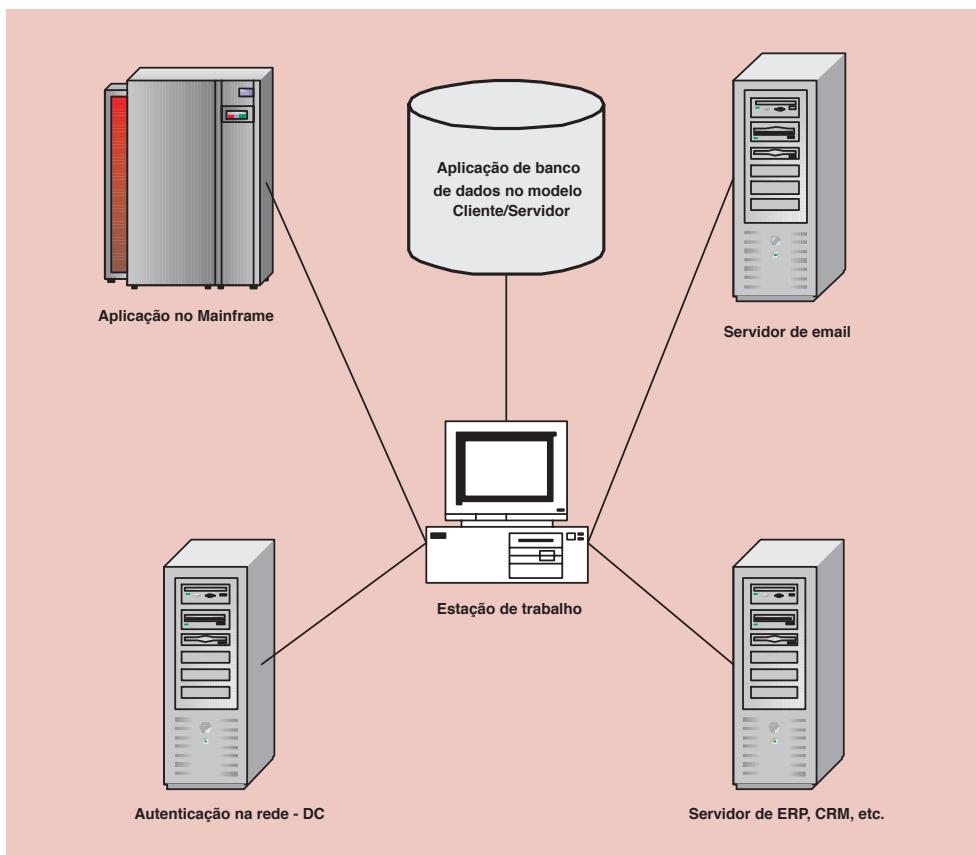


Figura 2.1 Aplicações em diferentes ambientes e baseadas em diferentes modelos.

Você pode pensar que dificilmente isso aconteceria na prática. É justamente o contrário. Esta é a situação na qual encontram-se a maioria das empresas, ou seja: Uma variedade de aplicações não integradas, em diferentes plataformas e modelos. Falando de uma maneira mais simples, uma verdadeira “salada-de-fruta”, ou de outras formas: salada de aplicações e modelos.

No exemplo descrito na Figura 1.1, o usuário, para realizar o seu trabalho diário, tem que acessar aplicações e serviços em diferentes plataformas e modelos:

- ♦ **No Mainframe:** Alguns sistemas da empresa (muitas vezes a maioria dos sistemas) ainda estão no Mainframe, com acesso através de aplicativos Emuladores de Terminal, instalados na estação de trabalho do usuário. Estes aplicativos mantêm a interface a caractere, típica da época do Mainframe. A tão famosa telinha preta com letras verdes. Por exemplo, pode ser que o sistema de RH (controle de férias, currículum, treinamentos, etc) ainda esteja no Mainframe.

- ◆ **Em aplicações cliente/servidor de 2 camadas:** A medida que houve uma migração do Mainframe em direção ao cliente/servidor, muitas aplicações do Mainframe foram substituídas por aplicações Cliente/Servidor tradicionais, conforme descrito no Capítulo 1. Por exemplo, podemos ter uma situação onde o sistema de vendas foi migrado do Mainframe para uma aplicação cliente/servidor de duas camadas. Os dados estão em um ou mais servidores da rede e a aplicação cliente é instalada na estação de trabalho do usuário.
- ◆ **Sistema de email e Intranet da empresa:** É praticamente impossível que a sua empresa não tenha um sistema de email instalado. Com isso você utiliza mais um aplicativo (o cliente de email), para acessar o seu correio eletrônico. Você também utiliza o navegador para acessar a Intranet da empresa. Se a sua empresa já evolui bastante no uso da Tecnologia da Informação, é provável que você use o navegador para acessar o Portal Corporativo da empresa.

Além desta variedade de aplicações você também precisa acesso aos recursos básicos da rede, tais como pastas e impressoras compartilhadas. Para ter acesso a estes recursos você deve estar identificado na rede, para que o servidor onde estão os recursos a serem acessados, possa liberar o acesso, dependendo de você ter ou não as permissões adequadas. Ou seja, o seu nome de usuário na rede e a respectiva senha, devem estar cadastrados em uma base de dados. Logo você descobrirá que base é esta.

Bem apresentado a provável ambiente atual no qual encontra-se a rede da sua empresa, vou salientar um dos principais problemas deste ambiente, problema este que está diretamente relacionado ao conceito de Diretório e também com o Active Directory.

## **Senhas demais, por favor alguém me ajude!**

No cenário descrito anteriormente, onde o usuário tem que acessar sistemas em diferentes ambientes, é necessário um logon e senha para cada ambiente. Por exemplo, no sistema de grande porte o logon pode ser a matrícula do funcionário e uma senha por ele escolhida. Na rede o logon é a primeira parte do seu email, por exemplo jsilva e uma senha por ele escolhida. No sistema de email mais uma senha. Em cada aplicação Cliente/Servidor mais uma senha e assim por diante.

Para piorar um pouco a situação, a senha do Mainframe expira, por exemplo, a cada 30 dias e ele não pode repetir as últimas cinco senhas. A da rede expira a cada 60 dias e ele não pode repetir as últimas treze. A do email expira a cada 45 dias e ele não pode repetir as últimas 10. A do sistema xyz expira a cada 40 dias e ele não pode repetir as últimas 6. Meu Deus, você deve estar pensando, a estas alturas o nosso usuário já deve estar “maluco”.

Na verdade maluco ele não está, mas acaba fazendo algo pior do que estivesse maluco: Ou seleciona senhas que facilmente são descobertas ou anota as senhas e guarda o papel na gaveta. A culpa é do usuário? Obviamente que não, mas sim de um ambiente onde existem múltiplas aplicações, com uma senha diferente para cada uma.

Mas espere aí um pouco. O que tem a ver este monte de senhas com o conceito de Diretório. Tem muito a ver. Observe que em cada ambiente existe um banco de dados para cadastro do nome do usuário, senha e outras informações, como por exemplo seção, matrícula e assim por diante. Este banco de dados com informações sobre os usuários da rede é um exemplo típico de Diretório.

Então no Mainframe, onde existe um cadastro de usuários, senhas e perfil de acesso de cada usuário, existe um Diretório. Na rede, onde existe um cadastro de usuários, senha, nome, seção, matrícula, etc, temos mais um diretório. No sistema de email, onde está cadastrado o email do usuário, senha, grupos, etc, temos um terceiro diretório e assim por diante. Observe que para cada diretório (o que implica cadastro em um determinado sistema), o usuário tem uma senha.

Então um diretório nada mais é do que um cadastro, ou melhor ainda, um banco de dados com informações sobre usuários, senhas e outros elementos necessários ao funcionamento de um sistema, quer seja um conjunto de aplicações no Mainframe, um grupo de servidores da rede local, o sistema de email ou outro sistema qualquer.

Saindo do mundo da computação, uma lista telefônica com o cadastro do nome do usuário, telefone e endereço, é um exemplo típico de diretório. O termo Diretório não é muito conhecido para nós, no idioma Português. Talvez um termo mais adequado fosse Cadastro, Banco de dados do sistema ou algo parecido. Mas o termo já é consagrado no idioma Inglês e acabou sendo adotado também no idioma Português (não sei se oficialmente, mas na prática, pelos profissionais de TI).

O Active Directory, introduzido inicialmente com o Windows 2000 Server e agora presente no Windows Server 2003 é também um exemplo típico de diretório. No Active Directory ficam gravadas informações sobre contas de usuários, senhas, grupos de usuários, membros de cada grupo, contas de computadores, informações sobre o Domínio, Relações de confiança, Unidades organizacionais, enfim, todas as informações necessárias ao funcionamento de uma rede baseada no Windows Server 2003.

## Um diretório único para todas as aplicações.

Porém o projeto do Active Directory é bem mais ambicioso do que simplesmente ser mais um diretório para conter informações dos elementos de uma rede baseada no Windows Server 2003. Ele foi projetado para tornar-se, com o tempo, o único diretório necessário na rede da empresa.

Mas como seria esta migração da situação atual, caótica, com múltiplos diretórios e senhas, para uma situação mais gerenciável, com um único diretório e senha: O TÃO SONHADO LOGON ÚNICO??

A proposta da Microsoft é que aos poucos as aplicações sejam integradas com o Active Directory. O que seria uma aplicação Integrada com o Active Directory? Seria uma aplicação que, ao invés de ter o seu próprio cadastro de usuários, senhas e grupos (seu próprio diretório), fosse capaz de acessar as contas e grupos do Active Directory e atribuir permissões de acesso diretamente as contas e grupos do Active Directory. Por exemplo, vamos supor que você utilize o Exchange 2000 como servidor de email. Este é um exemplo de aplicação que já é integrada com o Active Directory. Ao instalar o Exchange 2000, este é capaz de acessar a base de usuários do Active Directory e você pode criar contas de email para os usuários do Active Directory. Com isso quando o usuário faz o logon na rede, ele também está sendo autenticado com o Exchange e poderá ter acesso a sua caixa de correio sem ter que fornecer um login e senha novamente.

Chegará o dia do logon único quando todas as aplicações forem ou diretamente integradas com o Active Directory, o forem capazes de acessar a base de usuários do Active Directory e atribuir permissões de acesso aos usuários e grupos do Active Directory. Esta abordagem de um diretório único tem inúmeras vantagens. A mais saliente é o logon único, o que implica em uma única senha. Outra vantagem é o fato de que atualizações feitas no diretório já são refletidas, automaticamente, em todas as aplicações, uma vez que o diretório é único.

Quando o diretório não é único, as alterações devem ser feitas em todos os diretórios, senão ficarão desatualizadas. Vamos voltar um pouco ao ambiente de múltiplos diretórios. Vamos supor que um usuário foi transferido de setor e o seu número de telefone foi atualizado no diretório do Mainframe. Se este número não for também atualizado (e isto tem que ser feito pelo administrador de cada sistema) em todos os demais diretórios, corre-se o risco de alguém pesquisar um dos diretórios que não foi atualizado e obter o número de telefone antigo. Agora considere essa situação em uma empresa grande, onde estão em uso 5 ou 6 diretórios diferentes e multiplique isso por 4 ou 5 mil funcionários, você terá uma idéia do problema que é manter sempre atualizados os diversos diretórios em uso na empresa.

Por isso que a proposta do diretório único é interessante e muito bem vindas. É claro que não se faz a migração de um ambiente baseado em vários diretórios para um ambiente de diretório único, da noite para o dia. É um trabalho longo, que envolve um inventário das aplicações em uso. Uma análise do que é prioritário, do que pode ser integrado e do que

---

**NOTA:** No decorrer deste capítulo você aprenderá em detalhes sobre os diversos elementos do Active Directory, tais como Unidades organizacionais, sites, relações de confiança e assim por diante.

---

deverá ser reescrito e assim por diante. Mas é um trabalho que vale a pena, sob risco de chegar-se a um ambiente caótico, com inúmeros de diretórios, ambiente este praticamente impossível de gerenciar ou gerenciável a um custo muito elevado.

## Entendendo o conceito de Diretórios e Workgroups.

Nesta item mostrarei as diferenças entre uma rede baseada no modelo de Workgroup e uma rede baseada no modelo de diretórios.

Você entenderá porque uma rede baseada no conceito de Workgroup (Grupo de trabalho) somente é indicada para redes muito pequenas, entre cinco e dez usuários. E porque para redes maiores seria praticamente impossível administrar um modelo de redes baseado em Grupos de Trabalho ao invés de domínios.

### Domínios e Grupos de Trabalho (Workgroups):

Um rede baseada no Windows Server 2003 pode ser criada utilizando-se dois conceitos diferentes, dependendo da maneira com que os Servidores Windows Server 2003 são configurados. Os servidores podem ser configurados para fazerem parte de um Domínio ou de um Grupo de Trabalho, mais comumente chamado de Workgroup, termo que utilizarei de agora em diante.

### Entendendo o funcionamento de uma rede baseada no modelo de Workgroups:

Em uma rede baseada no modelo de Workgroups cada servidor é independente do outro. Em outras palavras, os servidores do Workgroup não compartilham uma lista de usuários, grupos e outras informações. Cada servidor tem a sua própria lista de usuários e grupos, conforme indicado no diagrama da Figura 2.2:

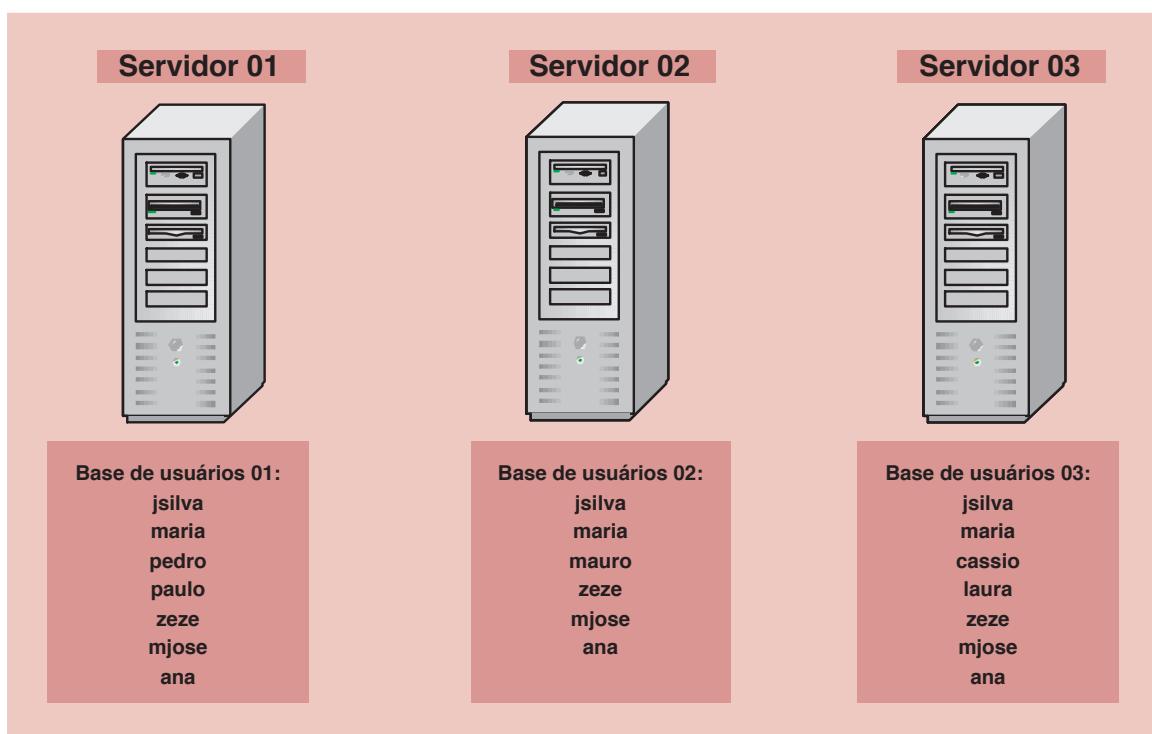


Figura 2.2 Uma rede baseada no conceito de Workgroup.

O diagrama demonstra uma rede baseada no modelo de Workgroup. Na rede de exemplo temos três servidores, onde cada servidor tem a sua própria base de usuários, senhas e grupos. Conforme pode ser visto no diagrama, as bases não estão sincronizadas, existem contas de usuários que foram criadas em um servidor mas não foram criadas nos demais. Por exemplo, a conta paulo somente existe no Servidor 01, a conta mauro só existe no Servidor 02 e a conta cassia só existe no servidor 03.

Agora imagine o usuário paulo, que está utilizando a sua estação de trabalho. Ele tenta acessar um recurso (por exemplo uma pasta compartilhada) no Servidor 01. Uma janela de logon é exibida. Ele fornece o seu nome de usuário e senha e o acesso (desde que ele tenha as devidas permissões) é liberado.

Agora este mesmo usuário – paulo, tenta acessar um recurso no Servidor 02. Novamente uma tela de logon é exibida e ele fornece o seu nome de usuário e senha. O acesso é negado, com uma mensagem de usuário inválido. E o usuário paulo fica sem entender o que está acontecendo. Orá, isso acontece porque o usuário paulo somente está cadastrado no Servidor 01; para o Servidor 02 e para o Servidor 03 é como se o usuário paulo não existisse (usuário inválido). Para que o usuário paulo possa acessar recursos dos servidores 02 e 03, o Administrador deveria criar uma conta chamada “paulo” nestes dois servidores.

Mas a “confusão” pode ser maior ainda. Imagine que o usuário paulo foi cadastrado pelo administrador com a conta paulo e senha: abc123de. Muito bem, o administrador fez o cadastro do usuário paulo nos três servidores: Servidor 01, Servidor 02 e Servidor 03. Agora, cerca de 30 dias depois, o usuário paulo resolveu alterar a sua senha. Vamos supor que ele estava conectado ao Servidor 01, quando fez a alteração da sua senha para: xyz123kj. Agora o usuário paulo está na situação indicada a seguir:

| Servidor    | Usuário | Senha    |
|-------------|---------|----------|
| Servidor 01 | paulo   | abc123de |
| Servidor 02 | paulo   | abc123de |
| Servidor 03 | paulo   | xyz123kj |

Na concepção do usuário, a partir de agora vale a nova senha, independentemente do servidor que ele esteja acessando. Pois para o usuário interessa o recurso que ele está acessando. Para o usuário não interessa se o recurso está no servidor 01, 02 ou outro servidor qualquer. Agora vamos ver o que acontece com o usuário paulo.

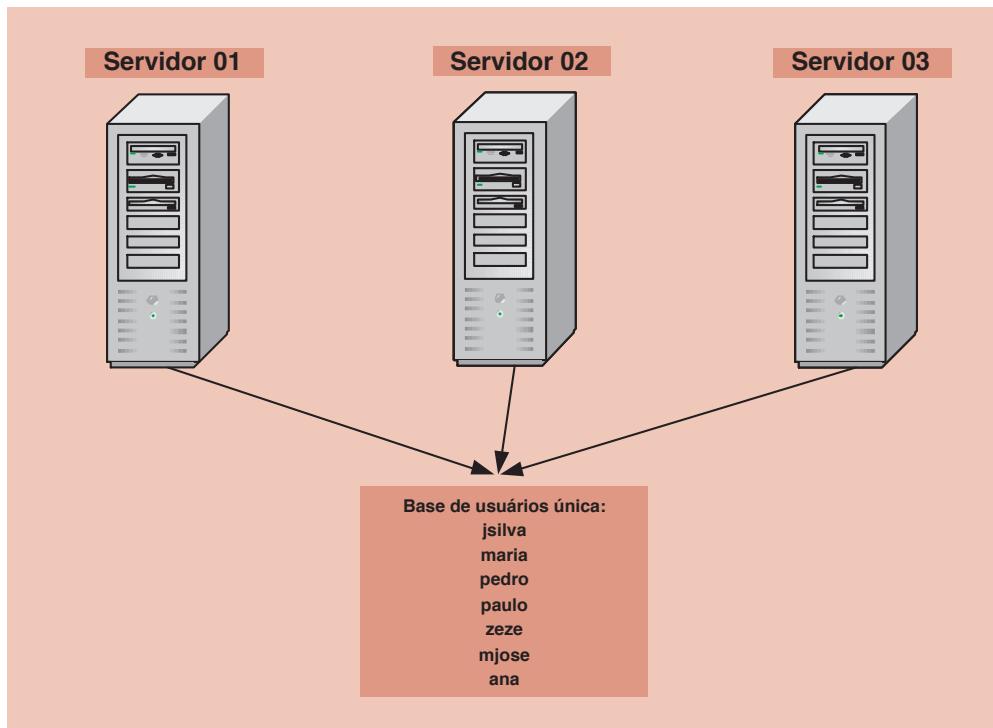
O usuário paulo, que está utilizando a sua estação de trabalho. Ele tenta acessar um recurso (por exemplo uma pasta compartilhada) no Servidor 01. Uma janela de logon é exibida. Ele fornece o seu nome de usuário e a nova senha e o acesso (desde que ele tenha as devidas permissões) é liberado.

Agora este mesmo usuário – paulo, tenta acessar um recurso no Servidor 02. Novamente uma tela de logon é exibida e ele fornece o seu nome de usuário e a nova senha e a surpresa: O acesso é negado, com uma mensagem de falha na autenticação. Aí o usuário fica pensando: mas como é possível, eu recém troquei a senha. Ele trocou a senha no Servidor 01. Para os demais servidores continua valendo a senha antiga. A única maneira de ele conseguir alterar a senha é fazendo o logon com a senha antiga e alterando para a nova senha, em todos os servidores da rede. Agora imagine o problema em uma rede de grandes proporções, com dezenas de servidores e milhares de funcionários. Fica fácil concluir que o modelo de Workgroup ficaria insustentável, impossível de ser implementado na prática.

Eu somente recomendaria modelo de Workgroup para redes pequenas, com um único servidor e com um número de, no máximo, 10 usuários.

## Entendendo o funcionamento de uma rede baseada no conceito de Diretório – Domínio:

Agora vou apresentar o modelo de rede baseado em um diretório. Vamos iniciar considerando o diagrama da Figura 2.3:



**Figura 2.3 Uma rede baseada no conceito de Diretório - Domínio.**

No modelo baseado em diretório, nos temos uma base de usuários única, ou seja, todos os servidores da rede compartilham a mesma base de usuários. O que acontece, na prática, não é que existe uma única base, armazenada em um determinado servidor, e todos os demais servidores acessam esta base. Não, não é isso. O que ocorre na prática, é que todos os servidores contém uma cópia da base de informações do diretório. Alterações efetuadas em um dos servidores são repassadas para os demais servidores da rede, para que todos fiquem com uma cópia idêntica da base de dados do diretório. Esta sincronização entre os servidores do domínio é conhecida como Replicação do Active Directory.

O que caracteriza uma rede baseada em diretório é o fato de todos os servidores terem acesso a mesma base de dados, ou seja, todos compartilham o mesmo diretório, as mesmas informações sobre usuários, grupos, servidores e recursos. Mais adiante será apresentado o conceito de domínio, floresta, relação de confiança, etc. Estes são outros elementos relacionados com o diretório e que permitem a criação de redes de grande extensão geográfica, como por exemplo redes de uma grande empresa com escritórios no mundo inteiro (Microsoft).

No modelo baseado em diretório, a vida do Administrador fica bem mais fácil. Vamos supor que o usuário paulo queira acessar um recurso em um dos servidores da rede. Sem problemas, qualquer servidor tem uma cópia da base de dados do diretório. Com isso a conta do usuário paulo estará disponível em qualquer servidor. Com isso ele poderá acessar recursos em qualquer um destes servidores. Há, mas se o usuário paulo alterar a sua senha. Isso será feito na cópia do banco de dados do diretório de um dos servidores. Correto? Correto, porém em pouco tempo esta alteração será replicada para todos os demais servidores e a senha do usuário paulo estará sincronizada em todos os servidores.

O modelo baseado em diretórios (e no conceito de domínios, florestas, etc) é bem mais fácil para administrar e permite a implementação de redes de grandes proporções, tanto geográficas quanto em números de usuários. Na empresa onde eu trabalho, temos uma rede baseada no Active Directory. A rede se estende por todos os estados do território nacional e tem cerca de 22.000 usuários. Uma rede e tanto. Seria literalmente impossível manter uma rede destas proporções sem utilizar o modelo baseado em diretórios.

# Domínios, Árvores de domínios e Unidades Organizacionais – Conceitos.

Agora que você já conhece bem a diferença entre um modelo de rede baseada em Workgroup e outro de rede baseada em diretórios, é hora de avançar um pouco mais e nós aproximar da terminologia do Active Directory. Neste item vou apresentar o conceito de diretório. Não um conceito formal, como o apresentado no início do capítulo, mas sim o conceito de diretório que é utilizado em redes baseadas no Active Directory e no Windows Server 2003 (ou Windows 2000 Server).

No Windows Server 2003 (e também no Windows 2000 Server), o conjunto de servidores, estações de trabalho, bem como as informações do diretório é que formam uma unidade conhecida como Domínio. Todos os servidores que contém uma cópia da base de dados do Active Directory, fazem parte do domínio. As estações de trabalho podem ser configuradas para fazer parte do domínio. No caso de estações de trabalho com o NT Workstation 4.0, Windows 2000 Professional ou Windows XP Professional, cada estação de trabalho que faz parte do domínio, tem uma conta de computador criada no domínio. A conta de computador tem o mesmo nome do computador. Por exemplo, a estação de trabalho micro-cont-001, tem uma conta de computador, na base de dados do Active Directory, com o nome de micro-cont-001.

Um domínio pode também ser definido com um limite administrativo e de segurança. Ele é um limite administrativo, pois as contas de Administrador tem permissões de acesso em todos os recursos do domínio, mas não em recursos de outros domínios. Ele é um limite de segurança porque cada domínio tem definições de políticas de segurança que se aplicam as contas de usuários e demais recursos dentro de domínio e não a outros domínios. Ou seja, diferentes domínios podem ter diferentes políticas e configurações de segurança. Por exemplo, no domínio A, posso ter uma política de segurança que define um tamanho mínimo de senha como 8 caracteres. Esta política será válida para todas as contas de usuário do domínio A. Um segundo domínio B, pode ter uma política de segurança diferente, a qual define um tamanho mínimo de senha de 12 caracteres. Esta política será válida para todas as contas de usuários do domínio B.

Um Domínio é simplesmente um agrupamento lógico de contas e recursos, os quais compartilham políticas de segurança. As informações sobre os diversos elementos do domínio (contas de usuários, contas de computador, grupos de usuários, políticas de segurança, etc), estão contidas no banco de dados do Active Directory.

Em um domínio baseado no Active Directory e no Windows Server 2003 é possível ter dois tipos de servidores Windows Server 2003:

- ◆ Controladores de Domínio (DC – Domain Controllers)
- ◆ Servidores Membro (Member Servers).

Falarei um pouco mais sobre Controladores de Domínio e Servidores Membro no final deste tópico.

A criação de contas de usuários, grupos de usuários e outros elementos do Active Directory, bem como alterações nas contas de usuários, nas políticas de segurança e em outros elementos do Active Directory, podem ser feitas em qualquer um dos Controladores de Domínio. Uma alteração feita em um DC será automaticamente repassadas (o termo técnico é “replicada”) para os demais Controladores de Domínio. Por isso se você cria uma conta para o usuário jsilva e cadastrá uma senha para este usuário, essa conta passa a ser válida em todo o domínio, sendo que o usuário jsilva pode receber permissões para acessar recursos e serviços em qualquer servidor do Domínio, seja em um Controlador de Domínio ou em um Servidor Membro.

Por isso que o Domínio transmite a idéia de um agrupamento lógico de Contas de Usuários e Grupos, bem como de políticas de segurança, uma vez que todo o Domínio compartilha a mesma lista de Usuários, Grupos e políticas de segurança. A criação de domínios facilita enormemente a administração de uma rede baseada no Windows Server

2003, sendo altamente recomendada para qualquer rede de maior porte seja criada com base em um ou mais domínios (dependendo do porte da rede).

Nos Servidores Membros podem ser criadas contas de usuários e grupos, as quais somente serão válidas no Servidor Membro onde foram criadas. Embora isso seja tecnicamente possível, essa é uma prática não recomendada, uma vez que isso dificulta enormemente a administração de um Domínio. Você pode atribuir permissões para os Recursos de um Servidor Membro, à contas de Usuários e Grupos do domínio, sem a necessidade de criar esses usuários ou grupos localmente. Por exemplo, um usuário jsilva, que pertence ao domínio, pode receber permissões de acesso em uma pasta compartilhada de um Servidor Membro. Com isso você pode concluir que um Servidor Membro, é um servidor que embora não mantenha uma cópia da lista de usuários e grupos do Active Directory, este tem acesso a essa lista. Com isso que podem ser atribuídas permissões nos recursos do Servidor Membro (tais como pastas compartilhadas, impressoras, etc ) para as contas e grupos do Domínio.

Em um Domínio todos os Controladores de Domínio, compartilham uma lista de usuários, grupos e políticas de segurança, além de algumas outras características que falarei no tópico sobre o Active Directory. Além disso alterações feitas em um dos Controladores de Domínio, são automaticamente replicadas para os demais. DCs

Os DCs também são responsáveis por fazer a autenticação dos usuários na rede. Por exemplo, vamos supor que o usuário jsilva trabalha em uma estação de trabalho com o Windows XP Professional instalado. Esta estação foi configurada para fazer parte do domínio. Quando o usuário jsilva liga a estação de trabalho e o Windows é inicializado, é apresentada a tela de logon para que ele forneça o seu nome de usuário e senha. O Windows precisa verificar se o nome de usuário e senha estão corretos. A Windows tenta localizar um DC na rede. É no DC que a verificação é feita, comparando as informações digitadas pelo usuário, com as informações da base de dados do Active Directory. Se as informações estão OK o logon é liberado, o usuário é autenticado e a área de trabalho do Windows é exibida. A partir deste momento, toda vez que o usuário tentar acessar um recurso do domínio, será apresentada a sua autenticação, com base nas informações de logon apresentadas, para provar a identidade do usuário para a rede. Isso evita que o usuário tenha que entrar com o seu logon e senha cada vez que for acessar um recurso em um servidor diferente (que é justamente o que acontece no modelo baseado em Workgroup, conforme descrito anteriormente).

Como os Servidores Membro não possuem uma cópia da lista de usuários e grupos, estes não efetuam a autenticação dos clientes e também não armazenam informações sobre as políticas de segurança para o Domínio – as quais também são conhecidas por GPO – Group Policies Objects.

Quando os servidores Windows Server 2003 são configurados para trabalhar com um Workgroup, não existe o conceito de domínio e nem de Controlador de Domínio. Cada servidor mantém uma lista separada para contas de usuários, grupos e políticas de segurança, conforme descrito anteriormente. Com isso se um usuário precisa acessar recursos em três servidores, por exemplo, será necessário criar uma conta para esse usuário nos três servidores diferentes. Um Workgroup somente é recomendado para redes extremamente pequenas, normalmente com um único servidor Windows Server 2003 e não mais do que 10 estações clientes, conforme descrito anteriormente.

## Active Directory

Lembro de já ter escrito a seguinte frase, em um dos capítulos deste livro:

“O Active Directory é, sem dúvidas, a mudança mais significativa incluída no Windows 2000 Server e que também faz parte do Windows Server 2003.”

---

**NOTA:** Estações de trabalho com o Windows XP Home, não podem ser configuradas para fazer parte de um domínio. Estações de trabalho com o Windows 95/98/Me podem ser configuradas para fazer parte de um domínio. Para ter acesso a maioria dos recursos do Active Directory, também é preciso instalar o Active Directory Client, nas estações de trabalho com o Windows 95/98/Me. Uma estação de trabalho com o NT Workstation 4.0 também pode ser configurada para fazer parte de um domínio baseado no Active Directory e no Windows Server 2003.

---

Mas de uma maneira simples, o que é o Active Directory ?

“O Active Directory é o serviço de diretórios do Windows Server 2003. Um Serviço de Diretórios é um serviço de rede, o qual identifica todos os recursos disponíveis em uma rede, mantendo informações sobre estes dispositivos (contas de usuários, grupos, computadores, recursos, políticas de segurança, etc) em um banco de dados e torna estes recursos disponíveis para usuários e aplicações.”

Pode parecer que o Active Directory é, na verdade um banco de dados. Mas não é só isso. Além do banco de dados com informações sobre os elementos (teoricamente conhecidos como objetos) que compõem o domínio, o Active Directory também disponibiliza uma série de serviços que executam as seguintes funções:

- ◆ Replicação entre os Controladores de domínio.
- ◆ Autenticação
- ◆ Pesquisa de objetos na base de dados
- ◆ Interface de programação para acesso aos objetos do diretório

Pela descrição formal, é possível inferir que o Active Directory é um serviço de rede, no qual ficam armazenadas informações sobre dados dos usuários, impressoras, servidores, grupos de usuários, computadores e políticas de segurança. Cada um desses elementos são conhecidos como objetos.

O Active Directory além de armazenar uma série de informações sobre os objetos disponíveis no domínio (contas de usuários, grupos de usuários, servidores, computadores, etc), torna fácil para o administrador localizar e fazer alterações nos objetos existentes, bem como criar novos objetos ou excluir objetos que não sejam mais necessários. Em resumo, com o conjunto de serviços oferecidos pelo Active Directory, a administração da rede fica bem fácil.

Os recursos de segurança são integrados com o Active Directory, através do mecanismo de logon e autenticação. Todo usuário tem que fazer o logon (informar o seu nome de usuário e senha), para ter acesso aos recursos da rede. Durante o logon o Active Directory verifica se as informações fornecidas pelo usuário estão corretas e então libera o acesso aos recursos para os quais o usuário tem permissão de acesso.

Os recursos disponíveis através do Active Directory , são organizados de uma maneira hierárquica, através do uso de Domínios. Uma rede na qual o Active Directory está instalado, pode ser formada por um ou mais Domínios. Com a utilização do Active Directory um usuário somente precisa estar cadastrado em um único Domínio, sendo que este usuário pode receber permissões para acessar recursos em qualquer um dos Domínios, que compõem a árvore de domínios da empresa.

A utilização do Active Directory simplifica em muito a administração, pois fornece um local centralizado, através do qual todos os recursos da rede podem ser administrados. Todos os Controladores de Domínio (DCs), possuem o Active Directory instalado. A Maneira de criar um domínio é instalar o Active Directory em um Member Server e informar que este é o primeiro Controlador de Domínio. Depois de criado o domínio (a parte prática da criação de domínios será vista na parte final do capítulo.) você pode criar DCs adicionais, simplesmente instalando o Active Directory outros servidores.

O Active Directory utiliza o DNS (Domain Name System) como serviço de nomeação de servidores e recursos e de resolução de nomes. Por isso um dos pré-requisitos para que o Active Directory possa ser instalado e funcionar perfeitamente é que o DNS deve estar instalado e corretamente configurado.

---

**Novidade: No Windows Server 2003, o assistente de instalação do Active Directory é capaz de instalar e configurar o DNS, caso ele não encontre um servidor DNS adequadamente configurado na rede. Esta não chega a ser exatamente uma novidade. O que ocorre na prática, é que o assistente de instalação do Active Directory, no Windows Server 2003, consegue na maioria das vezes configurar o DNS corretamente, o que não ocorria no Windows 2000 Server.**

---

O Agrupamento de objetos em um ou mais Domínios permite que a rede de computadores reflita a organização da sua empresa. Para que um usuário cadastrado em um domínio, possa receber permissões para acessar recursos em outros domínios, o Windows Server 2003 cria e mantém relações de confiança entre os diversos domínios. As relações de confiança são bidirecionais e transitivas. Isso significa se o Domínio A confia no Domínio B, o qual por sua vez confia em um Domínio C, então o Domínio A também confia no Domínio C. Isso é bastante diferente do que acontecia até o NT Server 4.0, uma vez que as relações de confiança tinham que ser criadas e mantidas pelos administradores dos domínios, uma a uma. Era um trabalho e tanto, o que dificultava a implementação de relações de confiança em uma rede com muitos domínios.

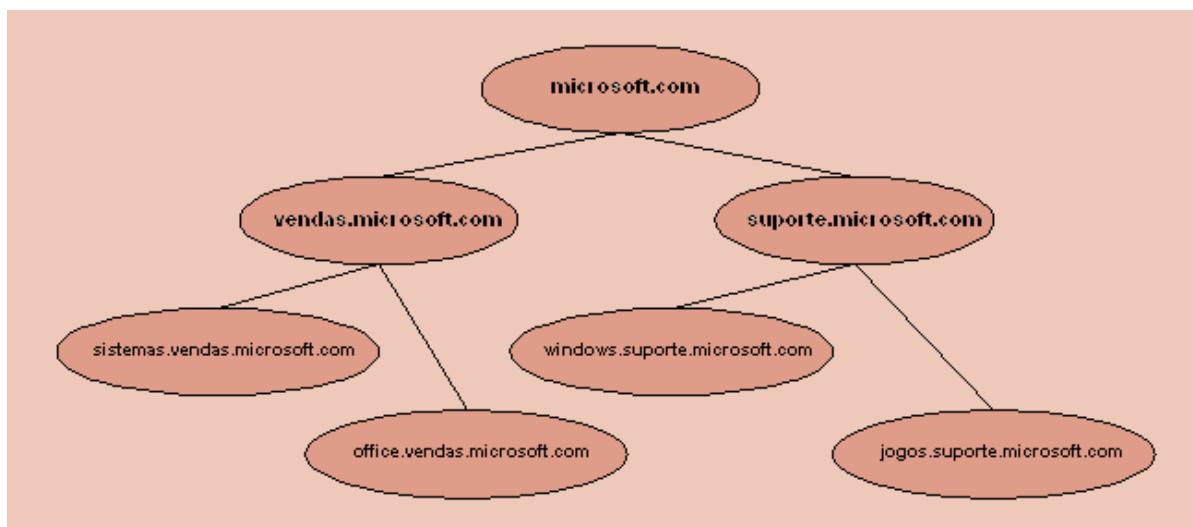
Todo Domínio possui as seguintes características:

- ◆ Todos os objetos de uma rede (contas de usuários, grupos, impressoras, políticas de segurança, etc) fazem parte de um único domínio. Cada domínio somente armazena informações sobre os objetos do próprio domínio.
- ◆ Cada domínio possui suas próprias políticas de segurança.

## Árvore de domínios:

Quando existem diversos domínios relacionados através de relações de confiança, criadas e mantidas automaticamente pelo Active Directory, temos uma Árvore de domínios. Uma árvore nada mais é do que um agrupamento ou arranjo hierárquico de um ou mais domínios do Windows Server 2003, os quais “compartilham um espaço de nome.”

Vou explicar em detalhes o que significa a expressão “compartilham um espaço de nome”. Primeiramente observe a Figura 2.4.



**Figura 2.4 Todos os domínios de uma árvore compartilham um espaço de nomes em comum.**

Observe que é exibida uma árvore com 7 domínios. Mas o que significa mesmo “compartilham um espaço de nome”?

Observe que o domínio inicial, também conhecido como domínio pai ou domínio root, é microsoft.com. Os domínios seguintes são: vendas.microsoft.com e suporte.microsoft.com. Quando é formada uma hierarquia de domínios, compartilhar um espaço de nomes, significa que os nomes dos objetos filho (de segundo nível, por exemplo: vendas.microsoft.com e suporte.microsoft.com), contém o nome do objeto pai (microsoft.com). Por exemplo, vendas.microsoft.com contém microsoft.com. Descendo mais ainda na hierarquia, você pode observar que este fato

continua verdadeiro. Por exemplo o objeto filho sistemas.vendas.microsoft.com contém o nome do objeto Pai vendas.microsoft.com.

Com isso uma árvore de diretórios deste tipo forma um espaço de nomes contínuo, onde o nome do objeto filho sempre contém o nome do objeto pai.

## Unidades Organizacionais

Você pode ainda dividir um Domínio em “Unidades Organizacionais”. Uma Unidade Organizacional é uma divisão lógica do domínio, a qual pode ser utilizada para organizar os objetos de um determinado domínio em um agrupamento lógico para efeitos de administração. Isso resolve uma série de problemas que existiam em redes baseadas no NT Server 4.0.

No Windows NT Server 4.0 se um usuário fosse adicionado ao grupo Administradores (grupo com poderes totais sobre qualquer recurso do domínio), ele poderia executar qualquer ação em qualquer servidor do domínio. Com a utilização de Unidades Organizacionais, é possível restringir os direitos administrativos apenas a nível da Unidade Organizacional, sem que com isso o usuário tenha poderes sobre todos os demais objetos do Domínio.

Cada domínio pode implementar a sua hierarquia de Unidades Organizacionais, independentemente dos demais domínios, isto é, os diversos domínios que formam uma árvore, não precisam ter a mesma estrutura hierárquica de unidades organizacionais.

No exemplo da Figura 2.4, o domínio vendas.microsoft.com, poderia ter uma estrutura hierárquica de Unidades Organizacionais, projetada para atender as necessidades do domínio vendas. Essa estrutura poderia ser completamente diferente da estrutura do domínio suporte.microsoft.com, a qual será projetada para atender as necessidades do domínio suporte. Com isso tem-se uma flexibilidade bastante grande, de tal forma que a árvore de domínios e a organização dos domínios em uma hierarquia de Unidades Organizacionais, possa atender perfeitamente as necessidades da empresa. A utilização de Unidades Organizacionais não é obrigatória, porém altamente recomendada, conforme mostrarei em alguns exemplos mais adiante.

Utilize Unidades Organizacionais quando:

- ◆ Você quiser representar a estrutura e organização da sua companhia em um domínio. Sem a utilização de Unidades Organizacionais, todas as contas de usuários são mantidas e exibidas em uma única lista, independente da localização, departamento ou função do usuário.
- ◆ Você quiser delegar tarefas administrativas sem para isso ter que dar poderes administrativos em todo o Domínio. Com o uso de Unidades Organizacionais, você pode dar permissões para um usuário somente a nível da Unidade Organizacional.
- ◆ Quiser facilitar e melhor acomodar alterações na estrutura da sua companhia. Por exemplo, é muito mais fácil mover contas de usuários entre Unidades Organizacionais do que entre domínios, embora no Windows Server 2003 seja bem mais fácil mover uma conta de um domínio para outro, do que era no Windows 2000 Server.

Com a apresentação destes conceitos, você já está habilitado a estudar os elementos do Active Directory em mais detalhes.

## Conhecendo os principais Objetos de um domínio.

Até aqui apresentei os conceitos básicos sobre diretórios, domínios, unidades organizacionais e árvores de diretórios. A partir deste item passarei a descrever os objetos que fazem parte do Active Directory. Na seqüência falarei sobre os serviços que dão suporte ao Active Directory, tais como os serviços de replicação e o conceito de relações de confiança entre diretórios.

# Contas de usuários, computadores e grupos de usuários

## Contas de usuários

Todo usuário que quer ter acesso aos recursos dos computadores do domínio (pastas compartilhadas, impressoras compartilhadas, etc) deve ser cadastrado no Active Directory. Cadastrar o usuário, significa criar uma conta de usuário e uma senha. Ao cadastrar um usuário, outras informações tais como seção, nome completo, endereço, telefone, etc, podem ser cadastradas, conforme veremos no Capítulo 4.

Uma conta de usuário é um objeto do Active Directory, o qual contém diversas informações sobre o usuário, conforme descrito anteriormente. É importante salientar que a conta somente precisa ser criada uma vez, em um dos Controladores de domínio. Uma vez criada, a conta será replicada para todos os demais DCs do domínio.

Você também pode criar contas nos servidores membros e nas estações de trabalho com Windows 2000 Professional ou Windows XP Professional. As contas criadas nestes computadores são ditas contas locais, ou seja, somente existem no computador onde foram criadas. Vamos imaginar que você está trabalhando em uma estação de trabalho com o Windows XP Professional instalado. Esta estação foi configurada para fazer parte do domínio abc.com.br. Como a estação de trabalho faz parte do domínio, você terá acesso a lista de usuários e grupos do domínio. Com isso você poderá, por exemplo, atribuir permissão de acesso para um usuário do domínio (ou um grupo de usuários) em uma pasta compartilhada na sua estação de trabalho. Nesta mesma estação você também poderá criar contas de usuários e grupos locais, os quais ficam gravados na base de usuários local e só existe neste computador. Estes usuários e grupos (criados localmente), somente podem receber permissões de acesso para os recursos do computador onde foram criados. Você não conseguirá atribuir permissão de acesso em uma pasta compartilhada no servidor, para um usuário local da sua estação de trabalho.

Embora seja tecnicamente possível a criação de usuários e grupos locais, nos Servidores Membros e nas estações de trabalho, esta prática não é recomendada. Quando você trabalha em um domínio, o ideal é que contas de usuários e grupos sejam criadas somente no domínio, isto é, nos DCs.

---

**IMPORTANTE:** O Administrador pode utilizar o recurso de GPOs – Group Policies Objects para impedir que os usuários possam criar contas de usuários e grupos locais, em suas estações de trabalho. O assunto GPOs é abordado, em detalhes, no Capítulo 18 do Livro: Windows Server 2003 – Curso Completo, 1568 páginas.

---

Algumas recomendações e observações sobre contas de usuários:

- ◆ Todo usuário que acessa a rede deve ter a sua própria conta. Não é recomendado que dois ou mais usuários compartilhem a mesma conta. A conta é a identidade do usuário para a rede. Por exemplo, quando o usuário jsilva faz o logon no domínio, a sua conta é a sua identidade para o sistema. Todas as ações realizadas pelo usuário estão associadas a sua conta. O Windows Server 2003 tem um sistema de auditoria de segurança, no qual o Administrador pode configurar quais ações devem ser registradas no Log de auditoria. Por exemplo, o administrador pode definir que toda tentativa de alterar um determinado arquivo seja registrada no log de auditoria. Se o usuário jsilva tentar alterar o referido arquivo, ficará registrado no log de auditoria que o usuário jsilva, no dia tal, hora tal, tentou alterar o arquivo tal. Se dois ou mais usuários estão compartilhando a mesma conta, fica difícil identificar qual o usuário que estava logado no momento. Para o sistema é o jsilva. Agora quem dos diversos usuários que utilizam a conta jsilva é que estava logado e tentou alterar o referido arquivo? Fica difícil saber. Por isso a recomendação para que cada usuário seja cadastrado e tenha a sua própria conta e senha.

- ♦ Com base nas contas de usuários e grupos, o administrador pode habilitar ou negar permissões de acesso aos recursos da rede. Por exemplo, o administrador pode restringir o acesso a pastas e arquivos compartilhados na rede, definindo quais usuários podem ter acesso e qual o nível de acesso de cada usuário – leitura, leitura e alteração, exclusão e assim por diante. Mais um bom motivo para que cada usuário tenha a sua própria conta e senha.

Outro detalhe que você deve observar, é a utilização de um padrão para o nome das contas de usuários. Você deve estabelecer um padrão para a criação de nomes, pois não podem existir dois usuários com o mesmo nome de logon dentro do mesmo Domínio. Por exemplo se existir no mesmo Domínio, dois “José da Silva” e os dois resolverem utilizar como logon “jsilva”, somente o primeiro conseguirá, o segundo terá que se conformar em escolher um outro nome de logon. Para isso é importante que seja definido um padrão e no caso de nomes iguais deve ser definido uma maneira de diferenciá-los. Por exemplo poderíamos usar como padrão a primeira letra do nome e o último sobrenome. No caso de nomes iguais, acrescenta-se números. No nosso exemplo o primeiro José da Silva cadastrado ficaria como jsilva, já o segundo a ser cadastrado ficaria como jsilva1. Caso no futuro tivéssemos mais um José da Silva dentro da mesma Unidade Organizacional, este seria o jsilva2 e assim por diante.

Quando for criar nomes de logon para os usuários, leve em consideração os seguintes detalhes:

- ♦ Nomes de Usuários do Domínio devem ser únicos dentro do Domínio.
- ♦ Podem ter no máximo 20 caracteres.
- ♦ Os seguintes caracteres não podem ser utilizados: “/ \ : ; [ ] | = , + \* ? < >

Sempre que você for cadastrar um usuário também deve ser cadastrada uma senha para o usuário. Conforme mostrarei no Capítulo 4, o administrador pode especificar um número mínimo de caracteres aceito para a senha. O número máximo de caracteres da senha é 128.

## Contas de Computador

Estações de trabalho que rodam o Windows NT Workstation 4.0, Windows 2000 Professional ou Windows XP Professional e que fazem parte do domínio, devem ter uma conta de computador no Active Directory. Servidores, quer sejam Member Servers ou DCs, rodando Windows NT Server 4.0, Windows 2000 Server ou Windows Server 2003, também tem contas de computador no Active Directory.

A conta de computador pode ser criada antes da instalação do computador ser adicionado ao domínio ou no momento em que o computador é configurado para fazer parte do domínio. A conta do computador deve ter o mesmo nome do computador na rede. Por exemplo, um computador com o nome de microxp01, terá uma conta no Active Directory, com o nome: microxp01.

## Grupos de usuários

Um grupo de usuários é uma coleção de contas de usuários. Por exemplo, podemos criar um grupo chamado Contabilidade, do qual farão parte todos os usuários do departamento de Contabilidade (todas as contas de usuários dos funcionários do departamento de Contabilidade).

A principal função dos grupos de usuários é facilitar a administração e a atribuição de permissões para acesso a recursos, tais como: pastas compartilhadas, impressoras remotas, serviços diversos, etc.

**IMPORTANTE:** Para as senhas, o Windows Server 2003 distingue letras maiúsculas de minúsculas. Por exemplo a senha “Abc123” é diferente da senha “abc123”.

**NOTA:** Computadores rodando Windows 95/98/Me, mesmo tendo acesso a lista de usuários e grupos do domínio, não terão contas de computador criadas no Active Directory.

Ao invés de dar permissões individualmente, para cada um dos usuários que necessitam acessar um determinado recurso, você cria um grupo, inclui os usuários no grupo e atribui permissões para o grupo. Para que um usuário tenha permissão ao recurso, basta incluir o usuário no grupo, pois todos os usuários de um determinado grupo, herdam as permissões dos grupos aos quais o usuário pertence.

Quando um usuário troca de seção, por exemplo, basta trocar o usuário de grupo. Vamos supor que o usuário jsilva trabalha na seção de contabilidade e pertence ao grupo Contabilidade. Com isso ele tem acesso a todos os recursos para os quais o grupo Contabilidade tem acesso. Ao ser transferido para a seção de Marketing, basta retirar o usuário jsilva do grupo Contabilidade e adicioná-lo ao grupo Marketing. Com isso o jsilva deixa de ter as permissões atribuídas ao grupo Contabilidade e passa a ter as mesmas permissões que tem o grupo Marketing. Este exemplo simples já consegue demonstrar o quanto a utilização de grupos pode facilitar a administração de atribuição de permissões.

Vamos analisar mais um exemplo. Suponha que exista um sistema chamado SEAT, para o qual somente um número restrito de usuários deve ter acesso, sendo que são usuários de diferentes seções. A maneira mais simples de definir as permissões de acesso ao sistema SEAT é criar um grupo chamado Seat e dar permissões para esse grupo. Assim cada usuário que precisar acessar o sistema SEAT, deve ser incluído no grupo Seat. Quando o usuário não deve mais ter acesso ao sistema SEAT, basta removê-lo do grupo Seat. Simples, fácil e muito prático.

Na Figura 2.5 apresento uma ilustração para o conceito de Grupo de usuários. O Grupo Contabilidade possui direito para um recurso compartilhado, o qual pode ser acessado através da rede. Todos os usuários que pertencem ao grupo contabilidade, também possuem permissão para o recurso compartilhado, uma vez que os usuários de um grupo, herdam as permissões do grupo.

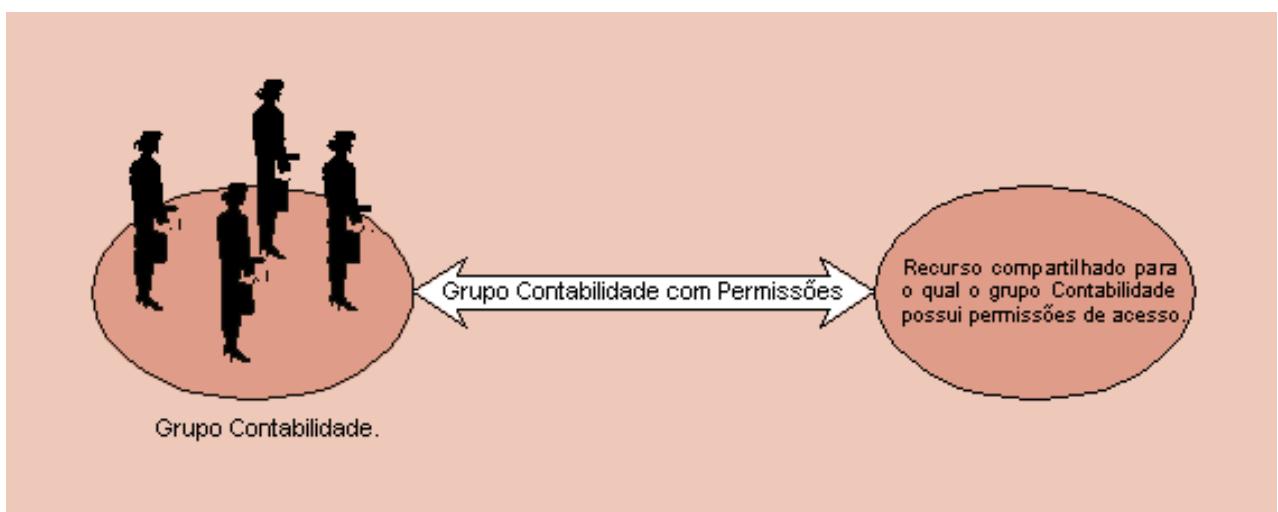


Figura 2.5 O Usuário herda as permissões do grupo.

Quando estiver trabalhando com grupos de usuários, considere os fatos a seguir:

- ◆ Grupos são uma coleção de contas de usuários.
- ◆ Os membros de um grupo, herdam as permissões atribuídas ao grupo.
- ◆ Os usuários podem ser membros de vários grupos
- ◆ Grupos podem ser membros de outros grupos.
- ◆ Contas de computadores podem ser membros de um grupo (novidade do Windows Server 2003).

Agora vou falar sobre os tipos de grupos existentes no Windows Server 2003. Os grupos são classificados de acordo com diferentes critérios, tais como: tipo, escopo e visibilidade.

Podemos ter dois tipos de grupos no Windows Server 2003 : Grupos de segurança ( Security Groups) e Grupos de distribuição (Distribution Groups).

Classificação dos grupos quanto ao tipo:

- ◆ **Grupos de segurança:** Normalmente utilizado para atribuir permissões de acesso aos recursos da rede. Por exemplo, ao criar um grupo Contabilidade, o qual conterá todas as contas dos funcionários do departamento de contabilidade, o qual será utilizado para atribuir permissões de acesso a uma pasta compartilhada, devo criar este grupo como sendo do tipo Grupo de segurança. Um grupo de segurança também pode ser utilizado como um grupo de distribuição, embora essa não seja uma situação muito comum. Esses grupos, assim como as contas de usuários são armazenados no Banco de dados do Active Directory.
- ◆ **Grupos de distribuição:** São utilizados para funções não relacionadas com segurança ( atribuição de permissões) . Normalmente são utilizados em conjunto com servidores de e-mail, tais como o Exchange 2000, para o envio de e-mail para um grupo de usuários. Uma das utilizações típicas para um Grupo de distribuição é o envio de mensagens de e-mail para um grupo de usuários de uma só vez. Somente programas que foram programados para trabalhar com o Active Directory, poderão utilizar Grupos de distribuição (como é o caso do Exchange 2000 citado anteriormente). Provavelmente as novas versões dos principais sistemas de correio eletrônico estarão habilitadas para trabalhar com o Active Directory. Não é possível utilizar grupos de distribuição para funções relacionadas com segurança.

Classificação dos grupos quanto ao Escopo:

Quando criamos um grupo de usuários, devemos selecionar um tipo (descrito anteriormente) e um escopo. O Escopo permite que o grupo seja utilizado de diferentes maneiras para a atribuição de permissões. O escopo de um grupo, determina em partes do domínio ou de uma floresta de domínios, o grupo é visível, ou seja, pode ser utilizado para receber permissões de acesso aos recursos da rede.

Existem três escopos para grupos de usuários, conforme descrito a seguir: Universal, Global e Local do domínio. Vamos apresentar as diversas características e usos de cada tipo de grupo.

Grupos universais (Universal group):

Como o próprio nome sugere são grupos que podem ser utilizados em qualquer parte de um domínio ou da árvore de domínios e podem conter como membros, grupos e usuários de quaisquer domínios. Em resumo:

- ◆ Pode conter: Contas de usuários, outros grupos universais, e grupos globais de qualquer domínio.
- ◆ Pode ser membro de: Grupos locais do domínio ou grupos universais de qualquer domínio.
- ◆ Pode receber permissões para recursos localizados em qualquer domínio.

Conforme detalharei mais adiante, um domínio baseado no Active Directory pode estar em diferentes modos (Windows 2000 Nativo, Misto ou Windows Server 2003). Para cada modo existem diferentes possibilidades em relação aos grupos Universais:

---

**NOTA:** É importante lembrar que, neste capítulo, estão sendo apresentados os conceitos teóricos do Active Directory. A parte prática será vista nos demais capítulos. Por exemplo, no Capítulo 4 você aprenderá a criar usuários, grupos de usuários e a adicionar contas de usuários como membro de um ou mais grupos.

---

---

**NOTA:** É possível converter um grupo do tipo Segurança para distribuição e vice-versa. Para tal é preciso que o domínio esteja, pelo menos, no modo Windows 2000 Nativo. Para domínios que ainda estejam no modo Windows 2000 Mixed, esta conversão não será possível. Mais adiante falarei sobre Modos de um Domínio e Modos de uma Árvore de Domínios.

---

- ◆ Quando o nível de funcionalidade do Domínio está configurado como Windows 2000 Nativo ou Windows Server 2003, os seguintes elementos podem ser incluídos como membros de um grupo universal: Usuários, grupos Globais e grupos Universais de qualquer domínio da floresta.
- ◆ Quando o nível de funcionalidade do Domínio está configurado como Windows 2000 Misto, não é possível criar grupos Universais.
- ◆ Quando o nível de funcionalidade do Domínio está configurado como Windows 2000 Nativo ou Windows Server 2003, um grupo Universal pode ser colocado como membro de um outro grupo Universal e permissões podem ser atribuídas em qualquer domínio.
- ◆ Um grupo pode ser convertido de Universal para Global ou de Universal para Local do domínio. Nos dois casos esta conversão somente pode ser feita se o grupo Universal não tiver como um de seus membros, outro grupo Universal.

Quando devemos utilizar grupos universais:

Quando você deseja consolidar diversos grupos globais. Você pode fazer isso criando um grupo Universal e adicionando os diversos grupos globais como membros do grupo Universal.

Grupo global:

Um grupo Global é “global” quanto aos locais onde ele pode receber permissões de acesso, ou seja, um grupo Global pode receber permissões de acesso em recursos (pastas compartilhadas, impressoras, etc) de qualquer domínio. Em resumo, considere as afirmações a seguir:

- ◆ **Pode conter:** Contas de usuários e grupos globais do mesmo domínio, ou seja, somente pode conter membros do domínio no qual o grupo é criado.
- ◆ **Pode ser membro de:** Grupos universais e Grupos locais do domínio, de qualquer domínio.

**IMPORTANTE:** Os grupos Universais devem ser muito bem planejados. Não devem ser feitas alterações freqüentes nos membros de um grupo Universal, uma vez que este tipo de ação causa um volume elevado de replicação no Active Directory. Mais adiante quando for apresentado o conceito de Catálogo Global e de replicação no Active Directory, você verá o quanto justificada é esta recomendação.

Grupos globais do mesmo domínio.

- ◆ **Pode receber permissões para recursos localizados em qualquer domínio.**

Conforme detalharei mais adiante, um domínio baseado no Active Directory pode estar em diferentes modos (Windows 2000 Nativo, Misto ou Windows Server 2003). Para cada modo existem diferentes possibilidades em relação aos grupos Globais:

- ◆ Quando o nível de funcionalidade do Domínio está configurado como Windows 2000 Nativo ou Windows Server 2003, os seguintes elementos podem ser incluídos como membros de um grupo Global: contas de usuários e grupos globais do mesmo domínio. Por exemplo, se você cria um grupo global chamado WebUsers, no domínio abc.com.br, este grupo poderá conter como membros, grupos globais do domínio abc.com.br e usuários do domínio abc.com.br
- ◆ Quando o nível de funcionalidade do Domínio está configurado como Windows 2000 Misto, somente contas de usuários do próprio domínio é que podem ser membros de um grupo Global.

Por exemplo, se você cria um grupo global chamado WebUsers, no domínio abc.com.br e este domínio está no modo Misto, então somente contas de usuários do domínio abc.com.br é que poderão ser membros do grupo WebUsers.

- ♦ Um grupo pode ser convertido de Global para Universal, desde que o grupo Global não seja membro de nenhum outro grupo Global.

Quando devemos utilizar grupos globais:

Os grupos Globais devem ser utilizados para o gerenciamento dos objetos que sofrem alterações constantemente, quase que diariamente, tais como contas de usuários e de computadores. As alterações feitas em um grupo Global são replicadas somente dentro do domínio onde foi criado o grupo Global e não através de toda a árvore de domínios. Com isso o volume de replicação é reduzido, o que permite a utilização de grupos Globais para a administração de objetos que mudam freqüentemente.

Grupos locais do domínio (Domain local group):

São grupos que somente podem receber permissões para os recursos do domínio onde foram criados, porém podem ter como membros, grupos e usuários de outros domínios. Em resumo:

- ♦ Pode conter membros de qualquer domínio.
- ♦ Somente pode receber permissões para o domínio no qual o grupo foi criado.
- ♦ Pode conter: Contas de usuários, grupos universais e grupos globais de qualquer domínio.

Outros grupos Locais do próprio domínio.

- ♦ Pode ser membro de: Grupos locais do próprio domínio.

Conforme detalharei mais adiante, um domínio baseado no Active Directory pode estar em diferentes modos (Windows 2000 Nativo, Misto ou Windows Server 2003). Para cada modo existem diferentes possibilidades em relação aos grupos Globais:

- ♦ Quando o nível de funcionalidade do Domínio está configurado como Windows 2000 Nativo ou Windows Server 2003, os seguintes elementos podem ser incluídos como membros de um grupo Local: contas de usuários, grupos universais e grupos globais de qualquer domínio. Outros grupos locais do próprio domínio.
- ♦ Um grupo pode ser convertido de Local para Universal, desde que o grupo não tenha como seu membro um outro grupo Local.

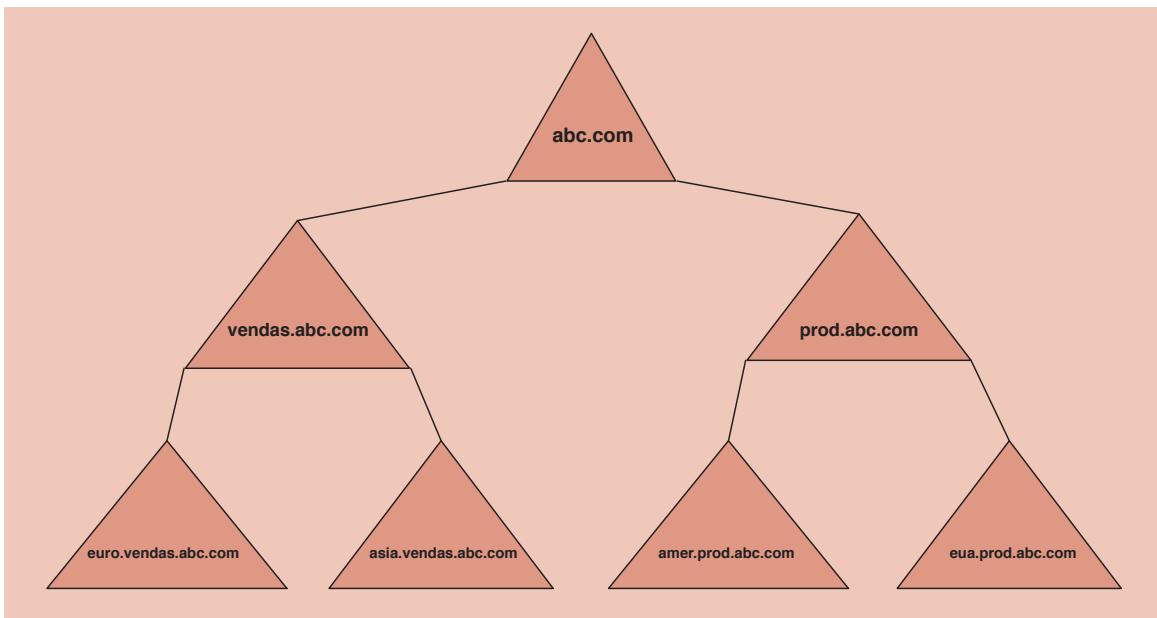
Quando devemos utilizar grupos Locais:

Os grupos Locais são utilizados para atribuir permissões de acesso aos recursos da rede. Conforme discutirei mais adiante, a Microsoft recomenda uma estratégia baseada nos seguintes passos:

- ♦ Criar as contas de usuários.
- ♦ Adicionar as contas de usuários a grupos Globais (confere com o que foi dito anteriormente, onde falei que os grupos Globais são utilizados para gerenciar os objetos do dia-a-dia, tais como contas de usuários).
- ♦ Adicione os grupos globais ou Universais (se for o caso) como membros dos grupos Locais.
- ♦ Atribua permissões de acesso para os grupos Locais.

## Atribuição de permissões em múltiplos domínios.

Neste tópico vou analisar um exemplo de uma rede onde existe uma árvore de domínios, ou seja, vários domínios formando uma árvore de domínios. Com base no diagrama apresentado na Figura 2.6, apresento alguns estudos de caso logo em seguida.



**Figura 2.6 Uma árvore de domínios.**

## Uma árvore com sete domínios:

No diagrama proposto na Figura 2.6, é exibida uma árvore com sete domínios. O domínio principal, também conhecido como domínio root tem o nome DNS: abc.com. Um domínio tem normalmente dois nomes:

- ◆ O nome DNS, que é o nome completo, no padrão do DNS. No nosso exemplo temos os domínios: abc.com, vendas.abc.com, prod.abc.com e assim por diante.
- ◆ O nome NETBIOS do domínio, que normalmente é a primeira parte do nome DNS. No nosso exemplo temos os domínios: ABC, VENDAS, PROD, EURO e assim por diante.

Observe que a árvore forma um espaço contínuo de nomes, conforme descrito anteriormente. Cada domínio filho contém o nome completo do domínio pai. Veja a descrição a seguir:

- ◆ Domínio root – principal:
- ◆ abc.com
- ◆ Domínios de segundo nível, “filhos” do abc.com – contém abc.com no nome:
- ◆ vendas.abc.com
- ◆ prod.abc.com

Domínios de terceiro nível, “filhos” dos domínios de segundo nível – contém o nome do domínio de segundo nível:

- ◆ Filhos do vendas.abc.com:
- ◆ euro.vendas.abc.com
- ◆ asia.vendas.abc.com
- ◆ Filhos do prod.abc.com:
- ◆ amer.prod.abc.com
- ◆ europa.prod.abc.com

---

**NOTA:** Estas são apenas sugestões de nomes. Eu procurei utilizar nomes que identificassem que o grupo é do tipo Global, a qual domínio ele pertence e qual a sua finalidade.

---

Neste exemplo temos uma árvore com sete domínios. Este é um exemplo de árvore de domínios perfeitamente possível de ser implementada com o uso do Windows Server 2003 e do Active Directory. Nesta árvore o primeiro domínio a ser instalado deve ser o domínio root: abc.com. Em seguida um dos domínios filhos, por exemplo vendas.abc.com e assim por diante.

## Um pouco sobre nomenclaturas de objetos no domínio, LDAP e caminhos UNC:

O Active Directory além de uma base de dados e um conjunto de serviços, também interage e depende de vários outros serviços e padrões para o seu completo funcionamento. Já citamos anteriormente que o DNS é o serviço de resolução de nomes no qual se baseia o Active Directory. O Active Directory foi projetado baseado em padrões de diretórios, definidos por entidades internacionais de padronização.

Entidades internacionais tais como a International Telecommunication Union (ITU), International Organization for Standardization (ISSO) e o Internet Engineering Task Force (IETF) trabalham em conjunto ou em colaboração para definir uma série de padrões que dão suporte a serviços de diretórios.

Um padrão de uso genérico é o X.500. Este padrão apesar de sua grande abrangência é bastante complexo e acabou por não ser adotado na sua íntegra como um padrão de mercado para a criação de serviços de diretórios. Um padrão mais “light” e que efetivamente tornou-se um padrão de mercado é o LDAP – Lightweight Directory Access Protocol. O protocolo LDAP fornece mecanismos de acesso aos objetos do Active Directory, de tal maneira que qualquer programa ou sistema habilitado ao padrão LDAP, seja capaz de acessar as informações do Active Directory, desde que devidamente identificado e tendo as devidas permissões. No início do capítulo, quando falei sobre diretórios, múltiplas senhas e afirmei que a visão de futuro da Microsoft é uma empresa onde todos os sistemas sejam integrados com o Active Directory, eu estava pensando no padrão LDAP. Com o uso deste padrão, é possível desenvolver sistemas integrados com o Active Directory.

O padrão LDAP define um sistema de nomeação hierárquico, através do qual é possível referenciar qualquer objeto do Active Directory. Você deve estar pensando que o LDAP e o DNS estão sendo utilizados para a mesma função. Não é exatamente isso. Sem entrar nas especificações técnicas de cada protocolo, arrisco a fazer as seguintes colocações:

- ◆ O DNS é o sistema de resolução de nomes utilizado pelos clientes para localizar recursos na rede, tais como o nome de um servidor ou uma pasta compartilhada em um servidor.
- ◆ O LDAP é um padrão para acesso e referência aos objetos do Active Directory. Com base neste padrão é possível criar APIs (Application Program Interfaces) que facilitam a criação de aplicações integradas ao Active Directory.

Um nome LDAP é formado pelo caminho completo do objeto, partindo do domínio raiz, até chegar ao objeto referenciado. Nesta nomenclatura hierárquica são utilizados algumas abreviaturas, conforme descrito a seguir:

- ◆ CN: common name: por exemplo, o nome da conta de um usuário, grupo ou computador.
- ◆ OU: faz referência a uma unidade organizacional.
- ◆ DC: um componente de domínio. Normalmente o nome de um domínio.
- ◆ O: Nome da organização. Normalmente representado pelo nome do domínio Root.
- ◆ C: Country: Identificação de país. Não é normalmente utilizado.

Para entender como é formado um nome LDAP, é melhor analisarmos alguns exemplos. Considere os exemplos a seguir:

- ◆ CN=jsilva,OU=contabilidade,DC=vendas,DC=abc.com -> Este nome representa o usuário jsilva, cuja conta está contida na unidade organizacional contabilidade, no domínio vendas.abc.com (observe que juntamos os dois componentes de domínio).

- ♦ CN=maria,OU=auditoria,OU=financias,DC=euro,DC=vendas,DC=abc.com -> Este nome representa o usuário maria, cuja conta está contida na unidade organizacional auditoria, a qual está contida dentro da unidade organizacional financias do domínio euro.vendas.abc.com.

Conforme já descrito anteriormente, os nomes LDAP e o protocolo LDAP são importantes para quem pretende desenvolver aplicações integradas com o Active Directory. Para efeitos de localização de recursos e identificação de objetos da rede, interessa mais o nome DNS e a nomenclatura de objetos do domínio, conforme descreverei logo a seguir.

A nomenclatura para localização de recursos em um servidor segue o padrão UNC Universal Naming Convention. Neste padrão um recurso é identificado pelo nome do servidor, separado do nome do recurso por uma barra. Considere os exemplos a seguir:

**\server01.vendas.abc.com\documentos**

Este é o caminho para uma pasta compartilhada com o nome de compartilhamento “documentos”, no servidor server01 do domínio vendas.abc.com. Ao invés do nome DNS do servidor também poderia ser utilizado o número IP do servidor, como no exemplo a seguir:

**\10.10.20.5\documentos**

Outro exemplo:

**\pr-server.prod.abc.com\laser01**

Este é o caminho para uma impressora compartilhada com o nome de compartilhamento “laser01”, no servidor pr-server do domínio prod.abc.com. Ao invés do nome DNS do servidor também poderia ser utilizado o número IP do servidor, como no exemplo a seguir:

**\10.10.30.5\laser01**

Outro ponto que convém ser abordado neste momento é a nomenclatura simplificada de identificação dos usuários. Considere o exemplo a seguir:

**vendas.abc.com\jsilva**

Este nome faz referência ao usuário jsilva do domínio vendas.abc.com. Outra forma de referência seria utilizar apenas o nome NETBIOS do domínio, ao invés do nome DNS completo, como no exemplo a seguir:

**VENDAS\jsilva**

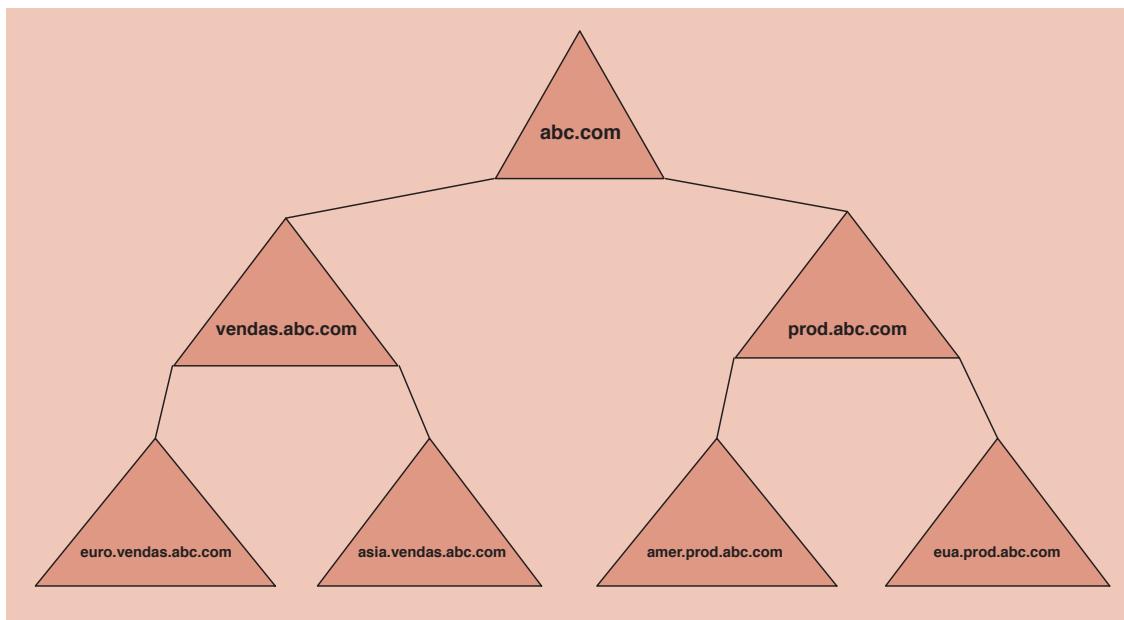
O padrão é NomeDoDomínio\NomeDoObjeto.

Agora que já apresentei os aspectos básicos de nomeação de objetos e recursos no Active Directory, é hora de apresentar alguns estudos de casos, para que você possa entender, na prática, os escopos de grupos (Universal, Global e Local) e como é feita a utilização de grupos para simplificar o processo de atribuição de permissões de acesso aos recursos da rede.

## **Estudo de caso 01: Exemplo de uso de Grupos Universais:**

Para este primeiro estudo de caso vamos imaginar a árvore de domínios indicada na Figura 2.7, onde todos os domínios estão no modo Windows Server 2003, o que implica que é possível a utilização de grupos Universais.

Neste exemplo, existe uma aplicação Web no servidor srv01.abc.com. Esta aplicação exige que o usuário seja autenticado antes de ter acesso a aplicação. Esta exigência é para que possa ser registrado no log do servidor, as ações realizadas por cada usuário. Em cada domínio, apenas alguns usuários, de diferentes seções, deverão ter permissão de acesso a esta aplicação. Qual a solução recomendada para simplificar a administração deste sistema de permissões de acesso?



**Figura 2.7 Uso de grupos Universais.**

Solução proposta: Este é um exemplo típico para o uso de uma combinação de Grupos Universais e Grupos Globais. Como os domínios estão no modo Windows Server 2003, é possível a criação de Grupos Universais (o que também seria possível se os domínios estivessem no modo Windows 2000 Nativo). Em cada domínio você cria um grupo Global. É aconselhável que o nome do grupo seja descritivo do seu objetivo. Você adiciona os usuários que devem ter acesso a aplicação Web, como membros do grupo Global do seu respectivo domínio. No domínio abc.com você cria um grupo Universal e, adiciona como membros deste grupo, o grupo global de cada domínio, grupos estes criados anteriormente e aos quais foram adicionados os usuários que devem ter acesso a aplicação Web. No servidor srv01.abc.com você atribui as permissões necessárias ao grupo Universal criado no domínio abc.com (do qual são membros os respectivos grupos globais de cada domínio).

Ao atribuir as permissões necessárias ao grupo universal do domínio abc.com, os grupos globais que são membros deste grupo irão herdar as mesmas permissões, as quais serão herdadas pelos membros do grupo. Observe que o efeito de atribuir a permissão ao grupo universal no domínio abc.com é que esta permissão propaga-se até os usuários em seus respectivos domínios.

Dando nome aos grupos e dividindo a solução em etapas, poderíamos descrever a solução proposta da seguinte maneira:

- ♦ Criar um grupo global em cada um dos domínios, conforme sugestão a seguir:

| Domínio             | Nome do Grupo Global                 |
|---------------------|--------------------------------------|
| abc.com             | G-Glob-abc-com-AcessoWeb             |
| vendas.abc.com      | G-Glob-vendas-abc-com-AcessoWeb      |
| euro.vendas.abc.com | G-Glob-euro-vendas-abc-com-AcessoWeb |
| asia.vendas.abc.com | G-Glob-asia-vendas-abc-com-AcessoWeb |
| prod.abc.com        | G-Glob-prod-abc-com-AcessoWeb        |
| amer.prod.abc.com   | G-Glob-prod-amer-abc-com-AcessoWeb   |
| eua.prod.abc.com    | G-Glob-prod-eua-abc-com-AcessoWeb    |

- ♦ Em cada domínio você inclui os usuários que devem ter acesso à aplicação Web, ao grupo global do respectivo domínio, criado no passo anterior.

- ◆ Crio um grupo Universal no domínio abc.com:

**Domínio    Nome do Grupo Universal**  
**abc.com    G-Univ-abc-com-AcessoWeb**

- ◆ Incluo os grupos globais criados na primeira etapa como membros do grupo Universal:

- ◆ Membros do grupo G-Univ-abc-com-AcessoWeb:

**G-Glob-abc-com-AcessoWeb**  
**G-Glob-vendas-abc-com-AcessoWeb**  
**G-Glob-euro-vendas-abc-com-AcessoWeb**  
**G-Glob-asia-vendas-abc-com-AcessoWeb**  
**G-Glob-prod-abc-com-AcessoWeb**  
**G-Glob-prod-amer-abc-com-AcessoWeb**  
**G-Glob-prod-eua-abc-com-AcessoWeb**

- ◆ Pronto, está implementada a solução para definição das permissões de acesso a aplicação Web no servidor srv01.abc.com. Com esta solução, sempre que um usuário precisar de acesso à aplicação Web, basta incluí-lo no grupo global do seu respectivo domínio. Se o usuário não deve mais ter acesso à aplicação, basta retirá-lo do respectivo grupo global. Observe que a administração das permissões fica bem simplificada. É uma simples questão de incluir ou retirar o usuário de um determinado grupo.

## **Estudo de caso 02: Analisando o escopo de grupos em relação a membros e permissões de acesso:**

Para este estudo de caso vou continuar considerando a árvore de domínios da Figura 5.6. Vamos colocar algumas questões para análise:

Questão 01: Vamos supor que você crie um grupo Global chamado AcessoFinança, no domínio vendas.abc.com. Considere os itens a seguir:

- ◆ O grupo AcessoFinança pode ter usuários e grupos de que domínio(os) como membros do grupo?

Como o grupo AcessoFinança é Global e foi criado no domínio vendas.abc.com, ele somente pode conter como membros, usuários e outros grupos globais do próprio domínio vendas.abc.com. Esta é uma das características dos grupos Globais, ou seja, somente podem conter como membros, usuários e outros grupos globais do seu próprio domínio.

- ◆ Em qual ou quais domínios o grupo AcessoFinança pode receber permissões de acesso?

Um grupo Global pode receber permissões de acesso a recursos em qualquer domínio na árvore de domínios. Normalmente para atribuir permissões a um grupo Global, em outro domínio, basta colocar o grupo Global como membro de um grupo Local do domínio de destino (onde está localizado o recurso) e atribuir permissão para o grupo Local. Este é o procedimento recomendado pela Microsoft. Por exemplo, vamos supor que o grupo global AcessoFinança, do domínio vendas.abc.com, precise de acesso a uma pasta compartilhada em um servidor do domínio prod.abc.com. O processo recomendado pela Microsoft é incluir o grupo global AcessoFinança, do domínio vendas.abc.com, como membro de um grupo local do domínio prod.abc.com e atribuir as permissões necessárias para este grupo local. Com isso o grupo global herda as permissões e todos os usuários do grupo Global também herdam as permissões.

Questão 02: Vamos supor que você crie um grupo Local chamado UsuáriosMemo, no domínio vendas.abc.com. Considere os itens a seguir:

◆ **O grupo UsuáriosMemo pode ter usuários e grupos de que domínio(os) como membros do grupo?**

Como o grupo UsuáriosMemo é Local, ele pode ter como membros, usuários e grupos do seu próprio domínio e também usuários e grupos de outros domínios. Por exemplo, posso incluir um grupo global do domínio prod.abc.com, como membro de um grupo local do domínio vendas.abc.com.

◆ **Em qual ou quais domínios o grupo UsuáriosMemo pode receber permissões de acesso?**

Como o grupo é Local ele somente pode receber permissão de acesso a recursos localizados em servidores do seu próprio domínio, ou seja, a recursos localizados em servidores do domínio vendas.abc.com, onde o grupo UsuáriosMemo foi criado.

Questão 03: Vamos supor que você crie um grupo Universal chamado AcessoWeb, no domínio abc.com. Considere os itens a seguir:

◆ **O grupo AcessspWeb pode ter usuários e grupos de que domínio(os) como membros do grupo?**

De qualquer domínio, pois ele é um grupo Universal.

◆ **Em qual ou quais domínios o grupo Acesso Web pode receber permissões de acesso?**

Em qualquer domínio, pois ele é um grupo Universal.

Agora é chegado o momento de analisar mais alguns elementos que formam a infra-estrutura que permite o funcionamento do Active Directory. Vou falar um pouco mais sobre Unidades organizacionais. Na seqüência falarei sobre Relações de confiança e florestas.

## Entendendo as Unidades organizacionais.

O conceito de Unidade organizacional foi introduzido no Windows 2000 Server, juntamente com o Active Directory e veio para solucionar um problema sério de Administração existente no Windows NT Server 4.0.

Com o NT Server 4.0, não havia como atribuir permissões de acesso apenas a uma parte do domínio. Ou você atribuía permissões de Administrador no domínio inteiro ou não tinha como atribuir permissões de administrador para um usuário. Imagine uma empresa que tem uma rede, com filiais em todos os estados brasileiros. Por questões de simplicidade vamos supor que a rede é composta de seis domínios, sendo que em cada domínio estão as filiais de 4 ou mais estados. Vamos supor que um dos domínios seja composto pelas redes das filiais do RS, SC, PR e SP. Com o NT Server 4.0, você não teria como definir que um usuário tivesse permissões de Administrador somente nos servidores da filial do RS. Uma vez que você atribuía permissões de Administrador, o usuário teria estas permissões em todos os recursos do domínio. No nosso exemplo, o usuário seria Administrador nos servidores das filiais do RS, SC, PR e SP, ou seja, em todos os servidores do domínio.

Esta situação gerava inconvenientes (e noites de sono perdidas) muito sérios. Era comum a situação onde um domínio tinha 10 ou mais contas de usuários com permissão de Administrador. Ora, eram 10 ou mais contas com permissões total em todos os servidores do domínio. Nada bom.

Com a disponibilidade de Unidades Organizacionais, a partir do Windows 2000 Server, este problema foi minimizado. Agora você pode criar, dentro do domínio, várias Unidades organizacionais. Em seguida você desloca para dentro de cada unidade organizacional, as contas de usuários e computadores, de acordo com critérios geográficos ou funcionais. Em seguida você pode delegar tarefas administrativas a nível de Unidade organizacional (OU – Organizational Unit).

Vamos considerar o exemplo anterior, onde tínhamos um domínio formado pelas redes das filiais do RS, SC, PR e SP. Neste exemplo, o Administrador do domínio poderia criar quatro unidades organizacionais:

- ◆ RS
- ◆ SC
- ◆ PR
- ◆ SP

Em seguida ele move as contas de usuários e computadores e contas de grupos para as respectivas OUs. O último passo é atribuir permissões de administração em cada OU. Por exemplo, para o Administrador da filial do RS, seriam delegadas permissões de administração na OU RS, para o Administrador da filial de SC, seriam delegadas permissões de administração na OU SC e assim por diante. O diagrama da Figura 2.8 ilustra a divisão de um domínio em OUs.

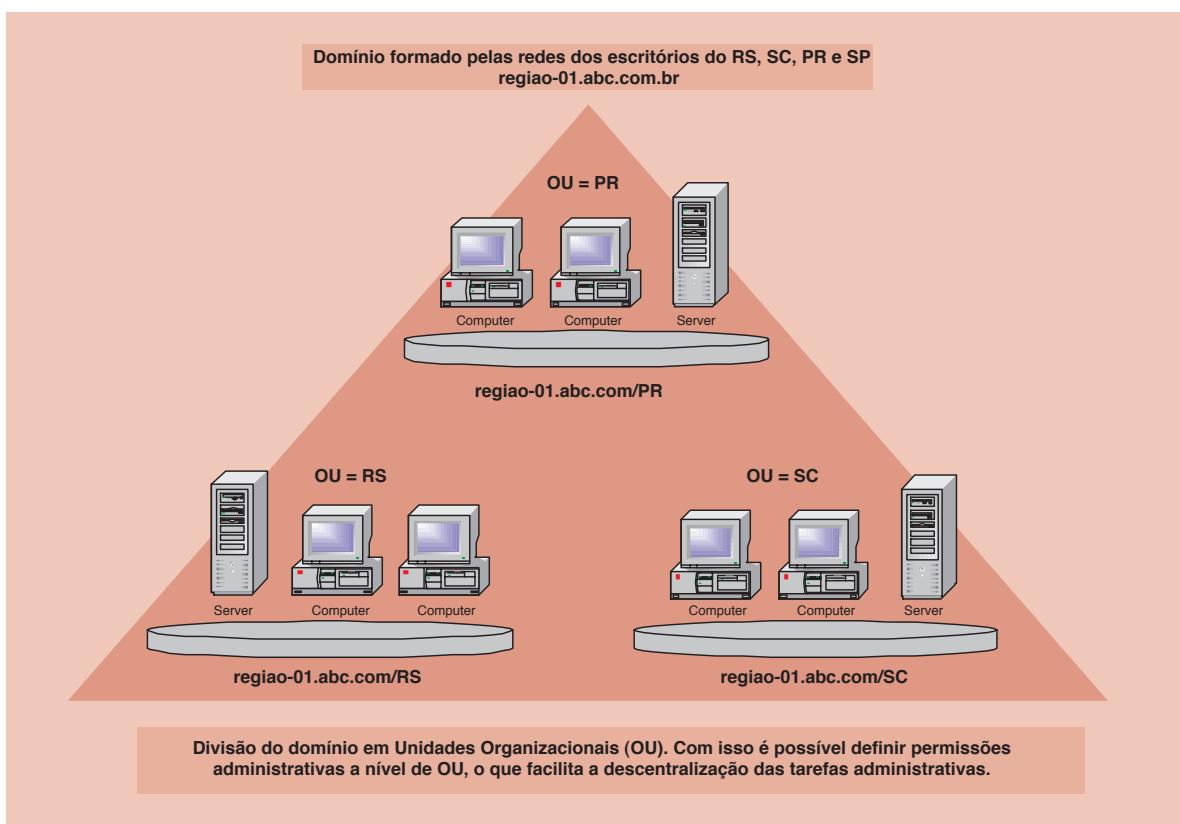


Figura 2.8 Divisão de um domínio em OUs.

No diagrama está representada a divisão do domínio `regiao-01.abc.com.br` em OUs. Dentro de uma OU é possível criar outras OUs. Por exemplo, dentro da Unidade Organizacional RS, o administrador poderia criar outras unidades organizacionais, tais como: Usuários, Grupos e Computadores. Em seguida, todas as contas de usuários da filial do RS, seriam deslocadas para a OU Usuários, dentro da OU RS; todas as contas dos computadores da filial do RS seriam deslocadas para a OU Computadores, dentro da OU RS e assim por diante.

Observem que, basicamente, a utilização de OUs facilita a descentralização das tarefas administrativas, através da delegação de tarefas para porções específicas de um domínio. A utilização de OUs também desempenha um papel importante no gerenciamento das políticas de segurança, através do uso de Group Policies Objects (GPOs). Para um estudo completo de GPOs, consulte o Capítulo 18 do livro [Windows Server 2003 – Curso Completo](#), 1568 páginas.

# Relações de confiança e florestas.

É através do uso de relações de confiança entre domínios, que é possível que um usuário de um domínio possa fazer o logon com sua conta de usuário e senha, mesmo utilizando um computador de um outro domínio. Por exemplo, o usuário jsilva está cadastrado no domínio A e viaja para a filial da empresa, a qual pertence ao domínio B. O usuário jsilva está utilizando um computador que faz parte do domínio B. Durante o processo de logon ele informa o seu nome de usuário, senha e seleciona o domínio no qual ele quer fazer o logon (no exemplo o domínio A) e consegue fazer o logon normalmente.

Como foi possível ao domínio B (mais especificamente a um DC do domínio B), verificar as credenciais do usuário (logon e senha) e permitir o logon? Isso foi possível graças ao mecanismo de relações de confiança existente no Windows Server 2003, o qual é muito semelhante ao que existe no Windows 2000 Server, porém completamente diferente do que acontecia no Windows NT Server 4.0. Neste item apresentarei em mais detalhes, o mecanismo de relações de confiança entre domínios no Windows Server 2003.

## Como eram as relações de confiança na época do NT Server 4.0?

As relações de confiança no NT Server 4.0 são definidas por três características principais:

- ◆ São unilaterais: Se o domínio A confia no domínio B, isso não significa que o domínio B confia no domínio A automaticamente. Para que haja essa confiança recíproca é preciso criar duas relações de confiança: uma para definir que o domínio A confia no domínio B e outra para definir que o domínio B confia no domínio A. A Figura 2.9, da ajuda do Windows Server 2003, ilustra este conceito:

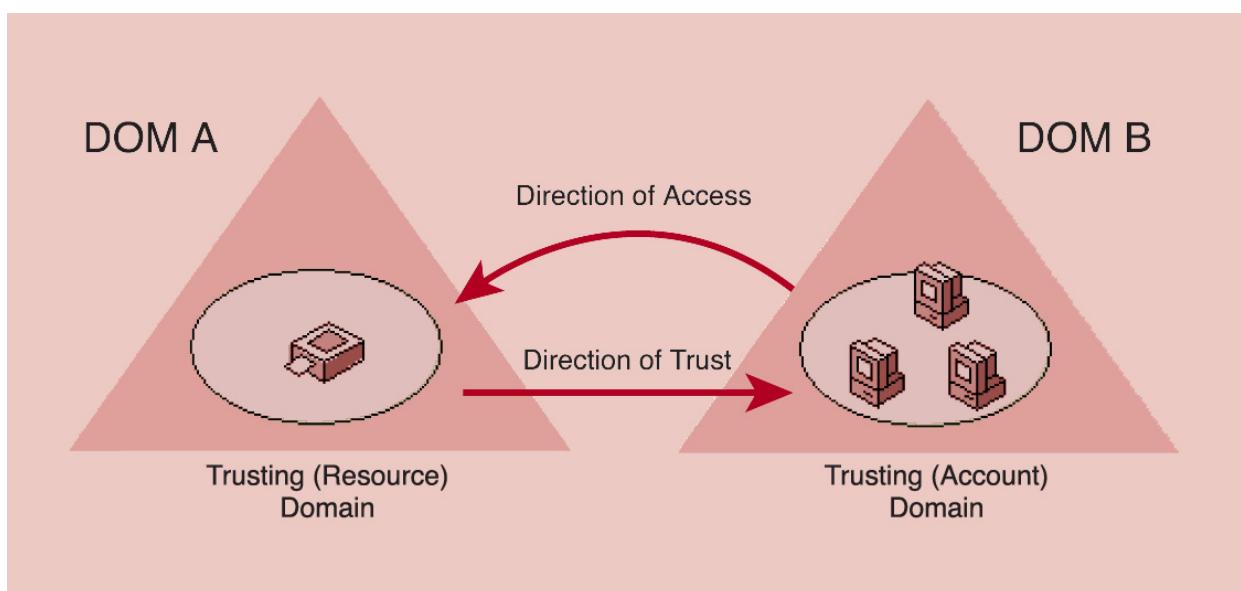


Figura 2.9 Relação de confiança unilateral.

Neste exemplo do Dom A confia no Dom B. Isso significa que as contas do Dom B são “visíveis” no Dom A, ou seja, é possível atribuir permissões de acesso para as contas do Dom B, em recursos do Dom A. O contrário não é verdadeiro, ou seja, não é possível atribuir permissões de acesso para as contas do Dom A, em recursos do domínio B. Para que isso fosse possível teria que ser criada mais uma relação de confiança, agora com o Dom B “confiando” nas contas do Dom A. Isso tudo acontece porque as relações de confiança no NT Server 4.0 são unilaterais.

- ◆ Não são transitivas: Se o Dom A confia no Dom B e o Dom B confia no domínio C, isso não implica que o Dom A também confia no Dom C. Para que o Dom A confie no Dom C, uma relação de confiança entre os dois domínios tem que ser manualmente criada pelo Administrador.
- ◆ Devem ser criadas manualmente pelos Administradores: As relações de confiança não são criadas automaticamente e devem ser criadas pelos Administradores de cada domínio. O processo é bem trabalhoso. Para que o Dom A possa confiar no Dom B, primeiro o Administrador do Dom B tem que fazer uma configuração “dizendo” que ele aceita que o Dom A confie no Dom B. O próximo passo é o Administrador do Dom A estabelecer a relação de confiança com o Dom B. Para que o Dom B também possa confiar no Dom A, todo o processo (só que na direção inversa) tem que ser repetido.

Para uma rede com 10 domínios, para que todos possam confiar em todos os outros, são necessárias 90 relações de confiança. O número de relações de confiança, com base no número de domínios, pode ser calculada pela fórmula a seguir:

$$n * (n - 1)$$

onde n é o número de domínios.

Para 10 domínios teremos:

$$10 * (10 - 1)$$

$$10 * 9$$

$$90$$

A Figura 2.10, obtida do Resource Kit do Windows 2000 Server, mostra como seria uma árvore de domínios no NT Server 4.0, onde foram implementadas relações de confianças entre todos os domínios:

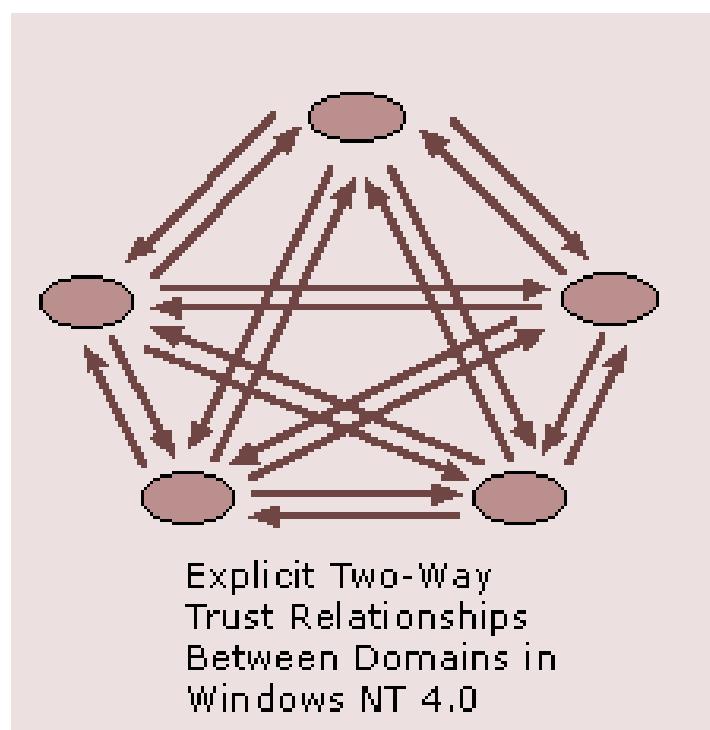


Figura 2.10 Relações de confiança unidirecionais, não transitivas do NT Server 4.0.

## E como são as relações de confiança no Windows Server 2003?

No Windows Server 2003 (bem como no Windows 2000 Server) as relações de confiança são criadas automaticamente entre os domínios de uma árvore de domínios. As relações são bi-direcionais, ou seja, se o Dom A confia no Dom A, isso significa que o Dom B também confia no Dom A. As relações de confiança são transitivas, ou seja se o Dom A confia no Dom B, o qual confia no Dom C, então o dom A também confia no Dom C e vice-versa. A Figura 2.11 ilustra as relações de confiança no Windows Server 2003.

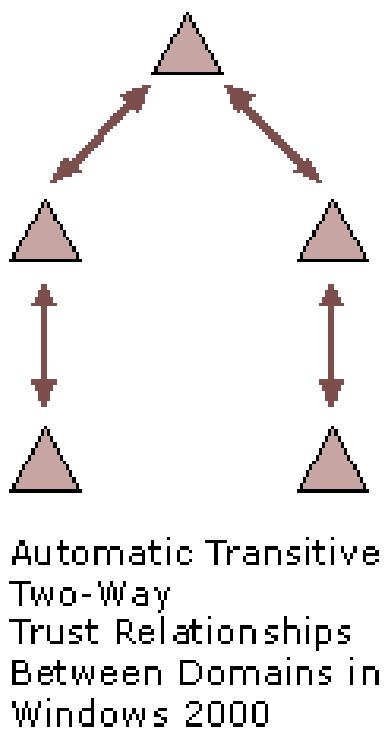


Figura 2.11 Relações de confiança bi-direcionais e transitivas do Windows Server 2003.

## Outros tipos de relações de confiança:

As relações de confiança criadas automaticamente, entre os domínios de uma árvore no Windows Server 2003, apresentam as características descritas anteriormente: Automaticamente criadas, bi-direcionais e transitivas.

Porém existem situações em que pode ser necessária a criação de outros tipos de relações de confiança. Por exemplo, pode ser necessária a criação de uma relação de confiança entre um dos domínios da sua rede, com um domínio baseado no Windows NT Server da rede de um fornecedor ou parceiro de negócio. Ou pode ser necessária a criação de uma relação de confiança entre um domínio da sua rede (baseado no Windows Server 2003) com um domínio da rede de outra empresa, também baseado no Windows Server 2003. Neste caso você teria que criar uma relação de confiança com um domínio em outra árvore de domínios. A seguir vou analisar e exemplificar os tipos de relações de confiança que existem.

## Tipos padrão de relações de confiança:

Existem dois tipos padrão de relação de confiança, conforme descrito a seguir:

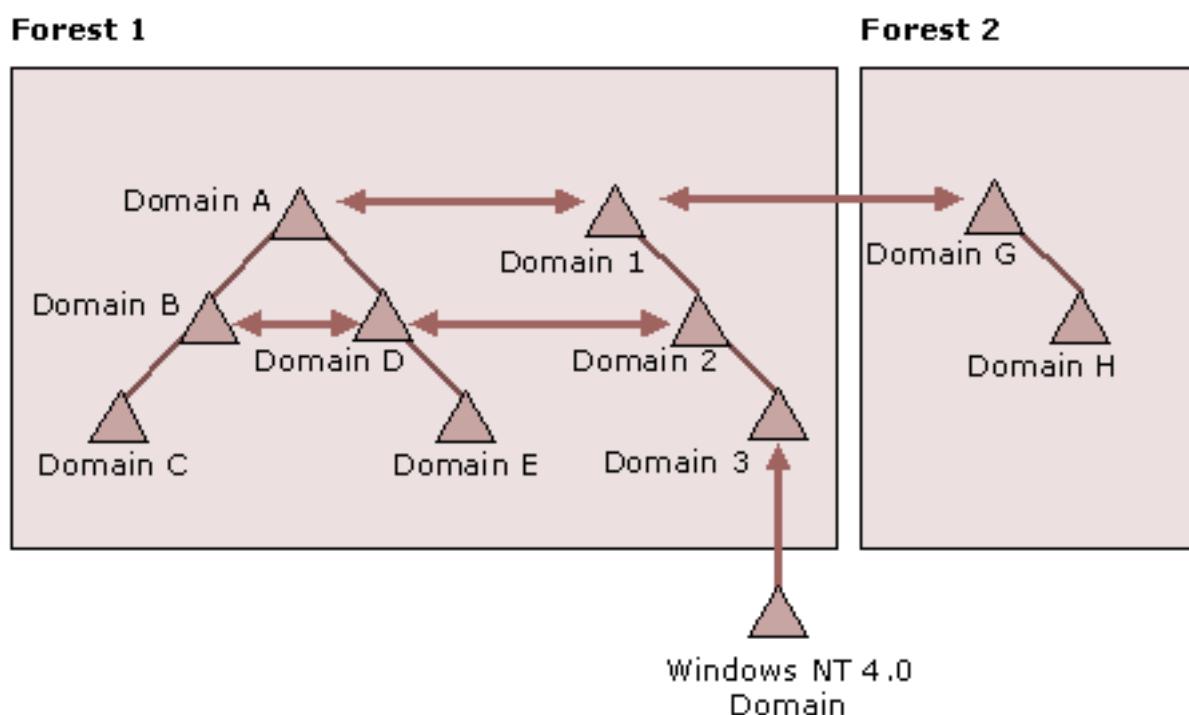
- ◆ **Transitiva bi-direcional entre um Domínio pai e um Domínio filho:** Quando o Administrador cria um domínio filho, uma relação de confiança bi-direcional e transitiva é criada, automaticamente, pelo assistente de instalação do Active Directory. Por exemplo, se você tem um domínio root chamado abc.com e cria um domínio filho chamado vendas.abc.com, o assistente de instalação do Active Directory, automaticamente cria durante a criação do domínio vendas.abc.com, uma relação de confiança bi-direcional e transitiva entre os dominios abc.com e vendas.abc.com.
- ◆ **Transitiva bi-direcional entre uma árvore de domínios e o domínio root de uma floresta:** Você pode juntar várias árvores de domínios para formar um floresta. Este tipo de relação de confiança é automaticamente criado, quando você cria um novo domínio em uma floresta já existente. A relação é estabelecida.

## Outros tipos de relações de confiança:

Existem outros tipos padrão de relação de confiança, conforme descrito a seguir:

- ◆ **Externa, não transitiva, unidirecional ou bi-direcional:** Este tipo de relacionamento é criado com um domínio externo, baseado no Windows NT Server 4.0 ou com um domínio baseado no Windows Server 2003 ou Windows 2000 Server, localizado em outra floresta. Se o domínio for baseado no NT Server 4.0 a relação será unidirecional, caso contrário será bi-direcional.

O exemplo da Figura 2.12 ilustra bem as situações onde pode ser criada uma relação de confiança deste tipo:



**Figura 2.12 Relações de confiança externas – unidirecional ou bi-direcional.**

- ◆ **Realm, transitiva ou não transitiva, unidirecional ou bi-direcional:** Este tipo de relação é criado entre um domínio baseado no Windows Server 2003 e outros domínios, também baseados no protocolo Kerberos, como por exemplo o UNIX. O protocolo Kerberos é um padrão de fato que fornece, dentre outros, serviços de autenticação em um domínio do Windows 2000 Server ou Windows Server 2003. Outros sistemas operacionais também utilizam o Kerberos. Este tipo de relacionamento poderia ser utilizado, por exemplo, para que as

contas de um domínio baseado no UNIX, pudessem receber permissões de acesso em recursos de um domínio baseado no Windows Server 2003.

- ◆ **Entre florestas, transitiva, unidirecional ou bi-direcional:** Este tipo de relacionamento é criado entre os domínios root de duas florestas. Pode ser do tipo unidirecional ou bi-direcional. Se for do tipo bi-direcional, os usuários de uma floresta podem acessar recursos nos domínios da outra floresta e vice-versa. Um exemplo prático de uso deste tipo de relação de confiança seria quando é feita a fusão de duas empresas e você precisa permitir que os usuários de uma empresa possam acessar recursos nos servidores da rede da outra empresa e vice-versa.
- ◆ **Shortcut, transitiva, unidirecional ou bi-direcional:** Este tipo de relação de confiança é utilizado para melhorar o tempo de logon entre dois domínios, em uma floresta. Considere o exemplo da Figura 2.13:

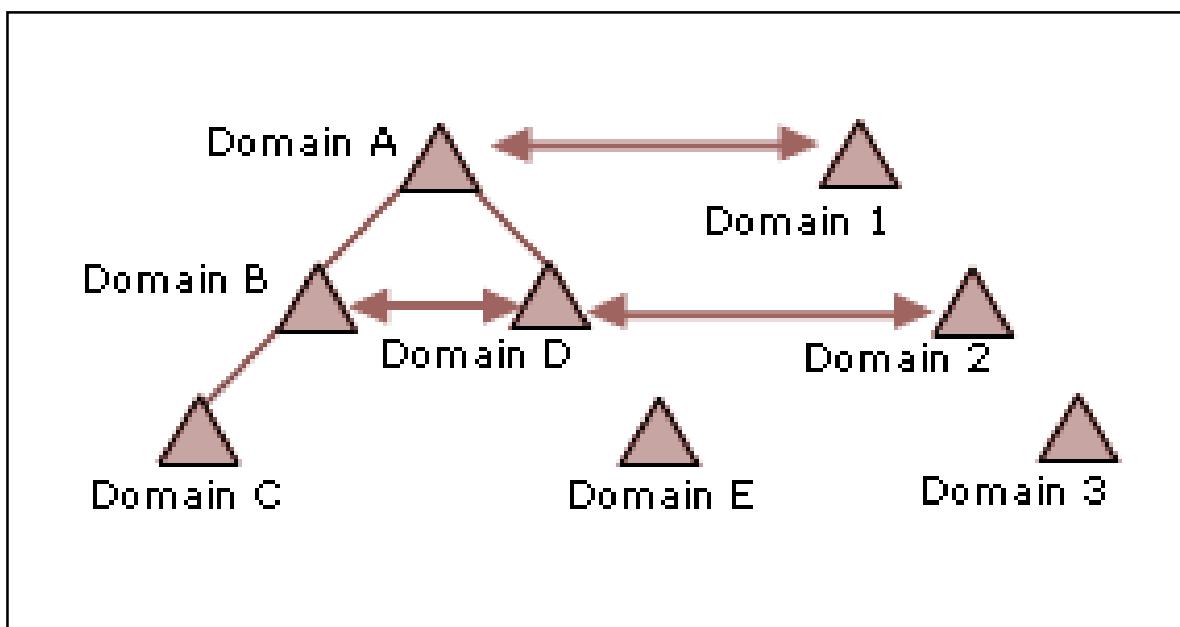


Figura 2.13 Relações de confiança do tipo Shortcut (atualho).

Neste exemplo foram criadas três relações de confiança do tipo Shortcut:

- ◆ Entre os domínios B e D.
- ◆ Entre os domínios A e 1.
- ◆ Entre os domínios D e 2.

O principal objetivo deste tipo de relação de confiança é otimizar os tempos de logon. No exemplo da Figura 2.13, vou analisar o que acontece quando um usuário do Dom B precisa acessar um recurso no Dom D. O primeiro passo é autenticar o usuário. Se não houver a relação do tipo Shortcut entre B e D, o Windows Server 2003 precisa percorrer o caminho de relações de confiança na árvore (de B para A e de A para D), para poder autenticar o usuário do domínio D. Já com a relação do tipo shortcut entre B e D, existe um caminho direto entre estes dois domínios, o que diminui o tempo de logon/autenticação. Quanto mais afastados (quanto maior o caminho e o número de relações de confiança a ser percorrido), mais será reduzido o tempo de logon entre os domínios, se o Administrador criar uma relação de confiança do tipo Shortcut.

**IMPORTANTES:** Só faz sentido criar este tipo de relação de confiança, se for comum usuários de um domínio acessarem recursos do outro domínio e se o tempo de logon estiver apresentando tempos muito elevados.

# Servidores de Catálogo Global (Global Catalogs)

Pelo que foi visto até aqui, é possível perceber que o Active Directory no Windows Server 2003 é bastante flexível, permitindo que usuários de um domínio acessem recursos em servidores de outro domínio ou até mesmo outra floresta, sem ter que entrar novamente com o seu login e senha. Para que isso seja possível, o Active Directory mantém uma base com algumas informações sobre objetos de todos os domínios. Esta base de informações é mantida em Controladores de Domínio (DCs), configurados para atuar como Servidores de Catálogo Global (Global Catalog Servers). Nem todo DC é um Global Catalog, mas para ser Global Catalog tem que ser um DC, não pode ser um Member Server. Neste item vou apresentar informações detalhadas sobre os Servidores de Catálogo Global.

Um Servidor de Catálogo Global armazena uma cópia de todos os objetos do Active Directory, de todos os domínios em uma ou mais árvores de domínios de uma floresta. No Servidor de Catálogo Global fica uma cópia completa de todos os objetos do próprio domínio do servidor e uma cópia parcial de todos os objetos dos demais domínios. Esta estrutura é indicada na Figura 2.14:

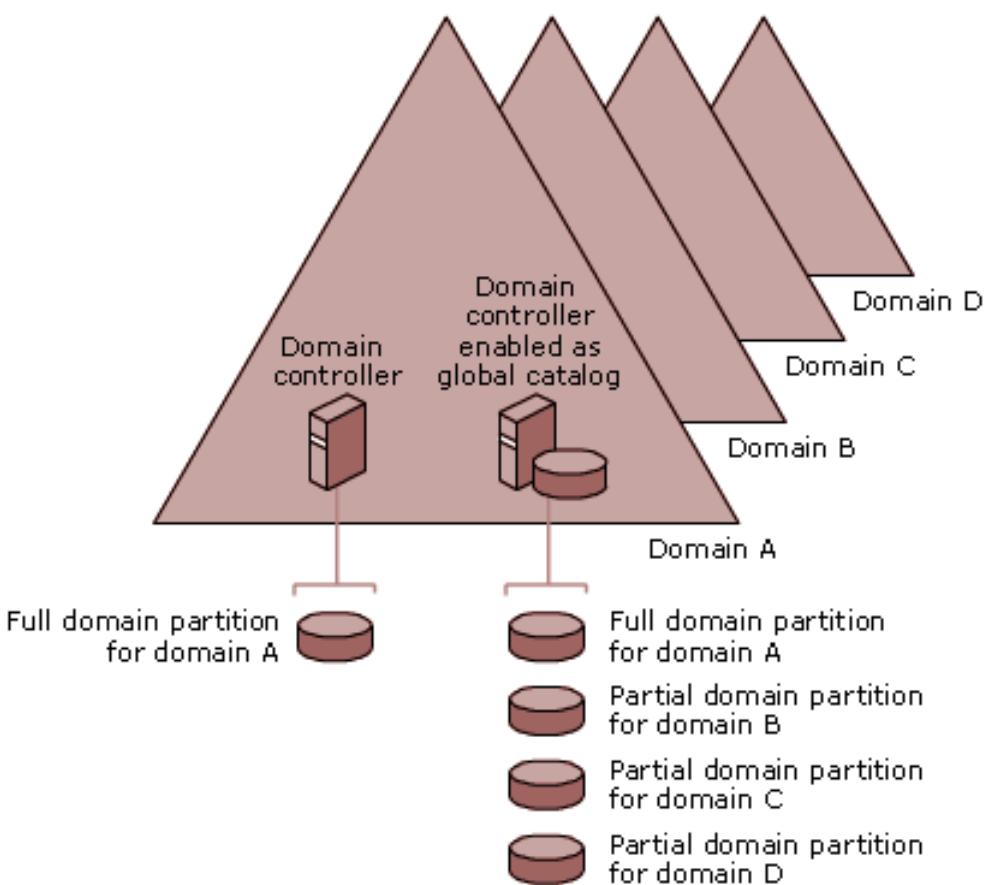


Figura 2.14 Informações armazenadas em um Servidor de Catálogo Global.

Observe que um servidor que é DC mas não está configurado como Servidor de Catálogo Global, contém uma cópia completa de todos os objetos do seu domínio, mas não tem cópia de objetos de outros domínios. Já um DC habilitado como Servidor de Catálogo Global, tem, além da cópia completa dos objetos do seu próprio domínio, cópias parciais de todos os objetos dos demais domínios. Quando se fala em cópias parciais, significa que o Servidor de Catálogo Global mantém cópia de todos os objetos, mas não de todos os atributos de um objeto de outro domínio. Por exemplo, o Servidor de Catálogo Global tem cópia de todos os usuários de outros domínios, mas para cada usuário apenas alguns atributos (nome, senha, etc) são armazenados no Catálogo Global e não todos os atributos.

Os atributos de cada objeto que são copiados para o Catálogo Global são aqueles atributos mais utilizados para a realização de pesquisas no Active Directory. Por exemplo nome do usuário, nome de compartilhamento e tipo da impressora e assim por diante. A definição de quais atributos são armazenados no Catálogo Global e quais não são é feita no Schema. Conforme mostrarei mais adiante o Schema é como se fosse (na prática eu considero que é) a definição da estrutura do banco de dados do Active Directory. Falarei mais sobre Schema no próximo item.

Ao armazenar os atributos mais utilizados no Catálogo Global, o Windows Server 2003 aumenta o desempenho das pesquisas no Active Directory. Se não houvesse um Catálogo Global, as pesquisas teriam que percorrer todo o caminho da rede, da origem, até encontrar um servidor (um DC) no domínio de destino e os resultados percorrer o caminho inverso. Em redes maiores, com mais domínios, isso representaria um sério problema de desempenho, além de gerar um excessivo tráfego de rede. Evidentemente que a manutenção do Catálogo Global atualizado em todos os Servidores de Catálogo Global, gera tráfego de replicação, mas o resultado final é um ganho de performance e redução do tráfego de rede, em comparação se não existisse o Catálogo Global.

Quando um domínio é criado, com a instalação do primeiro DC do domínio, este DC é automaticamente configurado como Servidor de Catálogo Global. Os próximos DCs do domínio não serão automaticamente configurados como Servidor de Catálogo Global, mas você poderá configurá-los posteriormente.

## Principais funções desempenhadas por um Servidor de Catálogo Global:

Um Servidor de Catálogo Global desempenha importantes funções, dentre as quais podemos destacar as indicadas a seguir:

- ◆ **Pesquisa de objetos no Active Directory:** Com o uso de Servidor de Catálogo Global, o usuário é capaz de pesquisar objetos em todos os domínios de uma floresta. A velocidade das pesquisas melhora bastante, uma vez que a pesquisa é feita no Servidor de Catálogo Global mais próximo do usuário, no seu próprio domínio e não no servidor de destino ou no caso de uma pesquisa genérica (por exemplo, pesquisar silva no campo Sobrenome dos objetos usuários) em todos os servidores de todos os domínios.
- ◆ **Fornece autenticação para nomes de usuários de outro domínio:** O Catálogo Global é utilizado para a resolução de nomes de usuários (ou de outros objetos do Active Directory), quando o DC que autenticou o usuário não tem informações sobre a referida conta. Por exemplo, se o usuário jsilva do domínio vendas.abc.com precisa fazer o logon como [jsilva@vendas.abc.com](mailto:jsilva@vendas.abc.com) em um computador pertencente ao domínio prod.abc.com, o DC do domínio prod.abc.com não será capaz de localizar o usuário [jsilva@vendas.abc.com](mailto:jsilva@vendas.abc.com) (pois o DC do domínio prod.abc.com tem informações somente sobre os usuários do seu próprio domínio e não dos demais domínios. Estas informações estão nos Servidores de Catálogo Global). O DC no domínio prod.abc.com irá contatar um Servidor de Catálogo Global para poder completar o processo de logon do usuário [jsilva@abc.com](mailto:jsilva@abc.com), com sucesso.
- ◆ **Disponibiliza informações sobre os membros dos grupos universais, em um ambiente com múltiplos domínios:** As informações sobre os membros dos grupos locais são armazenadas apenas no domínio onde o grupo é criado. Por isso que um grupo local somente pode receber permissões de acesso aos recursos do domínio onde o grupo foi criado. Já as informações sobre os membros dos grupos Universais são armazenadas somente nos Servidores de Catálogo Global. Por isso que recomenda-se que sejam inseridos como membros dos grupos Universais, apenas outros grupos e não usuários individualmente. Se forem inseridos usuários individualmente, cada vez que um usuário for adicionado ou excluído de um grupo universal, todas as informações do grupo Universal serão replicadas entre todos os Servidores de Catálogo Global da floresta. Por exemplo, quando um usuário que pertence a um grupo universal faz o logon em um domínio configurado para o modo Windows 2000 Nativo ou Windows Server 2003, o Catálogo Global fornece informações sobre a quais grupos universais a conta do usuário pertence.

Se não estiver disponível um Servidor de Catálogo Global, o computador no qual o usuário fez o logon irá utilizar as informações armazenadas no cache do computador, caso o usuário já tenha feito um logon anterior neste computador. Se for o primeiro logon do usuário neste computador e não estiver disponível um Servidor de Catálogo Global, o usuário não conseguirá fazer o logon no domínio. Ele conseguirá fazer o logon apenas localmente no computador, usando uma das contas locais ao invés de uma conta do domínio.

Existe uma exceção à esta regra, que é quando a conta do usuário pertence ao grupo Administradores do Domínio (Domain Admins). Neste caso, o usuário conseguirá fazer o logon, mesmo que um Servidor de Catálogo Global não esteja disponível e mesmo que seja o seu primeiro logon no computador.

- ◆ **Validação de referências a objetos em uma floresta:** O Catálogo Global é utilizado pelos DCs para validar referências a objetos de outros domínios de uma floresta. Quando um DC trata com um objeto onde um dos seus atributos contém referências a um objeto em outro domínio, esta referência é validada pelo Catálogo Global. Mais uma vez é importante salientar o papel dos Servidores de Catálogo Global em melhorar o desempenho do Active Directory. Nesta situação, se não existisse o Catálogo Global, a validação da referência ao objeto teria que ser feito por um DC do domínio do objeto referenciado. Só nestas situações (muito comuns na utilização diária da rede), imagine quanto tráfego de validação seria gerado através dos links de WAN da rede. Sem contar também a demora adicional até que a validação fosse feita através da rede, no domínio de destino e a resposta retornasse.

**NOTA:** Quando a rede é formada por um único domínio, não é necessário que os usuários obtenham informações sobre os grupos Universais durante o logon, a partir de um Servidor de Catálogo Global. Isso acontece porque quando existe um único domínio, o Active Directory é capaz de detectar que não existem outros domínios e que não é necessária uma pesquisa no Catálogo Global (uma vez que a pesquisa pode ser feita no próprio DC que está autenticando o usuário)

## Replicação de informações entre os Servidor de Catálogo Global:

Conforme descrito anteriormente, o Catálogo Global contém informações completas sobre todos os objetos do seu domínio e informações parciais sobre todos os objetos dos demais domínios. Alterações são efetuadas diariamente em diversos objetos da rede. Por exemplo, usuários são renomeados, novos grupos criados, usuários são adicionados ou retirados de grupos e assim por diante.

Todas estas alterações tem que ser replicadas entre os vários Servidores de Catálogo Global de todos os domínios, para que estes estejam sempre atualizados. A estrutura de replicação do Catálogo Global é criada e gerenciada automaticamente por um processo do Active Directory, conhecido como Knowledge Consistency Checker (KCC). O KCC é responsável por determinar a melhor “topologia” de replicação do Global Catalog, de tal maneira que a rede não seja sobrecarregada com tráfego excessivo devido à replicação.

Algumas considerações devem ser feitas em relação a replicação dos grupos Universais. Os grupos Universais e informações sobre os seus membros estão contidas somente no Catálogo Global, conforme descrito anteriormente. Grupos Globais e Locais são também listados no Catálogo Global, porém no Catálogo Global não são armazenadas informações sobre os membros dos grupos Globais e Locais. Com isso o tamanho do Catálogo Global é reduzido, bem como o tráfego de replicação associado com a atualização do Catálogo Global. Para recursos e objetos que sofrerão alterações constantes, é aconselhável que você utilize grupos Globais e Locais para a definição de permissões, pois com isso você reduzirá o tráfego de replicação, comparativamente se você utilizasse grupos Universais. Como as informações sobre os membros dos grupos Universais são armazenadas no Catálogo Global, sempre que houver uma alteração na lista de membros de um grupo Universal, será necessário replicar esta informação para todos os Servidores de Catálogo Global de todos os domínios. Isso justifica a recomendação feita anteriormente, de somente adicionar grupos como membros de grupos Universais e não usuários.

Além da replicação do Catálogo Global também temos a replicação do Active Directory, onde alterações feitas em um DC, devem ser repassadas para todos os demais DCs do domínio. Porém antes de tratar sobre Replicação do Active Directory, você deve entender o conceito de Site. Este será o assunto do próximo item.

Vamos ver esta questão da replicação com mais detalhes.

## Sites, replicação do Active Directory e estrutura física da rede.

### Introdução e definição de sites.

Florestas, árvores, domínios e unidades organizacionais representam a divisão lógica do Active Directory, normalmente definida com base em critérios administrativos, ou seja, visando facilitar a administração dos recursos e usuários da rede. O Active Directory tem também um elemento conhecido como site, o qual é utilizado para representar a divisão física da rede e é muito importante para a implementação de um sistema de replicação otimizado das informações do Active Directory entre os diversos DCs de um domínio.

Um site no Active Directory é utilizado para representar a estrutura física da rede da empresa. As informações sobre a topologia da rede, contidas nos objetos site e link entre sites, são utilizadas pelo Active Directory para a criação de configurações de replicação otimizadas, sempre procurando reduzir o máximo possível o tráfego através dos links de WAN.

Um site normalmente é definido com uma ou mais redes conectadas por um caminho de alta velocidade. O termo alta velocidade é um pouco vago. Na prática, um site está intimamente ligado a uma localização física, ou seja, uma ou mais redes locais no mesmo prédio ou em prédios de um Campus, interligadas através de um barramento de 10 MBps, 100 MBps (mais comum hoje em dia) ou de 1GBps (menos comum). Ou seja, um site é definido por um endereço IP e uma máscara de sub-rede, isto é: por uma rede local. No Capítulo 1 você aprendeu que uma rede é definida pelo número IP da rede (por exemplo 10.10.20.0) e por uma máscara de sub-rede (por exemplo 255.255.255.0). Um site é formado por um ou mais conjuntos de número de rede/máscara de sub-rede. Em outras palavras, um site é um conjunto de uma ou mais redes locais conectadas por um barramento de alta velocidade.

### Para que o Active Directory utiliza sites:

A utilização de sites e links entre sites facilita a implementação de várias atividades no Active Directory, dentre as quais destaco as listadas a seguir:

- ♦ **Replicação:** Esta sem dúvida é a principal utilização dos sites. O Active Directory procura equilibrar a necessidade de manter os dados atualizados em todos os DCs, com a necessidade de otimizar o volume de tráfego gerado devido a replicação. A replicação entre os DCs de um mesmo site ocorre mais freqüentemente do que a replicação entre DCs de sites diferentes. Isso faz sentido, pois os DCs de um mesmo site estão dentro da mesma rede local, conectados por um barramento de alta velocidade. Por isso é possível fazer a replicação mais freqüentemente. Já os DCs de sites diferentes estão conectados através de links de WAN de baixa velocidade (quando comparada com a velocidade do barramento de uma rede local), por isso a replicação deve ocorrer em intervalos maiores, para evitar um excesso de tráfego e um sobrecarga nos links de WAN da rede. Você também pode atribuir diferentes “custos” para os links entre sites, de tal maneira que a replicação através de links de baixa velocidade, ocorre em intervalos maiores do que a replicação através de links de maior velocidade. Todas estas possibilidades de configuração são sempre pensando na otimização do tráfego de WAN gerado pela replicação.

- ◆ **Autenticação:** A informação sobre sites auxilia o Active Directory a fazer a autenticação dos usuários de uma maneira mais rápida e eficiente. Quando o usuário faz o logon no domínio, o Active Directory primeiro tenta localizar um DC dentro do site definido para a rede do usuário. Com isso, se houver um DC no site do usuário, na maioria das vezes, este DC será utilizado para autenticar o logon do usuário no domínio, evitando que tráfego de autenticação seja gerado, desnecessariamente, no link de WAN.

## Definição de sites utilizando sub-redes:

Conforme descrito anteriormente, para o Active Directory, um site é um grupo de computadores “bem conectados”, onde bem conectado significa conectado através de um barramento de alta velocidade, tal como uma Rede Local com barramento de 100 Mbps. Normalmente um site é associado a uma rede local de um escritório da empresa. Um site é definido por uma ou mais sub-redes. Uma rede é definida pelo endereço de rede mais a máscara de sub-rede, conforme descrito no Capítulo 1. A figura 2.15 ilustra a utilização de uma sub-rede para a definição de um site:

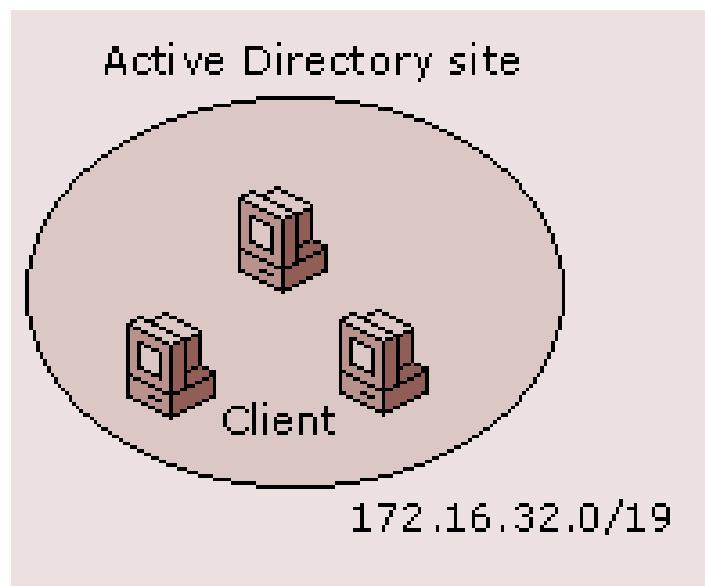


Figura 2.15 Definição de um site.

No Active Directory você pode criar objetos do tipo sub-rede e do tipo site, utilizando o console Active Directory Sites and Services. Após criar objetos do tipo sub-rede, você cria um objeto do tipo site, associando uma ou mais sub-redes com o objeto site que está sendo criado.

---

**NOTA:** 172.16.32.0/19, significa 19 bits para a máscara de sub-rede, é o mesmo que escrever 172.16.32.0/255.255.224.0

---

## A relação entre sites e domínios:

Conforme descrevi anteriormente, o domínio representa uma das divisões lógicas da rede e do Active Directory, já sites representam a estrutura física da rede. Com isso é possível ter computadores de diferentes domínios dentro do mesmo site, ou diferentes sites dentro do mesmo domínio e outras combinações possíveis.

Repetindo para fixar bem: “No Active Directory, sites estão relacionados com a estrutura física da rede, já domínios estão relacionados com a estrutura lógica da rede”. Esta separação traz alguns benefícios, dentre os quais destaco os indicados a seguir:

- ◆ É possível manter o design da estrutura lógica, independente da estrutura física. Ou seja, alterações em uma das estruturas não irão implicar, necessariamente, alterações na outra estrutura. Com isso você pode ter computadores de mais de um domínio no mesmo site ou mais de um site no mesmo domínio e assim por diante.
- ◆ A nomeação dos domínios é absolutamente independente da estrutura física/geográfica da rede, o que facilita alterações na estrutura física, sem que isso implique em um reestruturação lógica de toda a rede.
- ◆ Você pode instalar DCs de múltiplos domínios no mesmo site ou você pode colocar DCs do mesmo domínio em diferentes sites ou uma combinação destas duas configurações, conforme ilustrado na Figura 2.16:

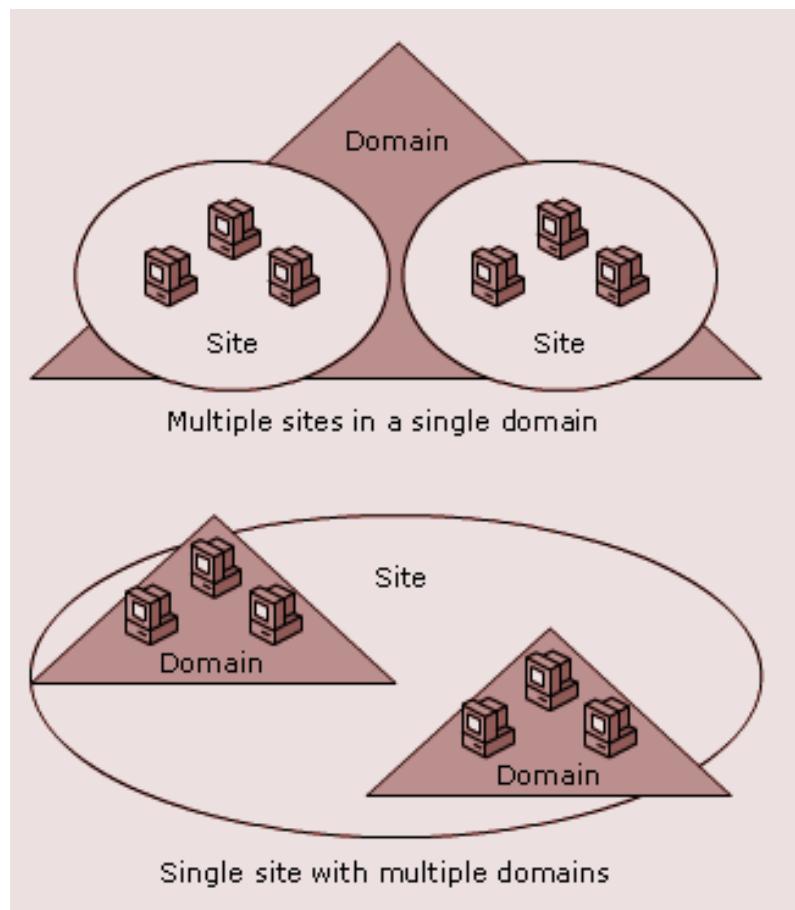


Figura 2.16 Flexibilidade na definição de sites e domínios.

## Replicação no Active Directory:

A base de dados do Active Directory, com informações completas sobre todos os objetos do Active Directory é armazenada nos DCs do domínio. Alterações podem ser efetuadas em qualquer DC. Estas alterações devem ser replicadas para todos os demais DCs do domínio, de tal maneira que todos os DCs estejam sincronizados e com uma cópia idêntica da base de dados do Active Directory. Este processo ocorre o tempo todo, pois alterações no Active Directory são feitas diariamente. Claro que existe um tempo entre o momento em que uma alteração é feita em um DC, até que esta alteração tenha sido replicada para todos os demais DCs do domínio. A replicação é um processo contínuo.

O Active Directory procura determinar, automaticamente, qual a melhor configuração de replicação, procurando obter o menor tempo possível para atualização dos DCs do domínio, mas平衡ando com o volume de tráfego gerado na rede, de tal maneira que o tráfego gerado pela replicação não venha a sobrecarregar os links de WAN.

As configurações de replicação do Active Directory são feitas, automaticamente, pelo processo conhecido como Knowledge Consistency Checker (KCC), que é um processo que roda em todos os DCs. O KCC automaticamente identifica as configurações de replicação mais eficientes, com base nas configurações de sites do Active Directory (estrutura física da rede). Por exemplo, a replicação entre DCs dentro do mesmo site são feitas mais frequentemente do que entre DCs de sites diferentes. O KCC regularmente recalcula a topologia de replicação para ajustar o processo para quaisquer alterações que tenham ocorrido na estrutura física da rede, como a criação de novos sites ou a inserção de novas sub-redes em um site existente.

## Replicação dentro do mesmo site – Intrasite Replication

Conforme já descrito anteriormente, o KCC trata a replicação dentro do mesmo site, de uma maneira diferente do que a replicação entre sites. Isso devida a diferença da velocidade de conexão dentro do mesmo site e entre sites (normalmente conectados através de links de WAN).

O KCC define a topologia de replicação dentro de um mesmo site, no formato de um anel bi-direcional. O KCC forma um anel bi-direcional entre os vários DCs dentro de um mesmo site. A replicação intrasite é otimizada para velocidade e as atualizações feitas em um DC do site são automaticamente repassadas para os demais DCs, com base em um mecanismo de notificação. As informações de replicação dentro do site não são compactadas, diferentemente do que acontece com a replicação entre sites diferentes, onde toda a informação de replicação é compactada antes de ser enviada através do link de WAN.

### Como o KCC configura a replicação intrasite:

O KCC, rodando em cada DC do site, foi projetado para criar uma topologia de replicação intrasite o mais eficiente possível, baseada em um anel bidirecional. Para criar o anel bi-direcional, o KCC tenta criar pelo menos duas conexões de replicação entre cada DC (para tolerância a falhas, caso uma das conexões esteja indisponível). O KCC também procura evitar que haja mais do que três DCs no caminho entre dois servidores quaisquer (tecnicamente dizemos que o KCC procura evitar que haja mais do que três “hops” entre dois DCs quaisquer). Para evitar mais do que três hops, a topologia de replicação pode incluir conexões do tipo atalho entre dois DCs. O KCC fica atualizando a topologia de replicação regularmente, buscando sempre a melhor eficiência e a menor latência (menor intervalo de atualização entre os DCs).

### Determinando quando a replicação intrasite ocorre:

Alterações feitas no Active Directory tem um impacto direto nos usuários localizados no próprio site, por isso a replicação intrasite é otimizada para a velocidade (menor tempo de latência). Por exemplo, quando você altera a senha de um usuário em um DC do site, é importante que esta alteração seja replicada, rapidamente, para todos os demais DCs do site. A replicação entre os DCs de um site ocorre automaticamente, com base em um mecanismo de notificação. A replicação Intrasite inicia quando uma alteração é feita em um objeto do Active Directory em um dos DCs do site. Por padrão, o DC onde foi feita a alteração aguarda 15 segundos e então envia uma notificação de atualização para o seu parceiro de replicação mais próximo (o DC que está mais próximo dele, no anel bi-direcional criado pelo KCC). Se o DC onde foi feita a alteração tiver mais do que um parceiro de replicação, as notificações subsequentes serão enviadas, por padrão, em intervalos de 3 segundos. Após receber uma notificação de alteração, um parceiro de replicação envia uma requisição de atualização do Active Directory para o DC onde foi feita a alteração. O DC onde foi feita a alteração responde à requisição feita pelo seu parceiro de replicação, enviando os dados sobre a alteração. O intervalo de 3 segundos entre o envio das notificações de alteração é importante para evitar que um mesmo DCs receba múltiplas notificações de alteração, simultaneamente.

Algumas alterações são conhecidas como atualizações críticas. Para as atualizações críticas não é observado o intervalo de 15 segundos antes que o DC onde houve a alteração envie uma notificação de alteração. Alterações como bloqueio

de contas, alterações nas políticas de bloqueio de contas, alterações nas políticas de senha do domínio e alterações de senha são consideradas atualizações críticas e devem ser replicadas imediatamente.

## Replicação entre sites:

O Active Directory trata a replicação entre sites (intersites) de maneira da replicação dentro do mesmo site (intrasite), pois a velocidade de conexão entre sites geralmente é bem menor do que dentro do mesmo site.

O KCC cria a topologia de replicação intersite sempre procurando otimizar a utilização dos links de WAN. A replicação intersite é configurada com base em um agendamento definido pelo KCC. As informações de replicação são compactadas antes de serem enviadas através dos links de WAN, para reduzir o tráfego nos links de WAN.

### Como a topologia de replicação intersite é criada pelo KCC:

A topologia de replicação intersite é criada pelo KCC, com base nas informações sobre sites e links entre sites que o Administrador cria. Em cada site um DC é o responsável pela definição da topologia de replicação intersite. Este DC é conhecido como “Intersite Topology Generator”. O tempo de replicação intersite pode ser controlado com base nas informações fornecidas quando o Administrador cria os objetos de links entre sites, utilizando o console Active Directory Sites and Services.

### Quando a replicação intersite ocorre:

Para reduzir a utilização dos links de WAN, a replicação intersite ocorre de acordo com um agendamento prévio e não instantaneamente (ou com base em notificações de alteração) como no caso da replicação intrasite. Por padrão, a replicação intersite ocorre, em cada link, a cada 3 horas (180 minutos). O Administrador pode alterar este agendamento para adatar a replicação a velocidade dos links de WAN da sua rede. O Administrador também pode definir em que horários do dia os links entre sites estarão disponíveis para que a replicação aconteça. Por exemplo, para escritórios conectados por links de WAN de baixa velocidade, como por exemplo 64 Kbps, você pode ajustar o link de replicação para estar disponível apenas à noite, após o expediente. Por padrão um link está configurado para estar disponível 24 horas por dia, 7 dias por semana.

## O Schema do Active Directory

A definição de todos os objetos do Active Directory e demais informações está contida no que é conhecido como Schema do Active Directory. O Active Directory utiliza um modelo de banco de dados hierárquico, diferente do Modelo Relacional de Dados com o qual estamos mais habituados. Mas, me permitam esta analogia, o Schema é como se fosse (na verdade é) a definição da estrutura do banco de dados do Active Directory. Por exemplo, a definição do objeto usuário, quais atributos tem este objeto, o tipo de cada atributo e demais informações sobre o objeto usuário, estão todas contidas no Schema. A definição de cada objeto, de cada atributo, está contida no Schema.

O Schema contém a definição para todos os objetos do Active Directory. Quando você cria um novo objeto, as informações fornecidas são validadas com base nas definições contidas no Schema, antes que o objeto seja salvo na base de dados do Active Directory. Por exemplo, se você preencheu um atributo do tipo número, com valores de texto, o Active Directory não irá gravar o objeto no Active Directory e uma mensagem de erro será exibida.

O Schema é feito de objetos, classes e atributos. O Schema definido por padrão com o Active Directory, contém um número de classes e atributos, os quais atendem as necessidades da maioria das empresas. Porém o Schema pode ser modificado, o Administrador pode modificar as classes existentes ou adicionar novas classes ou atributos. Qualquer alteração no Schema deve ser cuidadosamente planejada, pois alterações feitas no Schema afetam toda a árvore de

domínios. Todos os domínios de uma árvore tem que utilizar o mesmo Schema, ou seja, não podem ser utilizados diferentes esquemas para os diferentes domínios de uma árvore de domínios.

## Como os objetos do Active Directory são definidos no Schema:

No Schema, uma classe de objetos representa uma categoria de objetos do Active Directory, como por exemplo contas de usuários, contas de computadores, impressoras ou pastas compartilhadas publicadas no Active Directory e assim por diante. Na definição de cada classe de objetos do Active Directory, está contida uma lista de atributos que podem ser utilizadas para descrever um objeto da referida classe. Por exemplo, um objeto usuário contém atributos de nome, senha, validade da conta, descrição, etc. Quando um novo usuário é criado no Active Directory, o usuário torna-se uma nova instância da classe User do Schema e as informações que você digita sobre o usuário, tornam-se instâncias dos atributos definidos na classe user.

## Como o Schema é armazenado no Active Directory:

Cada floresta pode conter um único Schema, ou seja, o Schema tem que ser único ao longo de todos os domínios de uma floresta. O Schema é armazenado nas partições de schema do Active Directory. A partição de schema do Active Directory, bem como a partição de definição do Active Directory, são replicadas para todos os DCs da floresta. Porém um único DC controla a estrutura do Schema, DC este conhecido como Schema Master. Ou seja, somente no DC configurado como Schema Master é que o Administrador poderá fazer alterações no Schema.

## Cache do Schema.

Cada DC mantém uma cópia do Schema na memória do servidor (bem como uma cópia em disco), para melhorar a performance das operações relacionadas ao Schema, tais como validação de novos objetos. A versão armazenada no Cache do servidor é automaticamente atualizada (em intervalos de tempos definidos) cada vez que o Schema é atualizado (o que não ocorre com freqüência, na verdade é muito raro fazer alterações no Schema).

## Níveis de funcionalidade de um domínio.

É comum a rede da empresa “conviver” com diferentes versões do Windows. Isso aconteceu na migração do NT Server 4.0 para o Windows 2000 Server, onde durante um bom tempo ainda existiam (na prática sabemos que ainda existem) servidores com o NT Server 4.0 em utilização na rede.

O Windows Server 2003 (a exemplo do que acontecia com o Windows 2000 Server), tem diferentes níveis de funcionalidade, com base nos tipos de DCs instalados na rede. Neste tópico vou descrever os níveis de funcionalidade disponíveis e as diferentes funcionalidades que estão disponíveis em cada nível de funcionalidade.

Com o Windows Server 2003 foi introduzido o nível de funcionalidade da floresta, o que não existia com o Windows 2000 Server.

O nível de funcionalidade do domínio determina quais características estão ou não disponíveis.

Existem quatro níveis de funcionalidade no Windows Server 2003: Windows 2000 mixed, Windows 2000 native, Windows Server 2003 interim, and Windows Server 2003.

Por padrão é selecionado o nível de funcionalidade Windows 2000 mixed. Muitos dos recursos mais avançados, tais como grupos Universais, somente estão disponíveis nos demais níveis de funcionalidade: Windows 2000 native, Windows Server 2003 interim ou Windows Server 2003.

O nível de funcionalidade da floresta é uma novidade do Windows Server 2003. Existem três níveis de funcionalidade da floresta disponíveis: Windows 2000, Windows Server 2003 interim, and Windows Server 2003. Por padrão é selecionado o nível Windows 2000. Muitas das novidades do Windows Server 2003 em relação ao Active Directory somente estão disponíveis nos níveis mais avançados: Windows Server 2003 interim ou Windows Server 2003.

Para que o nível de funcionalidade da floresta seja configurado para Windows Server 2003, todos os DCs de todos os domínios devem estar com o Windows Server 2003 instalado. Somente neste nível é que estarão disponíveis todos os recursos do Active Directory, incluindo a maioria das novidades introduzidas com o Windows Server 2003.

O que define se é possível ou não utilizar um determinado nível de funcionalidade é a existência ou não de DCs com versões anteriores do Windows, tais como o Windows 2000 Server e o Windows NT Server 4.0.

A seguir descrevo quais as versões do Windows que podem ser utilizadas nos DCs, para cada um dos modos de funcionalidade de domínio:

- ◆ **Windows 2000 mixed:** Suporta DCs com o Windows NT Server 4.0, Windows 2000 Server ou Windows Server 2003. Neste nível de funcionalidade não é possível a utilização de grupos Universais.
- ◆ **Windows 2000 native:** Suporta DCs com o Windows 2000 Server ou com o Windows 2003 Server. Neste nível de funcionalidade são suportados grupos Universais.
- ◆ **Windows Server 2003 interim:** Suporta DCs com o NT Server 4.0 ou com o Windows Server 2003. Este nível de funcionalidade é utilizado quando você está em processo de migração de uma rede baseada no Windows NT Server 4.0 para o Windows Server 2003.
- ◆ **Windows Server 2003:** Somente DCs com o Windows Server 2003. Este é o nível onde estão disponíveis todos os recursos e novidades do Active Directory.

Muito bem, já vimos um bocado de teoria sobre o Active Directory. Nos próximos tópicos você aprenderá a instalar o Active Directory, transformando um Member Server em DC e também aprenderá sobre as modificações introduzidas pela instalação do Active Directory.

---

**NOTA:** Quando você altera de um modo de funcionalidade para o outro, não será mais possível criar DCs com versões não suportadas do Windows. Por exemplo, quando você passa do modo Windows 2000 mixed para o modo Windows 2000 Native, não será mais possível inserir DCs com o NT Server 4.0 e nem será voltar para o nível de funcionalidade anterior.

---

## Fundamentos em: Preparação para a instalação do Active Directory.

Para que o Active Directory possa ser instalado, transformando um Member Server em Controlador de Domínio, dois pré-requisitos básicos devem ser atendidos:

- ◆ Um volume formatado com NTFS
- ◆ Um servidor DNS padrão Windows 2000 Server ou Superior

O volume NTFS é necessário para gravar os arquivos da base de dados do Active Directory. Se não houver um volume com NTFS, o assistente de instalação do Active Directory será cancelado. Coloco esta recomendação apenas para deixar registrada esta exigência, mas é muito pouco provável que alguém utilize FAT ou FAT 32 em partições de um servidor. No Capítulo 5 falarei sobre as diferenças entre os sistemas de arquivo FAT/FAT 32 e NTFS. Você verá que, principalmente, em relação a segurança, a única escolha recomendada é NTFS.

## **Uma visão geral do DNS e de espaço de nomes de um domínio.**

O DNS é o serviço de resolução de nomes no qual se baseia o Active Directory. Por exemplo, quando o usuário faz o logon em uma estação de trabalho da rede, é o DNS que é consultado para informar o número IP de um controlador de domínio, para que possa ser feita a validação do nome e senha fornecidos pelo usuário.

Todo o computador que utiliza o protocolo TCP-IP, é identificado por um número e por um nome. O número é conhecido como Número IP ou Endereço IP, o qual é formado por quatro números separados por um ponto.

Exemplo de um número IP:

**10.200.300.1**

Não podem existir dois computadores com o mesmo Número IP, pois caso isso aconteça, haverá um conflito de Endereço IP e um dos computadores deixará de se comunicar com a rede.

Além de um número IP, os computadores possuem um nome, conhecido como “host name”, ou “nome de host”. Por exemplo, o computador com o IP 10.200.300.1, pode ter o nome contab-01. Além disso uma rede baseada no TCP/IP é dividida em domínios DNS, como por exemplo: abc.com, vendas.abc.com, marketing.abc.com.

Porém a utilização de um único nome para cada computador, torna difícil a localização dos milhões de computadores disponíveis na Internet, ou até mesmo dos milhares de computadores disponíveis em uma rede de uma grande empresa. Para que tenhamos um sistema de nomeação mais organizado e de fácil localização, foram criados os domínios, onde além do nome de host, o nome do domínio também faz parte do nome completo que identifica o computador.

Alguns exemplos de nomes completos, também conhecidos como Full Qualified Domain Name (FQDN) – Nomes de Domínios completamente qualificados:

- ◆ [www.juliobattisti.com.br](http://www.juliobattisti.com.br)
- ◆ [www.certificacoes.com.br](http://www.certificacoes.com.br)
- ◆ [www.axcel.com.br](http://www.axcel.com.br)
- ◆ [www.ufsm.br](http://www.ufsm.br)
- ◆ [www.altavista.digital.com](http://www.altavista.digital.com)
- ◆ [www.microsoft.com](http://www.microsoft.com)
- ◆ [server1.microsoft.com](http://server1.microsoft.com)
- ◆ [ftp.microsoft.com](http://ftp.microsoft.com)
- ◆ [contab-01.abc.com](http://contab-01.abc.com)
- ◆ [marketing-02.marketing.abc.com](http://marketing-02.marketing.abc.com)

A parte mais à esquerda do nome (o nome que aparece antes do primeiro ponto) é o host name, a parte restante é o Domínio. Embora cada computador de uma rede possua um nome, de tal forma que seja mais fácil identificá-los, toda a comunicação do protocolo TCP/IP é feita através do Endereço IP.

Por exemplo, quando você acessa o site da Microsoft ([www.microsoft.com](http://www.microsoft.com)), na verdade toda a comunicação do protocolo TCP-IP, está sendo feita através do endereço IP e não do nome [www.microsoft.com](http://www.microsoft.com).

“Mas que mágica é essa ? Eu digito o nome – [www.microsoft.com](http://www.microsoft.com) , porém a comunicação é feita através do endereço IP. Quem é que faz essa mágica de “descobrir” qual o endereço IP correspondente ao nome [www.microsoft.com](http://www.microsoft.com)?”

---

**NOTA: No Capítulo 16, do livro Windows Server 2003 – Curso Completo, 1568 páginas, apresento uma discussão completa sobre o DNS.**

---

Não é mágica nenhuma, este trabalho de descobrir o endereço IP associado com um determinado nome, é feito por um serviço denominado DNS – Domain Name System, ou traduzindo – Sistema de Nomeação de Domínios. O DNS é amplamente utilizado na Internet para que possa ser descoberto o endereço IP associado com um determinado nome. Quando você está utilizando o Navegador (Browser) e digita na linha de endereços: [www.juliobattisti.com.br](http://www.juliobattisti.com.br), quem descobre o endereço IP associado com esse nome é o DNS. Isso faz com que a comunicação seja possível.

Existem na Internet diversos Servidores DNS, os quais fazem este trabalho de tradução. Caso a rede da sua empresa esteja ligada a Internet, ele necessita de um servidor DNS, ou precisa ter acesso ao servidor DNS do Provedor de acesso a Internet, pois sem DNS, a comunicação fica praticamente impossível, pois ao invés do nome, você teria que utilizar os endereços IP, o que é inviável na prática. Já imaginou tendo que decorar milhares de endereços IP, uma para cada site que você tenta acessar na Internet?

O Windows 2000 Server e agora o Windows Server 2003, oferecem um servidor DNS que pode ser facilmente instalado e configurado, de tal forma que um servidor com o Windows Server 2003 possa atuar como um Servidor DNS interno da empresa.

Você já deve ter notado que existe uma certa hierarquia na formação dos nomes. Por exemplo, empresas comerciais normalmente possuem nomes na forma [www.nome-da-empresa.com](http://www.nome-da-empresa.com). Ou se for uma empresa comercial do Brasil, o nome fica [www.nome-da-empresa.com.br](http://www.nome-da-empresa.com.br). Isso acontece porque o domínio .com foi reservado para empresas comerciais. Já órgãos do governo, normalmente possuem nomes da seguinte forma: [www.nome-do-orgao.gov](http://www.nome-do-orgao.gov), ou no caso do Brasil, [www.nome-do-orgao.gov.br](http://www.nome-do-orgao.gov.br). Isso acontece porque o domínio .gov foi reservado para Órgãos governamentais.

Esses domínios mais conhecidos são chamados de “Top-level-domains”. Os mais conhecidos são os seguintes:

**Tabela 2.1 Top-level-domains**

| Top-level-domain | Descrição                        |
|------------------|----------------------------------|
| com              | Organizações comerciais          |
| gov              | Organizações governamentais      |
| edu              | Instituições educacionais        |
| org              | Organizações não comerciais      |
| net              | Diversos                         |
| br               | Código de país para o Brasil     |
| au               | Código de país para a Austrália. |

Existem organismos internacionais que administram o registro de nomes. Por exemplo, se você possui uma empresa chamada abc123 e deseja criar um site chamado [www.abc123.com.br](http://www.abc123.com.br), primeiro de tudo você precisa registrar este nome de domínio junto aos órgãos responsáveis. No caso do Brasil, você pode registrar nomes DNS no seguinte endereço: [www регистрация.рф](http://www регистрация.рф).

Caso o nome que você está tentando registrar já tenha sido registrado, você terá que escolher outro nome. Quando a Internet começou a crescer, existiram casos em que alguns “espertinhos”, registraram nomes de empresas conhecidas. Com o crescimento da Internet, quando a empresa tentou registrar o nome DNS junto às entidades competentes, o nome já estava registrado. Em alguns casos, os “espertinhos” se deram bem, e ganharam um bom dinheiro para liberar o nome registrado, em outros casos a empresa entrou na justiça e recuperou o direito sobre o nome DNS.

Mas os nomes DNS formam uma hierarquia. Por exemplo, quando a Microsoft resolveu entrar na Internet, ele registrou o domínio: microsoft.com. Dizemos que microsoft.com é um subdomínio do domínio com. Dentro do domínio microsoft.com, poderiam ser criados outros subdomínios, conforme a necessidade. Por exemplo poderíamos criar subdomínios para as seções de vendas, marketing e suporte. Aí teríamos os seguintes subdomínios:

- ◆ vendas.microsoft.com
- ◆ marketing.microsoft.com
- ◆ suporte.microsoft.com

Dentro de departamento de vendas, poderíamos ter diversos computadores, alguns atuando como servidores e outros como Clientes. Cada um destes computadores precisa ter um host name e um endereço IP. Poderíamos ter os seguintes exemplos:

- ◆ server1.vendas.microsoft.com
- ◆ server2.vendas.microsoft.com
- ◆ cliente1.vendas.microsoft.com
- ◆ cliente2.vendas.microsoft.com
- ◆ ftp.vendas.microsoft.com

Assim como a Microsoft pode ter os seus subdomínios, qualquer empresa pode fazer o mesmo, dependendo de suas necessidades e de sua estrutura interna. Observe nos exemplos anteriores, que o host name, conforme citado anteriormente, é a parte mais a esquerda do nome, sendo a parte mais a direita, o Top-level-domain.

Uma pergunta que você pode estar se fazendo é porque a grande maioria dos sites começa com www. Este é um padrão que foi adotado no início da era de Interface Gráfica para a Internet e continuou sendo utilizado. WWW significa World Wide Web – Teia mundial. Por isso que muitas vezes a Internet é chamada simplesmente de Web. Pelo fato de ter se tornado um padrão, é comum que um usuário ao procurar pelo site de uma empresa, digite [www.nome-da-empresa.com](http://www.nome-da-empresa.com) ou [www.nome-da-empresa.com.br](http://www.nome-da-empresa.com.br) no caso do Brasil.

Na Figura 2.17, é exibida uma representação da hierarquia de nomes do DNS.

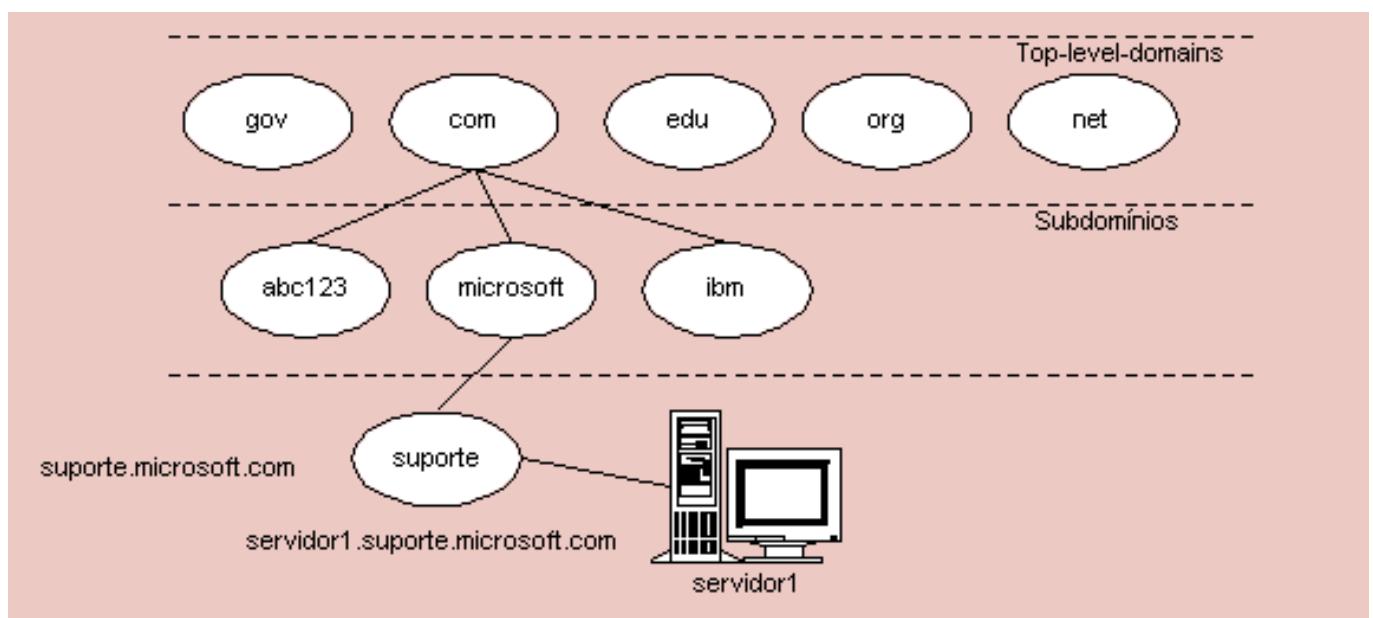


Figura 2.17 Estrutura Hierárquica do DNS.

Apresentei esta visão geral do DNS, porque é de fundamental importância entender os princípios básicos do DNS. Essas noções sobre DNS serão necessárias para o entendimento da nomeação de domínios e do espaço de nomes de uma árvore de domínios do Active Directory. Você verá, no exemplo prático, que ao criar um domínio, durante a instalação do Active Directory, você deverá fornecer o nome DNS do domínio. Por exemplo, ao criar o domínio root da empresa ABC Ltda, você, provavelmente iria utilizar um nome como abc.com ou abc.com.br.

De uma forma resumida, o DNS é um sistema hierárquico de nomeação. O DNS mantém um banco de dados com a associação entre nomes FQDN (Nomes de domínio completamente qualificados) e os respectivos endereços IP. De tal forma que é muito mais fácil lembrarmos de um nome como www.microsoft.com, do que termos que decorar um endereço IP para acessar o site da Microsoft. Quem faz esse meio-campo é o DNS, que uma vez digitado um endereço do tipo www.microsoft.com, o DNS consegue identificar o endereço IP associado e estabelecer a comunicação.

O DNS é também um pré-requisito para que você possa instalar o Active Directory em um servidor, promovendo-o de member server para controlador de domínio. Não é obrigatório que o DNS esteja instalado no mesmo servidor onde o Active Directory está sendo instalado, pode ser em um outro servidor da rede.

<body text>Importante: Nem mesmo precisa ser um servidor DNS baseado o Windows 2000 Server ou Windows Server 2003, basta que seja uma versão do DNS BIND 8.1.2 ou superior. Por exemplo, se você tiver um servidor UNIX, com uma versão do DNS BIND 8.1.2 ou superior, este servidor poderá ser utilizado durante a instalação do Active Directory.

Você pode ter o servidor DNS já previamente configurado ou pode fazer com que o assistente de instalação do Active Directory instale e configure o DNS automaticamente. No caso de estar criando um novo domínio, você pode deixar tudo por conta do assistente de instalação do Active Directory. Já no caso de estar instalando um DC adicional, em um domínio existente, você pode deixar que o assistente de instalação do Active Directory, tente acessar um servidor DNS já existente.

Em seguida farei alguns exemplos práticos de utilização do assistente de instalação do Active Directory.

## Instalação do Active Directory – Criação de um Novo Domínio

Neste tópico vou mostrar como instalar o Active Directory em um servidor com o Windows Server 2003, servidor este que será o primeiro DC do domínio. Na prática ao instalar o primeiro DC você está, efetivamente, criando o domínio. Existem outras situações em que você pode usar o assistente de instalação do Active Directory:

- ◆ Para criar um novo DC em um domínio já existente.
- ◆ Para criar um novo DC em um novo domínio de uma árvore já existente.
- ◆ Para rebaixar um DC de volta a member server.

Neste capítulo você aprenderá a executar algumas destas operações.

No Windows Server 2003 existem duas maneiras de iniciar o assistente de instalação do Active Directory:

- ◆ Executando o comando depromo
- ◆ Usando a ferramenta Gerenciar o servidor (Iniciar -> Todos os programas -> Ferramentas administrativas -> Gerenciar o servidor).

Ao executar o comando depromo, o assistente do Active Directory é iniciado automaticamente. Ao abrir a ferramenta Gerenciar o servidor, você deve clicar na opção Adicionar ou remover função, conforme destacado na Figura 2.18. Nos

exemplos práticos, vou deixar que o assistente de instalação do Active Directory faça a instalação e configuração do DNS. No Capítulo 16 do livro Windows Server 2003 – Curso Completo, 1568 páginas o DNS será apresentado em detalhes.

Exemplo 01: Instalação do Active Directory no primeiro DC – criação de um novo domínio – usando o comando dcpromo: Neste exemplo você acompanhará os passos para criação de um novo domínio. Vou instalar o Active Directory em um member server (srv70-290) para transformá-lo no primeiro DC do domínio abc.com, que será criado com a instalação deste primeiro DC.

Para criar o domínio abc.com, siga os passos indicados a seguir:

1. Faça o logon com a conta Administrador ou com uma conta com permissão de administrador.

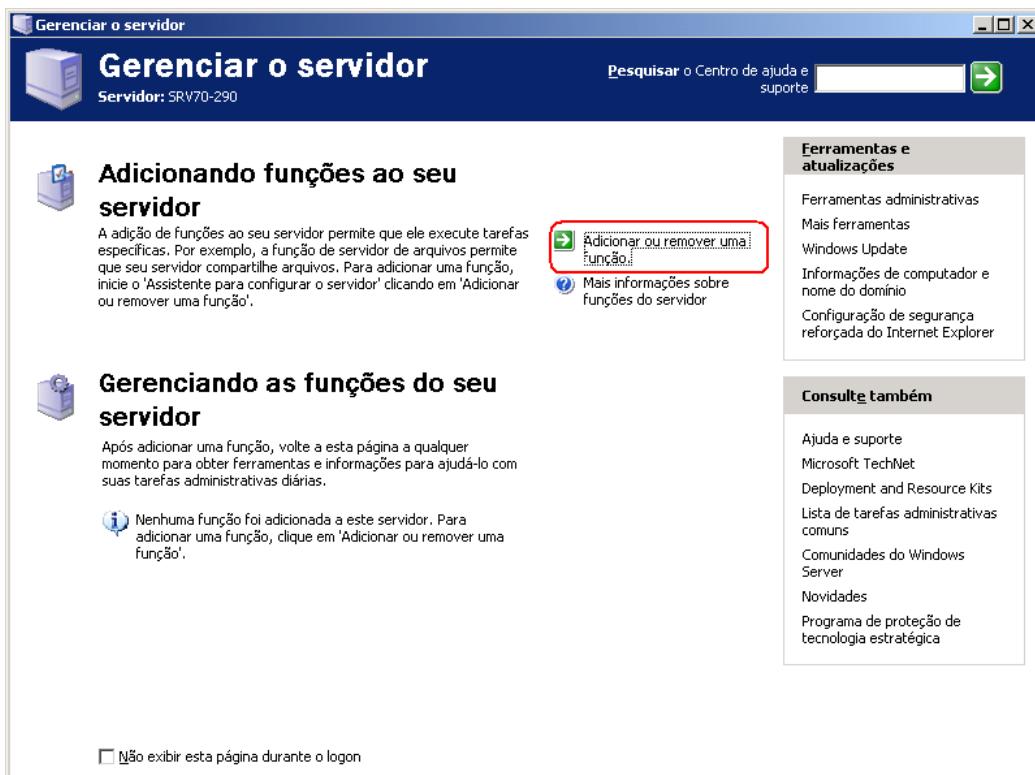


Figura 2.18 A ferramenta Gerenciar o servidor.

2. Selecione o comando Iniciar -> Executar.
3. Na linha Abrir digite dcpromo, conforme indicado na Figura 2.19 e clique em OK.

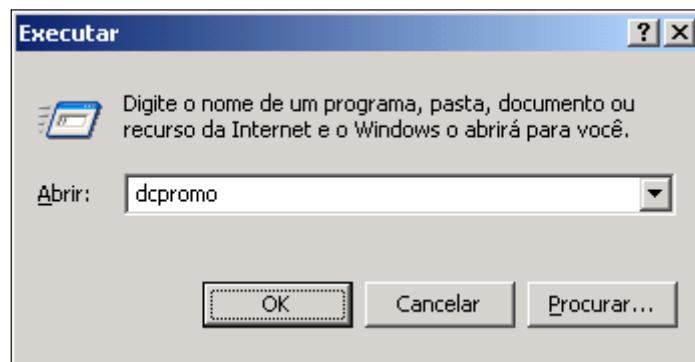


Figura 2.19 O comando dcpromo.

4. O assistente de instalação do Active Directory será aberto. A primeira tela é apenas informativa, descrevendo a função do assistente e fornecendo um link para a documentação sobre Active Directory, na Ajuda do Windows Server 2003.
5. Clique em Avançar, para seguir para a próxima etapa do assistente.
6. Na terceira etapa você deve informar se esta sendo instalado um DC para um novo domínio, ou seja, o primeiro DC e a criação do domínio, ou se você está instalando um DC adicional para um domínio já existente. Para o nosso exemplo selecione a opção Controlador de domínio para um novo domínio, conforme indicado na Figura 2.20:

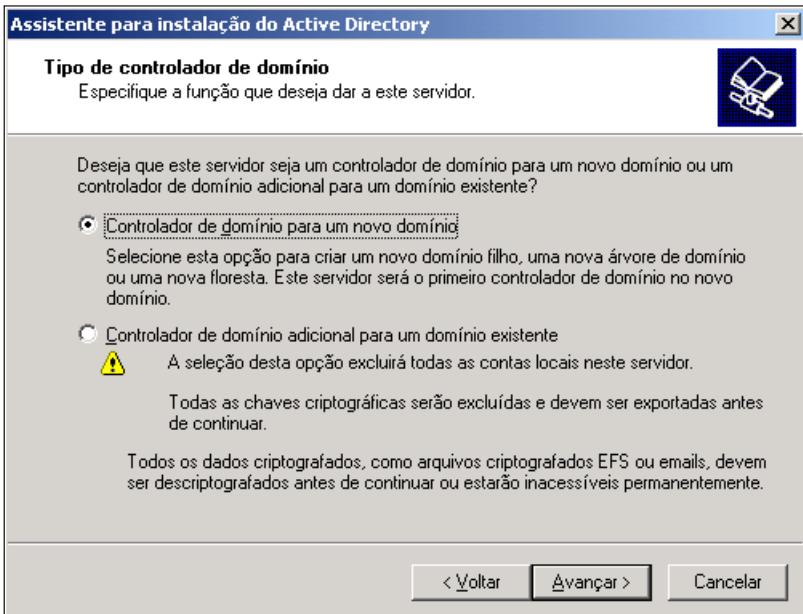


Figura 2.20 Criando um novo domínio.

7. Clique em Avançar, para seguir para a próxima etapa do assistente.

Na quarta etapa são disponibilizadas três diferentes opções, conforme indicado na figura a seguir:

- ◆ **Domínio em uma nova floresta:** Esta opção é utilizada quando você está criando o primeiro domínio da empresa. Ou seja, ainda não existe uma árvore de domínios e você está criando o primeiro domínio, também conhecido como domínio root.
  - ◆ **Domínio filho em uma árvore de domínio existente:** Selecione esta opção se você estiver criando um novo domínio em uma árvore de domínios já existente. Por exemplo, se você é o administrador de uma unidade regional da empresa e está criando um domínio para a sua unidade, domínio esse que fará parte da árvore de domínios da empresa.
  - ◆ **Árvore de domínio em uma floresta existente:** Selecione esta opção se você está criando uma nova árvore de domínios, a qual será integrada a uma ou mais árvores já existentes, para formar uma floresta.
8. Para o nosso exemplo, vamos criar o primeiro domínio de uma árvore de domínios. Para isso certifique-se de que a opção “Domínio em uma nova floresta” esteja selecionada, conforme indicado na Figura 2.21:

**IMPORTANTE:** Na segunda etapa é informado que clientes rodando o Windows 95 ou o Windows NT 4.0, com Service Pack 3.0 ou inferior, não serão capazes de fazer parte de um domínio baseado no Windows Server 2003. Esta etapa também é apenas informativa.

**NOTA:** Se o Terminal Server estiver instalado no servidor que está sendo promovido a DC, você receberá uma mensagem de alerta. Esta mensagem informa que a partir da instalação do Active Directory, somente contas com permissão de Administrador do domínio, poderão fazer o logon remotamente usando o terminal server. Para dar permissões de logon, via terminal server, para outras contas, você terá que alterar as políticas de segurança local do servidor, conforme mostrarei no Capítulo 4, no item sobre direitos de contas de usuário. Para continuar com a instalação do Active Directory, clique em OK para fechar a mensagem de aviso. 5. Clique em Avançar, para seguir para a próxima etapa do assistente.

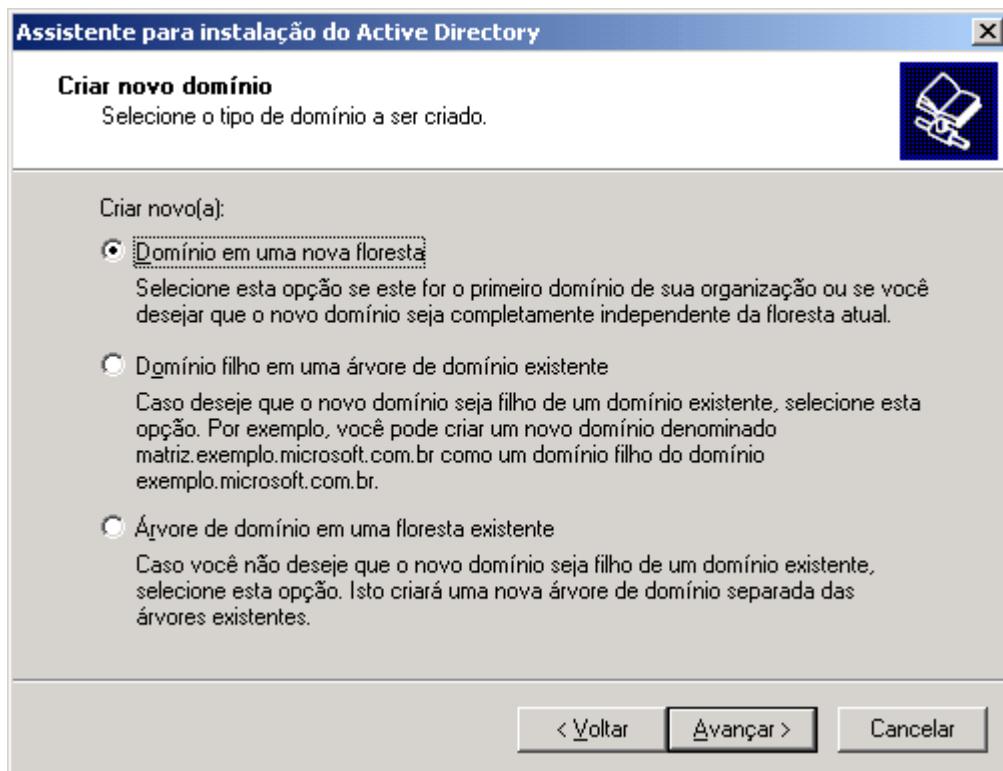


Figura 2.21 Criando o primeiro domínio de uma nova árvore de domínios.

9. Clique em Avançar, para seguir para a próxima etapa do assistente.
11. Nesta etapa você deve informar o nome DNS do domínio que está sendo criado. No campo “Nome DNS completo para o novo domínio”, digita abc.com e clique em Avançar para seguir para a próxima etapa do assistente.

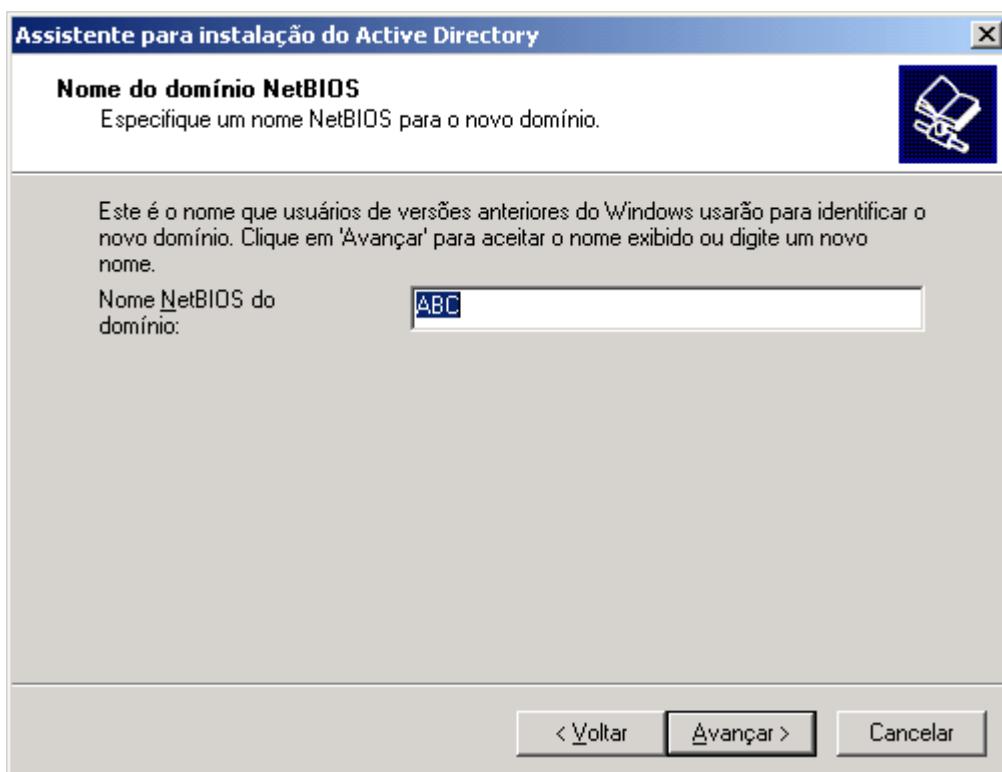
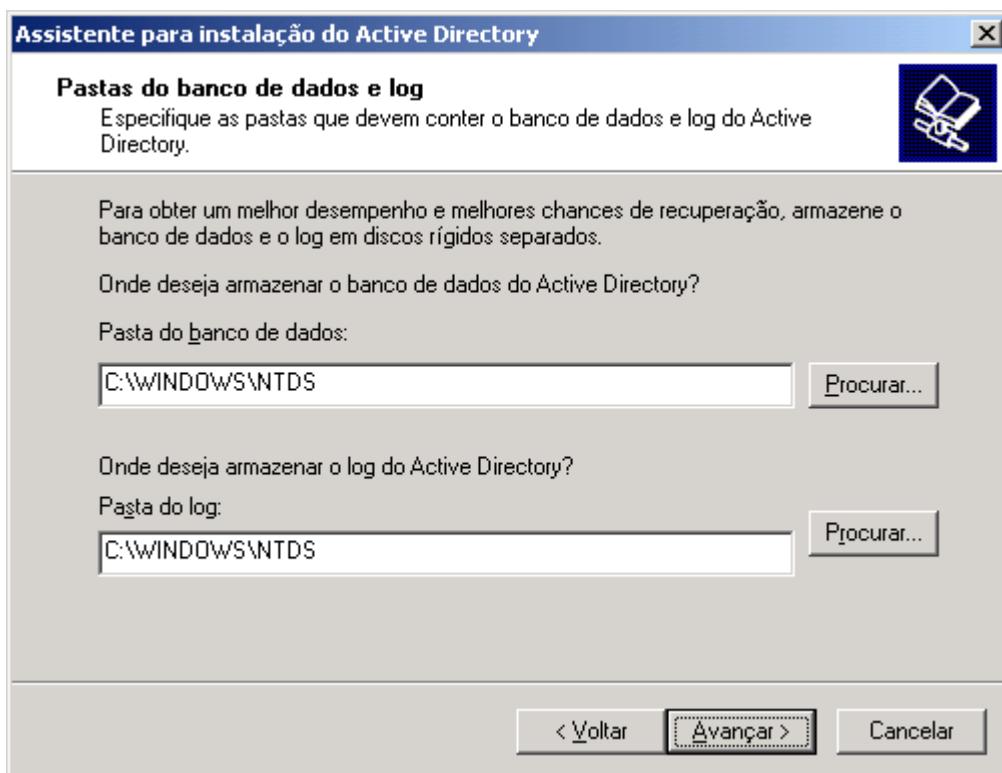


Figura 2.22 Informando o nome NetBIOS do domínio.

12. Em seguida é solicitado o nome NetBIOS do domínio. O nome NetBIOS é uma espécie de apelido, de nome curto para o domínio. Normalmente é utilizada a primeira parte do nome DNS, no nosso exemplo o nome DNS é abc.com, o nome NetBIOS será ABC. Observe que o campo “Nome NetBIOS do domínio”, já vem preenchido com o nome ABC. O nome NetBIOS é importante por questões de compatibilidade, para aplicações e clientes mais antigos, os quais não utilizam o DNS, mas sim o WINS (Windows Internet Name Service). O serviço WINS continua disponível no Windows Server 2003 por questões de compatibilidade.
13. Certifique-se de que o campo Domain NetBIOS name esteja preenchido com o valor ABC, conforme indicado na Figura 8.8.
14. Clique em Avançar, para seguir para a próxima etapa do assistente.
15. Nesta etapa você informa as pastas onde serão gravadas as informações sobre o Active Directory. Por padrão são utilizadas duas pastas, uma para a base de dados do Active Directory e outra para o log do Active Directory. Por padrão o assistente sugere a mesma pasta para a base de dados e para o log e sugere uma pasta chamada NTDS, dentro da pasta onde está instalado o Windows Server 2003. É recomendado que estas informações sejam gravadas em um volume formatado com o sistema de arquivos NTFS, por questões de segurança. Aceite as sugestões do assistente de instalação, conforme indicado na Figura 2.23:



**Figura 2.23 Informando a pasta onde serão gravadas as informações do Active Directory.**

16. Clique em Avançar, para seguir para a próxima etapa do assistente.
17. Nesta etapa é solicitado que você informe a pasta onde será criada a pasta SYSVOL, a qual contém uma série de informações fundamentais para o funcionamento do Active Directory, bem como para a implementação das políticas de segurança (GPOs). Esta pasta, obrigatoriamente, tem que estar em um volume formatado com o sistema de arquivos NTFS. Por padrão o assistente de instalação sugere a pasta SYSVOL, dentro da pasta onde está instalado o Windows Server 2003. Aceite a sugestão do assistente de instalação.

18. Clique em Avançar, para seguir para a próxima etapa do assistente.
19. Nesta etapa, o assistente informa que não pode localizar um servidor DNS para o domínio abc.com e oferece a opção de você deixar que o assistente instale e configure o DNS no servidor que está sendo promovido a DC. Certifique-se de que a opção Instalar e configurar o servidor DNS..., esteja selecionada, conforme indicado na Figura 2.24:

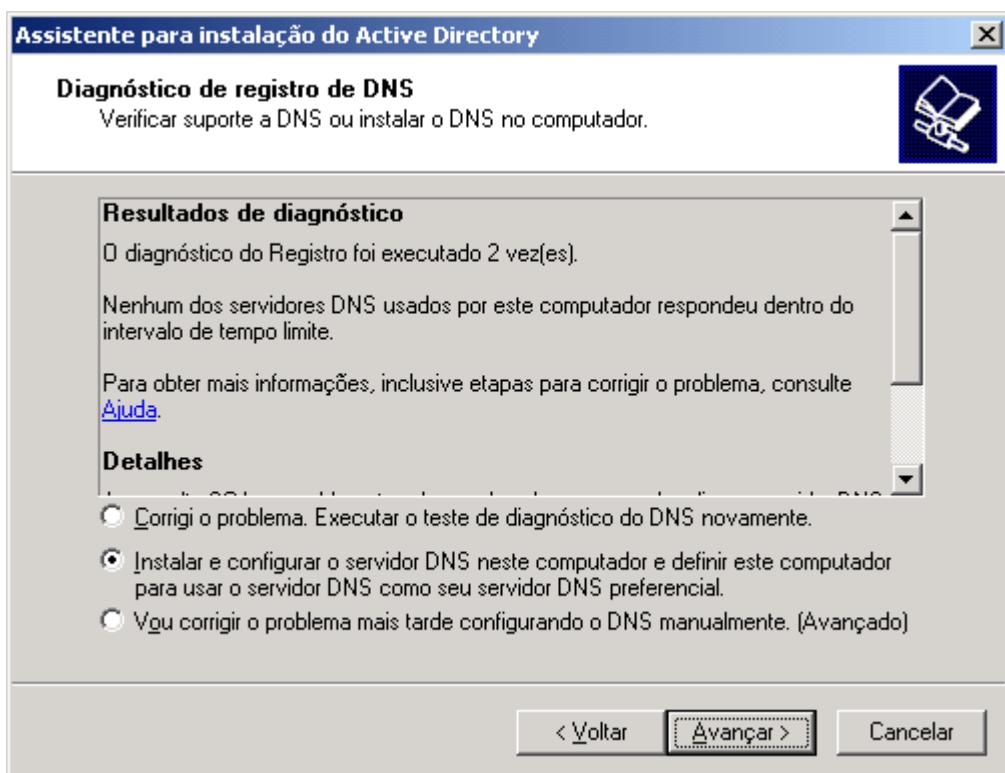


Figura 2.24 Permitindo que o assistente configure o DNS.

20. Clique em Avançar, para seguir para a próxima etapa do assistente.
21. Nesta etapa você precisa selecionar qual o tipo de permissão padrão será utilizada para os objetos usuários e grupos. Os diferentes tipos de permissão têm a ver com os diferentes modos de funcionalidade do domínio e da floresta, conforme descreverei mais adiante. A primeira opção – Permissões compatíveis com versões de sistemas operacionais de servidor anteriores ao Windows 2000, deve ser selecionada se você ainda tem programas que rodam em servidores com versões anteriores ao Windows 2000 Server ou se existem servidores Windows Server 2003, os quais são membros de um domínio baseado no NT Server 4.0 ou anterior. Com esta opção será permitido o acesso anônimo aos programas que rodam no servidor. A segunda opção – Permissões compatíveis somente com os sistemas operacionais de servidor Windows 2000 ou Windows Server 2003, deve ser selecionada se todos os programas que rodam no servidor estão em servidores com o Windows 2000 Server ou Windows Server 2003. Com esta opção somente usuários autenticados poderão acessar os programas que rodam nos servidores. Certifique-se de que a segunda opção – Permissões compatíveis somente com os sistemas operacionais de servidor Windows 2000 ou Windows Server 2003 – esteja selecionada.
22. Clique em Avançar, para seguir para a próxima etapa do assistente.
23. Nesta etapa é solicitado que você defina uma senha que será solicitada quando você inicializar o servidor no modo de restauração do Active Directory. Em algumas situações pode ser necessária a inicialização do servidor

neste modo. Esta senha pode ser diferente da senha da conta Administrador, porém você deve lembrar desta senha, senão não será possível fazer a inicialização no modo de restauração do Active Directory. Informe a senha duas vezes para confirmação.

24. Clique em Avançar, para seguir para a próxima etapa do assistente.
25. Nesta etapa é exibido um resumo de todas as informações que você forneceu para o assistente de instalação do Active Directory. Caso você tenha que fazer alguma alteração é só clicar no botão Voltar para fazer as alterações necessárias.
26. Clique em Avançar e o assistente começará a fazer todas as alterações necessárias para instalar o Active Directory e criar o domínio abc.com, transformando o servidor no primeiro DC do domínio abc.com. Esta etapa pode demorar vários minutos. Uma tela é exibida informando a etapa que está sendo executada, conforme indicado na Figura 2.25:



Figura 2.25 O assistente de instalação do Active Directory trabalhando.

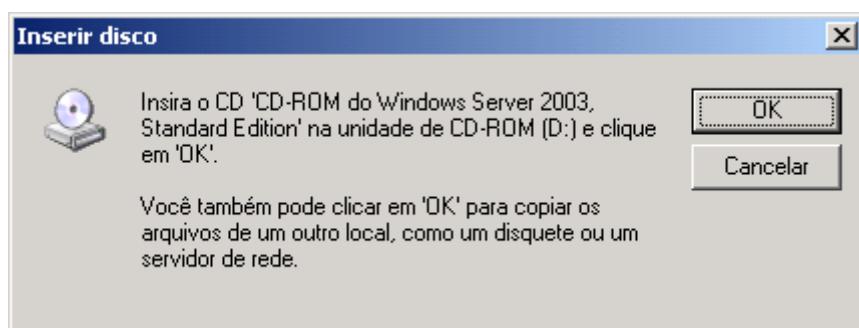


Figura 2.26 Mensagem solicitando o cd de instalação do Windows Server 2003.

**NOTA:** Durante a instalação do Active Directory poderá ser solicitado que você insira o CD do Windows Server 2003 no drive, conforme indicado na Figura 2.26. Se esta mensagem for exibida, insira o cd do Windows Server 2003 no drive e clique em OK.

27. O processo de instalação será concluído e uma mensagem será exibida, informando que a instalação foi concluída com sucesso.
28. Clique em Concluir.
29. Surge uma mensagem informando que o servidor tem que ser reinicializado, conforme indicado na Figura 2.27:

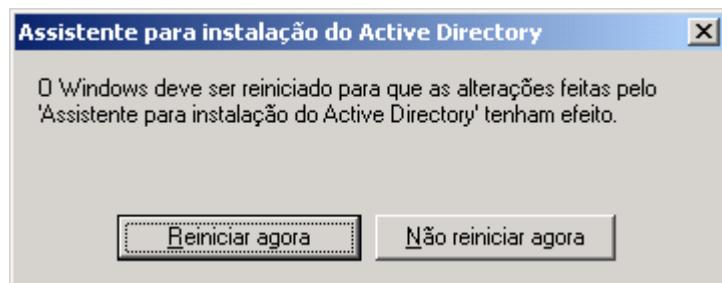


Figura 2.27 Mensagem informando que o computador deve ser reinicializado.

30. Clique em Reiniciar agora.
31. O servidor será reinicializado e no próximo logon, você já irá fazer o logon no domínio abc.com, conforme indicado na Figura 2.28. Observe que no campo Log on to, é exibido o nome NetBIOS do domínio: ABC.

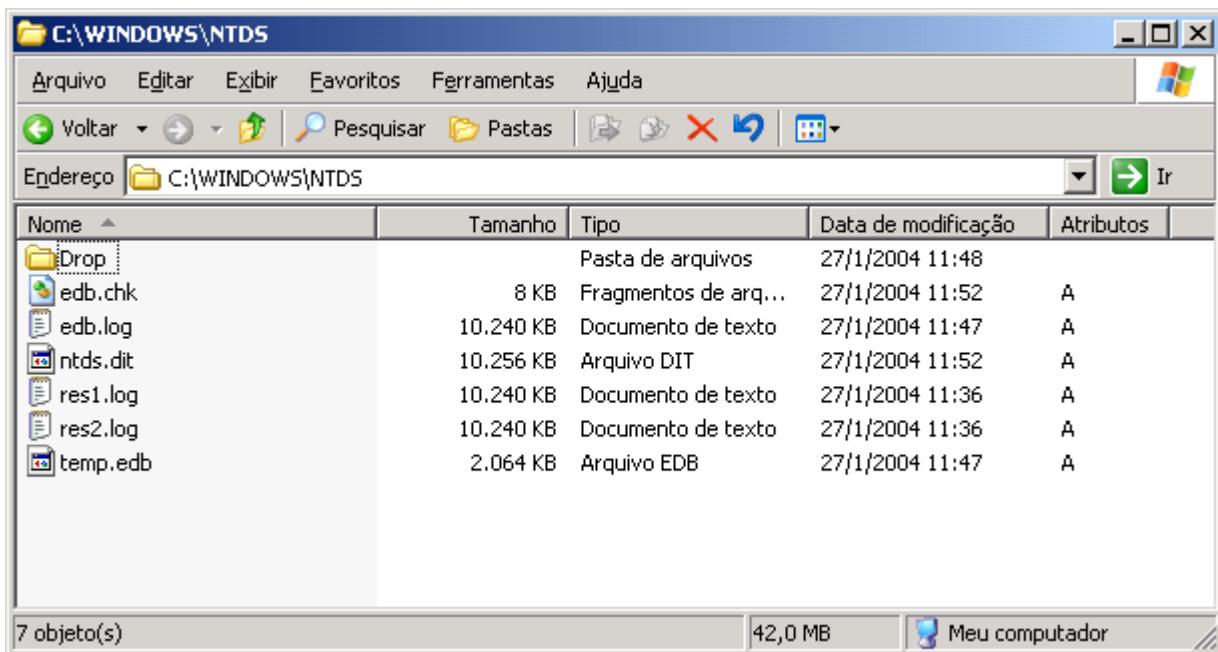


Figura 2.28 Fazendo o logon no domínio ABC.

Muito bem, instalado o Active Directory, agora é hora de analisar quais modificações foram feitas no servidor (além de ele ter sido transformado em um DC), após a instalação do Active Directory.

## Modificações feitas com a instalação do Active Directory.

A primeira e mais óbvia modificação é o fato do servidor ter sido promovido de Member Server para Controlador de Domínio (Domain Controller -DC). Também foram criadas as pastas NTDS e SYSVOL, dentro da pasta onde o Windows Server 2003 está instalado. Na pasta NTDS são gravados os arquivos com a base de dados do Active Directory e com o log de transações desta base de dados. Na Figura 2.29 estão indicados os arquivos que são criados na pasta NTDS:



**Figura 2.29 A pasta NTDS.**

Também é criada a pasta SYSVOL e, dentro desta pasta, uma estrutura de outras pastas que dão suporte a uma série de atividades do Active Directory, tais como scripts de logon, aplicações de Políticas de segurança e assim por diante.

Além destas alterações, novas ferramentas de administração são instaladas. Estas novas ferramentas estão disponíveis no menu Ferramentas Administrativas, do menu Iniciar. A seguir descrevo, brevemente, as novas ferramentas administrativas que são instaladas quando o Active Directory é instalado:

- ◆ Domínios e relações de confiança do Active Directory: Este console é utilizado para o gerenciamento das relações de confiança entre os domínios (relações que são criadas explicitamente pelo Administrador e não as relações de confiança criadas automaticamente pelo Windows Server 2003), para configurar o nível de funcionalidade do domínio (conforme descreverei mais adiante) e para gerenciar o sufixo que é utilizado pelas contas dos usuários. Por exemplo, o usuário jsilva, do domínio abc.com, pode fazer o logon como usuário jsilva@abc.com. Onde abc.com é o sufixo deste usuário.
- ◆ Serviços e sites do Active Directory: Este console é utilizado para gerenciar a replicação de dados do Active Directory. Com este console você cria sites e links entre sites, para implementar uma política de replicação otimizada.
- ◆ Usuários e computadores do Active Directory: Este é um dos consoles mais utilizados pelo Administrador. Com este console é possível gerenciar contas de usuários e grupos de usuários, criar unidades organizacionais e mover usuários e grupos para dentro de uma unidade organizacional. Utilizaremos bastante este console no Capítulo 4 e nos demais capítulos do livro.
- ◆ Diretiva de segurança do controlador de domínio: Este console é utilizado para administrar as políticas de segurança que serão aplicadas ao controlador de domínio com o qual o console está conectado, normalmente o servidor local. As políticas definidas com este console não terão efeito em todo o domínio, mas somente no servidor onde foram configuradas.
- ◆ Diretiva de segurança do domínio: Este console é utilizado para configurar as políticas de segurança que serão aplicados em todos os servidores e estações de trabalho do domínio.

No exemplo do item anterior, quando deixamos a cargo do assistente a instalação do DNS, foi instalado e configurado o DNS no próprio DC. Com isso mais uma modificação foi feita (a instalação do DNS) e mais um console está disponível, que é o console de administração do DNS: Iniciar -> Ferramentas Administrativas -> DNS.

Neste exemplo foi criada uma zona direta no DNS, com o mesmo nome do domínio, ou seja: abc.com, conforme indicado na Figura 2.30. Este fato ressalta bem a dependência entre o DNS e o Active Directory, conforme descrito no Capítulo 6. O nome do domínio é também o nome da zona DNS direta.

**NOTA:** Para um estudo completo sobre GPOs, consulte o Capítulo 18 do livro Windows Server 2003 – Curso Completo, 1568 páginas, de minha autoria, publicado pela Aexcel Books.

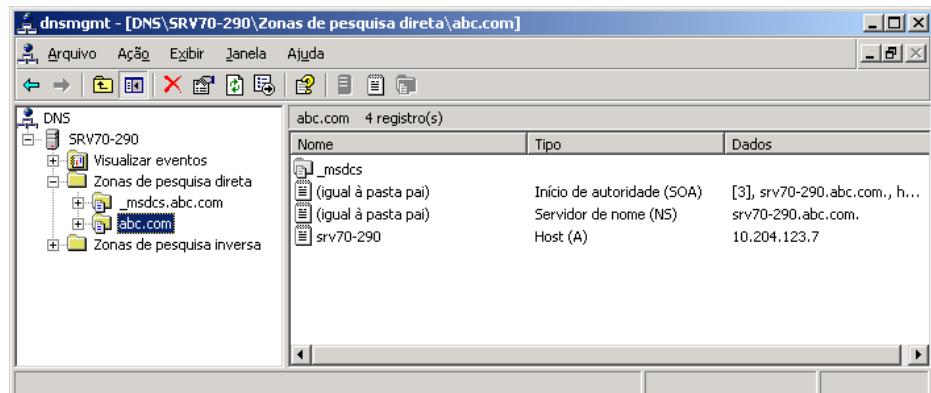


Figura 2.30 A zona DNS direta abc.com.

Outras mudanças, menos visíveis também são feitas com a instalação do Active Directory. Novos contadores são disponibilizados no console de monitoração de desempenho (Capítulo 11), uma nova opção é adicionada no menu de inicialização avançada (Capítulo 12) e assim por diante.

## Como rebaixar um DC de volta a Member Server.

Na época do NT Server 4.0 existiam dois tipos de servidores capazes de fazer a autenticação de usuários do domínio: Primary Domain Controller (PDC) e um ou mais Backup Domain Controller. Em cada domínio existia um único PDC e vários BDCs. Uma característica no NT Server 4.0 é que uma vez que um servidor tivesse sido configurado como PDC ou BDC, não seria possível rebaixá-lo novamente a Member Server. O único jeito seria formatando e reinstalando o NT Server 4.0.

A partir do Windows 2000 Server existem apenas DCs, não existe mais o conceito de PDC e BDCs. Outra novidade é que é possível configurar o servidor para que ele deixe de ser um DC e volte a ser um Member Server, sem que ter que formatar e reinstalar o Windows 2000 Server ou o Windows Server 2003. Esta possibilidade também existe no Windows Server 2003 e será o objeto de estudo deste item. Mostrarei um exemplo prático, onde rebaixarei um DC de volta a Member Server. Então vamos ao exemplo prático.

Exemplo: Como rebaixar um DC de volta a Member Server:

1. Faça o logon como Administrador ou com uma conta com permissão de administrador.
2. Selecione o comando Iniciar -> Executar.
3. Na linha Abrir (Open) digite dcpromo.

4. O assistente de instalação do Active Directory será aberto. A primeira tela é apenas informativa, descrevendo a função do assistente e fornecendo um link para a documentação sobre Active Directory, na Ajuda do Windows Server 2003. Observe que esta mensagem informa que o Active Directory já está instalado neste servidor e que você pode usar o assistente para desinstalar o Active Directory, rebaixando o servidor a member server (ainda pertencente ao domínio) ou um stand alone server, conforme indicado na Figura 2.31:

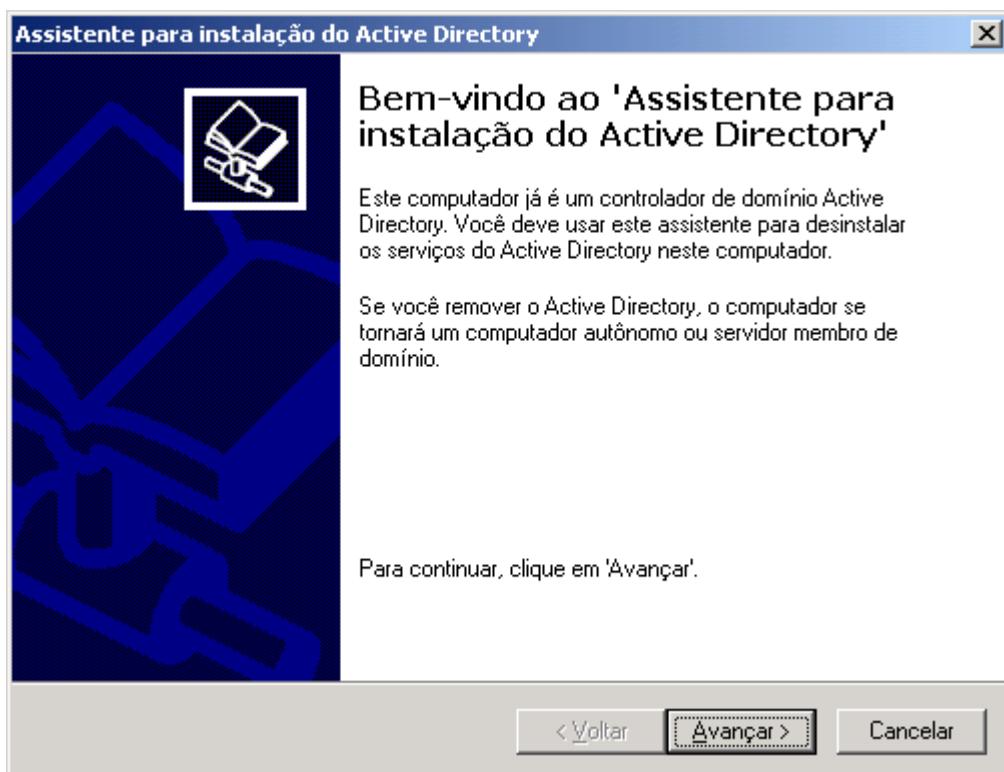


Figura 2.31 Mensagem informando que o Active Directory já está instalado.

5. Clique em Avançar, para seguir para a próxima etapa do assistente.

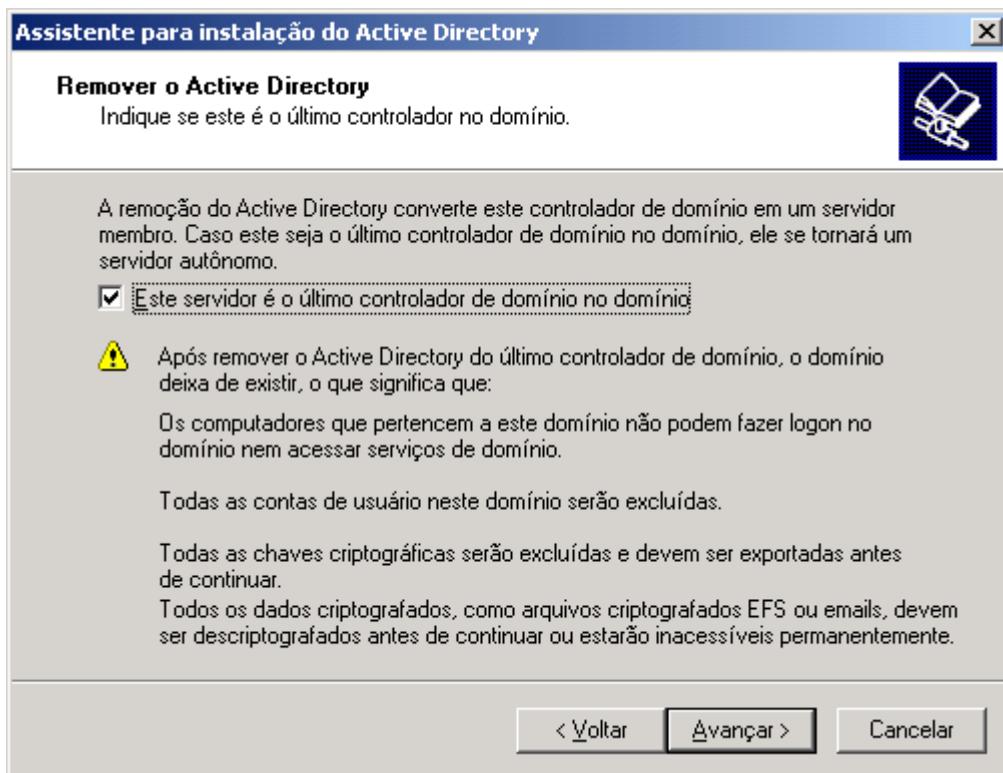


Figura 2.32 Mensagem de advertência.

Se o DC que está sendo rebaixado for o único DC do domínio, é exibida uma mensagem informando que se você rebaixar o último DC o domínio deixará de existir. A mensagem também informa que todas as contas de usuários do domínio serão excluídas, que todas as chaves de criptografia serão excluídas. Antes de excluir o domínio, você deverá exportar as chaves de criptografia para um disquete, senão as pastas que foram criptografadas com contas do domínio estarão inacessíveis após a exclusão do domínio. Nem mesmo criando o domínio novamente e recriando as contas com o mesmo nome e senha, será possível descriptografar estas pastas. Por isso é que você deve exportar as chaves de

**NOTA:** Se o servidor que você está rebaixando for um Servidor de Catálogo Global, surgirá uma mensagem de advertência, informando que pelo menos um Servidor de Catálogo Global deve estar disponível no domínio, senão os usuários não conseguirão fazer o logon no domínio. Esta mensagem está indicada na Figura 2.32. Clique em OK para fechar esta mensagem.

criptografia, antes de excluir o domínio. No Capítulo 6 você aprenderá sobre a exportação de chaves de criptografia. A mensagem de aviso está indicada na Figura 2.33:



**Figura 2.33** Ações a serem executadas antes de excluir um domínio.

6. Se o servidor for o último DC do domínio, marque a opção “Este servidor é o último controlador de domínio no domínio”, caso contrário deixe esta opção desmarcada.
7. Clique em Avançar, para seguir para a próxima etapa do assistente.
8. A próxima mensagem informa sobre as configurações do DNS relacionadas com o Active Directory. Nesta etapa são listadas as configurações que serão excluídas com a desinstalação do Active Directory.
9. Aceite as configurações sugeridas pelo assistente e clique em Avançar, para seguir para a próxima etapa do assistente.
10. Surge mais uma mensagem pedindo que você informe se deseja que o assistente exclua as partições de aplicação do Active Directory, as quais foram criadas durante a instalação do Active Directory. Marque a opção “Excluir todas as partições de diretório de aplicativos deste controlador de domínio”.
11. Clique em Avançar, para seguir para a próxima etapa do assistente.
12. Nesta etapa é solicitado que você informe a senha que será atribuída a conta Administrador, conta esta que será uma conta local depois que o Active Directory for desinstalado. Digite a senha duas vezes, conforme indicado na Figura 2.34:

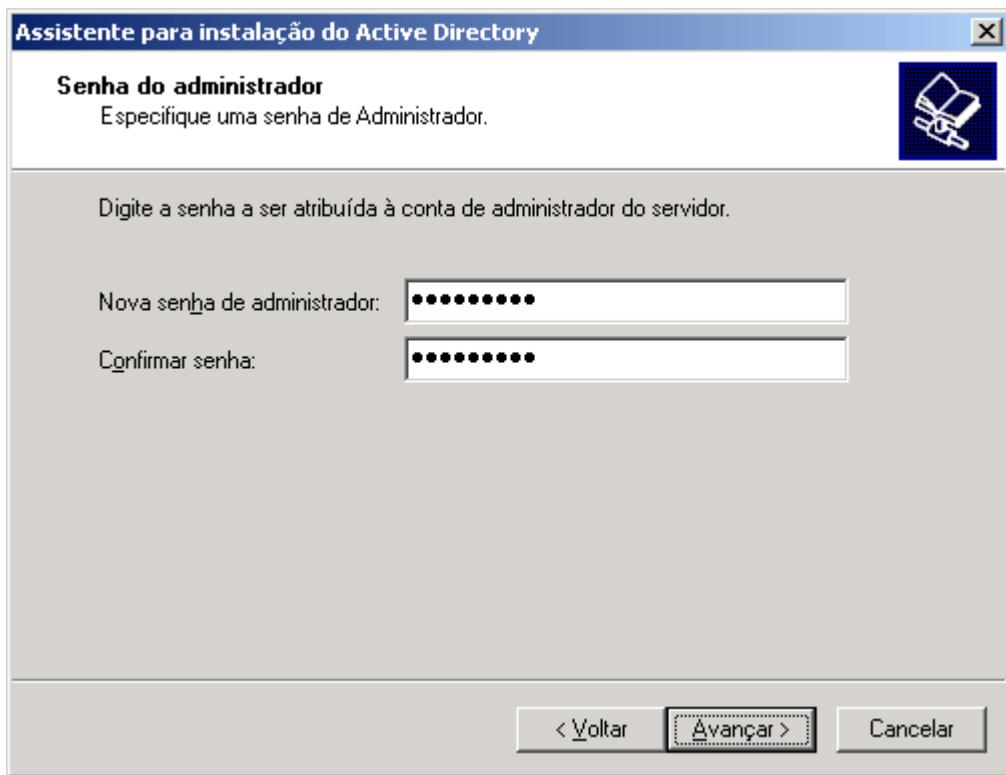


Figura 2.34 Informando a senha para a conta Administrator (Administrator).

13. Clique em Avançar, para seguir para a próxima etapa do assistente.
14. Será exibida a tela final do assistente com um resumo das opções selecionadas. Você pode utilizar o botão Voltar, para voltar a uma determinada etapa do assistente e fazer alterações. Clique no botão Avançar.
15. O processo de desinstalação do Active Directory inicia, conforme indicado na Figura 2.35. Esta etapa pode demorar alguns minutos.

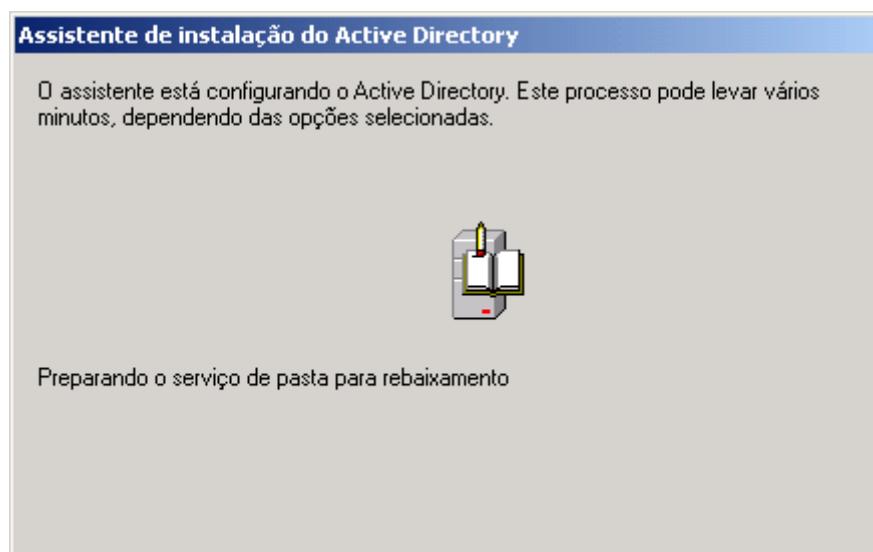


Figura 2.35 Desinstalando o Active Directory.

16. Ao final do processo é exibida uma mensagem informando que o Active Directory foi desinstalado. Clique em Concluir.

17. Será exibida uma mensagem informando que o servidor precisa ser reinicializado para que o processo de desinstalação esteja completo. Clique em Reiniciar Agora. O servidor será reinicializado e agora ele já é um member server (ou um stand alone server, caso o servidor tenha sido configurado para não pertencer a um domínio).

Após a desinstalação do Active Directory as ferramentas de administração do Active Directory deixam de estar disponíveis. Também podem ser perdidas algumas configurações (ícones da área de trabalho e atalhos da barra de inicialização rápida), as quais terão que ser refeitas.

## Criar um novo DC em um domínio já existente.

Neste item você acompanhará a utilização da ferramenta administrativa Gerenciar o servidor. Utilizarei esta ferramenta para criar um novo DC em um domínio já existente. Vou promover um member server a DC de um domínio já existente.

Exemplo: Para criar um novo DC em um domínio já existente, usando a ferramenta administrativa Gerenciar o servidor, siga os passos indicados a seguir:

1. Faça o logon como Administrador ou com uma conta com permissão de administrador no servidor que será promovido a DC.
2. Selecione o comando Iniciar -> Ferramentas Administrativas -> Gerenciar o Servidor.
3. Será aberta a janela Gerenciar o servidor.
4. Clique na opção Adicionar ou remover uma função.
5. Será aberto o assistente de configuração do servidor. A primeira etapa do assistente é apenas informativa.
6. Clique no botão Avançar. O assistente inicia uma fase de detecção das configurações de rede do seu servidor, conforme indicado na Figura 2.36:

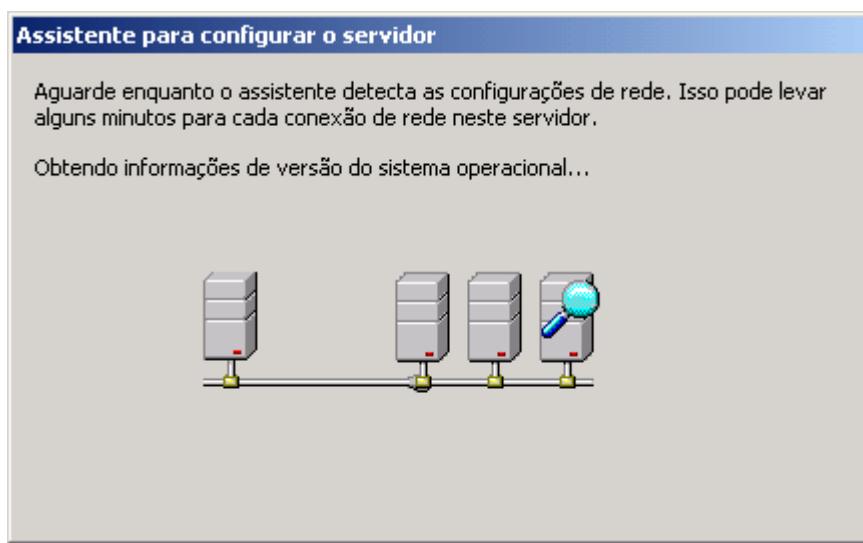


Figura 2.36 Detecção das conexões de rede.

7. Em seguida é exibida uma lista de funcionalidades (role) informando quais estão instaladas e quais ainda não estão instaladas no servidor. Marque a opção Controlador de domínio (Active Directory), conforme indicado na Figura 2.37:

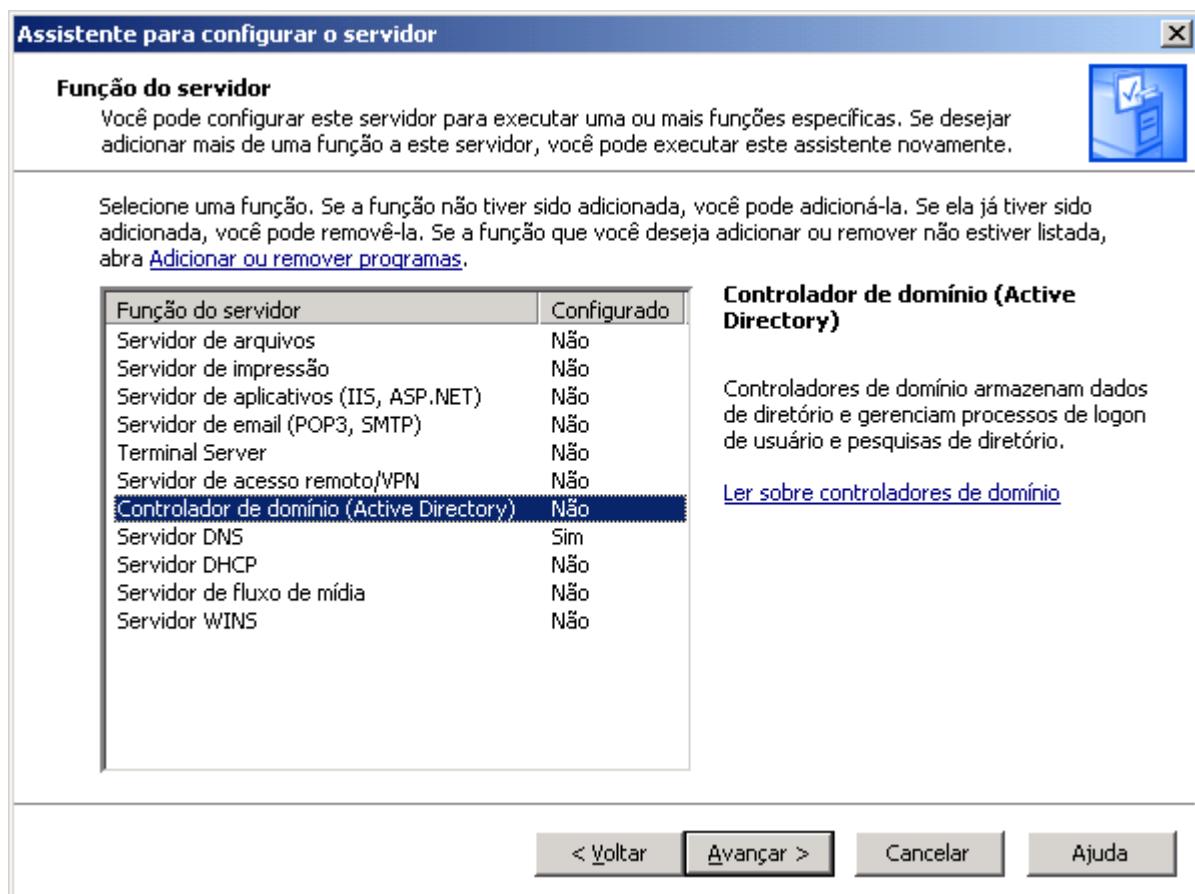


Figura 2.37 Marcando o Active Directory para instalação.

8. Clique em Avançar, para seguir para a próxima etapa do assistente.
  9. Será exibida uma lista das opções que você selecionou, no nosso exemplo somente a instalação do Active Directory.
  10. Clique em Avançar que será lançado o assistente do Active Directory, para que você possa instalar o Active Directory.
  4. O assistente de instalação/desinstalação do Active Directory será aberto. A primeira tela é apenas informativa, descrevendo a função do assistente e fornecendo um link para a documentação sobre Active Directory, na Ajuda do Windows Server 2003.
  5. Clique em Avançar, para seguir para a próxima etapa do assistente.
- Na segunda etapa é informado que clientes rodando o Windows 95 ou o Windows NT 4.0, com Service Pack 3.0 ou inferior, não serão capazes de fazer parte de um domínio baseado no Windows Server 2003. Esta etapa também é apenas informativa.
6. Clique em Avançar, para seguir para a próxima etapa do assistente.
  7. Na terceira etapa você deve informar se esta sendo instalado um DC para um novo domínio, ou seja, o primeiro DC e a criação do domínio, ou se você está instalando um DC adicional para um domínio já existente (que é o caso do nosso exemplo). Para o nosso exemplo selecione a opção Controlador de domínio adicional para um domínio já existente, conforme indicado na Figura 2.38:

**NOTA:** Se o Terminal Server estiver instalado no servidor que está sendo promovido a DC, você receberá uma mensagem de alerta. Esta mensagem informa que a partir da instalação do Active Directory, somente contas com permissão de Administrador do domínio, poderão fazer o logon remotamente usando o terminal server. Para dar permissões de logon, via terminal server, para outras contas, você terá que alterar as políticas de segurança local do servidor, conforme mostrarei no Capítulo 5, no item sobre direitos de contas de usuário. Para continuar com a instalação do Active Directory, clique em OK para fechar a mensagem de aviso.

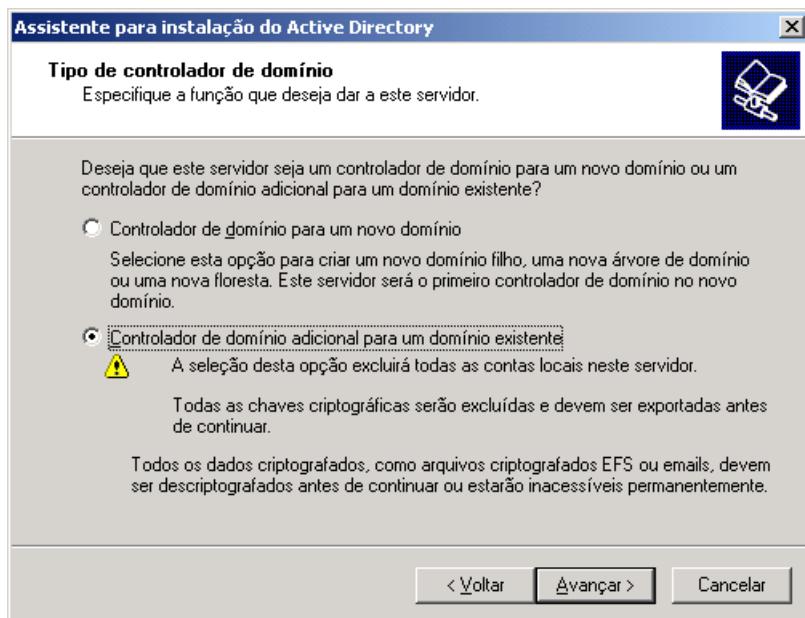


Figura 2.38 Criando um novo DC em um domínio já existente.

8. Clique em Avançar, para seguir para a próxima etapa do assistente.
9. Nesta etapa você tem que informar uma conta de usuário, uma senha e o nome do domínio. A conta informada tem que ter privilégios de administrador no domínio para o qual está sendo criado um novo DC. Informe os dados para uma conta de administrador do domínio. No exemplo da Figura 2.39, estou informando os dados de uma conta com permissão de administrador no domínio groza.com (que é o domínio que uso na rede em minha casa). Neste instante o servidor deve ter acesso a um servidor DNS do domínio groza.com. O número IP do servidor DNS pode ser configurado nas propriedades de rede do TCP/IP.

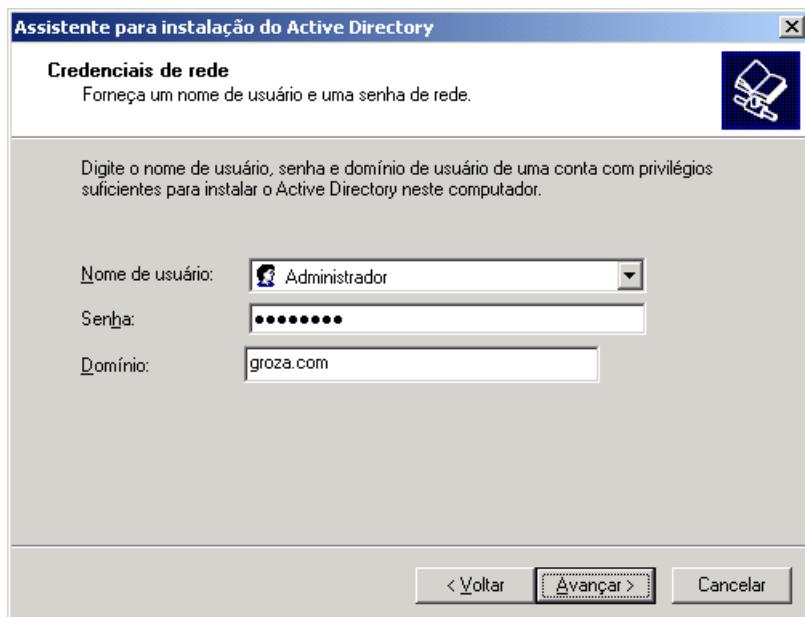


Figura 2.39 Informando uma conta com permissão de administrador e o nome do domínio.

10. Insira as informações de conta, senha e domínio e clique em Avançar, para seguir para a próxima etapa do assistente.

11. Nesta etapa você deve fornecer o nome DNS completo do domínio no qual você deseja criar o novo DC. Você pode clicar no botão Procurar..., para exibir uma lista dos domínios disponíveis. Neste exemplo clique no botão Procurar... e depois no domínio groza.com, conforme indicado na Figura 2.40:



Figura 2.40 Selecionando o domínio.

12. Ao clicar em OK você estará de volta ao assistente de instalação e o nome do domínio selecionado já estará no campo Nome do domínio.
13. Clique em Avançar, para seguir para a próxima etapa do assistente.
14. Nesta etapa você informa as pastas onde serão gravadas as informações sobre o Active Directory. Por padrão são utilizadas duas pastas, uma para a base de dados do Active Directory e outra para o log do Active Directory. Por padrão o assistente sugere a mesma pasta para a base de dados e para o log e sugere uma pasta chamada NTDS, dentro da pasta onde está instalado o Windows Server 2003. É recomendado que estas informações sejam gravadas em um volume formatado com o sistema de arquivos NTFS, por questões de segurança. Aceite as sugestões do assistente de instalação, conforme indicado na Figura 2.41.
15. Clique em Avançar, para seguir para a próxima etapa do assistente.
16. Nesta etapa é solicitado que você informe o caminho onde será criada a pasta SYSVOL, a qual contém uma série de informações fundamentais para o funcionamento do Active Directory, bem como para a implementação das políticas de segurança (GPOs). Esta pasta, obrigatoriamente, tem que estar em um volume formatado com o sistema de arquivos NTFS. Por padrão o assistente de instalação sugere a pasta SYSVOL, dentro da pasta onde está instalado o Windows Server 2003. Aceite a sugestão do assistente de instalação.
17. Clique em Avançar, para seguir para a próxima etapa do assistente.
18. Nesta etapa é solicitado que você defina uma senha que será solicitada quando você inicializar o servidor no modo de restauração do Active Directory. Em

**IMPORTANTE:** Por questões de desempenho, a Microsoft recomenda que o arquivo de dados e o arquivo de log sejam gravados em partições localizadas em discos rígidos diferentes, de preferência até mesmo discos em controladores diferentes.

algumas situações pode ser necessária a inicialização do servidor neste modo. Esta senha pode ser diferente da senha da conta Administrador, porém você deve lembrar desta senha, senão não será possível fazer a inicialização no modo de restauração do Active Directory. Informe a senha duas vezes para confirmação.

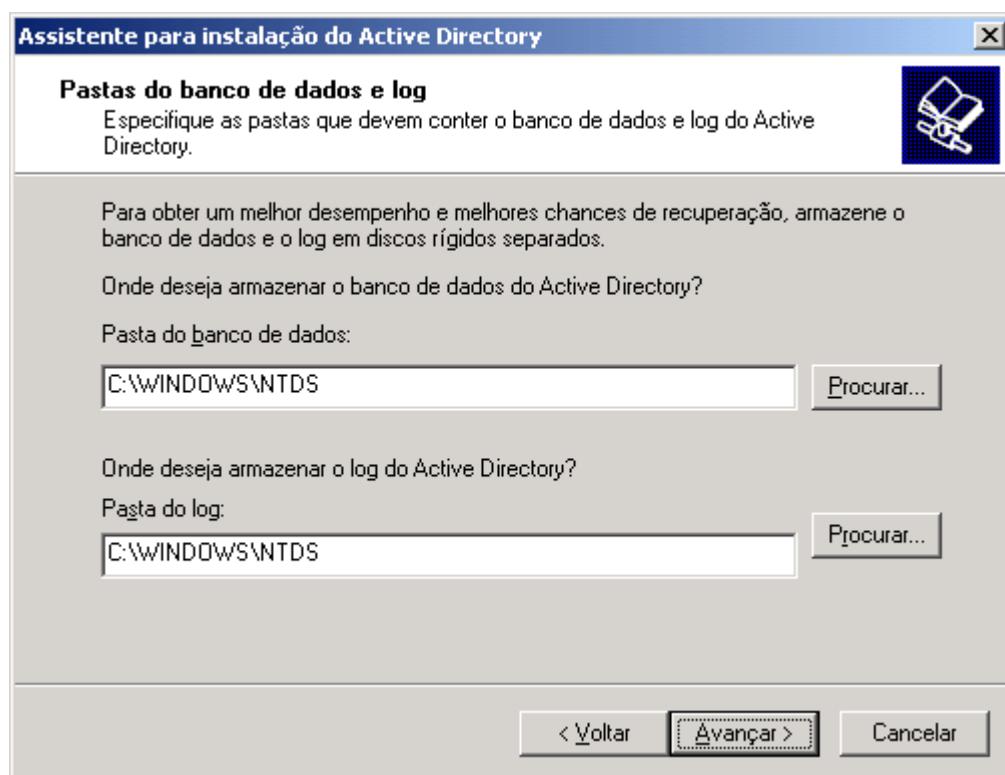


Figura 2.41 Informando a pasta onde serão gravadas as informações do Active Directory.

19. Clique em Avançar, para seguir para a próxima etapa do assistente.
20. Nesta etapa é exibido um resumo de todas as informações que você forneceu para o assistente de instalação do Active Directory. Caso você tenha que fazer alguma alteração é só clicar no botão Voltar para fazer as alterações necessárias.
21. Clique em Avançar e o assistente começará a fazer todas as alterações necessárias para instalar o Active Directory e criar um novo DC no domínio groza.com, transformando em um DC adicional do domínio groza.com. Esta etapa pode demorar vários minutos. Uma tela é exibida informando cada etapa do processo
22. O processo de instalação será concluído e uma mensagem será exibida, informando que a instalação foi concluída com sucesso.
23. Clique em Concluir.
24. Surge uma mensagem informando que o servidor tem que ser reinicializado
25. Clique em Reiniciar agora.
32. O servidor será reinicializado e no próximo logon, você já irá fazer o logon no domínio groza.com. Pronto, você acaba de adicionar mais um DC ao domínio groza.com

---

**NOTA:** Durante a instalação do Active Directory poderá ser solicitado que você insira o CD do Windows Server 2003 no drive. Se esta mensagem for exibida, insira o cd do Windows Server 2003 no drive e clique em OK.

---

A seguir você aprenderá mais alguns detalhes sobre o Active Directory, bem como aprenderá a utilizar algumas das ferramentas administrativas do Active Directory.

## Preparando um domínio do Windows 2000 Server para migração.

Antes de migrar um domínio baseado no Windows 2000 Server para o Windows Server 2003, existem algumas etapas de preparação que devem ser executadas. Estas etapas fazem alterações, principalmente, no Schema do Active Directory, preparando-o para o Windows Server 2003.

Se você for migrar uma árvore inteira de domínios ou até mesmo um floresta, existem comandos que deve ser executados para fazer a preparação da floresta e das árvores de domínios, para que possa ser feita a migração para o Windows Server 2003.

Para obter um relatório completo sobre a compatibilidade do Windows Server 2003 e as ações de preparação necessárias, você pode executar um teste de verificação de compatibilidade, executando o comando `winnt32/checkupgradeonly`, conforme exemplificado no Capítulo 1, quando da instalação do Windows Server 2003.

Para preparar uma floresta de domínios do Windows 2000 Server, para migração para o Windows Server 2003, você utiliza o seguinte comando:

```
adprep /forestprep
```

este comando irá fazer alterações no Schema do Active Directory, preparando-o para a migração para o Windows Server 2003. Estas alterações devem ser replicadas (o que é feito automaticamente) entre todos os domínios e árvores da floresta.

Feita a preparação da floresta você pode fazer a preparação de cada domínio individualmente, usando o comando a seguir:

```
adprep /domainprep
```

O comando adprep está disponível na pasta I386 do CD de instalação do Windows Server 2003. Não será possível atualizar um DC com o Windows 2000 Server para o Windows Server 2003 ou adicionar novos DCs rodando o Windows Server 2003 em um domínio baseado no Windows 2000 Server, até que o comando adprep tenha sido utilizado para preparar a floresta e o domínio para a migração.

---

**NOTA:** Para uma referência completa a todas as opções do comando `adprep`, execute o seguinte comando: `adprep/?`

---

## Operações diversas com o Active Directory.

A partir de agora passarei a mostrar uma série de operações que podem ser executadas no Active Directory e nos DCs. Estas operações são executadas usando as ferramentas administrativas que são instaladas juntamente com o Active Directory, conforme descrito anteriormente. Para acompanhar e entender os que mostrarei a seguir é importante que você tenha entendido bem todos os conceitos teóricos sobre Active Directory, apresentados no Capítulo 1.

## Modos de funcionalidade do domínio e da floresta.

É comum a rede da empresa “conviver” com diferentes versões do Windows em seus servidores. Isso aconteceu na migração do NT Server 4.0 para o Windows 2000 Server, onde durante um bom tempo ainda existiam (na prática

sabemos que ainda existem) servidores com o NT Server 4.0 em utilização na rede, juntamente com os servidores com o Windows 2000 Server. Agora com o Windows Server 2003, é provável que, no mesmo domínio, tenhamos servidores com o NT Server 4.0, Windows 2000 Server e Windows Server 2003. Dependendo de existir apenas servidores com o Windows Server 2003 ou uma “mescla” com outras versões (NT Server 4 e Windows 2000 Server), existem diferentes níveis de funcionalidade para um domínio e para a floresta como um todo. Em cada nível de funcionalidade estão disponíveis/habilitadas diferentes funcionalidades.

O Windows Server 2003 (a exemplo do que acontecia com o Windows 2000 Server), tem diferentes níveis de funcionalidade, com base nos tipos de DCs (com NT Server 4.0, com Windows 2000 Server, com Windows Server 2003 ou uma mescla destas versões) instalados na rede. Neste tópico vou descrever os níveis de funcionalidade disponíveis e as diferentes funcionalidades que estão disponíveis em cada nível.

Com o Windows Server 2003 foi introduzido o nível de funcionalidade da floresta, o que não existia com o Windows 2000 Server.

O nível de funcionalidade do domínio determina quais características estão ou não disponíveis.

Existem quatro níveis de funcionalidade do domínio no Windows Server 2003:

- ◆ Windows 2000 mixed
- ◆ Windows 2000 native
- ◆ Windows Server 2003 interim
- ◆ Windows Server 2003

Por padrão é selecionado o nível de funcionalidade Windows 2000 mixed. Muitos dos recursos mais avançados, tais como grupos Universais, somente estão disponíveis nos demais níveis de funcionalidade: Windows 2000 native, Windows Server 2003 interim ou Windows Server 2003.

O nível de funcionalidade da floresta é uma novidade do Windows Server 2003. Existem três níveis de funcionalidade da floresta disponíveis: Windows 2000, Windows Server 2003 interim e Windows Server 2003. Por padrão é selecionado o nível Windows 2000. Muitas das novidades do Windows Server 2003 em relação ao Active Directory somente estão disponíveis nos níveis mais avançados: Windows Server 2003 interim ou Windows Server 2003.

Para que o nível de funcionalidade da floresta seja configurado para Windows Server 2003, todos os DCs de todos os domínios devem estar com o Windows Server 2003 instalado. Somente neste nível é que estarão disponíveis todos os recursos do Active Directory, incluindo a maioria das novidades introduzidas com o Windows Server 2003.

O que define se é possível ou não utilizar um determinado nível de funcionalidade é a existência ou não de DCs com versões anteriores do Windows, tais como o Windows 2000 Server e o Windows NT Server 4.0.

- ◆ **Windows 2000 mixed:** Suporta DCs com o Windows NT Server 4.0, Windows 2000 Server ou Windows Server 2003. Neste nível de funcionalidade não é possível a utilização de grupos Universais e não é possível renomear um DC (ao invés disso o DC tem que ser rebaixado a member server, faz-se a renomeação e promove-se o servidor novamente a DC),
- ◆ **Windows 2000 native:** Suporta DCs com o Windows 2000 Server ou com o Windows Server 2003. Neste nível de funcionalidade são suportados grupos Universais. Neste nível é possível utilizar os grupos Universais porém não é possível renomear DCs sem antes rebaixa-los de volta a member server.
- ◆ **Windows Server 2003 interim:** Suporta DCs com o NT Server 4.0 ou com o Windows Server 2003. Este nível de funcionalidade é utilizado quando você está em processo de migração de uma rede baseada no Windows NT Server 4.0 para o Windows Server 2003.

♦ **Windows Server 2003:** Somente DCs com o Windows Server 2003. Este é o nível onde estão disponíveis todos os recursos e novidades do Active Directory. Agora vou falar sobre os níveis de funcionalidade da floresta e as características de cada nível. Esta é uma das novidades do Windows Server 2003, ou seja, o conceito de nível de funcionalidade da floresta. Conforme descrito anteriormente, estão disponíveis três diferentes níveis de funcionalidade de floresta, conforme detalhado a seguir:

- ♦ **Windows 2000:** Este é o nível de funcionalidade padrão. Neste nível podem coexistir DCs com o NT Server 4.0, Windows 2000 Server e Windows Server 2003. Normalmente é utilizado durante a fase de migração de uma rede baseada no NT Server 4.0 para o Windows Server 2003. Neste nível, a maioria das novidades do Active Directory no Windows Server 2003 estão desabilitadas, como por exemplo: melhorias na replicação do catálogo global (somente estarão disponíveis na replicação entre dois servidores de catálogo global baseados no Windows Server 2003), relação de confiança entre florestas, renomeação de domínio, melhorias na replicação do Active Directory, dentre outros.
- ♦ **Windows Server 2003 interim:** Este nível de funcionalidade da floresta é utilizado quando da migração de uma rede baseada no NT Server 4.0 diretamente para o Windows Server 2003. Suporta DCs baseados no NT Server 4.0 e no Windows Server 2003. A maioria das novidades do Active Directory não estão disponíveis neste nível de funcionalidade:
- ♦ **Windows Server 2003:** Este nível de funcionalidade da floresta é utilizado quando a migração já foi completada e somente existem DCs com o Windows Server 2003. Somente suporta DCs baseados no Windows Server 2003. É neste nível que estão disponíveis todas as novidades do Active Directory no Windows Server 2003.

Quando você configura o nível de funcionalidade mais alto, não poderão ser introduzidos DCs com as versões anteriores do Windows. Por exemplo, quando o nível de funcionalidade da floresta é configurado como Windows Server 2003, não será mais possível criar novos DCs baseados no NT Server 4.0 ou no Windows 2000 Server.

## Como configurar o nível de funcionalidade de um domínio e de uma floresta:

Os níveis de funcionalidade do domínio e da floresta são configurados com o console Domínios e relações de confiança do Active Directory, o qual é acessado através do menu Ferramentas administrativas.

Configurando o nível de funcionalidade do domínio:

1. Faça o logon como Administrador ou com uma conta com permissão de administrador no domínio.

**IMPORTANTE:** Quando você altera de um modo de funcionalidade para o outro, não será mais possível criar DCs com versões não suportadas do Windows. Por exemplo, quando você passa do modo Windows 2000 mixed para o modo Windows 2000 Native, não será mais possível inserir DCs com o NT Server 4.0 e nem será voltar para o nível de funcionalidade anterior.

2. Abra o console Domínios e relações de confiança do Active Directory: Iniciar -> Ferramentas administrativas -> Domínios e relações de confiança do Active Directory.
3. Será exibido o console Domínios e relações de confiança do Active Directory, onde é exibida a árvore de diretórios da sua rede, conforme exemplo da Figura 2.42:

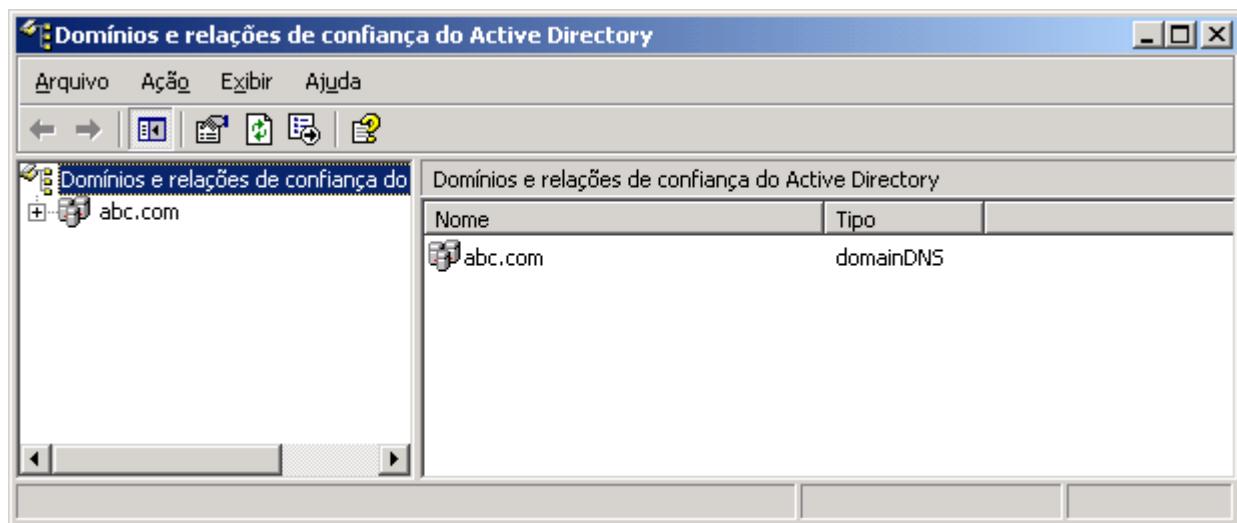


Figura 2.42 O console Active Directory Domains and Trusts.

4. Clique com o botão direito no domínio a ser configurado e no menu que é exibido clique em Aumentar nível funcional do domínio...
5. Será exibida a janela Aumentar nível funcional do domínio, indicada na Figura 2.43. Selecione o nível de funcionalidade desejado e clique em Aumentar. Surgirá uma mensagem informando que estas alterações afetarão todo o domínio. Clique em OK para fechar a mensagem e definir o nível de funcionalidade do domínio e que você não poderá voltar ao nível anterior. Por exemplo, quando você altera do nível Windows 2000 Mixed para o nível Windows 2000 Native, não será possível voltar ao nível Windows 2000 Mixed novamente.

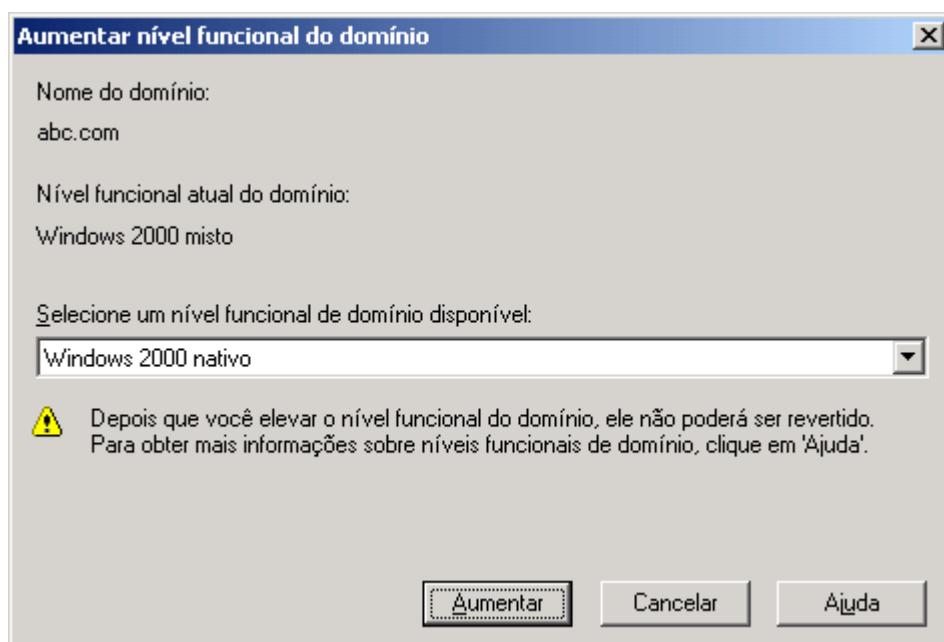


Figura 2.43 A janela Aumentar nível funcional do domínio.

6. Surge uma mensagem informando que o nível de funcionalidade do domínio foi alterado. Clique em OK. Você estará de volta ao consolo Active Directory Domain and Trusts.
7. Feche o console.

Agora vou mostrar os passos para configura o nível de funcionalidade da floresta. Para executar esta operação você deve fazer o logon com uma conta com permissão de Enterprise Admin., ou seja, uma conta pertencente ao grupo Administração de empresa.

Configurando o nível de funcionalidade da floresta:

1. Faça o logon com uma conta com permissão de Enterprise Admin.
2. Abra o console Domínios e relações de confiança do Active Directory: Iniciar -> Ferramentas administrativas -> Domínios e relações de confiança do Active Directory.
3. Será exibido o console Domínios e relações de confiança do Active Directory, onde é exibida a árvore de diretórios da sua rede.
4. Clique com o botão direito na raiz da árvore a ser configurada e no menu que é exibido clique em Aumentar nível funcional da floresta...
5. Será exibida a janela Aumentar nível funcional da floresta, indicada na Figura 2.44. Selecione o nível de funcionalidade desejado e clique em Aumentar. Surgirá uma mensagem informando que estas alterações afetarão todos os domínios. Clique em OK para fechar a mensagem e definir o nível de funcionalidade da floresta e você não poderá voltar ao nível anterior. Por exemplo, quando você altera do nível Windows 2000 para o nível Windows Server 2003, não será possível voltar ao nível Windows 2000 novamente.

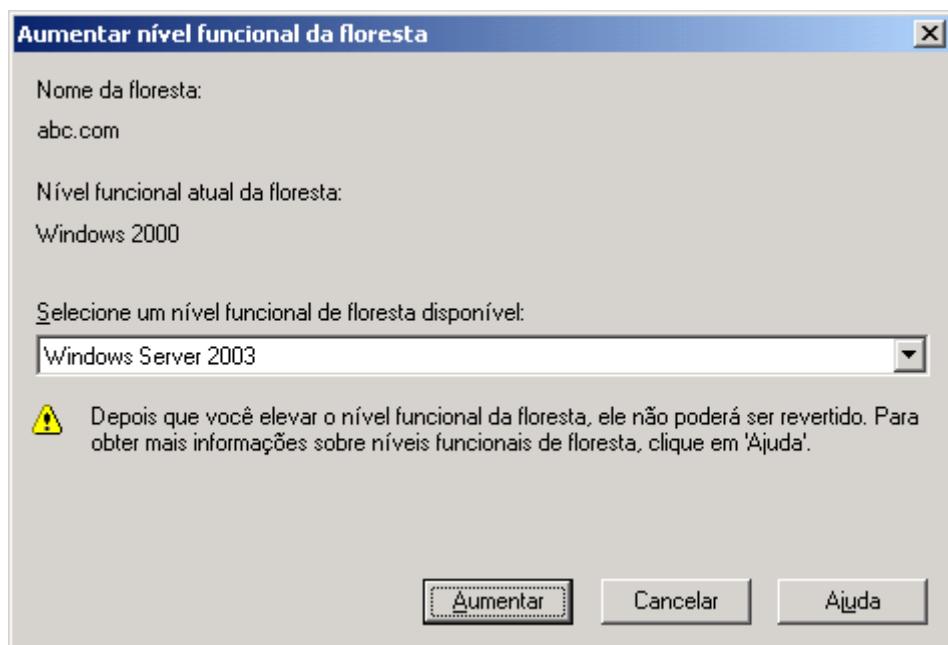


Figura 2.44 A janela Aumentar nível funcional da floresta.

## Gerenciando relações de confiança entre domínios.

Conforme descrito no Capítulo 1, o Windows Server 2003 (a exemplo do Windows 2000 Server) cria e gerencia, automaticamente, as relações de confiança entre os domínios de uma árvore de domínios. Porém em determinadas

situações, pode ser necessária a criação de relações de confiança, manualmente, pelo Administrador. Para criar relações de confiança manualmente (Trusts), o administrador utiliza console Domínios e relações de confiança do Active Directory. A seguir descrevo os passos para acessar a janela para criação de relações de confiança manualmente.

Configurando relações de confiança manualmente:

1. Faça o logon como Administrador ou com uma conta com permissão de administrador no domínio.
2. Abra o console Domínios e relações de confiança do Active Directory: Iniciar -> Ferramentas administrativas -> Domínios e relações de confiança do Active Directory.
3. Será exibido console Domínios e relações de confiança do Active Directory, onde é exibida a árvore de diretórios da sua rede.
4. Clique com o botão direito no domínio a ser configurado e no menu que é exibido clique em Propriedades.
5. Na janela de Propriedades dê um clique na guia Relações de confiança. Nesta guia, indicada na Figura 2.45, o administrador pode criar relações de confiança com outros domínios e definir as características desta relação de confiança.

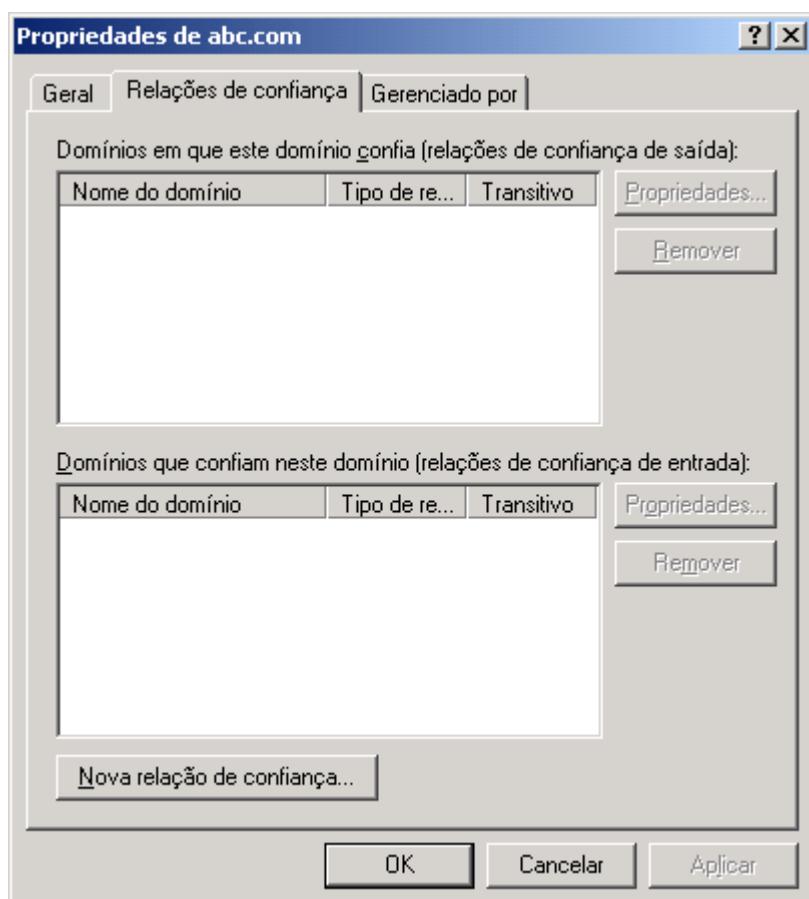


Figura 2.45 A guia Relações de confiança da janela de propriedades do domínio.

## Configurando um DC como Servidor de Catálogo Global.

Para que um usuário possa fazer o logon e ser autenticado na rede, ele precisa contatar um Servidor de Catálogo Global, conforme descrito no Capítulo 1. Por padrão, o primeiro DC de um domínio é, automaticamente, configurado

como Servidor de Catálogo Global. A recomendação da Microsoft é que você tenha, pelo menos, um Servidor de Catálogo Global em cada site, para reduzir o tempo necessário para o logon e evitar tráfego adicional nos links de Wan. A seguir mostrarei os passos necessários para configurar um DC como Servidor de Catálogo Global.

Como configurar um DC como Servidor de Catálogo Global:

1. Faça o logon com uma conta com permissão de Enterprise Admin.
2. Abra o console Serviços e sites do Active Directory: Iniciar -> Ferramentas administrativas -> Serviços e sites do Active Directory.
3. Será exibido o console Serviços e sites do Active Directory, onde é exibida a árvore de sites da sua rede. Lembrando, do Capítulo 1, que os sites representam a divisão física da rede e são utilizados para otimizar e gerenciar o tráfego de replicação entre os DCs de um domínio.
4. Acesse o site onde está o servidor que você quer configurar como Servidor de Catálogo Global, conforme exemplo da Figura 2.46, onde foi selecionado o servidor MCSE70-290.

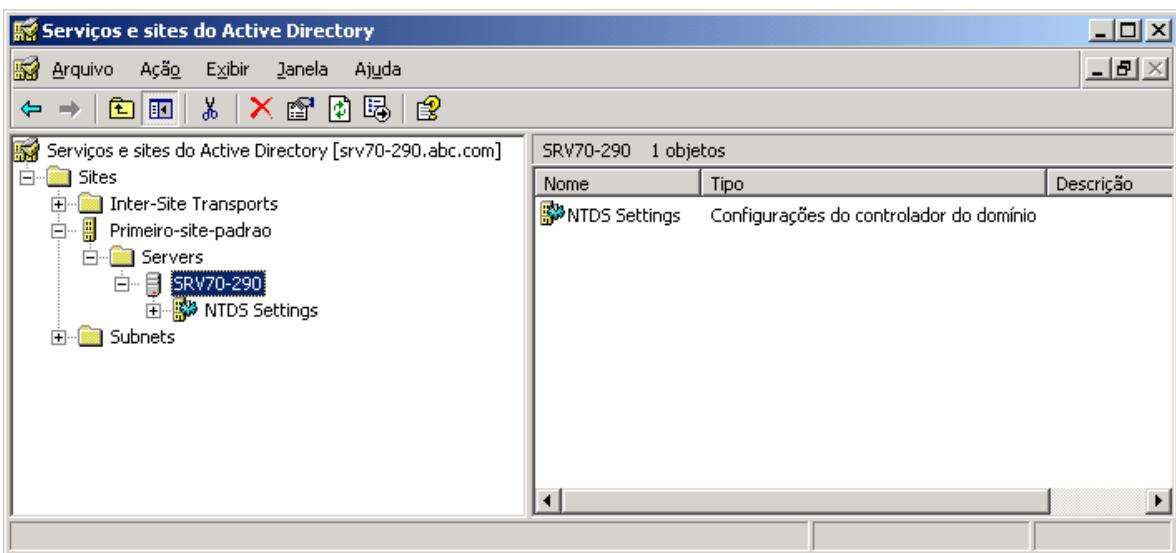


Figura 2.46 Selecionando o DC a ser configurado como Servidor de Catálogo Global.

5. Abaixo do nome do servidor, clique com o botão direito do mouse na opção NTDS Settings. No menu que é exibido clique em Propriedades.
6. Será exibida a janela NTDS Settings com a guia Geral selecionada. Para transformar o DC selecionado em um Servidor de Catálogo Global, marque a opção Catálogo Global, conforme exemplo da Figura 2.47.
7. Clique em OK e pronto, o DC MCSE70-290 será configurado como Servidor de Catálogo Global e, além da cópia completa de todos os objetos do seu próprio domínio, passará a ter uma cópia parcial (somente alguns atributos), de todos os objetos dos demais domínios, conforme explicado no Capítulo 1.

## Conclusão

Neste capítulo você foi apresentado aos principais conceitos do Active Directory. Este conhecimento teórico é fundamental e serve de suporte para todos os demais capítulos deste livro, onde sempre irei utilizar conceitos apresentados neste capítulo. Entender os fundamentos teóricos do Active Directory é fundamental. Sem isso você até pode seguir uma receita de bolo, passo-a-passo, mas dificilmente entenderá exatamente o que está fazendo.

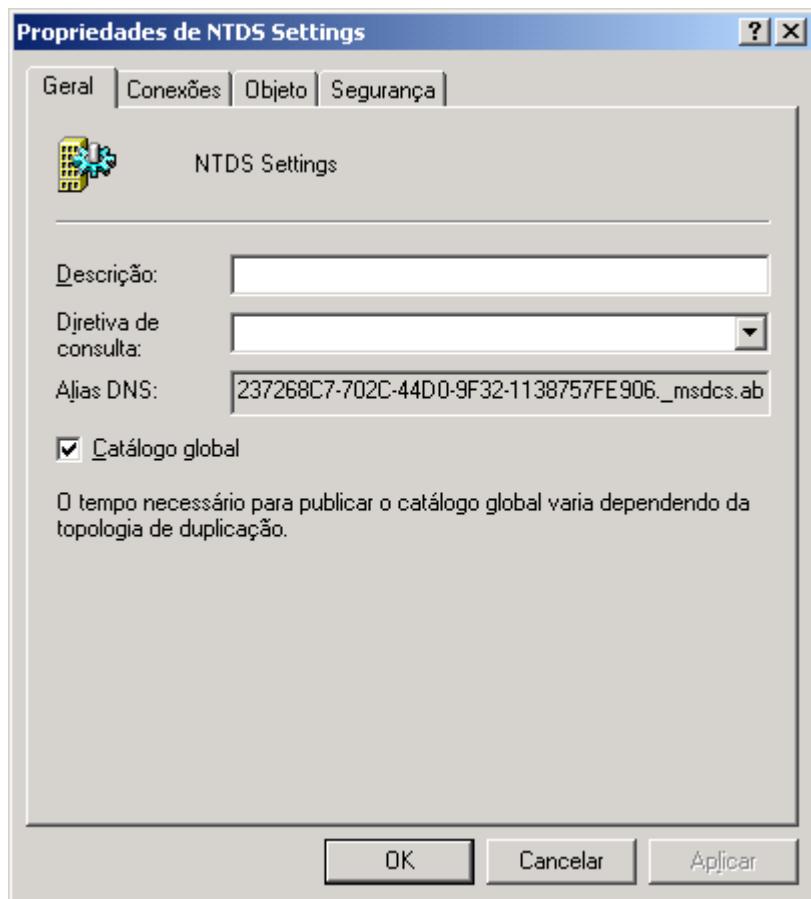


Figura 2.47 Transformando o DC selecionado em um Servidor de Catálog Global.

Você aprendeu que o Active Directory, basicamente, é uma base de dados e um conjunto de serviços. Na base de dados do Active Directory estão informações sobre todos os objetos da rede, tais como: usuários, grupos, computadores, impressoras, servidores, domínios, unidades organizacionais e assim por diante. Os serviços do Active Directory permitem a manutenção, atualização e replicação desta base de dados, além de fornecer serviços de pesquisa de objetos.

Iniciei o capítulo apresentando o conceito de diretório. Você aprendeu que até mesmo uma lista telefônica pode ser considerada um exemplo de diretório. Você também ficou sabendo que, na prática, existem vários diretórios na rede das empresas. Por isso que o usuário é obrigado a utilizar diferentes senhas para acessar os diferentes sistemas da empresa. De uma maneira simplificada, para cada diretório existente na rede, uma senha.

Também falei sobre as diferenças entre uma rede baseada no conceito de Workgroup e uma rede baseada em diretórios. A rede baseada em Workgroup é difícil de administrar, sendo recomendada somente para pequenas redes, onde existe um único servidor e não mais do que 10 estações de trabalho. Já redes baseadas em diretórios podem crescer e atender a milhares de usuários e dezenas, até mesmo centenas ou milhares de servidores.

Neste momento mostrei o papel do Windows Server 2003 dentro de uma rede baseada em domínios. Um servidor baseado no Windows Server 2003 pode assumir o papel de DC (Domain Controller – Controlador de domínio). No DC fica uma cópia integral da base de dados do Active Directory. Esta base pode sofrer alterações, as quais devem ser replicadas para os demais DCs do domínio.

Em seguida, já tratando sobre o Active Directory, apresentei o conceito de Domínio. Você aprendeu que um domínio, basicamente, é uma divisão lógica da rede. Um domínio consiste também em uma divisão administrativa e de segurança.

Um domínio pode conter diversos objetos, tais como usuários, grupos de usuários, contas de computadores e assim por diante. Todas estas informações ficam armazenadas na base de dados do Active Directory.

A utilização de Unidades Organizacionais ajuda a eliminar alguns problemas de Administração existentes no NT Server 4.0. Com o uso de Unidades Organizacionais é possível fazer uma divisão lógica do domínio, divisão esta baseada em critérios geográficos ou funcionais. Com o uso de Unidades Organizacionais é possível delegar permissões administrativas a nível da Unidade Organizacional e não somente no nível de domínio, como ocorria com o NT Server 4.0.

Você também aprendeu sobre os tipos de grupos existentes no Active Directory. Mostrei que, quanto ao tipo, os grupos são divididos em Grupos de distribuição e Grupos de segurança. Somente grupos de segurança podem ser utilizados para atribuir permissões de acesso a recursos tais como pastas compartilhadas, impressoras compartilhadas, etc. Os grupos de distribuição são utilizados para envio de mensagens de e-mail para todos os membros do grupo.

Os grupos também são classificados quanto ao escopo, em: Universais, Globais e Locais. Um grupo Universal pode conter membros e outros grupos de qualquer domínio e pode receber permissões de acesso em recursos de qualquer domínio. Os grupos Globais podem ter como membros somente objetos do próprio domínio, porém podem receber permissões de acesso em objetos de outros domínios. Os grupos locais podem conter membros de outros domínios, mas somente podem receber permissões de acesso a recursos do próprio domínio. Em seguida apresentei vários estudos de caso para fixação dos conceitos de grupos, principalmente em relação ao escopo de grupos: Universal, Global e Local.

Você pode dividir a rede da sua empresa em vários domínios, criando assim uma árvore de domínios. Mostrei que dentro da árvore deve ser utilizado um espaço de nomes contínuo, no qual o nome do objeto filho deve conter todo o nome do objeto pai.

Seguindo o estudo do Active Directory, apresentei o importante conceito de Catálogo Global. Pelo menos um DC de cada domínio atua também como Servidor de Catálogo Global. No DC está a cópia completa da base de dados do domínio do DC. No Servidor de Catálogo Global está a cópia completa da base de dados do domínio do Servidor de Catálogo Global e uma cópia parcial (somente alguns atributos) da base de dados de todos os demais domínios da floresta. O Servidor de Catálogo Global ajuda a reduzir o tráfego de rede e a agilizar as pesquisas realizadas no Active Directory. O Administrador pode configurar mais DCs do domínio para que também atuem como Servidores de Catálogo Global.

Avançando um pouco mais, você aprendeu que é possível reunir duas ou mais árvores de domínios para formar uma floresta. O que caracteriza uma árvore de domínios é o espaço de nomes contínuo, conforme descrito anteriormente. É possível juntar duas ou mais árvores para formar uma floresta de domínios.

Outro conceito muito importante é o de relações de confiança. Neste tópico fiz um pequeno histórico sobre como eram as relações de confiança na época do NT Server 4.0. Você aprendeu que no NT Server 4.0, as relações de confiança eram unidirecionais, não transitivas e tinham que ser criadas e mantidas manualmente pelo administrador. Já no Windows 2000 Server e no Windows Server 2003, as relações de confiança são criadas automaticamente, são transitivas e são bi-direcionais.

Em seguida foi o momento de falar sobre a divisão física do Active Directory e sobre replicação. Domínios, árvores, florestas, etc, constituem a estrutura e a divisão lógica do Active Directory. O conceito de sites representa a estrutura e a divisão física do Active Directory. O principal objetivo de dividir a rede em sites é para que o KCC (serviço do Active Directory responsável por determinar um esquema de replicação otimizado) possa determinar qual o melhor esquema de replicação a ser utilizado, mantendo um equilíbrio entre o tempo de atualização dos DCs e a quantidade de informações de replicação a ser gerada nos links de WAN.

Você também aprendeu um pouco sobre os níveis de funcionalidade de um domínio e também da floresta.

Reipo, os conceitos teóricos vistos neste capítulo são fundamentais e serão necessários em todos os demais capítulos do livro. Se você ficou com dúvida sobre um dos conceitos, peço que você volte e releia o referido conceito. É muito importante que você entenda os diversos elementos que compõem o Active Directory, tanto em sua estruturação lógica, quanto em sua estruturação física.

Em seguida partimos para a prática. Você aprendeu a instalar o Active Directory, usando o comando dcpromo e também a ferramenta administrativa Gerenciar o servidor. Inicialmente foi feito um exercício onde foi criado um novo domínio, chamado abc.com. Em seguida você aprendeu a rebaixar um DC de volta a member server. Em seguida mostrei como criar um novo DC em um domínio já existente.

Também mostrei quais as mudanças feitas pelo assistente de instalação do Active Directory, quando um servidor é promovido a DC.

O próximo passo foi aprender um pouco mais sobre os níveis de funcionalidade de domínio e de floresta. Para finalizar o capítulo apresentei a parte prática para algumas ações do Active Directory, tais como:

- ◆ Definir o nível de funcionalidade do domínio.
- ◆ Definir o nível de funcionalidade da floresta.
- ◆ Configurar relações de confiança manualmente.
- ◆ Definir um servidor como Servidor de Catálogo Global.

A partir do próximo capítulo passarei a apresentar as ferramentas de administração do Windows Server 2003. A partir do Capítulo 4 você aprenderá a utilizar as diversas ferramentas administrativas do Windows Server 2003.

# Introdução

Nos Capítulos 1 e 2, apresentei uma série de fundamentações teóricas. Desde uma retrospectiva da época do modelo baseado em mainframe, passando pela evolução do modelo Web, chegando em redes baseadas em diretórios. Também apresentei uma descrição completa dos elementos que compõem o Active Directory (Capítulo 2).

Você também aprendeu a instalar o Windows Server 2003. Agora já está mais do que na hora de começar a trabalhar e a aprender a utilizar os recursos de administração do Windows Server 2003, cobrados no Exame 70-290. É isso que mostrarei para você a partir deste capítulo, ou seja, a parte prática, a famosa “mão na massa”.

No Windows Server 2003, a exemplo do que já acontecia no Windows 2000 Server, todas as ferramentas administrativas são baseadas em uma interface padrão e em um conjunto de tecnologias comuns. Toda ferramenta administrativa é conhecida como Console. Assim temos:

- ◆ Console para administração de contas de usuários e grupos.
- ◆ Console para administração de sites.
- ◆ Console para administração do Schema.
- ◆ Console para monitoramento de desempenho.
- ◆ Console para acessar os logs de auditoria e assim por diante.

Todos os consoles tem uma interface semelhante. A interface das ferramentas administrativas é muito parecida com a interface do Windows Explorer. Temos um painel a esquerda, onde estão disponíveis as diversas opções relacionadas com o console que está sendo utilizado. Ao selecionar uma opção no painel da esquerda, são exibidas as opções relacionadas no painel da direita. Na Figura 3.1 você tem um exemplo do console de administração de pastas compartilhadas em um servidor:

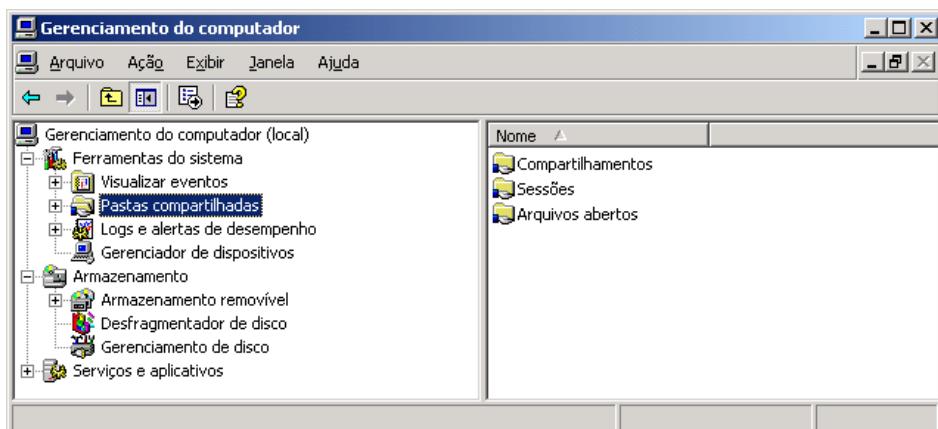


Figura 3.1 Exemplo de um console de administração.

As ferramentas administrativas são baseadas em dois elementos. O primeiro é o MMC – Microsoft Management Console. O MMC é o programa no qual são

# CAPÍTULO

# 3

## Consoles de Administração e Snap-in - interface padrão para Administração do Windows Server 2003

carregadas as diferentes ferramentas administrativas, isto é, os diferentes consoles de administração. Porém o MMC sozinho não serve para absolutamente nada, ou seja, não tem funcionalidade nenhuma. Para que o MMC se torne útil deve ser carregado um Snap-in. O Snap-in é o elemento que contém a definição de todas as funcionalidades de um console administrativo. O que diferencia um console de outro é o Snap-in que é carregado. De uma maneira simples até poderia dizer que: Console = MMC + Snap-in, ou em outras palavras: Um console é igual a um Snap-in carregado no MMC.

Neste capítulo vou explorar o conceito de MMC, Snap-in e consoles, através de exemplos práticos. O objetivo deste capítulo é apresentar estes conceitos e ensinar a trabalhar com a interface de um console administrativo. Também mostrarei como criar consoles personalizados, definir níveis de acesso a estes consoles e enviá-los para outros administradores.

## Microsoft Management Console (MMC) e Snap-in – Conceitos

O MMC foi criado para servir como uma interface unificada para a administração e gerenciamento dos mais variados recursos do Windows 2000, está presente no Windows XP e é também a base das ferramentas administrativas do Windows Server 2003 (na realidade o IIS 4.0, no NT Server 4.0 já utilizava o MMC). Em versões anteriores do Windows, como por exemplo o Windows NT Server 4.0 e 3.51, cada ferramenta administrativa apresentava uma interface diferente. Por exemplo a interface do User Manager for Domains (o qual é utilizado para criar contas e grupos de usuários em um servidor no NT Server 4.0) era completamente diferente da interface de outras ferramentas administrativas, tais como o Disk Manager (utilizado para gerenciar os discos rígidos e partições). Com isso o administrador precisava aprender a utilizar uma série de interfaces diferentes.

O MMC resolve esse problema, fornecendo uma interface padrão para todas as ferramentas administrativas. Na verdade o MMC vem sendo utilizado em alguns programas há algum tempo, como o Internet Information Server 4.0 (servidor Web da Microsoft), Proxy Server 2.0 (Firewall para proteção da rede interna), Microsoft SQL Server 7.0 e 2000 (servidor de Banco de dados da Microsoft), dentre outros programas da Microsoft. Com o Windows Server 2003 é disponibilizada a versão 2.0 do MMC.

Na prática o MMC por si só não oferece nenhuma funcionalidade. O MMC fornece uma maneira padronizada para a criação de ferramentas administrativas. Toda a funcionalidade do MMC é fornecida por aplicações de gerenciamento e administração chamadas Snap-Ins, o MMC funciona simplesmente como um “hospedeiro” para os diversos Snap-Ins. Conforme mostrarei nos exemplos práticos a seguir, ao abrir o MMC, nenhuma funcionalidade estará disponível, até que seja carregado um Snap-In. Por exemplo, quando você acessa uma ferramenta administrativa, como o Gerenciamento do computador, na prática está carregando o MMC e, dentro dele, uma Snap-In projetado para realizar um conjunto de funções administrativas. O conjunto MMC + Snap-In é conhecido como Console ou Console de administração.

Um console é composto por uma janela dividida em dois painéis, muito semelhante à janela do Windows Explorer. O painel da esquerda exibe a árvore de console, com as diversas opções do Snap-in carregado atualmente, idêntica a árvore de pastas e subpastas do Windows Explorer. A árvore de console mostra os itens que estão disponíveis em um determinado console. O painel da direita contém o painel de detalhes. O painel de detalhes mostra as informações e funções relativas ao item que está selecionado no painel da esquerda. Quando você clica em diferentes itens da árvore de console, as informações no painel de detalhes são alteradas. O painel de detalhes pode exibir vários tipos de informações, como páginas da Web, elementos gráficos, gráficos, tabelas e colunas.

Na Figura 3.2, mostro um exemplo de um console do MMC, no qual é exibido o console Gerenciamento do computador. Observe a divisão em dois painéis, muito parecida com a janela do Windows Explorer. Também observe que existe

uma opção – Usuários e grupos locais, a qual é utilizada para fazer o gerenciamento/administração de contas de usuários e de grupos em um Member Server ou em um servidor que não faz parte de um domínio.

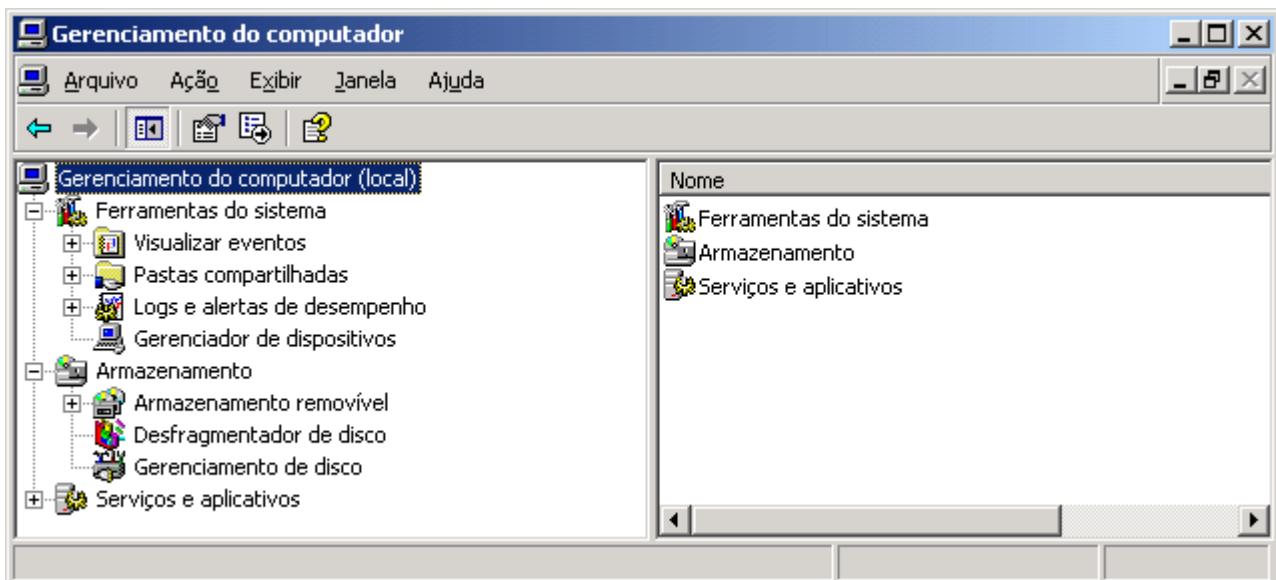


Figura 3.2 O console Gerenciamento do computador.

Cada console possui seus próprios menus e sua própria barra de ferramentas, separados dos menus e da barra de ferramentas da janela principal do MMC, que ajudam o usuário a executar tarefas.

O Windows Server 2003 já vem com uma série de consoles pré-configurados, os quais estão disponíveis através da opção Ferramentas administrativas: Iniciar -> Ferramentas administrativas. As opções disponíveis no menu Ferramentas administrativas variam dependendo do servidor ser um DC ou não. Por exemplo, quando você instala o Active Directory, transformando um member server em um DC, novas opções são instaladas no menu Ferramentas administrativas, conforme descrito no Capítulo 2. Quando você instala um novo serviço, como por exemplo o DHCP, uma nova opção é adicionada ao menu Ferramentas administrativas. Esta nova opção é o console de administração do serviço DHCP.

Você pode utilizar o MMC para uma série de atividades, tais como:

- ◆ Realizar a maioria das tarefas administrativas do dia-a-dia, tais como administração de contas de usuários, grupos e computadores, gerenciamento dos logs de segurança, monitoração de desempenho, administração do Active Directory e assim por diante.
- ◆ Fazer o gerenciamento e a administração de uma maneira centralizada, usando o MMC para conectar-se as ferramentas administrativas de outros servidores, remotamente através da rede. Por exemplo, você pode utilizar o console Gerenciamento do computador para conectar-se a qualquer computador da rede, desde que você tenha as devidas permissões. Com isso você pode administrar uma série de tarefas remotamente.

**NOTA:** Para a administração de contas de usuários e grupos, em servidores configurados como DCs, é utilizado o console Usuários e Computadores do Active Directory.

**NOTA:** Os consoles que foram criados com as versões anteriores do MMC (versões 1.1 e 1.2) podem ser lidos pelo MMC 2.0. No entanto, para salvar ou modificar os consoles antigos, o usuário será solicitado a fazer a conversão para o formato utilizado pelo MMC 2.0.

- ◆ Fazer administração e gerenciamento remoto, desde que você possua as permissões para isso. Veja item anterior.
- ◆ Criar consoles personalizados e definir permissões para delegar funções para um ou mais usuários.

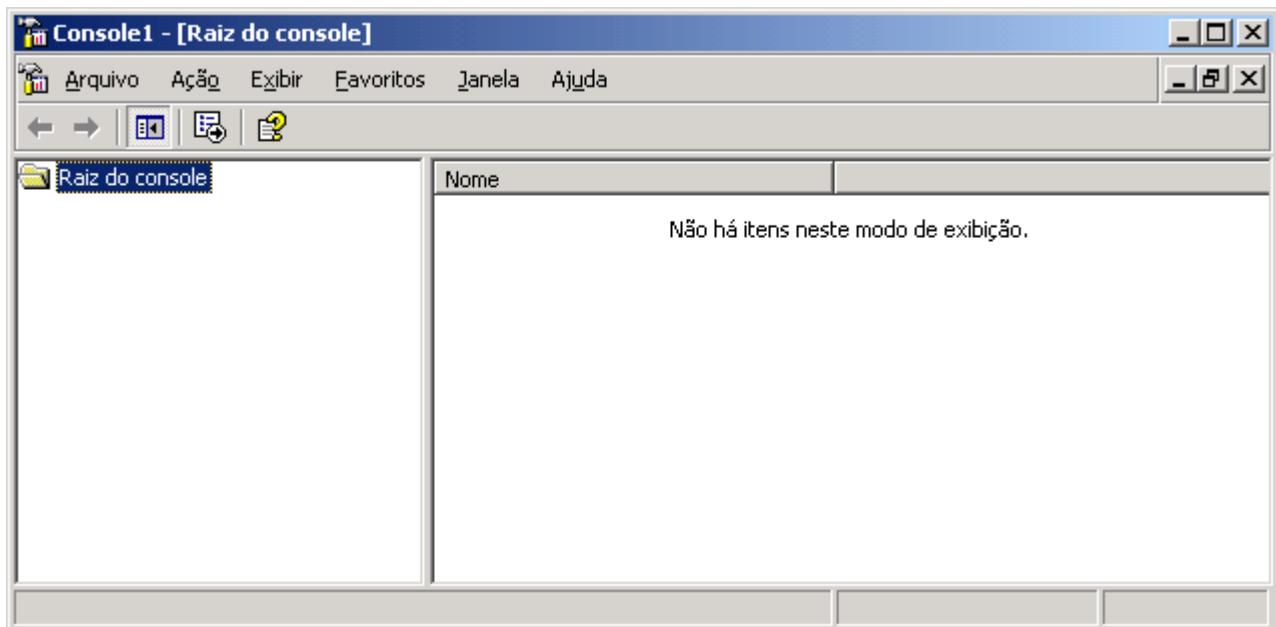
Quando você abre o console para administração de contas de usuários e grupos, na verdade está abrindo o MMC e carregando o Snap-In especialmente projetado para realizar as tarefas administrativas relativas à administração de contas de usuários e Grupos. É possível ter um ou mais Snap-In carregados, simultaneamente, no MMC, de tal forma que em uma mesma janela, seja possível realizar as mais variadas tarefas administrativas.

Vou apresentar alguns exemplos práticos de uso do MMC e de alguns consoles de administração.

Exemplo 01: Abrir o MMC sem nenhum Snap-In carregado. Conforme você poderá conferir na prática, o MMC em si, não oferece nenhuma funcionalidade. Usarei este exercício apenas para mostrar, para reforçar a ideia de que o MMC em si não oferece funcionalidade nenhuma. Funcionalidades são fornecidas pelos Snap-Ins que são carregados no MMC.

Para abrir o MMC sem nenhum Snap-In Carregado, faça o seguinte:

1. Faça o logon como Administrador ou com uma conta com permissão de Administrador.
2. Selecione o comando Iniciar -> Executar.
3. Na janela que surge, no campo Abrir digite mmc e dê um clique em OK.
4. Será aberta uma janela do MMC com um novo console chamado Console 1, conforme indicada na Figura 3.3. Esta janela mostra o MMC sem nenhum Snap-In Carregado.



**Figura 3.3 MMC sem nenhum Snap-In carregado.**

5. Feche o MMC aberto anteriormente.

Agora você irá abrir o MMC com alguns Snap-Ins já carregados. Também irá analisar a interface dos consoles abertos.

Exemplo 2: Para abrir o MMC para Gerenciamento do Computador, siga os passos indicados a seguir:

1. Se não estiver logado, faça o logon com uma conta com permissão de Administrador.

2. Abra o console Gerenciamento do computador: Iniciar -> Ferramentas administrativas -> Gerenciamento do computador.
3. Será aberto o console Gerenciamento do computador, indicado anteriormente na Figura 3.2.

A maneira de utilizar e navegar na janela de um console do MMC é exatamente igual à utilizada no Windows Explorer. Agora você irá “navegar” através do painel da esquerda e quando um elemento do painel da esquerda for selecionado, o seu conteúdo/detalhes será exibido no painel da direita.

Além disso os menus e botões da barra de ferramentas vão se modificando, dependendo do elemento selecionado. Isso porque as ações que podem ser executadas, por exemplo, quando uma conta de usuário está selecionada, são diferentes das ações que podem ser executadas quando está selecionado um objeto do tipo grupo. Essa mudança nos menus e na barra de ferramentas serve para refletir quais as ações são possíveis em relação ao objeto selecionado.

4. Para abrir a pasta Compartilhamentos, conforme indicado na Figura 3.4, dê um clique no sinal de + ao lado da opção Ferramentas do sistema. Nas opções que são abertas clique no sinal de + ao lado de Pastas compartilhadas.
5. Para ver uma listagem dos compartilhamentos disponíveis, clique em Compartilhamentos, abaixo de Pastas compartilhadas. Será exibida a lista de compartilhamentos disponíveis no servidor, conforme indicado na Figura 3.4:

| Nome de compartilhamento | Caminho da pasta   | Tipo    | Nº de conexões |
|--------------------------|--------------------|---------|----------------|
| ADMIN\$                  | C:\WINDOWS         | Windows | 0              |
| C\$                      | C:\                | Windows | 0              |
| IPC\$                    |                    | Windows | 0              |
| NETLOGON                 | C:\WINDOWS\SYSV... | Windows | 0              |
| SYSVOL                   | C:\WINDOWS\SYSV... | Windows | 0              |

Figura 3.4 Listagem de compartilhamentos.

6. Feche o MMC para Gerenciamento do Computador.

Um MMC com um ou mais Snap-Ins carregados é chamado de um Console . Quando você instala o Windows Server 2003, diversos consoles administrativos são adicionados para que o administrador possa executar as tarefas administrativas mais comuns. Nos demais capítulos deste livro, você utilizará os consoles pré-configurados, para realizar operações tais como verificar o desempenho do computador e acessar o log de eventos do Windows Server 2003.

## Criando consoles personalizados

Além dos consoles pré-configurados, você também pode criar consoles personalizados, os quais podem ser salvos em arquivos com a extensão .MSC. Depois para abrir um console pré-configurado basta abrirmos o respectivo arquivo .msc.

A criação de consoles personalizados é especialmente útil, quando o Administrador tem que delegar tarefas para um outro usuário. Vamos supor que você queira criar um console onde somente seja adicionado o Snap-In para gerenciar

usuários e grupos. Depois de criado este console, você envia o arquivo .msc para um usuário responsável pelo gerenciamento de usuários e grupos. Mostrarei que é possível criar o console de tal maneira que o usuário que vai utilizá-lo não possa modificá-lo, adicionando ou excluindo Snap-Ins. O resultado prático é que o usuário responsável pela administração de usuários e grupos, recebe um console personalizado, somente com as opções relacionadas à administração de usuários e grupos.

Exemplo 01: Vamos supor que você queira criar um console somente para administrar discos e volumes. Neste exemplo você abrirá o MMC sem nenhum Snap-In. Depois irá carregar apenas o Snap-In para administração de Discos e volumes. O próximo passo é salvar este console em um arquivo com a extensão .msc. Para este exemplo, o console será salvo com o nome de administra\_discos.msc na Área de trabalho do usuário.

Para abrir o MMC sem nenhum Snap-In Carregado, siga os seguintes passos:

1. Faça o logon com uma conta com permissão de Administrador.
2. Selecione o comando Iniciar -> Executar.
3. Na janela que surge, no campo Abrir, digite mmc e dê um clique em OK.
4. Será aberto o MMC sem nenhum Snap-In Carregado.

Para carregar apenas o Snap-In para administração de contas de discos e volumes, siga os seguintes passos:

5. Com o MMC carregado anteriormente, selecione o comando Arquivo -> Adicionar/remover snap-in .." (File -> Add/remove snap-in...). Será exibida a janela Adicionar/remover snap-in. Observe que não existe nenhum snap-in adicionado e a lista está vazia.
6. Na janela Adicionar/remover snap-in, dê um clique no botão Adicionar.
7. Será exibida a janela Adicionar snap-in autônomo. Nesta janela é exibida uma listagem com todos os snap-ins disponíveis, isto é, instalados no computador.
8. Localize na listagem o seguinte snap-in: Gerenciamento de disco, conforme indicado na Figura 3.5 e dê um clique sobre ele para selecioná-lo.

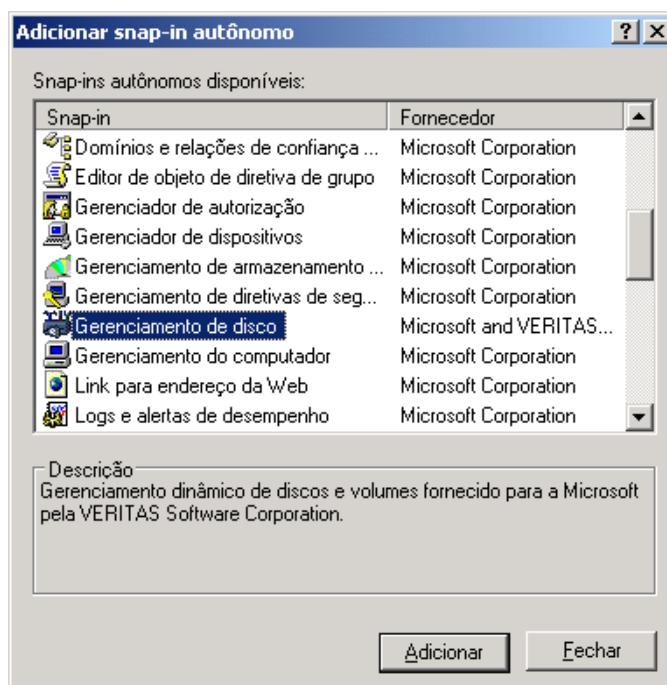


Figura 3.5 Adicionando o snap-in Gerenciamento de disco.

9. Dê um clique no botão Adicionar.
10. Surge a janela Escolher máquina de destino. Essa janela permite que você defina em qual computador você quer gerenciar as contas de usuários e grupos. Neste momento você pode gerenciar usuários e grupos de um computador remoto, desde que você tenha permissão para isso.
11. Por padrão vem selecionada a opção Computador local. Aceite a opção padrão e dê um clique no botão Concluir.
12. Você estará de volta a janela Adicionar snap-in autônomo. Caso você queira será possível adicionar outros snap-ins. Como não será adicionado mais nenhum snap-in, dê um clique no botão Fechar.
13. Você estará de volta à janela Adicionar / remover snap-in. Observe que o snap-in Usuários e grupos locais (local) já aparece na listagem, conforme indicado na Figura 3.6.

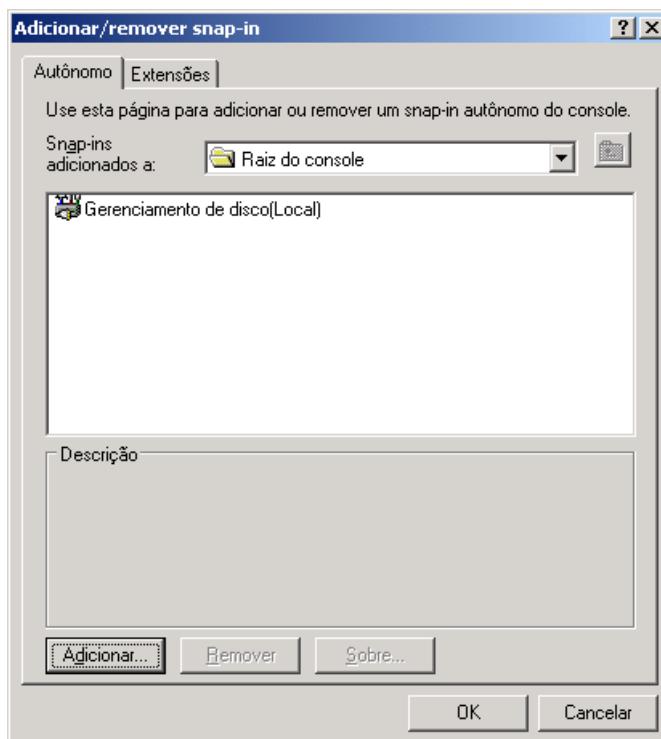


Figura 3.6 Snap-in Gerenciamento de disco, já adicionado.

14. Dê um clique em OK para fechar a janela Adicionar/remover snap-in.
15. Você estará de volta ao MMC, agora com o snap-in Gerenciamento de disco já carregado, conforme indicado pela Figura 3.7.

**NOTA:** O local entre parênteses indica o computador local.

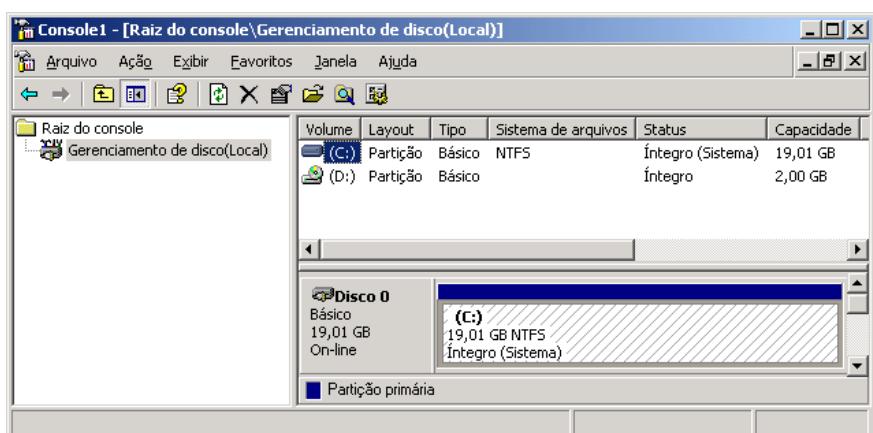


Figura 3.7 Console com um snap-in Gerenciamento de disco.

Agora é hora de salvar o console com o nome de administra\_discos.msc. O console será salvo na Área de trabalho do usuário logado.

Para salvar o console com o nome de administra\_usuarios.msc, faça o seguinte:

16. Selecione o comando Arquivo -> Salvar.
17. Será aberta a janela Salvar como. Nesta janela existe uma barra de atalhos, no lado esquerdo da janela. Nesta barra estão disponíveis os seguintes atalhos: Documentos recentes, Desktop, Meus documentos, Meu computador e Meus locais de rede. Para acessar a Área de trabalho, dê um clique no atalho Desktop. no campo nome do arquivo digite: administra\_discos.msc. A janela Salvar como deve estar conforme indicado na Figura 3.8.

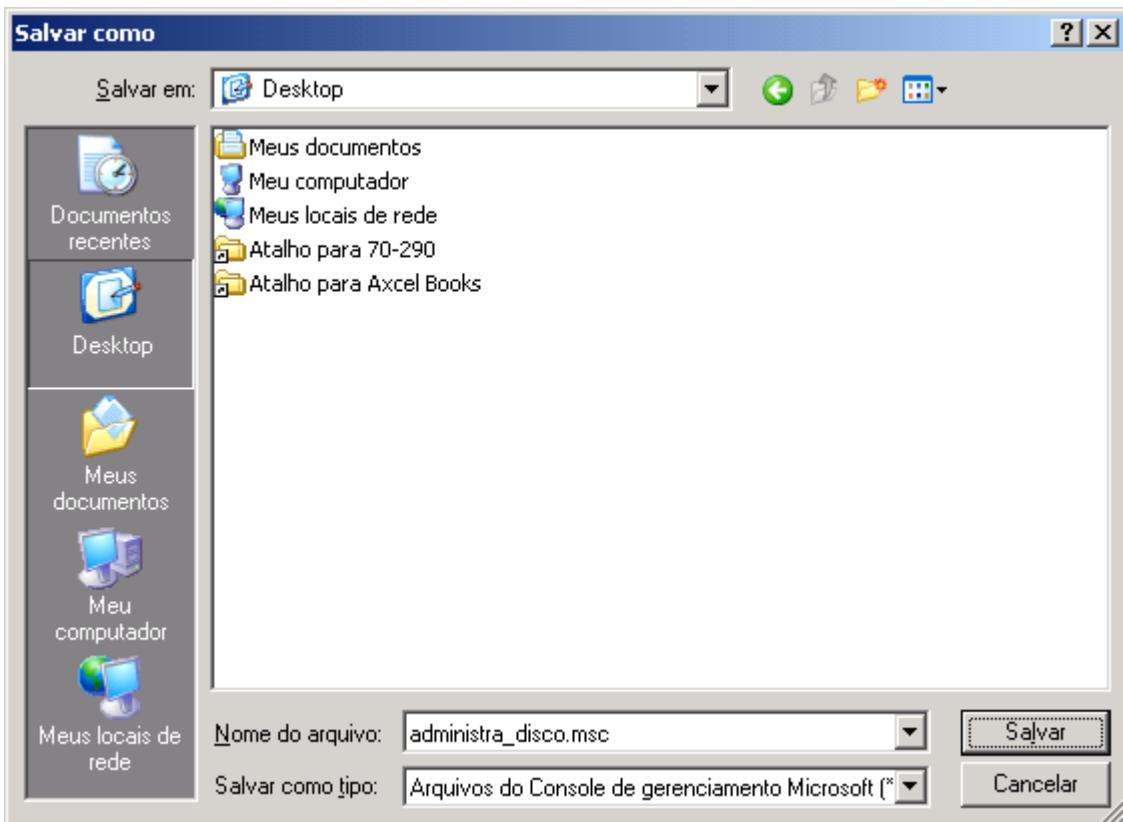


Figura 3.8 Salvando o console recém criado, na Área de trabalho.

18. Dê um clique no botão Salvar.

Agora você irá definir as configurações de segurança para o console recém criado. Ao criar um novo console, é possível definir diferentes modos de operação para o console. A cada modo de operação está associada um conjunto de operações permitidas. Ao criar um console personalizado, como o console administra\_discos , que recém foi criado, você pode atribuir a ele uma de duas opções gerais de acesso: modo de autor ou modo de usuário. Existem, por sua vez, três níveis de modo de usuário, de forma que existem quatro opções para acesso padrão a um console:

- ◆ **Modo de autor:** Concede aos usuários acesso completo a toda a funcionalidade do MMC, inclusive a capacidade de adicionar ou remover snap-ins, criar novas janelas, modos de exibição e exibir todas as partes da árvore de console.
- ◆ **Modo de usuário - acesso completo:** Concede ao usuário acesso completo a todos os comandos de gerenciamento de janelas e à árvore de console fornecida. Impede os usuários de adicionar ou remover snap-ins ou alterar as propriedades do console.

- ◆ **Modo de usuário – acesso limitado, várias janelas:** Concede ao usuário acesso somente às áreas da árvore de console visíveis quando o console foi salvo. O usuário pode criar novas janelas, mas não podem fechar as existentes.
- ◆ **Modo de usuário – acesso limitado, janela única:** Concede acesso ao usuário somente às áreas da árvore de console visíveis quando o console foi salvo. Impede que o usuário abra novas janelas.

Estas opções são acessíveis através do comando Arquivo -> Opções.

Você pode atribuir o modo de autor a um console para conceder acesso completo a todos os recursos do MMC, incluindo a capacidade de adicionar ou remover snap-ins, criar novas janelas, criar exibições de painel de tarefas e tarefas, adicionar itens à lista Favoritos e exibir todas as partes da árvore de console. Ao selecionar uma das opções do modo de usuário, os recursos de criação que provavelmente não serão necessários a um usuário serão eliminados. Por exemplo, se você atribuir a opção Modo de usuário - acesso completo a um console, todos os comandos de gerenciamento de janelas e o acesso completo à árvore de console serão fornecidos, mas o usuário estará impedido de adicionar ou remover snap-ins ou alterar as propriedades do console.

As alterações feitas nos consoles que estiverem no modo de autor e nos consoles que estiverem no modo de usuário serão salvas de maneira diferente. Se você estiver trabalhando com um console no modo de autor, será solicitado a salvar suas alterações ao fechá-lo. No entanto, se você estiver trabalhando com um console no modo de usuário e tiver desmarcado a caixa de seleção Não salvar alterações neste console, disponível quando se clica em Opções no menu Arquivo, as alterações serão automaticamente salvas quando você fechar o console.

Se uma das seguintes condições se aplicar, o modo padrão de um console será ignorado e um console será aberto no modo de autor:

- ◆ O MMC já está aberto quando um console é aberto.
- ◆ Um console é aberto através do comando de menu de atalho Autor.
- ◆ Um console é aberto no prompt de comando com a opção /a.

O acesso ao modo de autor do MMC é desnecessário para usuários que não precisam criar ou alterar os consoles do MMC. Um administrador de sistema pode definir configurações de perfil de usuário para impedir que os usuários abram o MMC no modo de autor. Para isso, ele deve inibir a opção /a ou a opção do menu de atalho.

Para configurar o modo de acesso para o console administra\_usuarios.msc, criado anteriormente, siga os passos indicados a seguir:

1. Selecione o comando Arquivo -> Opções.
2. Será aberta a janela opções. Dê um clique na guia Console.
3. Na lista Modo de console, selecione a opção: Modo de usuário – acesso limitado, janela única. Observe que as opções “Não salvar alterações neste console” e “Permitir que o usuário personalize opções” foram habilitadas, sendo que você pode marcá-las ou desmarcá-las de acordo com as necessidades de cada caso.
  - ◆ Não salvar alterações neste console: Se esta opção estiver marcada, o usuário não poderá fazer alterações no console, tais como adicionar ou remover snap-ins.
  - ◆ Permitir que o usuário personalize opções: Especifica se os usuários podem adicionar janelas cujas raízes se encontram em itens do console. Ou seja, clicar em um item do painel da esquerda e selecionar a opção Nova janela a partir daqui. Esta é uma opção interessante. Por exemplo, se o usuário clicar com o botão direito do mouse em uma opção do console e, no menu que é exibido, clicar na opção Nova janela a partir daqui, será aberto um novo console, somente com a opção selecionada. Esta é uma maneira de criar consoles com opções ainda mais específicas. Se esta opção estiver desmarcada, a opção Nova janela a partir daqui não estará disponível.

4. Marque as duas opções descritas anteriormente. Sua janela deve estar conforme indicado na Figura 3.9

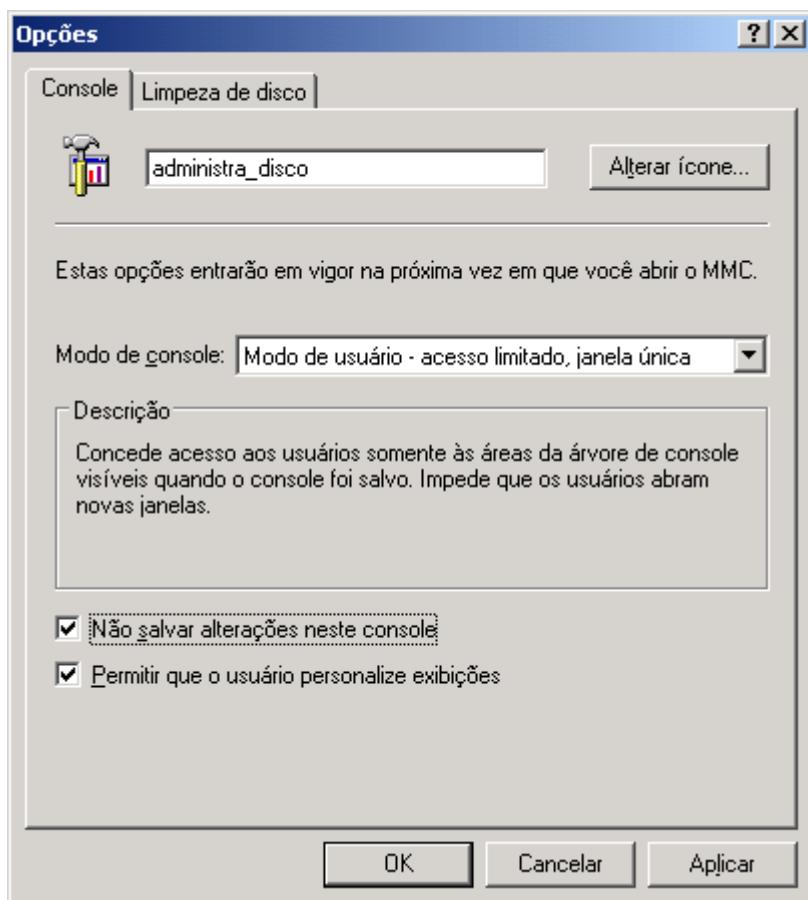


Figura 3.9 Definindo opções de Modo de console.

5. Dê um clique no botão OK.
6. Salve o console novamente, usando o comando Arquivo -> Salvar.
7. Feche o MMC.

Agora você irá abrir o console administras\_disco.msc, criado anteriormente e testar as novas configurações.

Para verificar se o Windows Server 2003 criou um atalho para o console administras\_usuarios.msc, na área de trabalho faça o seguinte.

1. Minimize quaisquer janelas que você tiver abertas.
2. Localize, na Área de trabalho, um atalho para administras\_disco.msc.
3. Dê um clique duplo no atalho para abri-lo.
4. Clique no menu Arquivo. Observe que uma série de opções foram retiradas, isto acontece porque este console foi configurado o console para funcionar no modo: "Modo de usuário - acesso limitado, janela única", o qual concede acesso aos usuários somente às áreas da árvore de console visíveis quando o console foi salvo, impede que os usuários abram novas janelas e também impede que sejam adicionados ou removidos snap-ins. No menu Arquivo estão disponíveis apenas dois comandos: Opções e Sair.

Existem muitas aplicações práticas para a criação de consoles personalizados. Por exemplo, caso um funcionário seja responsável apenas pelo gerenciamento de usuários e grupos, você pode criar um console personalizado somente com

o snap-in necessário. Isso facilita o trabalho, uma vez que a interface fica mais simples e impede o acesso a operações que não fazem parte das atribuições do funcionário.

## Consoles instalados com o Windows Server 2003.

Ao instalar o Windows Server 2003, é instalado um conjunto de consoles pré-configurados, os quais são utilizados para uma variedade de tarefas administrativas. Neste tópico descreverei brevemente os consoles instalados com o Windows Server 2003 e indicarei o capítulo onde as funções associadas com cada console serão estudadas em mais detalhes.

Todos os consoles de administração, instalados com o Windows Server 2003, estão disponíveis através do menu Iniciar -> Ferramentas administrativas, conforme indicado na Figura 3.10:

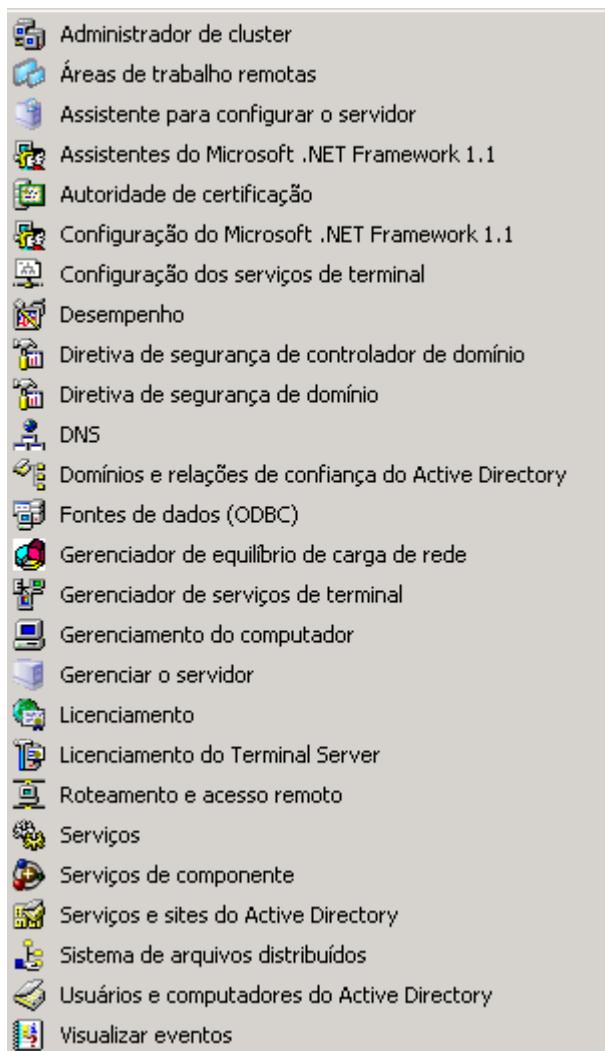


Figura 3.10 Consoles instalados durante a instalação do Windows Server 2003.

A seguir apresento uma breve descrição dos principais consoles:

- ◆ **Autoridade de Certificação:** Este console é utilizado para gerenciar servidores com o Microsoft Certification Services instalado. Com o Microsoft Certification Services, as empresas podem criar e gerenciar seus próprios certificados digitais, sem depender de uma autoridade certificadora externa. O Microsoft Certification Serv-

ices fornece todos os recursos necessários para a implementação de uma estrutura de segurança baseada em certificados digitais. O uso de certificados digitais é recomendado para ambientes altamente seguros, onde questões como autenticação de usuários são fatores preponderantes.

- ◆ **Administrador de cluster:** Um cluster é um conjunto de dois ou mais servidores que atuam em conjunto, aparecendo para os usuários como se fossem um único servidor. Cluster de servidores são utilizados para fornecer redundância (quando um dos servidores fica fora do ar, os serviços continuam sendo disponibilizados pelos demais servidores do cluster) e também para balanceamento de carga, onde as requisições dos clientes são distribuídas entre os servidores do cluster para obter um bom desempenho.
- ◆ **Serviços de componentes:** Este console é utilizado para o registro e gerenciamento de componentes de software. Toda a estrutura e o modelo do Framework .NET é baseado na criação de programas baseados em componentes. Por exemplo, um componente de software pode ser criado com o fim específico de fazer a validação de números de cartão de crédito. Este componente pode ser registrado no servidor e utilizado por quaisquer programas que precisem da funcionalidade de validação de números de cartão de crédito. Isso evita que a mesma funcionalidade tenha que ser codificada repetidas vezes, em cada aplicação onde ela for necessária. Isso também simplifica a atualização dos componentes. Os puristas de “orientação a objetos” que me perdoem, mas isso é reaproveitamento de código na prática, um dos pilares fundamentais da orientação a objetos. No Framework .NET, é recomendada a utilização dos chamados Web Services, como infra-estrutura para disponibilização e utilização de componentes de software. No Capítulo 25 do livro **Windows Server 2003 – Curso Completo**, 1568 páginas, eu falo sobre o Framework .NET, Web Services e o desenvolvimento de aplicações no Windows Server 2003.
- ◆ **Gerenciamento do computador:** Este é um dos consoles mais completos e oferece acesso a uma série de opções de configurações do computador. Vou descrever as opções deste console separadamente.
- ◆ **Ferramentas do sistema:** Visualizador de eventos: Esta opção fornece acesso aos logs de auditoria do sistema. Nos logs de auditoria ficam uma série de informações, tais como quem fez o logon no computador, quais serviços foram iniciados corretamente. Se houve erros na iniciação de um ou mais serviços também é gravado um evento no log de auditoria. Alguns eventos são salvos automaticamente e outros precisam ser configurados pelo administrador, para que sejam gravados no log de auditoria. Por exemplo, o acesso a pastas e arquivos não é gravado, por padrão, nos logs de auditoria. O administrador pode configurar para que o acesso a determinadas pastas e/ou arquivos seja auditado. Por padrão estão disponíveis três categorias de log: Application, Security e System. Descreverei os logs de auditoria em detalhes no Capítulo 10.
- ◆ **Ferramentas do sistema:** Pastas compartilhadas: Esta opção é utilizada para administrar as pastas compartilhadas no servidor. Você tem opção de exibir os compartilhamentos existentes, quais seções foram estabelecidas com cada pasta compartilhada e quais os arquivos estão abertos no momento. Você também tem opção de desconectar os usuários, enviar um aviso aos usuários conectados, etc. Você aprenderá a utilizar esta opção no Capítulo 6.
- ◆ **Ferramentas do sistema:** Usuários e grupos locais: Esta opção dá acesso a lista de contas de usuários e grupos locais do computador. Para computadores configurados como DCs, esta lista não estará acessível. Para DCs somente está acessível a lista de contas de usuários e grupos do domínio ao qual pertence o DC. Para computadores configurados como Member Servers ou como Standalone Servers (servidores que não fazem

---

**NOTA:** Para informações detalhadas sobre o Framework .NET, seus elementos, o conceito de Web Services e o desenvolvimento de aplicações Web baseadas na linguagem ASP.NET, consulte o livro: **“ASP.NET: Uma Nova Revolução na Criação de Sites e Aplicações Web”**.

---

parte de um domínio), estará disponível uma lista de usuários e grupos locais, lista esta que é administrada através das opções da pasta Local Users and Groups.

- ◆ **Ferramentas do sistema –Logs e alertas de desempenho:** Com esta opção você pode coletar dados sobre a desempenho do servidor local ou de um servidor remoto, através da rede. É possível visualizar os dados obtidos usando o Monitor do Sistema (System Monitor), o qual estudaremos no Capítulo 11. Os dados também podem ser exportados para uma planilha de dados como o Excel ou para um banco de dados como o Microsoft Access, o que facilita a criação de relatórios personalizados.
- ◆ **Ferramentas do sistema – Gerenciador de dispositivos:** Esta opção é o mesmo “Gerenciador de Dispositivos”, utilizado para o gerenciamento dos dispositivos de Hardware do computador. Você pode utilizar esta opção para resolver problemas com drivers que não estão funcionando, para desabilitar/habilitar determinados dispositivos e para fazer com que o Windows Server 2003 faça uma nova detecção de Hardware, na busca de novos dispositivos que tenham sido instalados.
- ◆ **Armazenamento – Armazenamento removível:** Esta opção fornece facilidades para que o administrador possa fazer o gerenciamento das mídias de armazenamento, tais como fitas de backup e discos ópticos, bem como o gerenciamento das bibliotecas de armazenamento em hardware, tais como jukeboxes. Com o uso desta opção é possível fazer com que múltiplos programas que precisam de acesso aos dados, compartilhem as mesmas mídias de armazenamento, o que reduz custos e simplifica a administração.
- ◆ **Armazenamento – Desfragmentador de disco:** Esta opção dá acesso ao utilitário de desfragmentação de discos e volumes. A medida que arquivos vão sendo gravados e excluídos em um volume, começa um processo conhecido como fragmentação. No processo de fragmentação, partes do mesmo arquivo são gravadas em pontos diferentes do disco rígido. O resultado prático a medida que a fragmentação aumenta é que o desempenho do volume como um todo começa a cair. Com o utilitário de desfragmentação é possível reduzir a fragmentação em um volume, melhorando novamente o desempenho. Você aprenderá a utilizar este utilitário no Capítulo 5.
- ◆ **Armazenamento – Gerenciamento de discos:** Esta opção é utilizada para fazer o gerenciamento de discos e volumes. Com esta opção é possível criar novos volumes, formata-los. Também é possível criar volumes com redundância à falhas, como por exemplo volumes espelhados e volumes do tipo Raid-5. No Capítulo 5 você aprenderá sobre os diferentes tipos de volumes existentes no Windows Server 2003 e aprenderá a utilizar esta opção para criar novos volumes, gerenciar os volumes existentes, formatar volumes e excluir volumes.
- ◆ **Serviços e aplicativos – Telefonia:** O Windows Server 2003 fornece uma API (Application Program Interface) para integração entre o computador e sistemas de telefonia. Esta API é conhecida como TAPI - Telephony Application Programming Interface. Através da opção Services and Applications – Telephony, o administrador pode gerenciar as configurações da TAPI no servidor local ou em um servidor remoto. Através desta opção você também pode gerenciar os dispositivos de comunicação instalados no servidor, como por exemplo uma placa da fax-modem.
- ◆ **Serviços e aplicativos – Serviços:** Esta opção fornece acesso aos serviços instalados no computador. Um serviço é um programa que fica ativo na memória do servidor, normalmente com a função de atender requisições dos clientes. Por exemplo, o IIS fornece um serviço de hospedagem de páginas Web, o qual após inicializado, fica respondendo a requisições dos clientes para acesso a páginas Web. Existe um serviço que permite o compartilhamento de arquivos (pastas compartilhadas), outro que permite a resolução de nomes (DNS ou WINS) e assim por diante. Através desta opção você pode configurar os diversos serviços instalados no computador. Por exemplo, um serviço pode ser configurado para inicializar automaticamente uma vez que o servidor seja ligado. Com isso mesmo que não seja feito o logon no servidor, o serviço será inicializado automaticamente e responderá às requisições dos clientes. Em diversos capítulos deste livro você utilizará as opções de gerenciamento de serviços.

- ◆ **Serviços e aplicativos – Controle WMI:** Windows Management Instrumentation (WMI) é um serviço disponível no Windows Server 2003, o qual é utilizado para disponibilizar informações sobre os computadores da rede. Estas informações são utilizadas, normalmente, para funções de gerenciamento e administração remota. Um exemplo de inovação do Windows Server 2003 em relação ao padrão WMI, é a possibilidade de aplicar políticas de segurança (GPOs), com base em filtros WMI. Por exemplo, você pode usar um filtro WMI para obter a lista de estações de trabalho da sua rede, as quais tem processador inferior a Pentium de 350 Mhz e menos de 128 MB de RAM. Com base no resultado do filtro WMI você pode aplicar um conjunto de políticas de segurança para este conjunto de computadores.
- ◆ **Serviços e aplicativos – Serviço de indexação:** Esta opção permite que você faça o gerenciamento do serviço de indexação do Windows Server 2003 – Indexing Service. Este serviço extrai informações de um conjunto de documentos e organiza estas informações para que seja fácil pesquisar o conjunto de documentos, com base nas informações extraídas pelo serviço de indexação. As pesquisas podem ser feitas usando a opção Iniciar -> Pesquisar, pode ser um formulário de pesquisa do serviço de indexação ou uma página Web, criada em ASP ou ASP.NET, programada para pesquisar um conjunto de documentos. As pesquisas podem ser feitas com base no conteúdo dos documentos ou com base em informações tais como data de alteração, nome do autor, etc. Após a criação do índice você pode pesquisar os documentos com base em palavras, expressões, frases ou propriedades dos documentos. Por exemplo, você pode pesquisar todos os documentos que contenham a expressão Access 97 ou que contenham as palavras Macros e Excel. O serviço de indexação retorna uma lista dos documentos que atendem aos critérios pesquisados. Para abrir um deste documentos basta dar um clique duplo no respectivo documento.
- ◆ **Assistente para configurar o servidor:** Esta opção abre um assistente para configuração do seu servidor. Este assistente é utilizado para definir um conjunto de configurações, com base no papel que o servidor fará desempenhar na rede. Por exemplo, as configurações definidas para um servidor Web são diferentes das configurações definidas para um servidor que atuará como servidor de arquivos e de impressão. Para cada função que o servidor irá desempenhar existe um conjunto de configurações otimizadas para a respectiva função. Este assistente define, automaticamente, o conjunto de configurações ideais, com base na função que o servidor irá desempenhar. As funções mais comuns que um servidor Windows Server 2003 pode desempenhar em uma rede, estão descritas a seguir:
  - ◆ Controlador de Domínio – DC
  - ◆ Servidor de arquivos
  - ◆ Servidor de impressão
  - ◆ Servidor de aplicações
  - ◆ Servidor de e-mail
  - ◆ Servidor de banco de dados
  - ◆ Servidor de Terminal Services
  - ◆ Servidor de Acesso Remoto e VPN
  - ◆ Servidor DNS
  - ◆ Servidor DHCP
  - ◆ Servidor WINS
  - ◆ Servidor de conteúdo de mídia
  - ◆ Servidor Web
- ◆ **Fontes de dados (ODBC):** Esta opção é utilizada para o gerenciamento de fontes de dados ODBC. O padrão ODBC foi e continua sendo muito utilizado. É uma maneira de facilitar o acesso dos programas a diferentes

fontes de dados. O Administrador cria uma fonte ODBC e os programas se comunicam com a fonte ODBC e não diretamente com a fonte de dados. Este padrão vem sendo menos utilizado, após o lançamento do padrão OLE-DB, o qual é o padrão recomendado pela Microsoft e padrão oficial no Framework .NET. Com a opção Data Sources (ODBC), o administrador pode criar novas fontes ODBC, alterar as fontes existentes e excluir fontes que não sejam mais necessárias.

- ◆ **Sistema de arquivos distribuídos:** O DFS (Distributed File System) é utilizado para simplificar e consolidar o acesso a múltiplas pastas compartilhas na rede. Com o DFS é possível através de um único drive de rede, ter acessos a diversos compartilhamentos, localizados em diferentes servidores. Também é possível criar uma ou mais réplicas de um compartilhamento para fornecer redundância. As configurações do DFS são feitas através desta opção e serão vistas no Capítulo 6.
- ◆ **Visualizar eventos:** Esta opção fornece acesso aos logs de auditoria do sistema. Nos logs de auditoria ficam uma série de informações, tais como quais usuários fizeram o logon no computador, quais serviços foram iniciados corretamente e assim por diante. Se houve erros na iniciação de um ou mais serviços também é gravado um evento no log de auditoria. Alguns eventos são salvos automaticamente e outros precisam ser configurados pelo administrador, para que sejam gravados no log de auditoria. Por exemplo, o acesso a pastas e arquivos não é gravado, por padrão, nos logs de auditoria. O administrador pode configurar para que o acesso a determinadas pastas e/ou arquivos seja auditado. Por padrão estão disponíveis três categorias de log: Application, Security e System. Descreverei os logs de auditoria em detalhes no Capítulo 10. Este é o mesmo console acessado através da opção “Ferramentas do sistema – Visualizador de eventos” do console Gerenciamento do Computador.
- ◆ **Licenciamento:** Este console é utilizado para gerenciamento das licenças e do tipo de licenciamento utilizado pelo servidor. Estão disponíveis os tipos de licenciamento Per Server e Per Device. A seguir descrevo as diferenças entre os dois modos de licenciamento:
  - ◆ **Per Server (Por Servidor):** Esta forma de licenciamento é mais indicado para pequenas empresas, nas quais existe um único servidor com o Windows Server 2003 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 no servidor, este último usuário 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 Licencio 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.
  - ◆ **Per Device (Por Dispositivo):** Neste modo de licenciamento, uma CAL é necessária para cada estação de trabalho que faz a conexão com o servidor, independentemente 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 CALs, uma para cada estação de trabalho. O preço de uma CAL para este modo de licenciamento é maior do que para o Per Server, mas em compensação com uma única CAL, a estação de trabalho pode acessar recursos em qualquer servidor que esteja utilizando o licenciamento Per Device.
- ◆ **Diretivas de segurança locais:** Esta opção não está disponível em DCs. Este console é utilizado para definir as configurações das políticas de segurança locais do servidor. Se o servidor fizer parte de um domínio, ele receberá as políticas de segurança do domínio e também as políticas de segurança locais. Pode até haver conflito entre as duas políticas. Neste caso, qual política irá prevalecer, depende das configurações feitas nas

políticas de segurança do domínio. As políticas de segurança local permitem a definição de uma série de configurações de segurança, tais como: quais contas de usuário podem fazer o logon localmente, quais contas de usuário podem acessar o computador através da rede, se o botão Desligar deve estar habilitado ou não durante o logon, quais contas de usuário podem acessar o drive de disquete e assim por diante. São centenas de configurações, as quais serão vistas no decorrer deste livro.

- ◆ **Gerenciar o servidor:** Este é um verdadeiro centro de configuração. Através desta opção você pode configurar diversos serviços do seu servidor. Esta opção é aberta, automaticamente, no primeiro logon após a instalação do Windows Server 2003 e continua sendo aberta a menos que você marque a opção Não mostrar esta página durante o logon (Don't display this page at logon). Nesta página você tem acesso a configurações de impressão, de terminal services, você pode adicionar novas funções ao servidor. Você também tem acesso aos links de ajuda e suporte via Internet do Windows Server 2003.
- ◆ **Configuração do Microsoft .NET Framework 1.1 e Assistente do Microsoft .NET Framework 1.1:** Estas opções são utilizadas para configuração e administração do Framework .NET. O Framework .NET é que dá suporte ao desenvolvimento de aplicações .NET, baseadas em conceitos tais como Web Services.
- ◆ **Gerenciador de equilíbrio de carga de rede:** Este console é utilizado para configurar o Software de balanceamento de cargas da Microsoft. Este software normalmente é utilizado em um cluster de servidores para distribuir as requisições dos clientes de uma maneira uniforme entre os diversos servidores do cluster.
- ◆ **Desempenho:** Este console é utilizado para coletar dados sobre o desempenho dos elementos de hardware e software do servidor. Por exemplo, posso fazer medidas para saber a taxa de ocupação dos processadores, da memória RAM, do arquivo de paginação, das interfaces de rede e assim por diante. Os dados coletados podem ser exibidos na forma de relatórios e gráficos. Você aprenderá a utilizar este console no Capítulo 11.
- ◆ **Áreas de trabalho remotas:** Com este console o administrador pode criar conexões para múltiplos servidores e administra-los remotamente. As conexões podem ser criadas via Terminal Services (Windows 2000 Server e Windows Server 2003) ou utilizando a funcionalidade de Desktop Remoto (Windows Server 2003). Com o uso de Desktop Remoto, o administrador tem acesso a Área de trabalho (Desktop) de um servidor remotamente.
- ◆ **Roteamento e acesso remoto:** Este console permite a administração de um servidor no qual está instalado o serviço Routing and Remote Access (RRAS). Com o uso do RRAS você pode transformar um servidor com o Windows Server 2003 em servidor de comunicação remota. Um usuário com um Notebook e uma linha telefônica pode discar para o servidor RRAS, fazer o logon no domínio e ter acesso a todos os recursos da rede, apenas com a diferença que a velocidade de conexão é definida pela linha que o usuário utilizou para fazer a discagem. No Capítulo 17 do livro Windows Server 2003 – Curso Completo, 1568 páginas, você aprende mais detalhes sobre a instalação, configuração e administração do RRAS. O RRAS não será abordado neste livro, pois não faz parte do programa oficial para o Exame 70-290.
- ◆ **Serviços:** Esta opção fornece acesso aos serviços instalados no computador. Um serviço é um programa que fica ativo na memória do servidor, normalmente com a função de atender requisições dos clientes. Por exemplo, o IIS fornece um serviço de hospedagem de páginas Web, o qual após inicializado, fica respondendo a requisições dos clientes para acesso a páginas Web. Existe um serviço que permite o compartilhamento de arquivos (pastas compartilhadas), outro que permite a resolução de nomes (DNS ou WINS) e assim por diante. Através desta opção você pode configurar os diversos serviços instalados no computador. Por exemplo, um serviço pode ser configurado para inicializar automaticamente uma vez que o servidor seja ligado. Com isso mesmo que não seja feito o logon no servidor, o serviço será inicializado automaticamente e responderá às requisições dos clientes. Em diversos capítulos deste livro você utilizará as opções de gerenciamento de serviços.
- ◆ **Licenciamento do Terminal Server, Configuração dos serviços de terminal e Gerenciador de Serviços de terminal:** Estes consoles são utilizados para administração e gerenciamento do Terminal Services. Somente

estarão disponíveis se o Terminal Services estiver instalado. No Capítulo 9 você irá estudar o terminal services em detalhes.

A medida que você instala novos serviços, novos consoles são adicionados a opção Administrative tools (Ferramentas administrativas). Por exemplo, quando você instala o DNS, um console DNS é adicionado, quando você instala o DHCP, um console para gerenciamento do DHCP é instalado e assim por diante.

Se você trabalha seguidamente com um determinado console, você pode facilmente adicionar um atalho para o referido console na sua Área de trabalho. Para isso siga os seguintes passos:

1. Clique em Iniciar -> Ferramentas Administrativas.
2. Clique com o botão direito do mouse no console desejado.
3. No menu de opções que é exibido clique em: Enviar para -> Área de trabalho (Criar atalho).

## Conclusão

Neste capítulo apresentei o conceito de MMC e Snap-in. Mostrei que o MMC é o padrão utilizado pela Microsoft para as ferramentas administrativas do Windows Server 2003, a exemplo do que já acontecia com o Windows 2000 Server. Com o uso de um padrão é possível manter todas as ferramentas administrativas com uma interface e com funcionalidades semelhantes. Isso simplifica o trabalho do administrador e reduz o tempo de aprendizagem.

O MMC em si é apenas um “hospedeiro” (um container falando tecnicamente), no qual são abertos os chamados Snap-ins. O MMC sozinho não tem funcionalidade (para não dizer utilidade) alguma. O MMC somente torna-se útil quando nele for carregado um Snap-in.

O administrador pode criar consoles personalizados e salva-los como arquivos .msc. O administrador também pode configurar diferentes níveis de acesso que o usuário do console personalizado terá. Após ter criado o console personalizado é só enviar o arquivo .msc para o usuário que irá utilizar o console para executar as tarefas administrativas relacionadas com as funcionalidades do console.

Para finalizar o capítulo apresentei uma breve descrição de vários consoles e opções administrativas que estão disponíveis no menu Ferramentas administrativas.

# Introdução

Neste capítulo você aprenderá sobre os seguintes assuntos:

- ◆ O conceito de contas de usuários, contas de computadores e grupos de usuários.
- ◆ Criação e administração de contas de usuários e de computadores.
- ◆ Criação e administração de grupos de usuários.
- ◆ Criação e administração de Unidades Organizacionais.
- ◆ O modelo de permissões do Windows Server 2003.
- ◆ Ferramentas para executar outras tarefas no Active Directory.

Quando você trabalha na rede da empresa, o Windows Server 2003 precisa de uma maneira para poder identificar quem é o usuário logado e quais ações ele está realizando. O Windows Server 2003 também precisa identificar cada usuário para liberar ou não o acesso a recursos protegidos por permissões de acesso. Por exemplo, suponha que você tem uma pasta compartilhada chamada Docs, no servidor SRV01. Nesta pasta o Administrador configurou as permissões de acesso, de tal maneira que somente o usuário José da Silva, logon jsilva, possa acessar esta pasta. O Windows Server 2003 precisa saber quem é o usuário que está “tentando” acessar a pasta. Se for o José da Silva, o Windows Server 2003 libera o acesso, caso contrário o acesso é negado.

O Windows Server 2003 identifica cada usuário pelas informações de logon. Quem informações são essas? Um nome com o qual o usuário foi cadastrado na rede e a respectiva senha. Por exemplo, o nosso usuário José da Silva poderia ser cadastrado como jsilva, já a Maria Aparecida poderia ser cadastrada como mariaap, e assim por diante. Ou seja, o primeiro passo para que um usuário possa ter acesso aos recursos da rede é cadastrar o usuário. Cadastrar o usuário significa criar uma conta de usuário e um senha no Active Directory. Na primeira parte deste capítulo você aprenderá sobre contas de usuários. Inicialmente apresentarei alguns detalhes teóricos sobre contas de usuário e após a teoria, mostrarei a parte prática, ou seja, como criar e administrar contas de usuários.

Uma vez entendido o conceito de usuários, você aprenderá sobre grupos de usuários. Mostarei que existem diferentes tipos de grupo e com diferentes escopos de utilização. No Capítulo 2 fiz uma discussão teórica (de fundamental importância para a eficiente administração das permissões de acesso aos recursos) sobre as estratégias de utilização de grupos de usuários, para atribuição de permissões aos recursos da rede: pastas e impressoras compartilhadas, aplicativos Web, bancos de dados e assim por diante. Neste capítulo você aprenderá a parte prática de criação de grupos. Nos Capítulo 6 você aprenderá a utilizar a estratégia explicada no Capítulo 2.

Entendidos os conceitos de contas de usuários e grupos de usuários, é hora de aprender sobre unidades organizacionais. Vou mostrar o que é uma Unidade organizacional, como ela difere de um domínio, quando usar Unidades Organizacionais e quando utilizar domínios. Também mostrarei a parte prática de criação e administração de Unidades Organizacionais, bem como operações de mover contas de usuários e grupos de uma unidade organizacional para outra.

# CAPÍTULO

# 4

## Administração de contas de usuários e grupos do Active Directory

Para encerrar o capítulo apresentarei mais uma ferramenta de administração do Active Directory: a ferramenta para gerenciamento do Schema (lembrando do Capítulo 2, o Schema é a definição da estrutura do banco de dados do Active Directory). Falarei da importância e da função do Schema e irei ressaltar que toda e qualquer alteração no Schema deve ser cuidadosamente (eu diria cuidadosamente ao quadrado) planejada e testada em laboratório, antes de ser implementada em um ambiente de produção. Erros nas alterações do Schema podem causar verdadeiros desastres.

Com os conceitos apresentados neste capítulo, você terá avançado mais um passo no entendimento do Active Directory e dos diversos elementos que o compõem.

## Contas de Usuários

Quando você trabalha em uma rede de computadores, segurança é um dos itens de maior importância. O Administrador deve ser capaz de permitir que cada usuário somente tenha acesso aos recursos – sejam eles arquivos, impressoras ou serviços – os quais sejam necessários para a realização do seu trabalho. Por exemplo, um usuário que trabalha no departamento de bagagem não deve ser capaz de acessar informações sobre salários contidas nos arquivos de um Computador do departamento de Recursos Humanos.

No Capítulo 1 você aprendeu sobre redes de computadores e os diferentes papéis que o Windows Server 2003 pode desempenhar em uma rede. Mostrei que, em uma configuração típica, o Windows Server 2003 pode estar configurado como um servidor de arquivos, onde existem pastas compartilhadas que os usuários acessam através da rede.

No Capítulo 2 você aprendeu sobre o conceito de Domínio. Quando você cria um domínio, os servidores e também as estações de trabalho dos usuários, devem ser configuradas para fazer parte do domínio. Quando um usuário liga a sua estação de trabalho (quer ele esteja configurada com o Windows 95/98/Me, 2000, NT Workstation ou XP Professional), o Windows é inicializado e em seguida é apresentada a tela de logon no domínio, conforme indicado na Figura 4.1, onde temos o exemplo do usuário jsilva fazendo o logon no domínio ABC.



Figura 4.1 A tela de logon no domínio.

As informações sobre as contas de usuários e grupos ficam gravadas na base de dados do Active Directory, nos servidores configurados como DCs do domínio. Quando o usuário liga a sua estação de trabalho e digita o seu nome de usuário e senha, estas informações são repassadas para um DC do domínio, onde as informações são verificadas. Se o nome de usuário existir, a senha estiver correta e a conta do usuário não estiver bloqueada, o logon será liberado e a área de trabalho do Windows será carregada. Uma vez que o usuário fez o logon no domínio, ele passou a estar identificado, ou seja, todas as ações que o usuário executar estarão associadas com a sua conta de usuário. Por exemplo, se o usuário jsilva fizer o logon no domínio ABC e tentar acessar um arquivo para o qual ele não tem permissão, ficará registrado nos logs de auditoria do servidor as seguintes informações (isso se o administrador configurou a auditoria de acesso a pastas e arquivos, conforme mostrarei no Capítulo 10):

- ◆ Identificação do usuário – no exemplo jsilva.
- ◆ Data e hora da tentativa de acesso.
- ◆ Nome do arquivo e/ou pasta que o usuário tentou acessar.

Observe que a conta do usuário é utilizada como a sua identidade na rede.

Em um domínio, além de servidores configurados como DCs, você pode ter servidores configurados como Member Servers. Um member server não tem o Active Directory instalado e, portanto, não tem uma cópia de toda a lista de usuários e grupos do domínio e nem das demais informações contidas no Active Directory. Um member server normalmente é um servidor que desempenha um papel específico, tal como servidor de arquivos, servidor de impressão, servidor de acesso remoto, servidor Web e assim por diante.

Como o servidor faz parte do domínio (member server), as contas de usuários e grupos do domínio podem receber permissões para acessar os recursos disponibilizados pelo member server. Um detalhe interessante é que é possível criar uma lista de usuários e grupos de usuários no próprio member server. Estas contas somente são válidas para o logon localmente no servidor onde foram criadas e são conhecidas como contas locais.

Por exemplo, ao instalar o Windows Server 2003 em um member server, automaticamente é criada a conta Administrador, com permissões de administrador em todos os recursos do member server. As contas e grupos locais, criados em um member server, somente podem receber permissões de acesso aos recursos do servidor onde foram criadas, já que estas contas não são “visíveis” em outro servidor que não o próprio onde foram criadas. Embora seja possível criar contas e grupos locais, esta não é uma prática recomendada. Sempre que possível você deve utilizar as contas e grupos do domínio. Uma exceção é a conta local Administrador, a qual é criada automaticamente com a instalação do Windows Server 2003. Esta conta tem permissões totais em todos os recursos do servidor. Um procedimento normalmente adotado é definir a mesma senha para todas as contas Administrador de todos os member servers do domínio. Normalmente esta senha é de conhecimento apenas dos administradores do domínio. A conta local Administrador pode ser utilizada para fazer configurações no servidor quando, por algum motivo, não for possível fazer o logon no domínio.

Contas criadas em um DC são chamadas de “Domain User Accounts” (Contas de Usuários do Domínio). Essas contas permitem que o usuário faça o logon em qualquer computador do domínio e receba permissões para acessar recursos em qualquer computador do domínio.

Contas criadas em um Servidor Membro são chamadas de “Local User Accounts” (Contas de Usuários Locais). Essas contas somente permitem que o usuário faça o logon e receba permissões para acessar recursos do servidor onde a conta foi criada. Sempre que possível evite criar Contas Locais em servidores que fazem parte de um domínio. Utilizar as contas do Domínio, as quais ficam armazenadas no Active Directory, torna a administração bem mais fácil.

---

**IMPORTANTE:** Uma conta pode ser criada em um DC – situação em que a conta é válida e reconhecida em todo o domínio; ou a conta pode ser criada em um member server – situação em que a conta somente é válida e reconhecida no member server onde ela foi criada.

---

Quando é exibida a tela de logon em um member server, o usuário pode escolher entre fornecer uma conta e senha do domínio ou uma conta e senha local. Na lista Log on to o usuário seleciona o nome do domínio no qual ele quer fazer o logon ou o nome do servidor local, para fazer o logon com uma conta local. A criação e administração de contas de usuários e grupos locais é feita utilizando-se o console Gerenciamento do Computador (Computer Management), descrito no Capítulo 7. As etapas para a criação e administração de contas e grupos locais são semelhantes as etapas para a criação e administração de contas do Active Directory. Nos exemplos deste capítulo utilizarei contas e grupos do domínio. A única diferença para as contas locais é que para estas haverá um número menor de campos disponíveis quando da criação da conta e as ferramentas utilizadas são diferentes. Para contas locais o console Gerenciamento do Computador e para contas do domínio, o console Computadores e Usuários do Domínio (Active Directory Users and Computers).

No Windows Server 2003, é possível limitar os recursos aos quais cada usuário tem acesso, através do uso de permissões de acesso . Por exemplo, o administrador pode definir uma lista de usuários com acesso a uma pasta compartilhada, podendo definir, inclusive, níveis de acesso diferentes. Um determinado grupo tem acesso completo (leitura, gravação e exclusão), já um segundo tem acesso mais restrito (leitura e gravação) e um terceiro grupo tem acesso ainda mais restrito (leitura). Para que seja possível atribuir permissões, cada usuário deve ser cadastrado no domínio. Cadastrar o usuário significa criar uma “Conta de Usuário”. Com uma conta o usuário pode efetuar o logon e receber permissões para acessar os mais variados recursos disponibilizados na rede.

Reunindo esta história toda, cada usuário deve ser cadastrado. Cadastrar o usuário significa criar uma conta de usuário no Active Directory (veja exemplos práticos mais adiante). Uma vez que a conta foi criada, o usuário pode utiliza-la para fazer o logon em qualquer computador da rede. Antes de partir para a parte prática, apresentarei mais algumas recomendações e detalhes relacionados com contas de usuários:

## Definindo um padrão de nomes para as contas de usuários.

Outro detalhe que você deve observar, é a utilização de um padrão para o nome das contas de usuários. Você deve estabelecer um padrão para a criação de nomes, pois não podemos existir dois usuários com o mesmo nome de logon dentro do mesmo domínio. Por exemplo se existir no mesmo Domínio, dois funcionários com o nome José da Silva e os dois resolverem utilizar como logon “jsilva”, o administrador terá um problema para resolver, pois não é possível ter dois usuários com o mesmo nome de logon, no mesmo domínio. Para isso é importante que seja definido um padrão e no caso de nomes iguais deve ser definido uma maneira de diferenciá-los. Por exemplo você poderia usar como padrão a primeira letra do nome e o último sobrenome. No caso de nomes iguais, acrescentam-se números. No exemplo citado, o primeiro José da Silva cadastrado ficaria como jsilva, já o segundo a ser cadastrado ficaria como jsilva1. Caso no futuro houvesse mais um José da Silva dentro do mesmo domínio, este seria o jsilva2 e assim por diante.

## Observações Sobre o Nome das Contas de Usuários

Quando o administrador cria nomes de logon para os usuários, devem ser levados em consideração os seguintes fatos:

- ◆ O nome de logon deve ser único no domínio. Veja o exemplo do item anterior, onde mostrei que não seria possível criar dois usuários com nome de logon jsilva, no mesmo domínio.
- ◆ O nome de logon também não pode ser igual ao nome de um grupo do domínio. Por exemplo, se já existe um grupo chamado Contabilidade, você não poderá criar uma conta de usuário com o campo nome de logon preenchido como Contabilidade.
- ◆ O nome de logon pode conter espaços em branco e pontos, porém não pode ser formado somente por espaços e pontos. É conveniente evitar o uso de espaços em branco, pois contas com espaços em branco no nome, terão que ser escritas entre aspas, quando você utiliza scripts para administração do Windows Server 2003.

- ◆ Podem ter no máximo 20 caracteres.
- ◆ Os seguintes caracteres não podem ser utilizados: “ / \ : ; [ ] | = , + \* ? < >
- ◆ O Windows Server 2003 não diferencia entre maiúsculas e minúsculas para o nome de logon. Por exemplo, para o Windows Server 2003 jsilva, JSILVA ou Jsilva representa o mesmo usuário.

## Questões relacionadas com a definição da senha do usuário

Sempre que você for cadastrar um usuário também deve ser cadastrada uma senha para ele. No Windows 2000 Server, por padrão, era aceito que o administrador definisse uma senha em branco. Caso fosse necessário, o administrador poderia definir um número mínimo de caracteres para as senhas dos usuários. No Windows Server 2003, a preocupação com a segurança está presente desde o momento da instalação. No Windows Server 2003.

No Windows Server 2003, por padrão, são definidas as seguintes políticas de segurança em relação as senhas de usuários:

- ◆ Quando o usuário vai trocar a senha, não pode ser utilizada uma senha igual as 24 últimas (haja criatividade para inventar senhas).
- ◆ A senha expira (isto é, deve ser alterada) a cada 42 dias.
- ◆ O tempo mínimo de vida de senha é um dia. Ou seja, você trocou a senha hoje, não poderá trocá-lo novamente daqui a uma ou duas horas, somente após um dia.
- ◆ Tamanho mínimo de sete caracteres.
- ◆ A opção “A senha deve atender critérios de complexidade (Password must meet complexity requirements) é habilitada por padrão”.
- ◆ A senha não pode conter parte ou todo o nome da conta. Por exemplo, se o nome da conta for jsilva, a senha não poderá conter a sílaba “sil” ou a palavra “silva”.
- ◆ Ter pelo menos seis caracteres. O número mínimo de caracteres pode ser aumentado, configurando-se as políticas de segurança para senhas, conforme mostrarei mais adiante.
- ◆ Deve conter caracteres de pelo menos três dos quatro grupos a seguir: letras maiúsculas de A até Z, letras minúsculas de a até z, dígitos de 0 a 9 ou caracteres especiais (:, !, @, #, \$, %, etc.).

**IMPORTANTE:** Com a opção A senha deve atender critérios de complexidade (Password must meet complexity requirements) é habilitada por padrão, uma série de requisitos devem ser atendidos para que a senha seja aceita.

Estes requisitos de complexidade são verificados quando a senha é criada pela primeira vez, durante o cadastramento do usuário e toda vez que a senha for alterada. Com os requisitos de complexidade habilitados, as senhas a seguir seriam válidas:

- ◆ AbCsenha1
- ◆ AbcSenha#
- ◆ Abc123
- ◆ Abc;;senha

**IMPORTANTE:** Para as senhas, o Windows Server 2003 distingue letras maiúsculas de minúsculas. Por exemplo a senha “Abc123” é diferente da senha “abc123”.

Já as senhas a seguir não seriam válidas:

- ◆ abcsenha123: Contém somente caracteres de dois dos quatro grupos (letras minúsculas e números).

- ◆ abc;senha: Contém somente caracteres de dois dos quatro grupos (letras minúsculas e caracteres especiais).

Agora que a teoria sobre as contas de usuários e senhas já foi apresentada, vou mostrar como criar e administrar contas de usuários. Você aprenderá as diversas tarefas relacionadas com a administração das contas de usuários em um domínio do Windows Server 2003.

**NOTA:** Mais no final deste capítulo, você aprenderá a configurar as definições das políticas de segurança para senhas do domínio.

## Criação e administração de contas de usuários.

Neste item você aprenderá as ações práticas para a criação e administração de contas de usuários de um domínio. Você aprenderá a criar novas contas, configurar as diversas propriedades das contas já existentes, ativar e desativar contas, desbloquear contas, excluir e renomear contas. Todas estas ações são executadas com o console Usuários e computadores do Active Directory (Active Directory Users and Computers). Vamos iniciar os exemplos pela criação de uma nova conta.

### Criando uma nova conta de usuário no domínio:

Para criar uma nova conta de usuário no Active Directory, siga os passos indicados a seguir:

1. Faça o logon como Administrador ou com uma conta pertencente ao grupo Oper. de contas (Account Operators).
2. Abra o console Usuários e computadores do Active Directory: Iniciar -> Ferramentas Administrativas -> Usuários e computadores do Active Directory.
3. Será aberto o console Usuários e computadores do Active Directory, indicado na Figura 4.2:

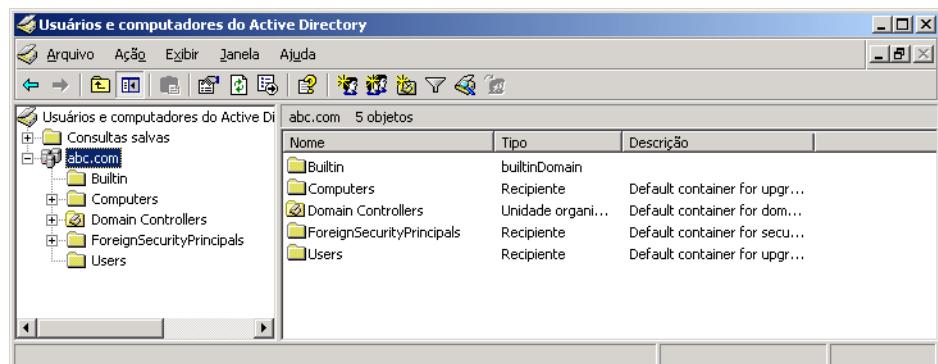


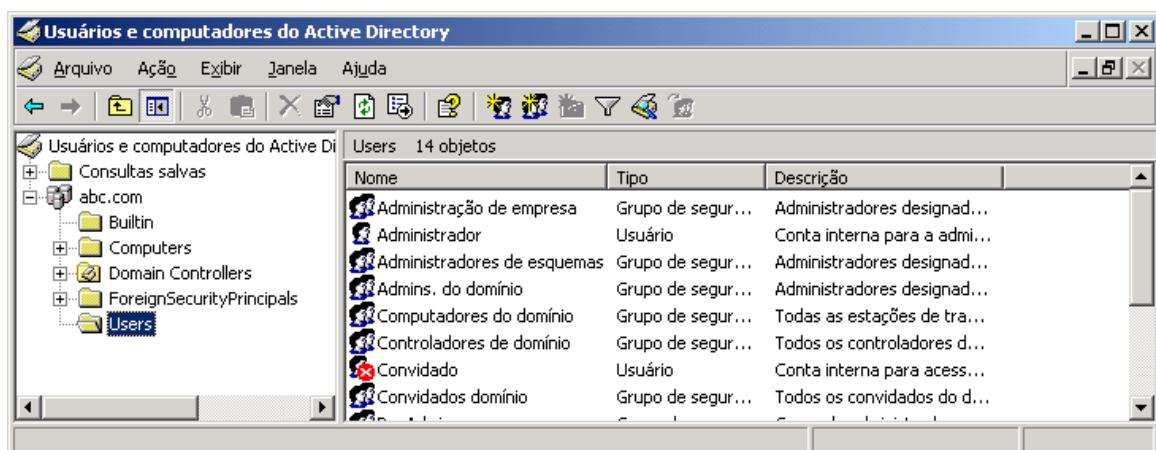
Figura 4.2 O console Usuários e computadores do Active Directory.

4. Clique no sinal de + ao lado do nome do domínio no qual você irá criar a conta.
5. Abaixo do nome do domínio é exibida uma lista de opções criadas automaticamente quando o Active Directory é instalado:
  - ◆ **Builtin:** Nesta opção estão os chamados grupos Builtin, ou seja, aqueles grupos criados automaticamente quando o Active Directory é instalado. Estes grupos são utilizados para funções de administração do domínio. Por exemplo, os membros do grupo Administradores (Administrators) tem permissões administrativas em todo o domínio, já membros do grupo Oper. de contas (Account Operators) tem permissões para criar e administrar contas de

**IMPORTANTE:** O grupo Oper. de contas é criado automaticamente durante a instalação do Active Directory. Membros deste grupo podem realizar tarefas relacionadas a criação e administração de contas de usuários no domínio. Mais adiante, no item sobre Grupos, descreverei os grupos que são criados automaticamente quando da instalação do Active Directory, os chamados Built-in Groups.

usuários no domínio e assim por diante. Os grupos que ficam nesta opção são grupos Locais do domínio. Mais adiante neste capítulo, descreverei as diferenças entre grupos Locais, Globais e Universais.

- ◆ **Computers (Computadores):** Nesta opção ficam as contas de todos os computadores do domínio, a não ser que tenham sido criadas outras unidades organizacionais e contas tenham sido movidas para estas unidades organizacionais. É importante lembrar que somente computadores com o Windows NT 4.0, Windows 2000, Windows Server 2003 ou Windows XP Professional, possuem conta de computador. Computadores com o Windows 95/98/Me não tem contas de computador no domínio.
  - ◆ **Domain Controllers (Controladores de domínio):** Nesta opção ficam as contas de computadores dos DCs do domínio.
  - ◆ **ForeignSecurityPrincipals:** Nesta opção ficam objetos relacionados a relações de confiança criadas manualmente pelo administrador.
  - ◆ **Users:** Nesta opção ficam as contas que foram criadas automaticamente pelo Active Directory, bem como os grupos Globais criados automaticamente. Um exemplo de conta criada automaticamente é a conta Administrador (Administrator), a qual tem permissões de administrador em todos os recursos de todos os servidores do domínio. Por padrão é nesta opção que criamos novas contas de usuários. Conforme mostrarei mais adiante você também pode criar novas unidades organizacionais e criar contas de usuários dentro destas unidades organizacionais, o que também será visto neste capítulo.



**Figura 4.3** A opção Users.

7. Para criar um novo usuário você pode utilizar uma das seguintes opções:
    - ◆ Clicar com o botão direito do mouse em Users e, no menu que é exibido clicar em Novo -> Usuário.
    - ◆ Selecionar o comando Ação -> Novo -> Usuário.
    - ◆ Clicar no botão New User (Novo Usuário) (Fig 9-4.TIF) – Capítulo 9, pág 353 do livro do 2003.
  8. Usando qualquer uma das opções indicadas a seguir, será aberta a janela Novo Objeto – Usuário, na qual você deve preencher o nome, sobrenome, nome completo, User name logon (Nome de logon do usuário) e User logon name (pré-windows 2000), conforme exemplo da figura 4.4. O nome de logon (User logon name) é o nome que o usuário utiliza para efetuar o logon no domínio (jsilva, maria, etc.). Já User logon name (pré-Windows 2000) é o nome que o usuário utiliza para efetuar o logon em computadores com versões mais antigas do Windows, tais como o Windows NT Server 4.0. Por simplicidade estes dois nomes devem ser iguais, observe

que a medida que você digitar o primeiro, o segundo será automaticamente preenchido. Preencha os dados da nova conta e clique em Avançar.

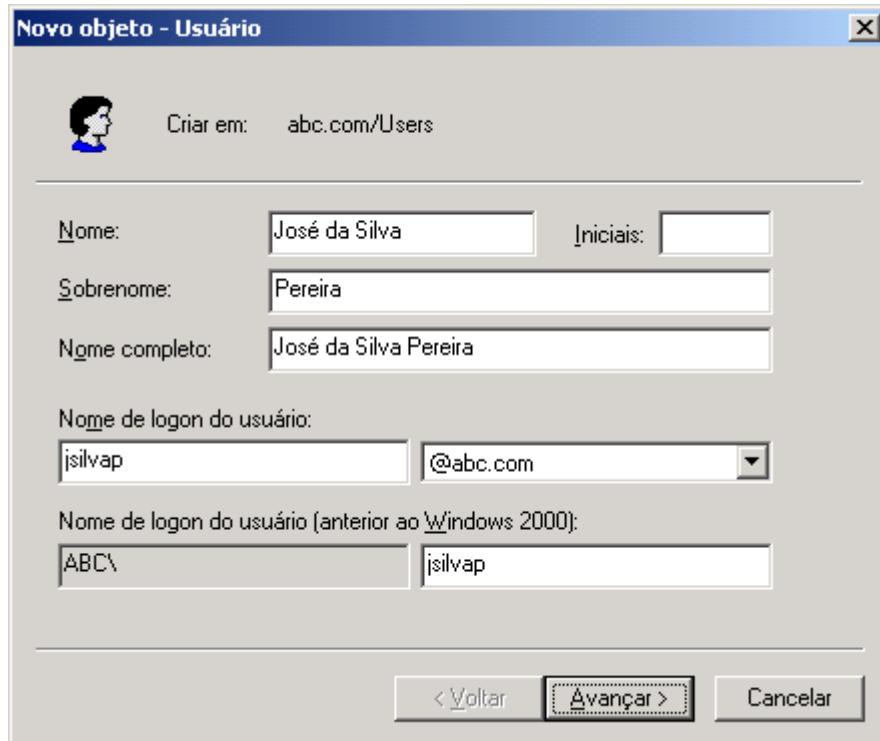


Figura 4.4 Criando a conta jsilvap.

9. Nesta etapa você tem que definir a senha e configurar algumas características da conta. Lembre que, por padrão, os requisitos de complexidade para senha estão habilitados, conforme descrito anteriormente. No campo Senha, informe uma senha que atenda aos requisitos de complexidade descritos anteriormente. Digite a senha novamente no campo Confirmar a senha.
10. Além da senha você pode configurar uma das quatro opções descritas a seguir:
  - ◆ **O usuário deve alterar a senha no próximo logon**: Se esta opção estiver marcada, a primeira vez que o usuário fizer o logon, será solicitado que ele altere a sua senha. Esta opção é utilizada para que o usuário possa colocar uma senha que somente ele conhece. Quando o usuário é cadastrado, a senha é digitada pelo Administrador, o qual fica sabendo a senha do usuário. No próximo logon o usuário é obrigado a alterar a senha de tal maneira que somente ele saiba qual a senha está definida para a sua conta.
  - ◆ **O usuário não pode alterar a senha**: Se esta opção estiver marcada, a senha somente pode ser alterada pelo Administrador. Normalmente utilizada para empregados temporários e para estagiários. Para as contas utilizadas pelos funcionários da empresa, esta opção normalmente é desabilitada.
  - ◆ **A senha nunca expira**: Ao marcar esta opção, independente das políticas de segurança do domínio, o usuário nunca precisará trocar a sua senha. Caso contrário de tempos em tempos (conforme configurado nas políticas de segurança do domínio ), o usuário deve trocar a senha.
  - ◆ **Conta desativada**: O Administrador marca esta opção para desativar/bloquear a conta de um usuário. Usuários com a conta bloqueada não podem mais efetuar logon e, consequentemente, não podem mais acessar recursos da rede. Esta opção normalmente é utilizada para desativar, temporariamente, a conta de empregados que estão em férias. Quando o empregado retorna ao serviço, o Administrador libera a sua conta, simplesmente desmarcando esta opção.

11. Defina as opções para a conta que está sendo criada, conforme exemplo da Figura 4.5:

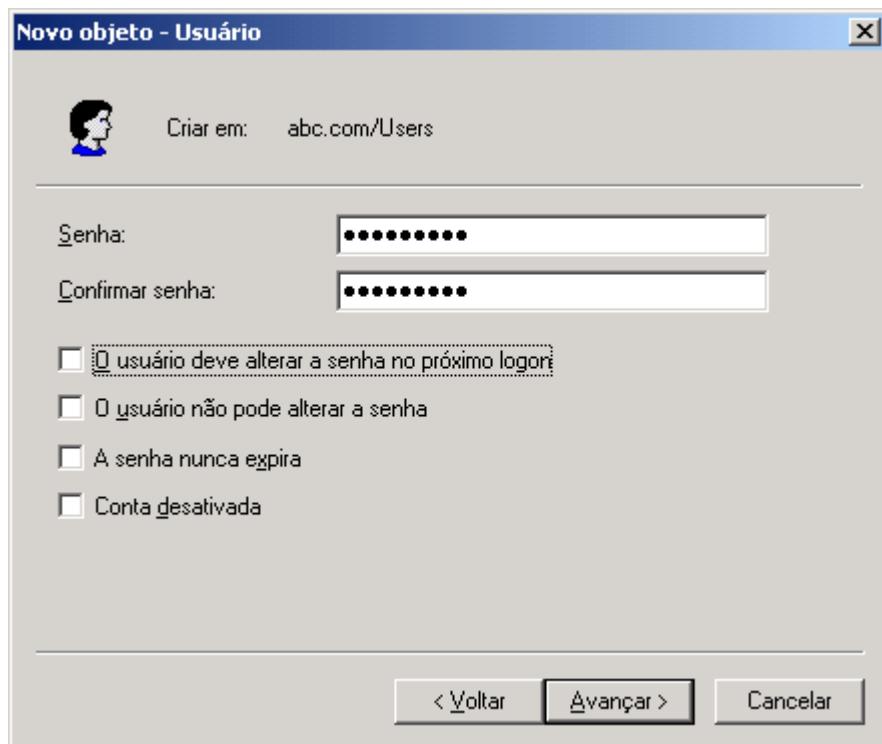


Figura 4.5 Definindo a senha e as opções da nova conta.

12. Clique em Avançar para seguir para a próxima etapa.  
13. Esta etapa é apenas informativa. Você pode utilizar o botão Voltar para voltar a uma determinada etapa e fazer alterações. Clique em Concluir.  
14. A conta jsilvap será criada e já será listada na opção Users. Observe que o que aparece na listagem é o nome completo do usuário. No nosso exemplo está sendo exibido o usuário José da Silva Pereira, conforme indicado na Figura 4.6. Nesta figura eu activei o modo de visualização ícones grandes. Para tal utilizei o comando Exibir -> Ícones Grandes do console Usuários e computadores do Active Directory.

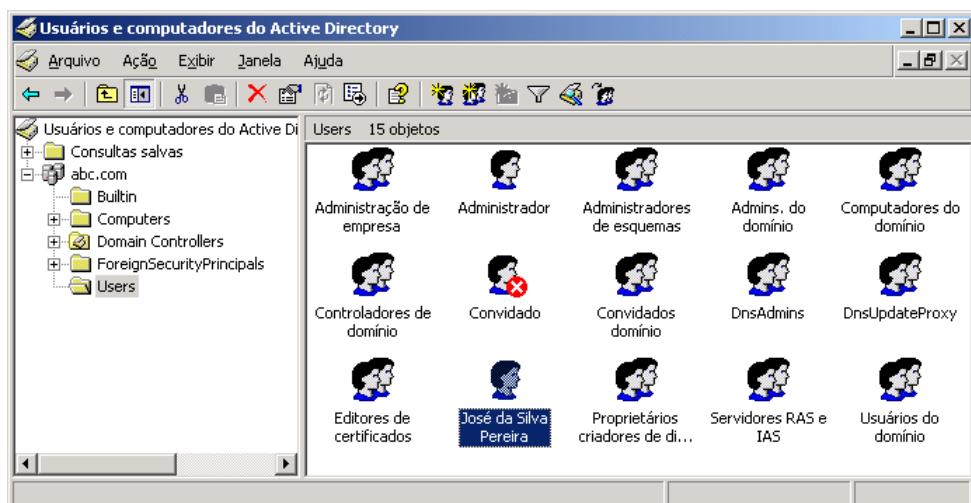


Figura 4.6 O usuário já é exibido na lista de usuários.

Muito bem, agora o usuário José da Silva Pereira foi cadastrado com o nome de logon jsilvap e poderá fazer o logon nas estações de trabalho do domínio. Por padrão, quando uma nova conta de usuário é criada, ela não tem permissão para fazer logon localmente nos member servers e nem nos DCs do domínio. Ou seja, o usuário poderá fazer o logon nas estações de trabalho do domínio, mas não poderá fazer o logon diretamente nos servidores, quer DCs, quer member servers, do domínio. A permissão para fazer o logon localmente nos servidores do domínio é um direito que por padrão somente é atribuído a alguns grupos especiais, tais como Administradores, Oper. de contas e assim por diante. Em um dos próximos itens você aprenderá a configurar os direitos de usuários e a atribuir estes direitos para uma ou mais contas ou grupos de usuários.

## Configurando uma conta de usuário

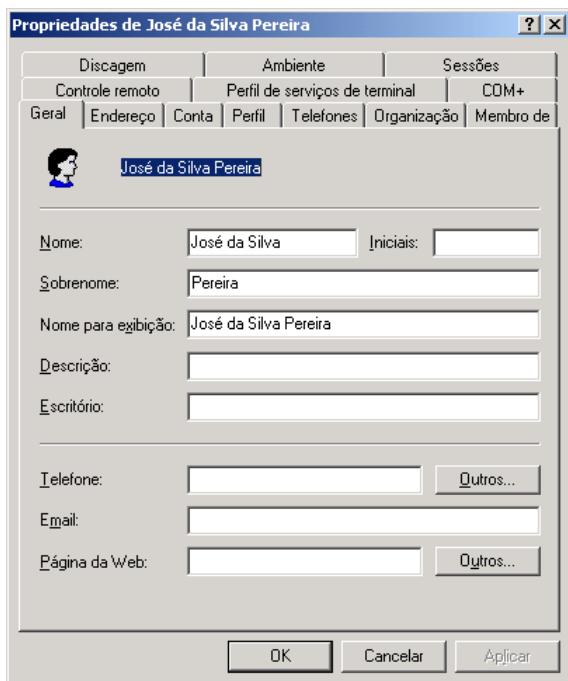
Durante a criação de uma conta de usuário, apenas algumas propriedades da conta são configuradas. Depois que a conta é criada, você pode acessar as propriedades da conta para configurar dezenas de outras propriedades. Por exemplo, você pode definir em que horas durante o dia é permitido que seja feito o logon com a respectiva conta, em quais computadores a conta pode ser utilizada para fazer o logon, qual o script de logon associado a conta e assim por diante. Neste item descreverei as principais propriedades que podem ser configuradas para uma conta de usuário do domínio. Vou dividir as configurações em etapas. Em cada etapa mostrarei como configurar determinadas propriedades relacionadas com um tópico específico. Por exemplo, como configurar as horas de logon, como configurar as informações pessoais e assim por diante. Em todos os exemplos, será solicitado que você acesse as propriedades da conta. Para acessar as propriedades de uma conta, você deve seguir os passos que indico logo a seguir. Nos demais exemplos, não irei repetir estes passos, apenas usarei a expressão “Acesse as propriedades da conta a ser configurada”.

Para acessar as propriedades da conta a ser configurada siga os passos indicados a seguir:

1. Faça o logon como Administrador, com uma conta com permissão de Administrador ou com uma conta pertencente ao grupo Oper. de contas (Account Operators).
2. Abra o console Usuários e computadores do Active Directory: Iniciar -> Ferramentas Administrativas -> Usuários e computadores do Active Directory.
3. Será aberto o console Usuários e computadores do Active Directory.
4. Clique no sinal de + ao lado do nome do domínio da conta a ser configurada.
5. Abaixo do nome do domínio é exibida uma lista de opções criadas automaticamente quando o Active Directory é instalado. Clique na opção Users (ou na Unidade Organizacional onde a conta está contida, caso a conta esteja em uma Unidade Organizacional).
6. Para acessar as propriedades da conta basta dar um clique duplo no nome da conta. A janela de propriedades da conta será exibida, com a guia Geral selecionada, conforme exemplo da Figura 4.7:
7. Observe que estão disponíveis uma série de guias, com diversas propriedades em cada guia. Após ter configurado as propriedades da conta, clique em OK. Nos exemplos a seguir mostrarei como configurar diversas destas propriedades.

### Configurando informações gerais e de endereço para a conta do usuário:

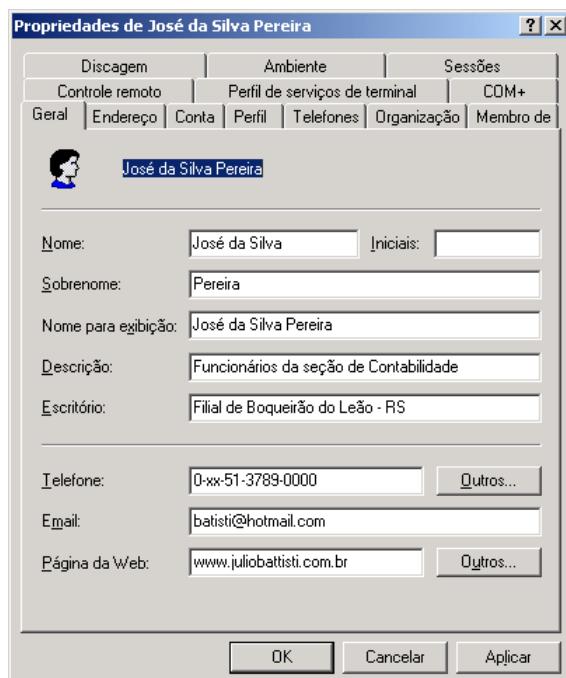
A seguir você acompanhará um exemplo prático sobre a configuração das propriedades da guia Geral, Endereço, Telefones e Organização. Estas guias servem como um cadastro, com os dados do funcionário na empresa. Qualquer aplicação desenvolvida na empresa, pode fazer acesso aos dados do Active Directory, como dados de cadastro dos funcionários. Este é o princípio básico de uso de um único diretório, como repositório central de informações, ao invés de uma diversidade de diretórios, espalhados pela rede da empresa, conforme descrito no início do Capítulo 2.



**Figura 4.7 A janela de propriedades de uma conta de usuário do domínio.**

Para configurar informações gerais e de endereço para uma conta de usuário, siga os passos indicados a seguir:

1. Acesse as propriedades da conta a ser configurada.
2. A guia Geral será exibida por padrão. Nesta guia, além das informações de nome, sobrenome e nome completo, definidas durante a criação da conta, você pode preencher uma descrição para o usuário (Descrição), informações sobre a seção/ou empresa (Escritório), bem como informações de telefone de contato (Telefone), E-mail e site (Página Web), conforme exemplo da Figura 4.8:



**Figura 4.8 Definindo propriedades da guia General (Geral).**

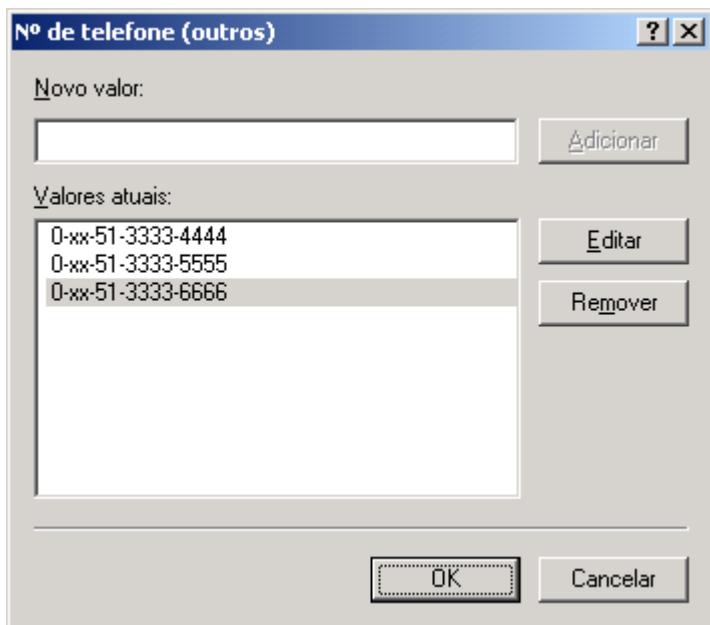


Figura 4.9 Inserindo mais números de telefone.

3. Para preencher os campos sobre o endereço do usuário, clique na guia Endereço. Preencha os campos conforme exemplo da Figura 4.10:

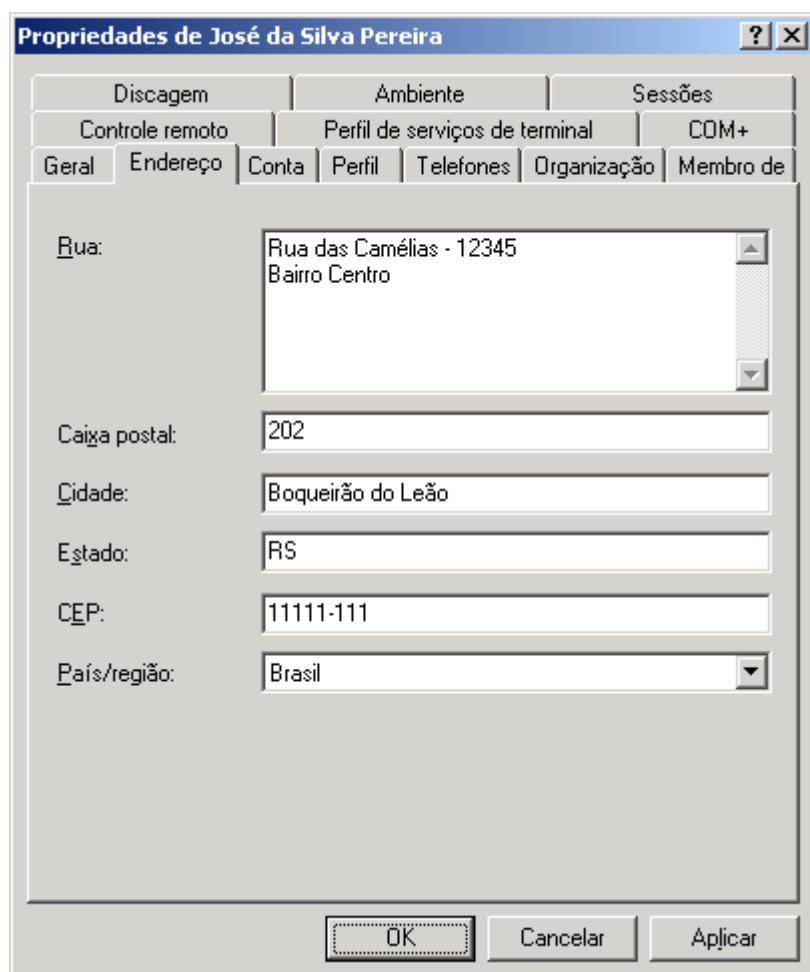
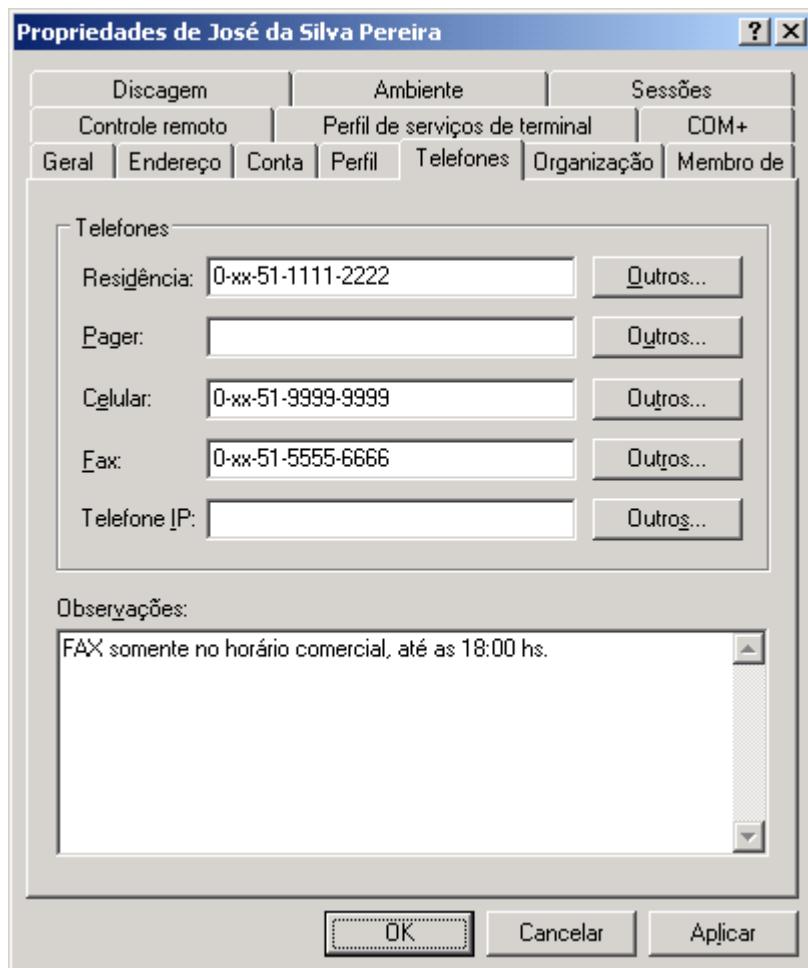


Figura 4.10 Inserindo informações do endereço do usuário.

**NOTA:** Você pode informar mais do que um número de telefone ou de página Web. Para isso basta clicar no botão Outros..., ao lado do respectivo campo. Será aberta uma janela onde você pode adicionar novos valores. No exemplo da Figura 4.9, foram adicionados mais três números de telefone. Para adicionar um novo número basta digitá-lo no campo Novo valor e depois clicar no botão Adicionar. Repita estes passos para cada novo número a ser adicionado. Para finalizar a entrada de novos números é só clicar no botão OK. Para alterar um número clique no respectivo número e depois no botão Editar. O número a ser editado será selecionado. Faça as alterações desejadas e clique no espaço em branco abaixo do último número. As alterações serão efetuadas. Para remover um número clique no número a ser excluído e depois no botão Remover. Feitas as configurações desejada clique em OK para fechar a janela para entrada de novos valores.

4. Para preencher os campos com dados sobre telefones de contato do usuário, clique na guia Telefones. Preencha os campos conforme exemplo da Figura 4.11:



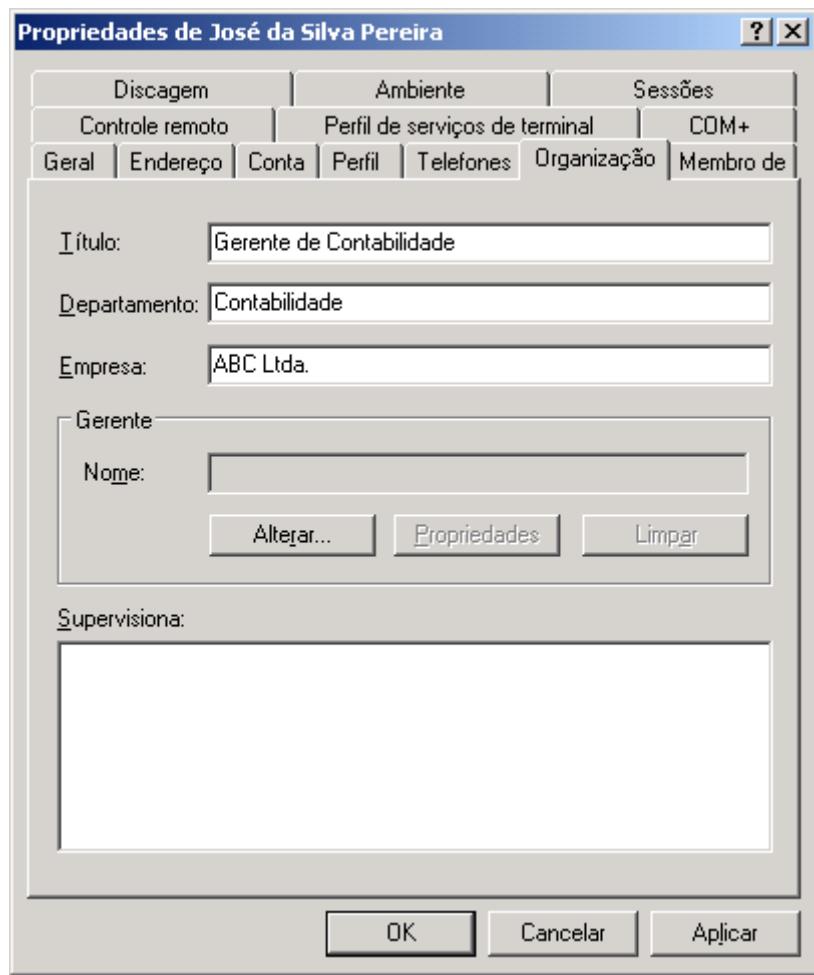
**Figura 4.11 Inserindo informações dos telefones de contato.**

5. Para preencher os campos com dados da empresa, clique na guia Organização. Preencha os campos conforme exemplo da Figura 4.12.  
 6. Preenchida as informações e clique em OK para salva-las.

As informações das guias Geral, Endereço, Telefones e Organização são utilizadas como uma espécie de cadastro, de banco de dados dos usuários cadastrados na rede. Embora não seja obrigatório, é recomendado que sejam preenchidas estas informações. Isso facilita a pesquisa no Active Directory. Por exemplo, é possível fazer uma pesquisa para localizar todos os usuários da seção de Tecnologia da Informação, ou todos os usuários de uma determinada cidade e assim por diante. Mais adiante você aprenderá a utilizar a ferramenta de pesquisa no Active Directory.

### Configurando informações sobre a conta do usuário:

Na guia Conta você tem acesso a uma série de opções relacionadas com a conta do usuário. Por exemplo, nesta guia tem uma opção para bloquear/desbloquear a conta do usuário, outra opção para definir um prazo de expiração para a conta, os horários em que o usuário pode fazer o logon, em quais computadores ele pode fazer o logon e assim por diante. Você aprenderá a utilizar as opções desta guia, no exemplo prático a seguir:



**Figura 4.12 Inserindo informações da empresa.**

Para configurar informações da guia Conta, siga os passos indicados a seguir:

1. Acesse as propriedades da conta a ser configurada.
2. Dê um clique na guia Conta. Nesta guia estão disponíveis uma série de configurações, conforme indicado na Figura 4.13.

Na parte de cima da janela é exibido o nome de logon do usuário, o domínio no qual o usuário foi cadastrado e o nome de logon pré-windows 2000. Observe que para o Windows 2000 Server e para o Windows Server 2003, o nome de logon completo do usuário é composto pelo nome DNS do domínio e a conta do usuário, como no exemplo a seguir: abc.com\jsilvap. Já para versões anteriores, como o NT Server 4.0, que são baseadas no WINS para a resolução de nomes, é usado o nome NetBIOS do domínio, como no exemplo a seguir: ABC\jsilvap. Observe que em ambos os casos o padrão é o nome do domínio (nome DNS no Windows 2000 ou Windows Server 2003 e nome NetBIOS no NT Server 4.0) uma barra invertida e o nome de logon do usuário.

A opção A conta está bloqueada: Por padrão, é definido no domínio, um número máximo de tentativas de logon sem sucesso que o usuário pode fazer, dentro de um período de tempo. Se este limite for ultrapassado, a conta será bloqueada automaticamente. Por exemplo, pode ser definido que se o usuário fizer três tentativas de logon sem sucesso, dentro de 20 minutos, a conta fique bloqueada por 24 horas. Ou também é possível definir que, uma vez bloqueada, a conta

---

**NOTA:** As opções Horário de logon... e Fazer logon em..., serão explicadas no próximo item.

---

somente possa ser desbloqueada pelo administrador. Estas configurações fazem parte das diretivas de segurança do domínio e serão explicadas mais adiante. Quando uma conta está bloqueada, a opção Conta bloqueada aparece habilitada e marcada. Para desbloquear a conta, basta que o administrador desmarque esta opção. O Administrador não pode bloquear uma conta. Ele pode desativar a conta, conforme veremos mais adiante, mas a única maneira de bloquear uma conta é o usuário fazer o número definido de tentativas de logon sem sucesso, dentro do período configurado no domínio.

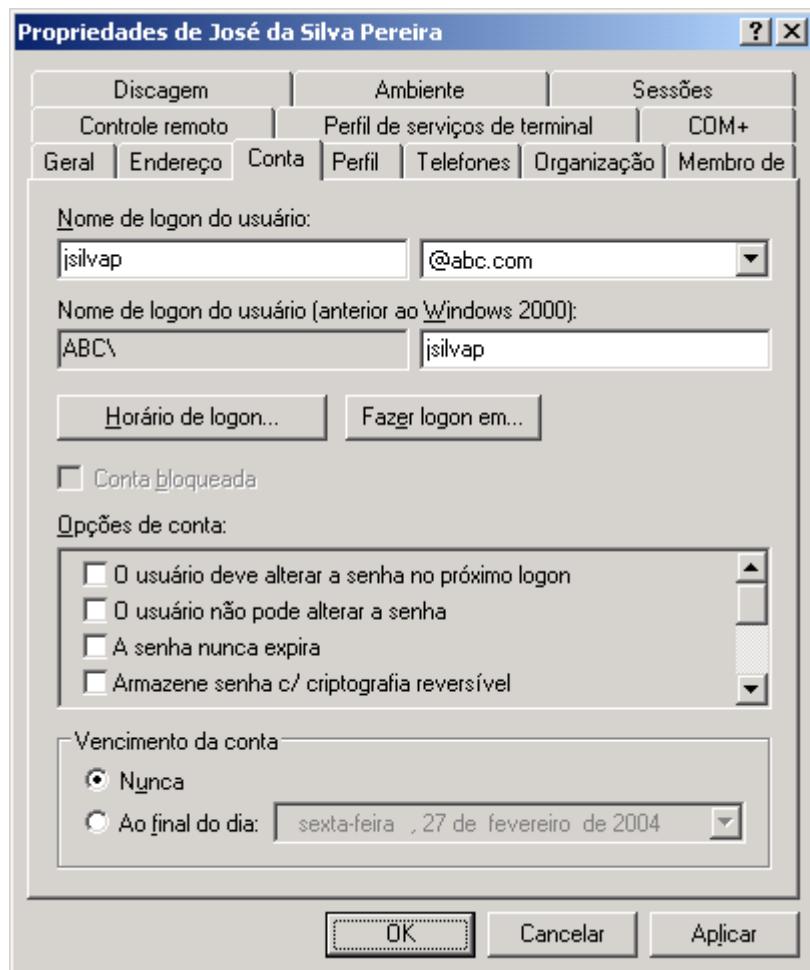


Figura 4.13 Opções de configuração da guia Account (Conta).

Na lista Opções da conta, o administrador pode configurar uma série de opções, descritas a seguir:

- ◆ **O usuário deve alterar a senha no próximo logon:** Se esta opção estiver marcada, a próxima vez que o usuário fizer o logon, será solicitado que ele altere a sua senha. Esta opção é utilizada para que o usuário possa colocar uma senha que somente ele conhece. Quando o usuário é cadastrado, a senha é digitada pelo Administrador, o qual fica sabendo a senha do usuário. No próximo logon o usuário é obrigado a alterar a senha de tal maneira que somente ele saiba qual a senha está definida para a sua conta.
- ◆ **O usuário não pode alterar a senha:** Se esta opção estiver marcada, a senha somente pode ser alterada pelo Administrador. Normalmente utilizada para empregados temporários e para estagiários. Para as contas utilizadas pelos funcionários da empresa, esta opção normalmente é desabilitada.

- ◆ **A senha nunca expira:** Ao marcar esta opção, independente das políticas de segurança do domínio, o usuário nunca precisará trocar a sua senha. Caso contrário de tempos em tempos (conforme configurado nas políticas de segurança do domínio ), o usuário deve trocar a senha.
- ◆ **Gravar senha c/ criptografia reversível:** Esta opção somente deve ser marcada se o usuário precisa fazer o logon no domínio, a partir de estações de trabalho padrão Apple.
- ◆ **Conta desativada:** O Administrador marca esta opção para desativar a conta de um usuário. Usuários com a conta desativada não podem mais efetuar o logon no domínio e, consequentemente, não podem mais acessar recursos da rede. Esta opção normalmente é utilizada para desativar, temporariamente, a conta de empregados que estão em férias. Quando o empregado retorna ao serviço, o Administrador libera a sua conta, simplesmente desmarcando esta opção.
- ◆ **Cartão inteligente necess. p/ logon interativo:** Se esta opção estiver marcada, o usuário somente poderá fazer o logon se estiver utilizando um Smart card. O uso de Smart card aumenta bastante a segurança no logon, uma vez que mesmo de posse da senha do usuário, outra pessoa não conseguirá fazer o logon se não tiver também o Smart card do usuário. É um nível de segurança adicional. Um dos fatores que impedem (ou estão atrasando) o uso em larga escala de Smart card é o custo dos leitores de Smart card.. Quando esta opção for utilizada, a senha da conta do usuário é automaticamente e aleatoriamente criada pelo Windows Server 2003, usando requisitos de complexidade e a opção Password never expires (A senha nunca expira) é selecionada.
- ◆ **Conta sensível à segurança não pode ser deleg.:** Esta é uma opção que deve ser utilizada com muito cuidado, pois pode gerar problemas em relação à segurança. Com esta opção marcada, um hacker poderia tentar fazer se passar por um serviço válido para executar em nome da conta. Com isso o “falso serviço” teria todas as permissões atribuídas a conta. Já imaginou se isso acontecesse com a conta Administrador? O falso serviço simplesmente teria permissões totais em todo o domínio, ou seja, um verdadeiro desastre.
- ◆ **Use tipos de criptografia DES p/ esta conta:** Habilita suporte para o tipo de criptografia conhecido como DES, o qual suporta diversos níveis de criptografia, incluindo MPPE Standard (40-bit), MPPE Standard (56-bit), MPPE Strong (128-bit) IPsec DES (40-bit), Ipsec 56-bit DES e IPsec Triple DES (3DES). Falarei mais sobre criptografia e os mecanismos de autenticação do Windows Server 2003, na parte sobre segurança, nos Capítulos 19 e 20.
- ◆ **Não exige pré-autenticação Kerberos:** O Kerberos é um protocolo de autenticação. Ao marcar esta opção você permite que a conta seja autenticada por servidores utilizando diferentes versões e implementações do protocolo Kerberos.

**IMPORTANTE:** Na parte de baixo da janela você pode definir se a conta nunca expira (Nunca) ou se a conta deve expirar em um determinada data. Expirar significa que a partir da data de expiração, não será mais possível utilizar a conta que expirou para fazer o logon no domínio, a não ser que o administrador acesse as propriedades da conta e defina uma nova data de expiração. Um exemplo prático onde você utiliza esta opção é para contas utilizadas por estagiários. Vamos supor que você contrata os estagiários por períodos definidos. Com isso você pode cadastrar o estagiário e já configurar esta conta para que expire na data de encerramento do estágio. Com isso exatamente no dia do encerramento do estágio a conta será desativada. Agora vamos supor que um novo estagiário tenha sido contratado para substituir o que saiu. Basta ativar novamente a conta, renomeá-la. Informe a conta renomeada para o estagiário. Com isso não é preciso reconfigurar as permissões de acesso, uma vez que a conta é a mesma (apenas foi renomeada), o estagiário que chega tem exatamente as mesmas permissões de acesso do que o que saiu. O que faz sentido, já que ele está substituindo o anterior.

3. Selecione as opções desejadas.
4. Para definir um prazo de expiração para a conta clique na opção Ao final do dia. A lista ao lado desta opção será exibida. Abra esta lista. Será exibido um calendário com o mês corrente. Você pode clicar no botão com a seta para a esquerda para voltar um mês e no botão com a seta para a direita para avançar um mês, conforme destacado na Figura 4.14:



Figura 4.14 Definindo a data de expiração da conta.

5. Para selecionar uma data de expiração basta clicar na respectiva data. A data na qual você clicou é exibida na lista ao lado do campo Ao final do dia.
6. Feitas as configurações desejadas é só clicar em OK para aplicá-las.

### Definindo o horário de logon e os computadores na qual a conta pode fazer o logon.

Por padrão, ao criar uma conta, é permitido que ela seja utilizada para fazer o logon nas 24 horas do dia, nos sete dias da semana. Também é permitido que ele faça o logon em qualquer estação de trabalho. Conforme descrevi anteriormente, por padrão, as contas de usuários não tem permissão para fazer o logon em servidores e DCs do domínio, a menos que pertençam a um grupo que tem estas permissões. Neste item mostrarei como definir o horário em que uma conta pode fazer o logon, bem como limitar os computadores nos quais a conta pode fazer o logon. Por exemplo, vamos supor que você tem um estagiário (sempre os estagiários) que somente deve poder fazer o logon das 8:00 as 12:00, de segunda a sexta-feira e somente em duas estações de trabalho da seção na qual ele trabalha. Você pode configurar estas limitações, facilmente, através das propriedades da conta de usuário do estagiário.

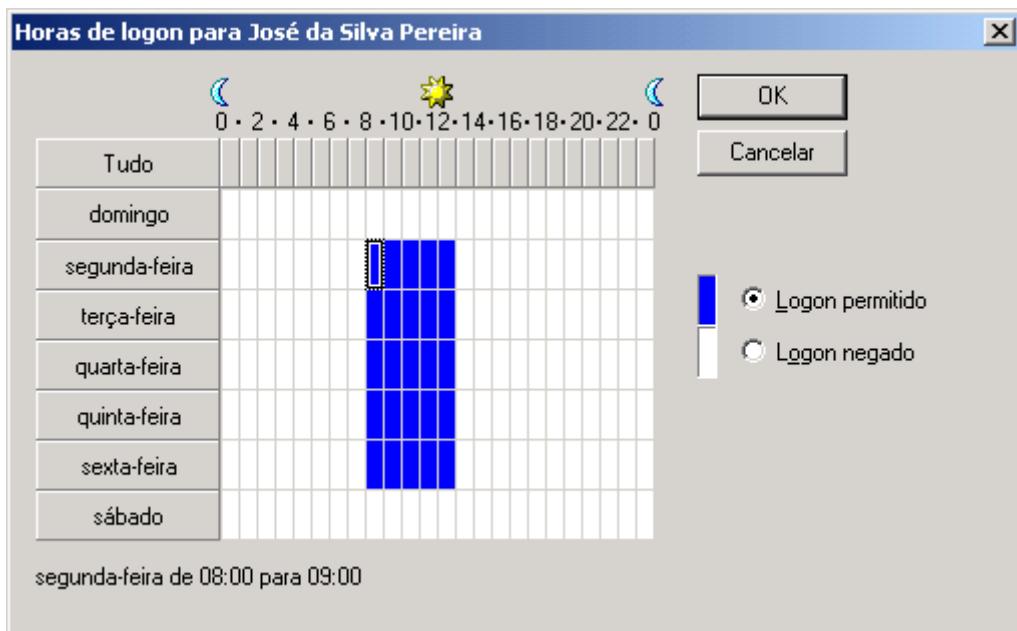
Para limitar o horário em que uma conta pode fazer o logon, siga os passos indicados a seguir:

1. Acesse as propriedades da conta a ser configurada.
2. Dê um clique na guia Conta.
3. Clique no botão Horário de logon...
4. Será exibida a janela Horário de logon para [nome da conta]. Conforme indicado na Figura 4.15. Por padrão é permitido o logon nas 24 horas do dia e nos sete dias da semana.



Figura 4.15 A janela para definir o horário de logon para a conta.

- Quadrinho azul indica horário permitido e quadrinho branco, horário não permitido. Para alterar a cor de um faixa de horário, basta clicar na primeira hora da faixa, manter o botão esquerdo do mouse pressionado e ir arrastando para selecionar um ou mais quadrinhos. A medida que você vai arrastando os quadrinhos vão sendo selecionados. Depois de selecionados basta dar um clique na opção desejada: Logon permitido ou Logon Negado, que o Windows Server 2003 altera a cor do quadrinho de acordo com a opção escolhida.
- Utilize a técnica de arrastar, para configurar os horários permitidos conforme exemplo da Figura 4.16, onde foi habilitado o logon somente no período das 8:00 as 12:00, de segunda à sexta-feira. Neste exemplo você pode primeiro clicar na palavra domingo. Todas as horas do domingo serão selecionadas. Depois clique em Logon denied para negar o logon em todas as horas do domingo. Repita a operação para o sábado. Em seguida você pode marcar a faixa de horário das 13 as 24 horas de segunda à sexta-feira e depois clicar em Logon Denied. Com isso você está limitando o logon somente ao horário proposto, ou seja, de segunda à sexta-feira, das 8:00 as 12:00.



**Figura 4.16 Logon permitido somente de segunda à sexta-feira, das 8:00 às 12:00 hs.**

- Dê um clique no botão OK para aplicar as alterações. Você estará de volta a guia Conta. Clique em OK para fechar a janela de propriedades da conta. Pronto, agora esta conta somente poderá fazer o logon nos horários configurados pelo Administrador.

### Limitando os computadores nos quais o usuário pode fazer o logon.

Agora você aprenderá a limitar os computadores nos quais o usuário pode efetuar o logon. Esse procedimento normalmente é adotado com empregados temporários ou estagiários, de tal forma que o Administrador possa controlar em quais computadores esses usuários podem efetuar o logon. Por padrão, ao ser criada uma conta, não é aplicada restrição em relação as estações de trabalho da rede na qual a conta pode fazer o logon. Neste item você limitará as estações nas quais uma conta pode fazer o logon.

**NOTA:** Para selecionar um dia todo, por exemplo domingo, basta clicar no botão domingo. Isso é muito mais fácil do que arrastar o mouse sobre todos os quadrinhos do domingo. O mesmo é válido para o botão das horas. Se você clicar no botão 8, você selecionará o quadrinho correspondente as 8 horas de todos os dias.

Para definir em quais estações uma conta pode fazer o logon, siga os passos indicados a seguir:

1. Acesse as propriedades da conta a ser configurada.
2. Dê um clique na guia Conta.
3. Clique no botão Fazer logon em...
4. Será exibida a janela Estações de trabalho de logon, conforme indicado na Figura 4.17, por padrão é permitido o logon em todas as estações de trabalho (Todos os computadores).

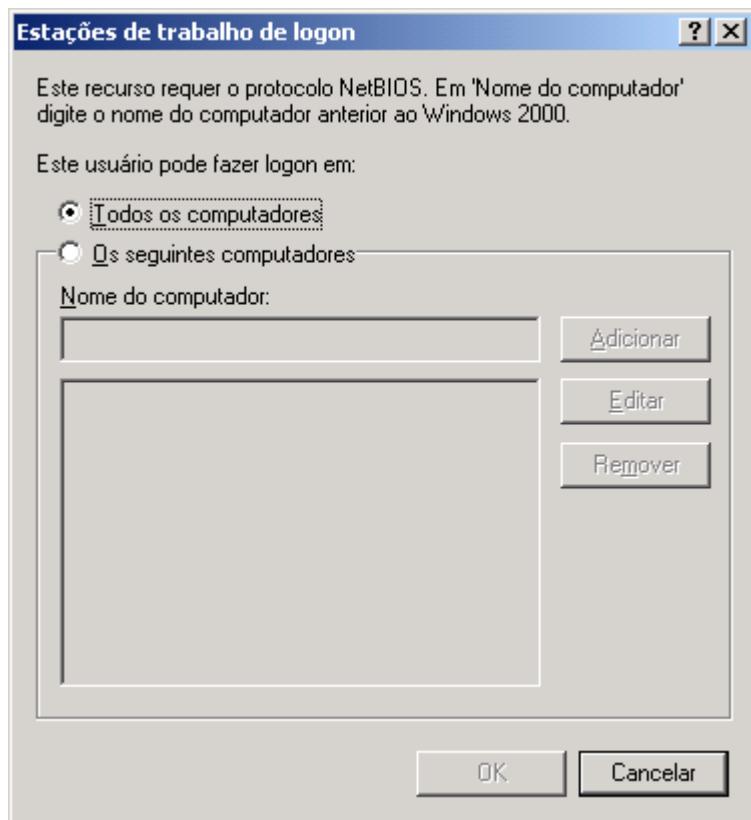


Figura 4.17 Logon permitido, por padrão, em todas as estações de trabalho.

5. Clique na opção Os seguintes computadores. No campo Nome do computador digite o nome da estação de trabalho e clique no botão Adicionar. Repita estes passos para adicionar os demais computadores para os quais a conta terá permissão de logon, conforme exemplo da Figura 4.18, onde foi dada permissão de logon em três computadores: micro01, micro02 e micro03.
6. Após ter inserido o nome dos computadores em que a conta terá permissão de logon, clique em OK.
7. Você estará de volta a guia Conta. Clique em OK para fechar a janela de propriedades da conta e salvar as alterações. Pronto, agora esta limitada a fazer o logon somente nos computadores listados na janela Logon Workstations.

A seguir mostrarei como criar vários contas de usuários, simultaneamente, usando o conceito de modelo de objeto.

---

**NOTA:** Para remover um computador da lista basta clivar no nome do computador para selecioná-lo e em seguida clicar no botão Remover. Para alterar o nome de um computador clique no nome a ser alterado, clique no botão Editar, digite o novo nome e clique em qualquer espaço em branco.



Figura 4.18 Definindo permissão de logon em três computadores.

## Criando e utilizando uma conta modelo

As contas de usuários de uma mesma seção, normalmente, compartilham algumas propriedades em comum. Por exemplo, todas as contas dos funcionários da seção de contabilidade (ou a maioria das contas), terá campos em comum, tais como número de telefone, escritório, grupos aos quais a conta pertence e assim por diante.

Nestas situações, é indicado que você crie uma conta modelo. Por exemplo, você poderia criar uma conta chamada Modelo\_Contabilidade. Ao criar a conta modelo contabilidade, você define as propriedades que serão comuns a todas as contas da seção de contabilidade. Depois você pode usar este modelo, para criar novas contas. As novas contas já irão vir com as propriedades da conta modelo e você só precisará definir as propriedades que são diferentes para cada conta, tais como senha e nome de logon. A vantagem do uso de um modelo de conta é que a criação de novas contas é facilitada e você consegue manter um padrão, para as propriedades que são comuns a todas as contas. A desvantagem é que não é mantido um vínculo entre as contas criadas a partir de um modelo e o respectivo modelo. Por exemplo, se você alterar a conta modelo, as contas que foram criadas a partir do modelo, não irão ser atualizadas com as alterações feitas na conta modelo. Talvez em uma próxima versão do Windows, tenhamos este mecanismo de herança implementado.

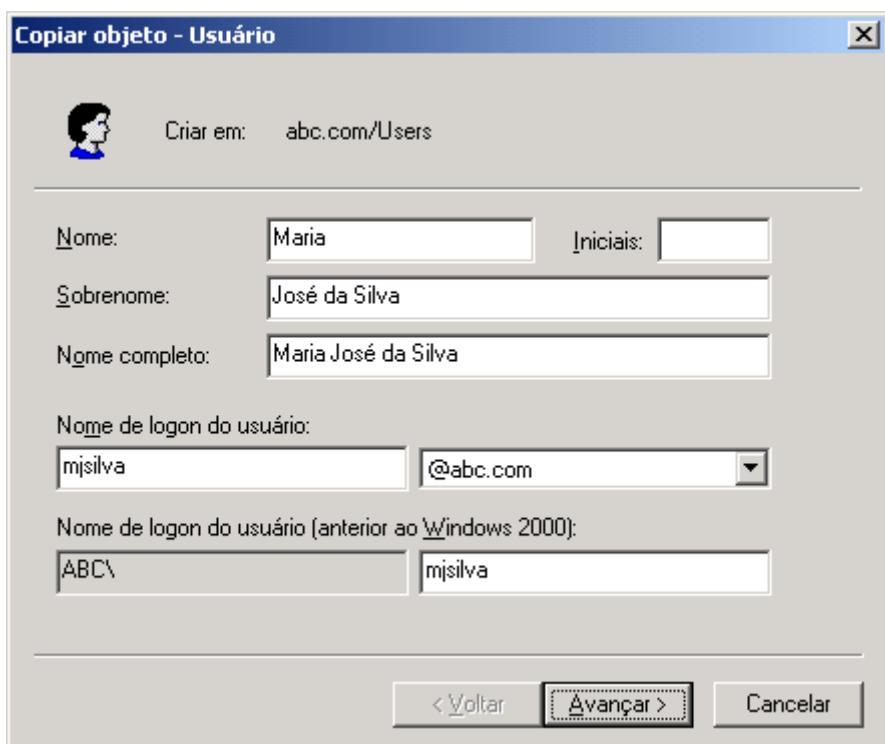
Para criar uma conta modelo você usa os passos descritos nos exemplos práticos anteriores, ou seja, a conta modelo é uma conta normal, como qualquer outra.

No exemplo prático a seguir, mostro como criar uma nova conta, a partir de uma conta modelo.

Exemplo: Para criar uma nova conta, tomando como modelo uma conta já existente, siga os passos indicados a seguir:

1. Faça o logon como Administrador, com uma conta com permissão de Administrador ou com uma conta pertencente ao grupo Oper. de contas (Account Operators).

2. Abra o console Usuários e computadores do Active Directory: Iniciar -> Ferramentas Administrativas -> Usuários e computadores do Active Directory.
3. Localize a conta a ser utilizada como modelo e clique na conta para selecioná-la.
4. Selecione o comando Ação -> Copiar...
5. Será aberta a janela Copiar objeto – Usuário, na qual você deve informar os dados para a nova conta, tais como nome de logon e nome completo, conforme exemplo da Figura 4.19:



**Figura 4.19 Definindo propriedades da nova conta.**

6. Preencha as informações da nova conta e clique em Avançar.
7. Nesta etapa você deve definir uma senha para a nova conta e configurar as opções disponíveis, tais como se o usuário deve ou não trocar a senha no próximo logon, conforme descrito anteriormente.
8. Preencha as informações e clique no botão Avançar.
9. Será exibida a tela final do assistente. Você pode utilizar o botão Voltar, para alterar alguma das configurações feitas nas etapas anteriores. Para criar a conta clique em Concluir.
10. Pronto, a nova conta foi criada e herdou uma série de propriedades da conta utilizada como modelo.

A seguir descrevo quais propriedades, uma nova conta herda da conta modelo:

- ◆ **Guia Geral:** Nenhuma propriedade é herdada do modelo.
- ◆ **Guia Endereço:** Todas as propriedades são herdadas, com exceção do campo Rua.
- ◆ **Guia Conta:** Todas as propriedades são herdadas, com exceção dos campos Nome de logon do usuário e Nome de logon do usuário (anterior ao Windows 2000).

**IMPORTANTE: Como a conta modelo será usada para a criação de novas contas, a partir dela, a conta modelo deve estar com a opção Conta desativada, marcada. Isso porque a conta modelo não deve ser usada para fazer o logon no domínio. Por isso, para impedir que a conta possa ser usada para fazer o logon no domínio, é que você deve marcar a opção Conta desativada.**

- ◆ **Guia Perfil:** Todas as propriedades são copiadas, porém são adaptadas para refletir o nome de logon do usuário que está sendo criado. Por exemplo, se a Pasta base do modelo está em: \\servidor\profiles\modelocont, e está sendo criado um usuário chamado jsilva2, a pasta base do usuário que está sendo criado, será: \\servidor\profiles\jsilva2.
- ◆ **Guia Telefones:** Nenhuma propriedade é copiada.
- ◆ **Guia Organização:** Todas as propriedades são copiadas, com exceção do campo Título.
- ◆ **Guia Membro de:** Todas as informações são copiadas, ou seja, a nova conta, criada a partir de um modelo, pertencerá exatamente aos mesmos grupos aos quais pertence a conta modelo.
- ◆ **Guias Discagem, Ambiente, Sessões, Controle remoto, Perfil de serviços de terminal e COM+:** Nenhuma informação é copiada destas guias, do modelo para a nova conta que está sendo criada.

---

**NOTA:** Mais adiante neste capítulo você aprenderá sobre o conceito de Profiles e sobre como gerenciá-las.

---

## Comandos para trabalhar com contas de usuários.

Além da interface gráfica, usando o console Usuários e computadores do Active Directory, o Administrador tem acesso a uma série de comandos, os quais estão diretamente relacionados com a criação, edição e administração de contas de usuários, bem como a Administração do Active Directory. Estes comandos, normalmente, são utilizados em scripts, para executar uma série de tarefas repetitivas, em um grande número de contas no Active Directory.

A seguir descrevo os principais comandos relacionados ao gerenciamento de contas de usuários e ao gerenciamento do Active Directory.

### O comando CSVDE:

Este comando é utilizado para importar e exportar dados do Active Directory usando arquivos que armazenam dados no formato de valores separados por vírgula (CSV). Você também pode oferecer suporte a operações em lotes no padrão do formato de arquivo CSV. Um arquivo no formato CSV, apresenta um registro em cada linha e os campos de cada registro são separados por vírgula.

Sintaxe para o comando CSVDE:

```
csvde [-i] [-f NomeDoArquivo] [-s NomeDoServidor] [-c Seqüência1 Seqüência2] [-v] [-j Caminho] [-t NúmeroDaPorta] [-d NDBase] [-r FiltroLDAP] [-p Escopo] [-l ListaDeAtributosLDAP] [-o ListaDeAtributosLDAP] [-g] [-m] [-n] [-k] [-a NomeDistintoDoUsuário Senha] [-b NomeDoUsuário Domínio Senha]
```

A seguir a descrição das opções do comando CSVDE:

- ◆ **-i :** Especifica o modo de importação. Se não for especificado, o modo padrão será o de exportação.
- ◆ **-f NomeDoArquivo:** Identifica o nome do arquivo de importação ou de exportação.
- ◆ **-s NomeDoServidor:** Especifica o controlador de domínio que executará a operação de importação ou de exportação.
- ◆ **-c Seqüência1 Seqüência2:** Substitui todas as ocorrências de Seqüência1 por Seqüência2. Em geral, é usado quando os dados são importados de um domínio para outro e o nome distinto do domínio de exportação (Seqüência1) precisa ser substituído pelo domínio de importação (Seqüência2).

---

**IMPORTANTE:** Quando você cria uma nova conta, a partir de um modelo, a nova conta pertencerá aos mesmos grupos aos quais pertence a conta modelo. Com isso, a nova conta, herdará as permissões de acesso, que forem atribuídas a estes grupos. Porém, permissões que tenham sido atribuídas diretamente a conta modelo, não serão herdadas pela nova conta, criada a partir da conta modelo. Fique atento a este detalhe, pois ele pode ser a diferença entre acertar e errar uma ou mais questões no exame.

---

- ◆ **-v:** Define o modo detalhado.
- ◆ **-j Caminho:** Define o local do arquivo de log. O padrão é o caminho atual.
- ◆ **-t NúmeroDaPorta:** Especifica o número da porta LDAP. A porta LDAP padrão é 389. A porta de catálogo global é 3268.
- ◆ **-d NDBase:** Define o nome distinto da base de pesquisa para exportar dados.
- ◆ **-r FiltroLDAP:** Cria um filtro de pesquisa LDAP para exportar dados.
- ◆ **-p Escopo:** Define o escopo da pesquisa. As opções de escopo de pesquisa são Base, OneLevel (um nível) ou SubTree (subárvore).
- ◆ **-l ListaDeAtributosLDAP:** Define a lista de atributos a serem apresentados nos resultados de uma consulta de exportação. Se esse parâmetro for omitido, serão apresentados todos os atributos.
- ◆ **-o ListaDeAtributosLDAP:** Define a lista de atributos a serem omitidos dos resultados de uma consulta de exportação. Normalmente, essa opção é usada quando os objetos são exportados do Active Directory e, em seguida, importados para outro diretório compatível com LDAP. Se não houver suporte a atributos em outro diretório, você poderá omiti-los do conjunto de resultados usando essa opção.
- ◆ **-g:** Omite pesquisas paginadas.
- ◆ **-m:** Omite os atributos que se aplicam somente aos objetos do Active Directory como, por exemplo, os atributos ObjectGUID, objectSID, pwdLastSet e samAccountType.
- ◆ **-n:** Omite a exportação de valores binários.
- ◆ **-k:** Ignora erros durante a operação de importação e continua o processamento. São os seguintes os erros ignorados: “Objeto já existe,” “Violação de restrição” e “Atributo ou valor já existe”.
- ◆ **-a NomeDistintoDoUsuário Senha:** Define o comando a ser executado usando o NomeDistintoDoUsuário e a Senha fornecidos. Por padrão, o comando será executado usando as credenciais do usuário conectado à rede no momento.
- ◆ **-b NomeDoUsuário Domínio Senha:** Define que o comando seja executado como NomeDoUsuário Domínio Senha. Por padrão, o comando será executado usando as credenciais do usuário conectado à rede no momento.
- ◆ **-?:** Exibe uma tela de ajuda sobre o comando.

Aplicativos como o Microsoft Excel são capazes de ler e salvar dados no formato CSV. Além disso, as ferramentas de administração do Microsoft Exchange Server também podem importar e exportar dados usando o formato CSV, assim como outras ferramentas que não foram desenvolvidas pela Microsoft.

O formato CSV consiste em uma ou mais linhas de dados, com cada valor separado por uma vírgula. A primeira linha (algumas vezes chamada de cabeçalho) do arquivo CSV deve conter os nomes de cada atributo na mesma ordem que os dados de todas as linhas seguintes à primeira. Por exemplo:

```
NC, Nome, Sobrenome, Descrição
NomeDeLogonDoPrimeiroUsuário, NomeDoPrimeiroUsuário, SobrenomeDoPrimeiroUsuário, Gerente
NomeDeLogonDoSegundoUsuário, NomeDoSegundoUsuário, SobrenomeDoSegundoUsuário, Presidente
```

Você pode usar csvde -r para criar um filtro de pesquisa LDAP para exportar dados. Por exemplo, o filtro a seguir exporta todos os usuários com determinado sobrenome:

```
csvde -r (and(objectClass=Usuário) (sn=Sobrenome))
```

## O comando DSADD:

Este comando é utilizado para adicionar tipos específicos de objetos ao Active Directory, tais como usuários, grupos, etc. A seguir descrevo as diferentes opções do comando DSADD

### dsadd computer

É utilizado para adicionar um único computador ao diretório.

Sintaxe:

```
dsadd computer NDComputador [-samid NomeSAM] [-desc Descrição] [-loc Local] [-memberof NDGrupo ...] [{-s Servidor | -d Domínio}] [-u NomeDoUsuário] [-p {Senha | *}] [-q] [{-uc | -uco | -uci}]
```

Os parâmetros deste comando são os seguintes:

- ◆ **NDComputador:** Obrigatório. Especifica o nome distinto do computador a ser adicionado. Se o nome distinto for omitido, ele será retirado da entrada padrão (stdin).
- ◆ **-samid NomeSAM:** Determina a utilização do nome SAM como único nome de conta SAM para este computador (por exemplo, TESTPC2\$). Se este parâmetro não for especificado, um nome de conta SAM será obtido a partir do valor do atributo nome comum utilizado em NDComputador.
- ◆ **-desc Descrição:** Especifica a descrição do computador a ser adicionado.
- ◆ **-loc Local:** Especifica o local do computador a ser adicionado.
- ◆ **-memberof NDGrupo ...:** Especifica os grupos nos quais você deseja o computador como membro.
- ◆ **{-s Servidor | -d Domínio}:** Conecta o computador com um servidor ou domínio especificado. Por padrão, o computador é conectado com o controlador de domínio no domínio de logon.
- ◆ **-u NomeDoUsuário:** Especifica o nome de usuário utilizado para logon em um servidor remoto. Por padrão, -u utiliza o nome de usuário com o qual o usuário fez logon. Qualquer um dos formatos a seguir pode ser utilizado para especificar um nome de usuário:
  - ◆ nome de usuário (por exemplo, Raquel)
  - ◆ domínio\nome de usuário (por exemplo, widgets\Raquel)
  - ◆ UPN (nome principal do usuário) (por exemplo, Raquel@widgets.microsoft.com)
- ◆ **-p {Senha | \*}:** Especifica o uso de uma senha ou de um \* para fazer logon em um servidor remoto. Se você digitar \*, deverá fornecer uma senha.
- ◆ **-q:** Elimina toda a saída para a saída padrão (modo silencioso).
- ◆ **{-uc | -uco | -uci}:** Especifica que os dados de saída ou de entrada serão formatados em Unicode. A tabela a seguir lista e descreve cada formato, conforme indicado a seguir:
  - ◆ **-uc:** Especifica um formato Unicode para entrada de um pipe ou saída para um pipe ()|.
  - ◆ **-uco:** Especifica um formato Unicode para saída para um pipe ()| ou para um arquivo.
  - ◆ **-uci:** Especifica um formato Unicode para entrada de um pipe ()| ou para um arquivo.
- ◆ **/?:** Exibe ajuda no prompt de comando.

Se você não fornecer um objeto de destino no prompt de comando, ele será obtido na saída padrão (stdin). Os dados de stdin podem ser aceitos a partir do teclado, de um arquivo redirecionado ou como saída em pipe de outro comando. Para marcar o fim dos dados stdin a partir do teclado ou em um arquivo redirecionado, use o caractere de fim de arquivo (CTRL+Z).

Se o valor fornecido contiver espaços, utilize o texto entre aspas (por exemplo, “CN=DC 2,OU=Controladores domínio,DC=Microsoft,DC=Com”).

Se você fornecer diversos valores para um parâmetro, use espaços para separá-los (por exemplo, uma lista de nomes distintos).

## dsadd group

Este comando é utilizado para adicionar um único grupo ao diretório.

Sintaxe:

```
dsadd group NDGrupo [-secgrp {yes | no}] [-scope {l | g | u}] [-samid NomeSAM] [-desc Descrição] [-memberof Grupo ...] [-members Membro ...] [{-s Servidor | -d Domínio}] [-u NomeDoUsuário] [-p {Senha | *}] [-q] [{-uc | -uco | -uci}]
```

Descrição dos parâmetros utilizados pelo comando dsadd group:

- ◆ **NDGrupo:** Obrigatório. Especifica o nome distinto do grupo a ser adicionado. Se o nome distinto for omitido, será obtido da entrada padrão (stdin).
- ◆ **-secgrp {yes | no}:** Especifica se o grupo a ser adicionado é um grupo de segurança (yes) ou um grupo de distribuição (no). Por padrão, o grupo é adicionado como grupo de segurança (yes).
- ◆ **-scope {l | g | u}:** Especifica se o escopo do grupo a ser adicionado é domínio local (l), global (g), ou universal (u). Se o domínio estiver no modo misto, não haverá suporte a escopo universal. Por padrão, o escopo do grupo é definido como global.
- ◆ **-samid NomeSAM:** Especifica a utilização do nome SAM como o único nome de conta SAM para este grupo (por exemplo, operadores). Se este parâmetro não for especificado, será gerado a partir do nome distinto relativo.
- ◆ **-desc Descrição:** Especifica a descrição do grupo a ser adicionado.
- ◆ **-memberof Grupo ... :** Especifica os grupos aos quais este novo grupo deverá ser adicionado.
- ◆ **-members Membros ...:** Especifica os membros a serem adicionados ao novo grupo.
- ◆ **{-s Servidor | -d Domínio}:** Estabelece conexão com um servidor ou domínio remoto especificado. Por padrão, o computador fica conectado ao controlador de domínio no domínio de logon.
- ◆ **-u NomeDoUsuário:** Especifica o nome usado pelo usuário para fazer logon em um servidor remoto. Por padrão, -u utiliza o nome de usuário com o qual o usuário fez logon. Qualquer um dos formatos a seguir pode ser utilizado para especificar um nome de usuário:
  - ◆ nome do usuário (por exemplo, Raquel)
  - ◆ domínio\nome do usuário (por exemplo, widgets\Raquel)
  - ◆ UPN (nome principal do usuário) (por exemplo, Raquel@widgets.microsoft.com)
- ◆ **-p {Senha | \*}:** Especifica o uso de uma senha ou de um \* para fazer logon em um servidor remoto. Se você digitar \*, deverá fornecer uma senha.
- ◆ **-q:** Elimina toda a saída para a saída padrão (modo silencioso).
- ◆ **{-uc | -uco | -uci}:** Especifica que os dados de saída ou de entrada serão formatados em Unicode. A tabela a seguir lista e descreve cada formato:
  - ◆ **-uc** Especifica um formato Unicode para entrada de um pipe ou saída para um pipe (|).
  - ◆ **-uco** Especifica um formato Unicode para saída para um pipe (|) ou para um arquivo.
  - ◆ **-uci** Especifica um formato Unicode para entrada de um pipe (|) ou para um arquivo.
- ◆ **/?:** Exibe ajuda no prompt de comando.

## dsadd ou

Este comando é utilizado para adicionar uma única unidade organizacional ao diretório.

Sintaxe:

```
dsadd ou NDUnidadeOrganizacional [-desc Descrição] [{-s Servidor | -d Domínio}] [-u NomeDoUsuário] [-p {Senha | *}] [-q] [{-uc | -uco | -uci}]
```

Parâmetros utilizados pelo comando dsadd ou:

- ◆ **NDUnidadeOrganizacional**: Obrigatório. Especifica o nome distinto da unidade organizacional a ser adicionada. Se o nome distinto for omitido, será obtido da entrada padrão (stdin).
- ◆ **-desc Descrição**: Especifica a descrição da unidade organizacional a ser adicionada.
- ◆ **{-s Servidor | -d Domínio}**: Estabelece conexão com um servidor ou domínio remoto especificado. Por padrão, o computador fica conectado ao controlador de domínio no domínio de logon.
- ◆ **-u NomeDoUsuário**: Especifica o nome usado pelo usuário para fazer logon em um servidor remoto. Por padrão, é utilizado o nome do usuário que fez logon. É possível especificar um nome de usuário usando um dos seguintes formatos:
  - ◆ nome do usuário (por exemplo, Raquel)
  - ◆ domínio\nome do usuário (por exemplo, widgets\Raquel)
  - ◆ UPN (nome principal do usuário) (por exemplo, [Raquel@widgets.microsoft.com](mailto:Raquel@widgets.microsoft.com))
- ◆ **-p {Senha | \*}**: Especifica o uso de uma senha ou de um \* para fazer logon em um servidor remoto. Se você digitar \*, deverá fornecer uma senha.
- ◆ **-q**: Elimina toda a saída para a saída padrão (modo silencioso).
- ◆ **{-uc | -uco | -uci}**: Especifica que os dados de saída ou de entrada serão formatados em Unicode. A tabela a seguir lista e descreve cada formato:
  - ◆ **-uc** Especifica um formato Unicode para entrada de um pipe ou saída para um pipe () .
  - ◆ **-uco** Especifica um formato Unicode para saída para um pipe () ou para um arquivo.
  - ◆ **-uci** Especifica um formato Unicode para entrada de um pipe () ou para um arquivo.
- ◆ **/?**: Exibe ajuda no prompt de comando.

## dsadd user

Adiciona um usuário único ao diretório.

Sintaxe:

```
dsadd user NDUsuário [-samid NomeSAM] [-upn UPN] [-fn Nome] [-mi Inicial] [-ln Sobrenome] [-display NomeParaExibição] [-empid IdentificaçãoFuncional] [-pwd {Senha | *}] [-desc Descrição] [-memberof Grupo ...] [-office Escritório] [-tel Telefone] [-email Email] [-hometel TelefoneResidencial] [-pager Pager] [-mobile Celular] [-fax Fax] [-iptel TelefoneIP] [-webpg PáginaDaWeb] [-title Cargo] [-dept Departamento] [-company Empresa] [-mgr Gerente] [-hmdir DiretórioBase] [-hmdrv LetraDaUnidade:] [-profile CaminhoDoPerfil] [-loscr CaminhoDoScript] [-mustchpwd {yes | no}] [-canchpwd {yes | no}] [-reversiblepwd {yes | no}] [-pwdneverexpires {yes | no}] [-acctexpires NúmeroDeDias] [-disabled {yes | no}] [{-s Servidor | -d Domínio}] [-u NomeDoUsuário] [-p {Senha | *}] [-q] [{-uc | -uco | -uci}]
```

Parâmetros utilizados pelo comando dsadd user:

- ◆ **NDUsuário:** Obrigatório. Especifica o nome distinto do usuário a ser adicionado. Se o nome distinto for omitido, será obtido da entrada padrão (stdin).
- ◆ **-samid NomeSAM:** Determina o nome SAM como único nome de conta SAM para este usuário (por exemplo, Raquel). Se não for especificado, o dsadd tentará criar um nome de conta SAM utilizando (no máximo) os 20 primeiros caracteres do valor nome comum (CN) do NDUsuário.
- ◆ **-upn UPN:** Especifica o nome principal do usuário a ser adicionado, (por exemplo, Linda@widgets.microsoft.com).
- ◆ **-fn Nome:** Especifica o nome do usuário a ser adicionado.
- ◆ **-mi Inicial:** Especifica a letra inicial central do usuário a ser adicionado.
- ◆ **-ln Sobrenome:** Especifica o sobrenome do usuário a ser adicionado.
- ◆ **-display NomeParaExibição:** Especifica o nome para exibição do usuário a ser adicionado.
- ◆ **-empid IdentificaçãoFuncional:** Especifica a identificação funcional do usuário a ser adicionado.
- ◆ **-pwd {Senha | \*}:** Especifica a senha do usuário a ser definida como Senha ou \*. Se for definida como \*, você será solicitado a fornecer uma senha de usuário.
- ◆ **-desc Descrição:** Especifica a descrição do usuário a ser adicionado.
- ◆ **-memberof NDGrupo ...:** Especifica os nomes distintos dos grupos nos quais você deseja incluir o usuário como membro.
- ◆ **-office Escritório:** Especifica o local do escritório do usuário a ser adicionado.
- ◆ **-tel Telefone:** Especifica o número do telefone do usuário a ser adicionado.
- ◆ **-email Email:** Especifica o endereço de email do usuário a ser adicionado.
- ◆ **-hometel TelefoneResidencial:** Especifica o número do telefone residencial do usuário a ser adicionado.
- ◆ **-pager Pager:** Especifica o número do pager do usuário a ser adicionado.
- ◆ **-mobile Celular:** Especifica o número do telefone celular do usuário a ser adicionado.
- ◆ **-fax Fax:** Especifica o número do fax do usuário a ser adicionado.
- ◆ **-iptel TelefoneIP:** Especifica o número do telefone IP do usuário a ser adicionado.
- ◆ **-webpg PáginaDaWeb:** Especifica a URL de página da Web do usuário a ser adicionado.
- ◆ **-title Cargo:** Especifica o cargo do usuário a ser adicionado.
- ◆ **-dept Departamento:** Especifica o departamento do usuário a ser adicionado.
- ◆ **-company Empresa:** Especifica as informações sobre a empresa do usuário a ser adicionado.
- ◆ **-mgr NDGerente:** Especifica o nome distinto do gerente do usuário a ser adicionado.
- ◆ **-hmdir DiretórioBase:** Especifica o local do diretório base do usuário a ser adicionado. Se o DiretórioBase for apresentado como um caminho UNC, você deverá especificar uma letra de unidade a ser mapeada até esse caminho utilizando o parâmetro -hmdrv.
- ◆ **-hmdrv LetraDaUnidade:** Especifica a letra de unidade do diretório base (por exemplo, E:) do usuário a ser adicionado.
- ◆ **-profile CaminhoDoPerfil:** Especifica o caminho do perfil do usuário a ser adicionado.
- ◆ **-loscr CaminhoDoScript:** Especifica o caminho do script de logon do usuário a ser adicionado.
- ◆ **-mustchpwd {yes | no}:** Especifica se os usuários deverão alterar suas senhas no próximo logon (yes) ou não (no). Por padrão, o usuário não precisa mudar a senha (no).
- ◆ **-canchpwd {yes | no}:** Especifica se os usuários poderão alterar suas senhas (yes) ou não (no). Por padrão, é permitido ao usuário mudar a senha (yes). O valor desse parâmetro deverá ser yes se o valor do parâmetro -mustchpwd for yes.
- ◆ **-reversiblepwd {yes | no}:** Especifica se a senha do usuário deverá ser armazenada utilizando criptografia reversível (yes) ou não (no). Por padrão, o usuário não pode utilizar a criptografia reversível (no).

- ◆ **-pwdneverexpires {yes | no}**: Especifica se a senha do usuário nunca expira (yes) ou expira (no). Por padrão, a senha do usuário expira (no).
- ◆ **-acctexpires NúmeroDeDias**: Especifica o número de dias a partir da data atual para expiração da conta do usuário. Um valor 0 define a expiração para o final do dia de hoje. Um valor positivo define a expiração no futuro. Um valor negativo define a expiração no passado. O valor never define que a conta nunca deverá expirar. Por exemplo, um valor 0 fará a conta perder a validade no final do dia de hoje. Um valor -5 indica que a conta já expirou há cinco dias e define uma data de validade no passado. Um valor 5 define a expiração da conta para daqui a cinco dias.
- ◆ **-disabled {yes | no}**: Especifica se a conta de usuário será desativada para o logon (yes) ou não (no). Por padrão, a conta do usuário fica habilitada para logon (no).
- ◆ **{-s Servidor | -d Domínio}**: Estabelece conexão com um servidor ou domínio remoto especificado. Por padrão, o computador fica conectado ao controlador de domínio no domínio de logon.
- ◆ **-u NomeDoUsuário**: Especifica o nome usado pelo usuário para fazer logon em um servidor remoto. Por padrão, -u utiliza o nome de usuário com o qual o usuário fez logon. Qualquer um dos formatos a seguir pode ser utilizado para especificar um nome de usuário:
  - ◆ nome do usuário (por exemplo, Raquel)
  - ◆ domínio\nome do usuário (por exemplo, widgets\Raquel)
  - ◆ UPN (nome principal do usuário) (por exemplo, Raquel@widgets.microsoft.com)
- ◆ **-p {Senha | \*}**: Especifica o uso de uma senha ou de um \* para fazer logon em um servidor remoto. Se você digitar \*, deverá fornecer uma senha.
- ◆ **-q**: Elimina toda a saída para a saída padrão (modo silencioso).
- ◆ **{-uc | -uco | -uci}**: Especifica que os dados de saída ou de entrada serão formatados em Unicode. A tabela a seguir lista e descreve cada formato.
  - ◆ **-uc** Especifica um formato Unicode para entrada de um pipe ou saída para um pipe () .
  - ◆ **-uco** Especifica um formato Unicode para saída para um pipe () ou para um arquivo.
  - ◆ **-uci** Especifica um formato Unicode para entrada de um pipe () ou para um arquivo.
- ◆ **/?**: Exibe ajuda no prompt de comando.

O símbolo especial \$username\$ (sem diferenciação de maiúsculas ou minúsculas) pode substituir o nome de conta SAM no valor dos parâmetros -email, -hmdir, -profile e -webpg. Por exemplo, se um nome de conta SAM for “Denise”, o parâmetro -hmdir poderá ser escrito num dos seguintes formatos:

```
-hmdir\usuarios\Denise\base
-hmdir\usuarios\$username$\base
```

O uso de senhas de alta segurança em todas as contas de usuário ajuda a minimizar os riscos de segurança. Para obter mais informações sobre senhas de alta segurança, consulte Tópicos relacionados.

## **dsget user**

Este comando é utilizado para exibir as várias propriedades de um usuário no diretório. Esse comando dispõe de duas variações. A primeira permite exibir as propriedades de vários usuários. A segunda permite exibir as informações de participação em um grupo de um usuário único.

Sintaxe:

```
dsget user NDUsuário ... [-dn] [-samid] [-sid] [-upn] [-fn] [-mi] [-ln] [-display] [-empid] [-desc] [-office] [-tel] [-email] [-hometel] [-pager] [-mobile] [-fax] [-iptel] [-webpg] [-title] [-dept] [-company] [-mgr] [-hmdir] [-hmdrv] [-profile] [-loscr] [-mustchpwd] [-canchpwd] [-pwdneverexpires] [-disabled] [-acctexpires] [-reversiblepwd] [{-uc | -uco | -uci}] [-part ND_da_partição [-qlimit] [-qused]]  
dsget user ND_do_usuário [-memberof] [-expand] [{-uc | -uco | -uci}]
```

Parâmetros:

- ◆ **NDUsuário ...**: Obrigatório. Especifica os nomes distintos dos objetos de usuário a serem exibidos. Se algum valor for omitido, ele será obtido através da entrada padrão (stdin) para oferecer suporte ao pipe de saída de outro comando para entrada deste comando. Compare com NDUsuário na próxima variação de comando.
- ◆ **-dn**: Exibe os nomes distintos dos usuários.
- ◆ **-samid**: Exibe os nomes de conta SAM dos usuários.
- ◆ **-sid**: Exibe as identificações de segurança do usuário (SIDs).
- ◆ **-upn**: Exibe os nomes principais dos usuários.
- ◆ **-fn**: Exibe os nomes dos usuários.
- ◆ **-mi**: Exibe as iniciais centrais dos usuários.
- ◆ **-ln**: Exibe os sobrenomes dos usuários.
- ◆ **-display**: Exibe os nomes para exibição dos usuários.
- ◆ **-empid**: Exibe as identificações funcionais dos usuários.
- ◆ **-desc**: Exibe as descrições dos usuários.
- ◆ **-full**: Exibe os nomes completos dos usuários.
- ◆ **-office**: Exibe a localização dos escritórios dos usuários.
- ◆ **-tel**: Exibe os números de telefone dos usuários.
- ◆ **-email**: Exibe os endereços de email dos usuários.
- ◆ **-hometel**: Exibe os números de telefone residencial dos usuários.
- ◆ **-pager**: Exibe os números de pager dos usuários.
- ◆ **-mobile**: Exibe os números de telefone celular dos usuários.
- ◆ **-fax**: Exibe os números de fax dos usuários.
- ◆ **-iptel**: Exibe os números de telefone IP dos usuários.
- ◆ **-webpg**: Exibe as URLs das páginas na Web dos usuários.
- ◆ **-title**: Exibe os cargos dos usuários.
- ◆ **-dept**: Exibe os departamentos dos usuários.
- ◆ **-company**: Exibe as informações sobre a empresa dos usuários.
- ◆ **-mgr**: Exibe os gerentes dos usuários.
- ◆ **-hmdir**: Exibe a letra de unidade à qual o diretório base do usuário está mapeado se o caminho desse diretório for UNC.
- ◆ **-hmdrv**: Exibe a letra de unidade da base do usuário se o diretório base for um caminho UNC.
- ◆ **-profile**: Exibe os caminhos dos perfis de usuário.
- ◆ **-loscr**: Exibe os caminhos dos scripts de logon dos usuários.
- ◆ **-mustchpwd**: Exibe informações que especificam se os usuários devem alterar suas senhas no próximo logon (yes) ou não (no).

- ◆ **-canchpwd:** Exibe informações que especificam se os usuários podem alterar suas senhas (yes) ou não (no).
- ◆ **-pwdneverexpires:** Exibe informações que especificam se as senhas de usuário nunca expiram (yes) ou expiram (no).
- ◆ **-disabled:** Exibe informações que especificam se as contas de usuário são desabilitadas para logon (yes) ou não (no).
- ◆ **-acctexpires:** Exibe datas indicando quando as contas de usuário expiram. Se as contas nunca expirarem, será exibido never.
- ◆ **-reversiblepwd:** Exibe informações que especificam se as senhas de usuário podem ser armazenadas com uso de criptografia reversível (yes) ou não (no).
- ◆ **NDUsuário:** Obrigatório. Especifica o nome distinto do usuário a ser exibido.
- ◆ **-memberof:** Exibe a lista de grupos imediatos dos quais o usuário é membro.
- ◆ **-expand:** Exibe a lista expandida em modo recursivo dos grupos dos quais o usuário é membro. Esta opção obtém a lista de grupos imediatos dos quais o usuário é membro e, em seguida, expande de forma recursiva cada grupo da lista para determinar seus membros e também chegar a um conjunto final completo dos grupos.
- ◆ **{-uc | -uco | -uci}:** Especifica que os dados de saída ou de entrada sejam formatados em Unicode. A tabela a seguir lista e descreve cada formato.
  - ◆ **-uc** Especifica um formato Unicode para entrada de um pipe ou saída para um pipe ()|.
  - ◆ **-uco** Especifica um formato Unicode para saída para um pipe ()| ou para um arquivo.
  - ◆ **-uci** Especifica um formato Unicode para entrada de um pipe ()| ou para um arquivo.
- ◆ **-part NDPartição:** Faz conexão com a partição de diretório com o nome distinto de NDPartição.
- ◆ **-qlimit:** Exibe a cota efetiva do usuário na partição de diretório especificada.
- ◆ **-qused:** Exibe quanto da cota o usuário usou na partição de diretório especificada. Valor Descrição
- ◆ **/?:** exibe ajuda no prompt de comando.

O -canchpwd é uma estimativa sobre a questão do usuário ter permissão para alterar sua senha. Essa estimativa tem a ver com o modo como as ACLs (listas de controle de acesso) no objeto são interpretadas a fim de chegar a uma resposta afirmativa ou negativa. A certeza quanto à capacidade do usuário de mudar uma senha só poderá ser conhecida mediante a tentativa. Essa resposta não-autorizada não é específica desta ferramenta de linha de comando, mas é também inerente à caixa de diálogo Propriedades do usuário em Usuários e computadores do Active Directory no Console de gerenciamento Microsoft (MMC).

Quando nenhum parâmetro de propriedade específico for definido para o comando dsget user, o conjunto padrão de propriedades do usuário a ser exibido incluirá o seguinte: nome distinto, nome da conta SAM e descrição.

Quando o parâmetro -memberof é especificado, ele cancela todos os outros parâmetros e somente a lista de participação do usuário é exibida.

Exemplos:

Para localizar todos os usuários em determinada unidade organizacional cujos nomes começam com “jon” e exibir suas descrições, digite:

```
dsquery user OU=Test,dc=ms,dc=tld -name jon* | dsget user -desc
```

Para exibir a lista de grupos, expandida de modo recursivo, à qual pertence o usuário “Mike Danseglio”, digite:

```
dsget user "CN=Mike Danseglio,CN=users,dc=ms,dc=tld" -memberof -expand
```

## Outros comandos disponíveis:

A seguir apresenta uma lista de outros comandos disponíveis. Você encontra informações detalhadas sobre estes comandos, na Ajuda do Windows Server 2003, digitando o nome do comando, no campo de pesquisa da Ajuda.

- ◆ **dsmod:** É utilizado para modificar atributos selecionados de um objeto existente no Active directory. Por exemplo, pode ser utilizado para modificar informações sobre um usuário, grupo ou unidade organizacional do Active Directory.
- ◆ **dsquery:** É utilizado para localizar objetos no Active Directory, de acordo com um ou mais critérios de pesquisa, especificados.
- ◆ **dsmove:** É utilizado para mover um objeto de seu local atual para um novo local pai.
- ◆ **dsrm:** É utilizado para remover um objeto, a subárvore completa abaixo de um objeto no diretório, ou ambos.

Muito bem, feita a apresentação dos principais comandos para gerenciamento de objetos no Active Directory, a seguir falarei sobre o conceito de Profile e mostrarei como configurar a profile associada a um usuário, através das propriedades da conta do usuário.

## O Conceito de Profiles

O Windows Server 2003 (a exemplo do que ocorre no Windows 2000 e no Windows XP), mantém configurações de ambiente separadas para cada usuário. Por exemplo, o usuário jsilva faz o logon e cria um ícone na área de trabalho. Este ícone não será exibido na área de trabalho de outros usuários, quando estes fizerem o logon no computador. O Windows também mantém diversas outras configurações separadamente para cada usuário, como por exemplo: papel de parede, opções do menu iniciar, configurações do Internet Explorer e do Outlook Express, associação de extensões de arquivos, configurações da barra de tarefas e assim por diante. A pasta Meus documentos também é individualizada para cada usuário. O Windows Server 2003 mantém estas configurações separadamente para cada usuário, através de uma estrutura de pastas e subpastas, dentro da pasta C:\Documents and settings. Dentro desta pasta o Windows Server 2003 cria uma pasta para cada usuário, pasta esta com o nome de logon do usuário.

Por exemplo, todas as configurações do usuário jsilvap são gravadas e mantidas em uma estrutura de subpastas, dentro de C:\Documents and settings\jsilvap; todas as configurações do usuário pedro2 são gravadas e mantidas em uma estrutura de subpastas, dentro de C:\Documents and settings\paulo2 e assim por diante.

Este conjunto de configurações, que define o ambiente de trabalho de cada usuário, é conhecido como Profile do usuário (User Profile). Quando você trabalha em um ambiente de rede, baseado em um domínio do Windows 2000 Server ou do Windows Server 2003, é possível salvar as configurações da Profile de cada usuário em pastas em um servidor da rede. Este tipo de Profile é conhecido como Roaming Profile (eu me arriscaria a traduzir como Profile Viajante).

O Roaming significa que a Profile acompanha (viaja com) o usuário através da rede. Ou seja, independente da estação de trabalho que o usuário estiver utilizando, ele receberá as configurações de sua Profile, as quais serão carregadas a partir da rede. Com a combinação do recurso de User Profiles com a distribuição de Software via GPO (assunto abordado em detalhes no Capítulo 18 do livro: [Windows Server 2003 – Curso Completo](#), 1568 páginas), é possível fazer com que os programas e as configurações “sigam” o usuário através da rede, ou seja, em qualquer estação de trabalho que o usuário faça o logon, ele terá a mesma área de trabalho, com o mesmo conjunto de ícones, atalhos e programas. Neste tópico você aprenderá sobre Profiles.

## Vantagens de se Utilizar Profiles:

- ◆ Vários usuários podem utilizar o mesmo computador, sem que as configurações feitas por um dos usuários, afetem o ambiente de trabalho dos demais usuários. Quando o usuário faz o logon ele recebe exatamente o mesmo ambiente de trabalho que ele deixou, quando fez o último log off.
- ◆ User profiles podem ser gravadas em uma pasta compartilhada em um servidor, de tal maneira que as configurações “sigam” o usuário através da rede. Esta opção está disponíveis para computadores rodando o Windows NT, Windows 2000, Windows XP ou Windows Server 2003. Não está disponível para o Windows 95/98/Me. O uso de User Profiles é uma ferramenta de grande auxílio para o administrador, principalmente para a padronização do ambiente de trabalho dos usuários. O administrador pode utilizar o conceito de User Profiles para executar, dentre outras, as seguintes configurações:
- ◆ Criar uma profile padrão e distribuir esta profile para um grupo de usuários da rede. Esta opção é útil para usuários que devam ter acesso restrito as opções de personalização do windows. Por exemplo, posso usar uma profile para definir, automaticamente, os ícones da área de trabalho para um grupo de usuários.
- ◆ Você pode criar as chamadas “Mandatory user profile”. Este tipo de profile não permite que o usuário faça alterações nas configurações definidas na profile. O usuário até consegue alterar o seu ambiente de trabalho, mas no momento em que for feito o log off, as alterações não serão salvas. Ao fazer o próximo logon, o usuário receberá as configurações definidas na profile, sem as alterações que ele fez, mas que não foram salvas. As configurações são copiadas para o computador do usuário cada vez que este faz o logon. Quando o usuário faz alterações, estas são feitas na sua cópia local da profile. Ao fazer o logoff, estas alterações não são repassadas para a profile que está gravada no servidor. No próximo logon é esta profile que está no servidor (sem alterações) que é novamente copiada para a estação de trabalho do usuário, sobrescrevendo as alterações que por ventura ele tenha feito. O resultado prático é que sempre que o logon é feito, são carregadas as configurações definidas na profile do tipo Mandatory, armazenada no servidor e para a qual somente o Administrador tem permissão para fazer alterações.

## Tipos de User Profile:

- ◆ **Local user profile (profile de usuário – local):** Este tipo de profile é criada a primeira vez que o usuário faz o logon em um computador com o Windows NT 4.0 (Server ou Workstation), com o Windows 2000 (Server ou Professional), com o Windows XP (Home ou Professional) ou com o Windows Server 2003. A profile é criada dentro de uma pasta com o mesmo nome do usuário, em C:\Documents and settings. Por exemplo, a primeira vez que o usuário jsilva fizer o logon no computador, a sua profile será criada em C:\Documents and settings\jsilva. Dentro de jsilva serão criadas diversas pastas onde estão as configurações do usuário jsilva. Um profile local é específica para o computador onde ela foi criada. Por exemplo, se o usuário jsilva faz o logon no computador micro01 e faz alterações em sua profile local, estas alterações não estarão presentes quando ele fizer o logon no micro02. Cada micro tem a sua própria profile local para o usuário jsilva.
- ◆ **Roaming user profile:** Este tipo de profile é criada pelo administrador e depois armazenada em um servidor. Por exemplo, o administrador faz o logon em uma estação de trabalho e faz as configurações padrão para a profile. Vamos supor que o administrador fez o logon com a conta Administrator (Administrador). A sua profile será armazenada em C:\Documents and settings\Administrator. Se for uma conta do domínio, o nome do domínio é anexado ao nome da conta por um ponto. Por exemplo, a profile para o usuário Administrator, do domínio ABC, seria gravada na pasta C:\Documents and settings\zAdministrator.Abc, do computador onde o administrador fez o logon. O administrador faz as alterações necessárias. Estas são salvas na sua profile local. Em seguida o administrador pode fazer uma cópia desta profile padrão para o servidor. Por exemplo, pode ser criada uma pasta

compartilhada chamada Profiles, no servidor srv01. Neste caso o caminho para esta pasta seria: \\srv01\profiles. Dentro da pasta profiles pode ser criada uma pasta para cada usuário, por exemplo: \\srv01\profiles\jsilva, \\srv01\profiles\maria, \\srv01\profiles\Pedro e assim por diante. Para copiar a profile da sua máquina local para a rede, basta que o administrador copie todo o conteúdo da pasta C:\Documents and settings\Administrator para a pasta de cada usuário. Depois o administrador deve definir as permissões de acesso em cada profile criada no compartilhamento profiles. Por exemplo, na pasta \\srv01\profiles\jsilva, somente o usuário jsilva deve ter permissão de acesso, na pasta \\srv01\profiles\maria, somente o usuário maria deve ter permissão de acesso e assim por diante. O passo final, para que o usuário possa utilizar esta profile armazenada no servidor, é informar nas propriedades da conta do usuário, o caminho para a respectiva profile. Isso é feito na guia Perfil, das propriedades da conta do usuário. Por exemplo, nas propriedades da conta do usuário jsilva o administrador informa o caminho \\srv01\profiles\jsilva, nas propriedades da conta do usuário maria o administrador informa o caminho \\srv01\profiles\maria e por aí vai (veremos como fazer estas configurações logo a seguir). Feito isso, sempre que o usuário fizer alterações em suas configurações do ambiente de trabalho do Windows, estas alterações serão salvas na profile armazenada no servidor. Por exemplo, quando o usuário jsilva faz alterações nas configurações do ambiente de trabalho, estas alterações são salvas em \\srv01\profiles\jsilva. Quando o usuário jsilva fizer o logon em uma outra estação de trabalho da rede (diferente da estação na qual ele fez as alterações), as suas configurações serão carregadas (durante o logon), a partir de \\srv01\profiles\jsilva, em qualquer computador do domínio, onde o usuário faça o logon. Com isso as alterações que ele fez em uma estação de trabalho, estarão disponíveis em quaisquer estação da rede na qual ele fizer o logon, pois estas configurações são copiada a partir do servidor e “seguem” (viajam com – Roaming) o usuário em qualquer estação de trabalho na qual ele fizer o logon. Combinando o uso de Roaming Profiles com GPOs (Capítulo 18 do livro: Windows Server 2003 – Curso Completo, 1568 páginas), é possível que o ambiente de trabalho do usuário “sigam o usuário” através da rede.

- ◆ **Mandatory user profile:** Este tipo de profile é uma profile do tipo somente leitura. As alterações feitas pelo usuário não serão salvas na profile. Quando o usuário fizer o logon, ele obtém sempre o mesmo ambiente de trabalho, independente das alterações que ele fez durante o seu último logon (alterações estas que são abandonadas). Este tipo de profile não permite que o usuário faça alterações nas configurações definidas na profile. O usuário até consegue alterar o seu ambiente de trabalho, mas no momento em que ele fizer o log off, as alterações não serão salvas. Ao fazer o próximo logon, o usuário receberá as configurações definidas na profile que está no servidor, sem as alterações que ele fez, mas que não foram salvas. As configurações são copiadas para o computador do usuário cada vez que este faz o logon. Quando o usuário faz alterações, estas são feitas na sua cópia local da profile. Ao fazer o log off, estas alterações não são repassadas para a profile que está gravada no servidor. No próximo logon é esta profile que está no servidor (sem alterações) que é novamente copiada para a estação de trabalho do usuário, sobrescrevendo as alterações que por ventura ele tenha feito. O resultado prático é que sempre que o logon é feito, são carregadas as configurações definidas na profile do tipo Mandatory, armazenada no servidor e para a qual somente o Administrador tem permissão para fazer alterações. Este tipo de profile é utilizado para manter ambientes altamente padronizados, onde os usuários não devem poder fazer alterações nas configurações do seu ambiente de trabalho. Somente o administrador pode fazer alterações na profile do tipo Mandatory, armazenada no servidor. Na prática, a maioria das configurações de uma profile estão em um arquivo chamada NTUser.dat. Para tornar uma profile do tipo Mandatory, basta renomear este arquivo para NTUser.man.
- ◆ **Temporary user profile:** Uma profile temporária será criada sempre que algum erro ocorrer durante o logon do usuário, erro este que impeça que uma profile seja carregada, quer seja uma profile local, quer seja uma profile carregada a partir de um servidor. Alterações feitas nesta profile temporária (enquanto o usuário está logado) serão descartadas quando o usuário fizer o log off.

## Entendendo o conteúdo de uma User profile

Neste item descreverei em detalhes as configurações e o conteúdo que é salvo em um profile de usuário. Conforme descrito anteriormente, todas as informações de configuração contidas na Profile do usuário são gravadas em um conjunto de arquivos e pastas dentro de uma pasta com o nome de logon de usuário, no caminho C:\Documents and settings. Por exemplo, as configurações da profile local para o usuário jsilva são gravadas em um conjunto de arquivos e pastas dentro de C:\Documents and settings\jsilva.

A primeira vez que o usuário faz o logon em um computador, o Windows Server 2003 (ou Windows 2000 ou NT 4 ou XP) cria a profile do usuário, baseada na profile Default User (C:\Documents and settings\Default User). A maioria das configurações da profile estão contidas no arquivo NTUser.dat. Por exemplo, para o usuário jsilva as configurações estão no arquivo C:\Documents and settings\jsilva\NTUser.dat. As configurações do menu Todos os programas (All programs) são copiadas da profile All Users (C:\Documents and settings\All Users\Start Menu\Programs. Ou seja, os atalhos que estão dentro desta pasta, automaticamente serão copiados para a nova profile que é criada, a primeira vez que o usuário faz o logon no computador. No Capítulo 4 eu mostrei que para criar um atalho que apareça para qualquer usuário logado, este atalho deve ser criado em All Users.

Dentro da pasta onde fica a profile de cada usuário, existem uma série de subpastas. Por exemplo, dentro da pasta C:\Documents and settings\Administrator existem diversas outras pastas, conforme indicado na Figura 4.20. Cada uma tem uma função específica.

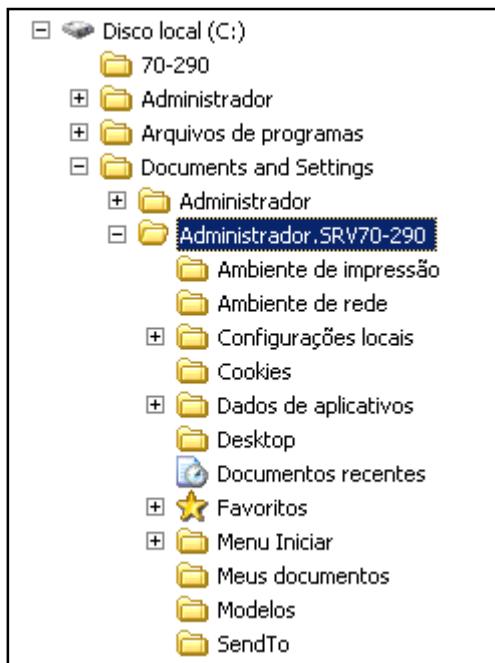


Figura 4.20 Subpastas da profile de usuário.

A seguir descrevo o conteúdo destas pastas:

- ◆ **Application Data (Dados de Aplicativo):** Nesta pasta ficam configurações dos programas utilizados no computador. Por exemplo, configurações do Outlook Express, do Office, tais como modelos e dicionários personalizados criados pelo usuário e assim por diante.
- ◆ **Cookies:** Informações do usuário referentes a sites que ele visitou. Por exemplo, existem sites no qual você deve fazer um cadastro para fazer compras. A maioria dos sites de livrarias online, por exemplo, exige o

cadsat. Você faz o cadastro e preenche um formulário. Algumas destas informações são gravadas em pequenos arquivos conhecidos como Cookies. Futuramente, quando você visita o site novamente, você é surpreendido com uma mensagem Bem vindo fulano de tal. Mas como é que o site sabe que você é o fulano de tal? Ele leu as informações no Cookie que ele havia gravado anteriormente. Os cookies gravados pelos diversos sites que você visita ficam gravados na pasta Cookies, dentro da profile do usuário.

- ◆ **Desktop:** Esta pasta contém os atalhos, arquivos, pastas e demais itens que são exibidos na área de trabalho do usuário.
- ◆ **Favoritos:** Contém a estrutura de Favoritos do Internet Explorer.
- ◆ **Configurações locais:** Configurações de aplicativos locais, o histórico de navegação na Internet e arquivos temporários. Estas informações “viajam” com o usuário, isto é, acompanham o usuário pela rede quando este está utilizando Roaming Profiles.
- ◆ **Meus documentos:** Esta é a pasta padrão para gravação dos arquivos de dados do usuário. Por exemplo, quando você executa o comando Arquivo -> Salvar, no Word, por padrão é selecionada a pasta Meus documentos.
- ◆ **Documentos Recentes:** Contém atalhos para os documentos recentemente utilizados pelo usuário. Estes atalhos facilitam a abertura de documentos e pastas que o usuário está utilizando seguidamente.
- ◆ **Ambiente de rede:** Contém atalhos para os itens contidos na opção Meus locais de rede.
- ◆ **Ambiente de impressão:** Atalhos para as impressoras instaladas pelo usuário.
- ◆ **SendTo:** Contém atalhos para os itens que aparecem quando você clica com o botão direito do mouse em um arquivo ou pasta e seleciona o comando Enviar para. Por exemplo, se você quer que apareça no menu Enviar para o nome de uma pasta onde você faz cópias de Backup, basta adicionar um atalho para esta pasta, dentro da pasta SendTo, na profile do usuário.
- ◆ **Menu Iniciar:** Esta pasta contém uma subpasta chamada Programas. Esta subpasta contém todos os itens do menu Todos os programas.
- ◆ **Modelos:** Arquivos de modelos do Office, utilizados pelo usuário.
- ◆ **A profile do usuário também contém o arquivo NTUser.dat:** O arquivo NTUser.dat contém a parte das configurações que são armazenadas na Registry do sistema (para mais detalhes sobre a Registry consulte o Capítulo 12). Enquanto o usuário está logado e faz alterações em suas configurações, estas são feitas diretamente na Registry (mais especificamente na chave HKEY\_CURRENT\_USER). Quando o usuário faz o log off, o Windows grava as alterações feitas pelo usuário no arquivo NTUser.dat. Com isso na próxima vez que o usuário fizer o logon, o Windows lê as configurações a partir do arquivo NTUser.dat e carrega-as novamente na Registry. O efeito prático é que as alterações são mantidas e o usuário recebe o mesmo ambiente de trabalho de quando ele fez o log off pela última vez.

## A pasta All Users

Dentro da pasta Documents and Settings, existe uma profile chamada All Users. As configurações desta pasta definem itens do menu programas e atalhos da área de trabalho, os quais estarão disponíveis para qualquer usuário que fizer o logon no computador. Por exemplo, se você quer que um atalho para uma determinada pasta seja exibida na área de trabalho, independentemente do usuário logado. É só colocar este atalho na pasta Desktop da profile All Users. Quando o usuário faz o logon, o Windows utiliza as configurações da profile do próprio usuário, mas os atalhos da área de trabalho, do menu Todos os programas e da barra de tarefas da profile All Users.

A profile All Users contém atalhos para os chamados programas comuns, ou seja, programas que estão disponíveis para todos os usuários que fizerem o logon no computador. Os atalhos para programas individuais ou privativos, ou seja, somente disponíveis para um determinado usuário, são gravados na profile do respectivo usuário.

Em um computador com o Windows Server 2003, somente usuários com permissão de administrador terão permissão para modificar a pasta All Users. Neste caso, se você deseja instalar um programa cujo atalho deve estar disponíveis para todos os usuários do computador, você deve estar logado com uma conta com permissão de administrador, para fazer a instalação do programa. Se a instalação for feita com uma conta que não tem permissão de administrador, o atalho será criado somente na profile da conta logada. Quando outros usuários fizerem o logon, o respectivo atalho não estará disponível. Este é um dos erros mais comuns e que geram muitas chamadas do suporte. Do outro lado da linha o usuário diz: "O Programa X não está instalado na minha máquina". Na verdade o programa X está instalado, o que acontece é que não foi criado o atalho para o programa.

A seguir descrevo quais as configurações que são gravadas na profile de cada usuário e, portanto, são individualizadas para cada usuário que faz o logon no computador.

- ◆ Configurações feitas no Windows Explorer, tais como Opções de pasta, de visualização e assim por diante.
- ◆ Arquivos da pasta Meus documentos. A pasta Meus documentos é individualizada para cada usuário.
- ◆ Minhas figuras: Esta pasta fica dentro da pasta Meus documentos e é a pasta padrão para gravação de figuras. Por exemplo, quando você usa o comando Arquivo -> Salvar no Paint Brush, por padrão já vem selecionada a pasta Minhas figuras.
- ◆ Favoritos do Internet Explorar. A lista de favoritas também é individual, ou seja, fica gravada na profile de cada usuário.
- ◆ Drives de rede mapeados via script de logon ou manualmente mapeados pelo usuário.
- ◆ Informações da pasta Meus locais de rede, a qual contém atalhos para outros computadores e recursos da rede.
- ◆ Os itens da área de trabalho.
- ◆ Configurações do vídeo.
- ◆ Configurações de aplicativos (tais como Office, Outlook Express, Internet Explorer, etc.)
- ◆ Configurações de impressoras.
- ◆ Conexões de rede.
- ◆ Configurações feitas através das opções do Painel de controle
- ◆ Menu Acessórios
- ◆ Outros programas instalados e que tenham sido programados para manter configurações separadas para cada usuário e salvar estas configurações na profile do usuário. Os programas que tem o logo do Windows Server 2003, ou seja, aprovados para uso no Windows Server 2003, devem ser capazes de gravar configurações separadas para cada usuário.
- ◆ Atalhos colocados como favoritos na documentação do Windows Server 2003, também são individualizados por usuário.

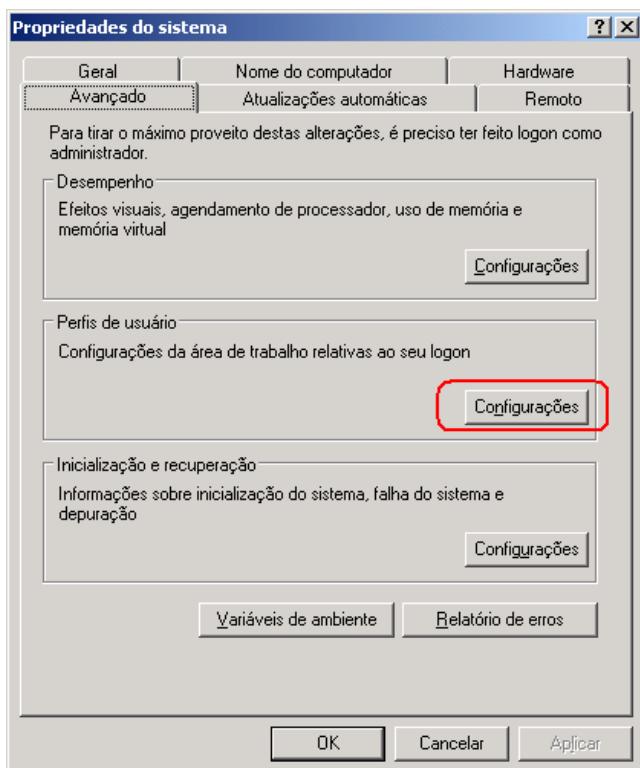
**IMPORTANTE:** Por padrão algumas pastas da profile do usuário são marcadas como pastas ocultas e não serão exibidas no Windows Explorer, a não ser que você configure o Windows para exibir pastas e arquivos ocultos. Por padrão as seguintes pastas são ocultas: Ambiente de rede, Ambiente de impressão, Configurações locais, Arquivos recentes e Modelos. Para exibir os arquivos e pastas ocultas abra o Windows Explorer, selecione o comando Ferramentas -> Opções de pasta, clique na guia Exibir e marque a opção Exibir pastas e arquivos ocultos. Clique em OK.

## Criando um Profile a ser aplicada a vários usuários

Em determinadas situações você pode ter a necessidade de criar uma profile com um determinado conjunto de configurações (atalhos na área de trabalho, configurações, atalhos no menu Todos os programas e assim por diante), depois copiar esta profile para um servidor e aplicá-la a um grupo de usuários.

O processo de criação de uma profile padrão é bastante simples. Para criar uma profile padrão você deve seguir os passos indicados a seguir:

1. Instale o Windows Server 2003 em um computador. Faça uma instalação nova, a partir do zero.
2. Faça o logon com uma conta que tenha permissões para fazer as configurações desejadas para a Profile.
3. Faça as configurações desejadas em termos de criação de atalhos, configurações do ambiente e assim por diante.
4. Todas as configurações efetuadas serão gravadas na profile local, do usuário logado. Por exemplo, se você estiver logado como jsilva, todas as configurações serão gravadas na pasta C:\Documents and Settings\jsilva.
5. Faça o logoff do usuário jsilva e faça o logon como Administrador, ou com uma conta com permissão de administrador.
6. Feitas as configurações desejadas, é hora de copiar a profile para uma pasta compartilhada, em um servidor da rede, para que esta profile possa ser associada a outros usuários, conforme mostrarei no próximo item.
7. Para copiar uma profile, clique com o botão direito do mouse em Meu computador e, no menu de opções que é exibido clique em Propriedades.
8. Na janela de propriedades que é exibida clique na guia Avançado. Nesta guia, clique no botão Configurações, abaixo de Perfis de usuário, indicado na Figura 4.21:



**IMPORTANTE:** As configurações armazenadas em um Profile, se referem a configurações do ambiente, tais como ícones na área de trabalho, configurações do Painel de controle e assim por diante. Na Profile não ficam informações sobre os programas instalados no computador. Por exemplo, se você copiar a Profile de um computador onde o Office está instalado, para outro onde o Office não está instalado, isso não fará como que o Office esteja disponível no computador de destino.

Figura 4.21 O botão Copiar Perfis de usuário.

8. Será aberta a janela Perfis de usuário, com uma lista dos perfis disponíveis no computador. Clique na profile a ser copiada, para selecioná-la. No nosso exemplo, vou clicar na profile do usuário jsilva.
9. Clique no botão Copiar para.
10. Será aberta a janela Copiar para. No campo Copiar o perfil para, você informa o caminho para onde a profile deverá ser copiada. Conforme descrito anteriormente, normalmente é um caminho para uma pasta compartilhada, em um servidor da rede. No exemplo da Figura 4.22, estou copiando para uma pasta chamada contabilidade, do compartilhamento profiles, no computador chamado servidor.

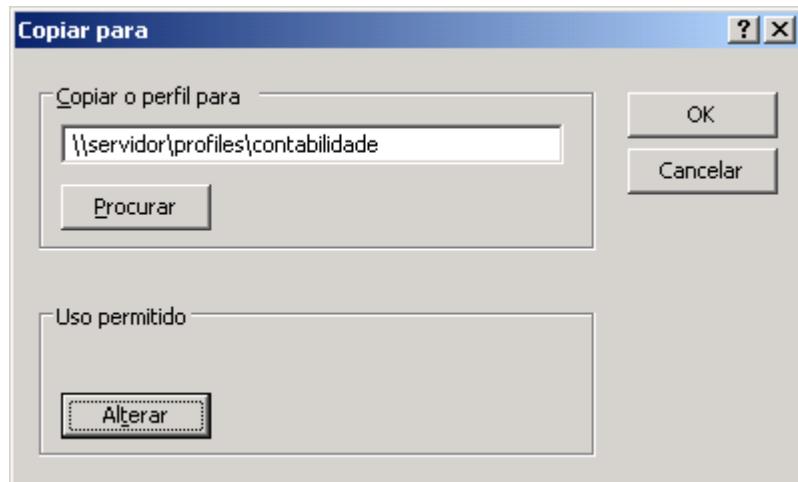


Figura 4.22 Informando o caminho para copiar a profile.

11. Você pode usar o botão Alterar, abaixo de uso permitido, para definir as permissões NTFS na profile que será copiada para o servidor. Por exemplo, se a profile que está sendo copiada, deve ser acessada apenas pelos membros do grupo Contabilidade, você pode usar o botão Alterar, para dar permissões de acesso apenas a este grupo.
12. Clique no botão alterar e, na janela que é exibida, digite o nome dos usuários e grupos que deverão ter acesso à profile. Se houver mais de um usuário e/ou grupo, os nomes devem ser separados por ponto-e-vírgula, como no exemplo da Figura 4.23, onde estou dando permissão para os grupos Contabilidade e Finanças:

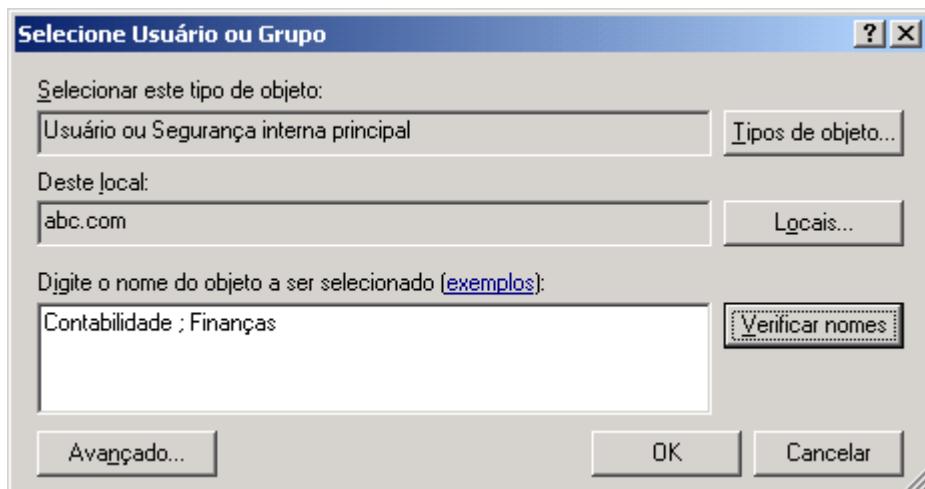


Figura 4.23 Definindo as permissões de acesso à profile.

13. Clique em OK. Você estará de volta à janela Copiar para. Clique em OK. Dependendo do tamanho da profile, a cópia poderá demorar alguns minutos.
14. Após a cópia ter sido encerrada, você estará de volta à janela Perfis de usuários. Clique em OK para fechá-la. Você estará de volta a janela de propriedades do Meu computador. Clique em OK para fechá-la.
15. Muito bem, a profile modelo já foi copiada para uma pasta compartilhada em um servidor da rede e as permissões NTFS devidamente definidas (para mais detalhes sobre permissões NTFS, consulte o Capítulo 6). O próximo passo é configurar as propriedades da conta de todos os usuários que devam ter acesso à profile. Desta maneira vamos criar uma Roaming profile, conforme descrito anteriormente. Os passos para configurar a conta de um usuário, para que este passe a utilizar uma Roaming profile, estão descritos no próximo item.

## Configurando uma profile no Perfil do usuário:

Agora que você já sabe bastante sobre profiles de usuários, é hora de aprender como configurar uma Roaming Profile para a conta do usuário. A seguir apresento um exemplo prático sobre estas configurações.

Exemplo: Como associar uma profile em um servidor (Roaming Profile), com uma conta de usuário:

1. Acesse as propriedades da conta a ser configurada.
2. Dê um clique na guia Perfil.
3. No campo Caminho do perfil, informe o caminho completo onde está gravada a profile do usuário, conforme exemplo da Figura 4.24:

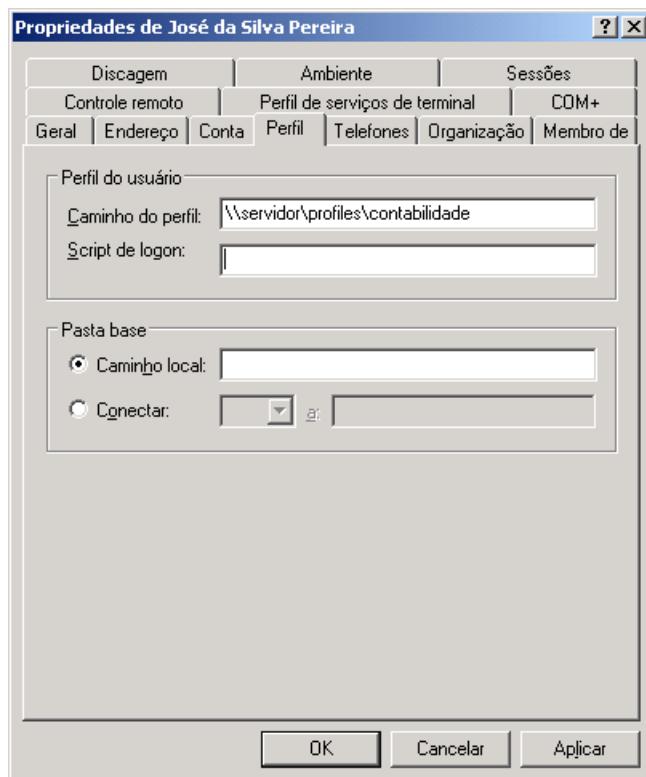


Figura 4.24 Informando onde está gravada a profile do usuário.

Na guia Profile você pode informar mais algumas configurações, conforme descrito a seguir:

- ◆ **Script de logon:** Neste campo você informa o nome do script de logon (normalmente um arquivo .bat ou .cmd), que será executado quando o usuário fizer o logon. O script de logon normalmente é um arquivo .bat e deve ser

gravado em uma pasta específica nos controladores de domínio. Em todo DC do domínio existe um compartilhamento chamado Netlogon. É neste compartilhamento que deve ser gravado um ou mais arquivos que serão utilizados como script de logon. O próximo passo é informar, no campo Script de logon, o nome do script associado com a conta do usuário. Durante o logon, o Windows Server 2003 procura, no compartilhamento Netlogon, do DC que está autenticando o usuário, um arquivo com o nome informado no campo Script de logon. Se o arquivo for encontrado e for um arquivo com comandos válidos, os comando serão executados. Neste script devem ser colocados comandos que devem ser executados automaticamente quando o usuário faz o logon, como por exemplo comandos para mapear unidades de rede, atulizar o anti-vírus e assim por diante. O conteúdo do compartilhamento Netlogon é replcado, automaticamente, pelo Active Directory, entre todos os DCs do domínio.

- ◆ **Pasta base (Home folder)** : Neste grupo o administrador pode informar um caminho local, como por exemplo c:\documentos ou um drive de rede por exemploX:, associado com o caminho \\srv01\home\jsilva. O conceito de pasta base pode ser utilizado para consolidar os arquivos de dados dos usuários em um ou mais servidores da rede. Isso traz muitas vantagens, sendo a principal delas a possibilidade de fazer o backup dos dados dos usuários de uma maneira centralizada. Ao invés de gravar os dados no próprio computador, o usuário pode salvá-los em sua pasta base, diretamente no servidor. A grande vantagem é que o usuário terá acesso a esta pasta em qualquer computador da rede onde ele fizer o logon e não apenas no seu próprio computador. A desvantagem é que se o usuário estiver sem acesso a rede, ele perderá acesso a estes dados (este problema pode ser minimizado com o uso de Pastas Off-line, conforme mostrarei no Capítulo 6). Para montar uma estrutura de pastas base, o administrador deve reservar espaço em um volume em um dos servidores da rede. Em seguida ele cria uma pasta, por exemplo ele pode criar uma pasta chamada homeusers. Dentro desta pasta o administrador cria uma subpasta para cada usuário que irá utilizar uma pasta base. Por exemplo, ele cria uma subpasta jsilva, a qual será a pasta base da conta de logon jsilva, cria uma subpasta maria, a qual será a pasta base da conta de logon maria e assim por diante. Cada pasta individual é compartilhada, com o nome de compartilhamento igual ao nome de logon. Por exemplo, a pasta jsilva é compartilhada como jsilva, a pasta maria é compartilhada como maria e assim por diante. Com isso o caminha da pasta base dos usuários jsila e maria fica conforme exemplo a seguir:

`\\\srv01\homeusers\jsilva`  
`\\\srv01\homeusers\maria`

O próximo passo é definir as permissões de acesso em cada pasta. Por padrão deve ser definido que apenas o próprio usuário deve ter permissão de acesso a sua pasta base. Dependendo das políticas de segurança da empresa, pode ser necessário definir permissão de acesso também para o grupo Administradores do domínio. Criada a estrutura de pastas em um dos servidores da rede, agora é só informar no campo Conectar, a letra do drive que será associado a pasta base do usuário. No campo “a”, o administrador informa o caminho de rede para a pasta base do usuário. No exemplo da Figura 4.25 está sendo associado o drive X, com a pasta base \\srv01\homeusers\jsilva. Neste exemplo, toda vez que o usuário jsilva fizer o logon, em qualquer computador da rede, será disponibilizado um drive X:, o qual está associado com o caminho \\srv01\homeusers\jsilva.

`\\\srv01\homeusers\%username%`

Ao salvar as alterações, o Windows Server 2003 substitui %username% pelo nome de logon do usuário, o que reduz erros devido a erros de digitação no nome de logon do usuário.

4. Após ter definido as configurações da guia Perfil, clique em OK para fechar a janela de propriedades e salvar as alterações.

---

**IMPORTANTE:** Ao invés de informar o nome do usuário, no caminho da pasta base, você pode utilizar a variável %username%.

---

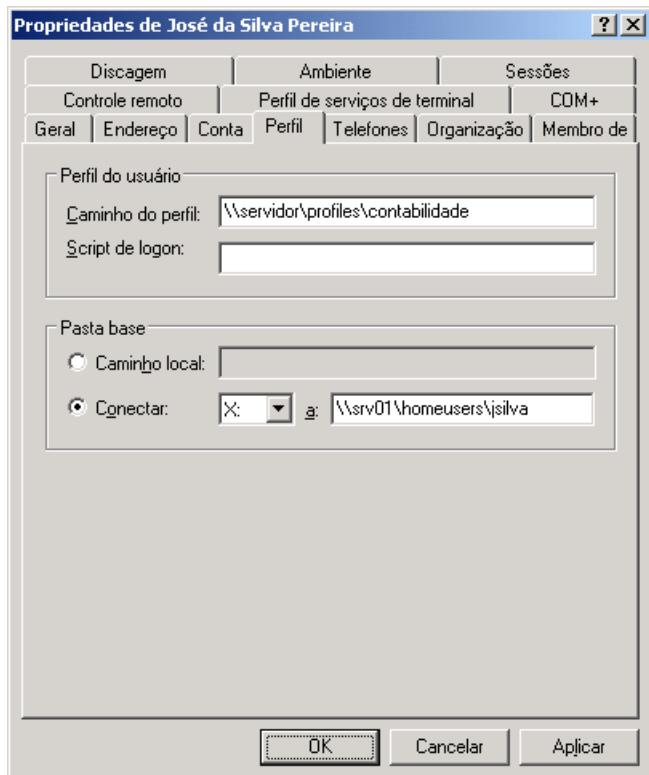


Figura 4.25 Informando o caminho da pasta base e da profile do usuário.

## Conhecendo as chamadas “Contas Built-in”

Ao criar um domínio, algumas contas são criadas automaticamente. Estas contas são conhecidas como Built-in accounts. A seguir descrevo as contas criadas automaticamente no Active Directory:

- ◆ **Administrador (Administrator):** Esta conta pertence a diversos grupos do domínio. O resultado prático é que a conta Administrator tem poderes totais em todos os computadores do domínio, ou seja, é a conta com o mais alto nível de permissões no domínio. Esta conta pertence, automaticamente, aos seguintes grupos: Administrators (Administradores), Domain Admins (Admins. do Domínio), Domain Users (Usuários do Domínio), Enterprise Admins (Administradores de empresa – este é um exemplo de uma das tantas traduções “indecifráveis” que você encontra na versão em Português do Windows Server 2003), Group Police Creator Owners (Proprietários criadores de diretivas de grupo – mais um “bela” tradução) e Schema Admins (Administradores de esquemas – outra maravilha na tradução, como pode existir “esquemas” se o esquema é único em toda a árvore de domínios?). Na Figura 4.26 é exibida a lista de grupos ao qual pertence a conta Administrador, por padrão. Esta lista é obtida a partir da guia Membro de, da janela de propriedades da conta Administrador.

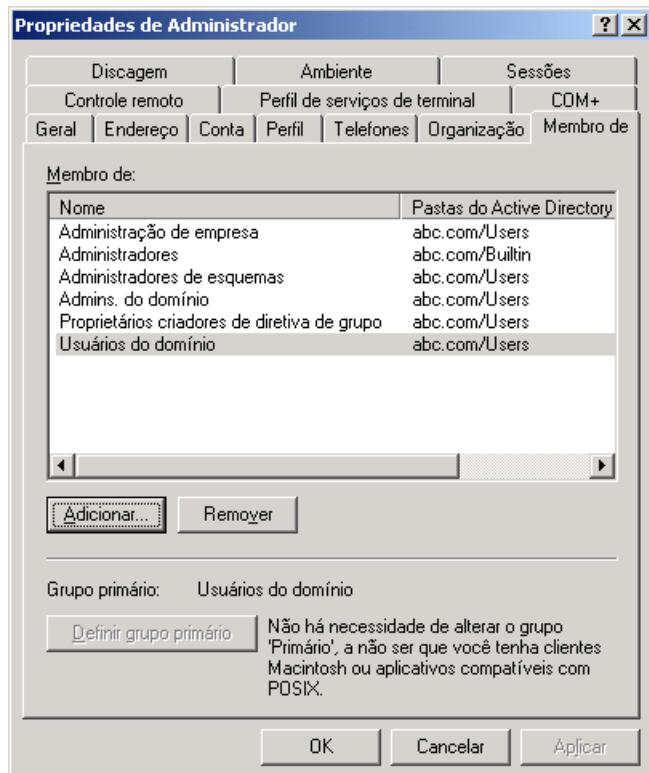


Figura 4.26 Grupos aos quais pertence a conta Administrador.

Como a conta Administrator é a conta com o maior nível de permissões do domínio, algumas recomendações adicionais de segurança são necessárias:

- ◆ Defina uma senha “forte” para esta conta. Senha forte significa uma senha com 10 ou mais caracteres e que de preferência utiliza caracteres dos quatro grupos: maiúsculas, minúsculas, dígitos e caracteres especiais.
- ◆ É recomendado que você renomeie a conta Administrator. Com isso, se alguém quiser fazer o logon como administrador, além da senha desta conta terá também que tentar descobrir o novo nome. Ao renomear a conta administrador, você dificulta a vida de um hacker, ao fazer com que ele tenha que descobrir o nome e também a senha da conta com permissões de administrador.
- ◆ É recomendado que o administrador do domínio tenha também uma conta de usuário comum, com permissões limitadas. Somente quando for necessário realizar tarefas administrativas é que este usuário deve fazer o logon como administrador. Isso reduz a possibilidades de erros de operação, os quais podem ser desastrosos se cometidos quando o usuário está logado como administrador do domínio.
- ◆ Conta Convidado (Guest): Esta conta é criada automaticamente e por padrão está bloqueada, ou seja, não está habilitada para ser usada para logon no domínio. Esta conta normalmente é utilizada por pessoas de fora da empresa, que estão na empresa prestando um serviço específico ou participando de uma reunião e precisam, por algum motivo, fazer o logon na rede. A conta Convidado pode ter senha em branco e por padrão tem acesso bastante limitado aos recursos da rede, por questões de segurança. Esta conta pertence ao grupo Domain Guests (Convidados do Domínio), ao grupo Local do Domínio Guests (Convidados) e ao grupo global Domain Users (Usuários do domínio). A conta Guest (Convidado) somente deve ser utilizadas em ocasiões específicas, onde um usuário não cadastrado precisa fazer o logon no domínio. A conta Guest (Convidado) pode receber permissões de acesso a recursos do domínio, como outra conta qualquer.

Esta é uma questão fundamental e um erro comum que Administradores com pouca experiência podem cometer. Me explico melhor. Quando você cria uma conta de usuário (quer seja uma conta local quer seja uma conta no domínio), você atribui um nome de logon para a conta, por exemplo: jsilva. Além do nome, o Windows Server 2003 cria um SID – Security Identifier (Identificador de segurança) para cada objeto do Active Directory. Para o Windows Server 2003 o que vale, na prática, é o SID do objeto. Agora imagine que você criou o usuário jsilva, incluiu ele em diversos grupos e atribuiu permissões de acesso para este usuário. Internamente, o que o Windows Server 2003 usa para identificar o usuário jsilva é o SID associado a conta jsilva. O erro que muitos administradores cometem é o seguinte:

Vamos supor que, por engano, a conta jsilva foi excluída. Você pode raciocinar assim: não tem problema, é só criar a conta jsilva novamente, definir a mesma senha e incluí-la nos mesmos grupos de antes que automaticamente a conta jsilva terá todas as permissões de acesso que tinha antes. Certo? Nada disso, absolutamente errado. Ao excluir a conta e cria-la novamente, um novo SID será gerado para a conta jsilva. Embora o nome de logon seja o mesmo, para o Windows Server 2003 é como se fossem contas completamente diferentes. Porém, nos recursos da rede, está a permissão de acesso para o SID antigo. Por isso que a nova conta, mesmo com o mesmo nome, não consegue acessar os recursos que a antiga acessava, pois são SIDs diferentes. Na prática o que tem que ser feito é excluir a conta jsilva das listas de permissão de todos os recursos e incluí-la novamente, para que seja utilizado o novo SID. Veja que é um trabalho e tanto, mas existem motivos relacionados à segurança, para que seja utilizado um SID associado com cada objeto do Active Directory, conforme descreverei na parte de segurança, mais adiante.

Então não esqueça: Ao excluir uma conta e cria-la novamente, com o mesmo nome e a mesma senha, para o Windows Server 2003 não é a mesma conta, porque um novo SID foi gerado quando a conta é criada novamente.

## Demais operações com contas de usuários

Neste item descreverei os passos para executar uma série de operações básicas com as contas de usuários, tais como: renomear conta, bloquear/desbloquear conta, desativar conta, excluir conta e assim por diante. Descreverei cada uma destas ações através de exemplos práticos.

Para Renomear uma conta de usuário siga os passos indicados a seguir:

1. Acesse as propriedades da conta a ser configurada.
2. Dê um clique na guia Conta.
3. No campo Nome de logon do usuário digite o novo nome de logon para a conta. Se necessário altere também o valor do campo Nome de logon do usuário (anterior ao Windows 2000).
4. Clique em OK para salvar as alterações.

Pronto, a partir de agora o usuário já pode utilizar o novo nome de logon.

Para Excluir uma conta de usuário siga os passos indicados a seguir:

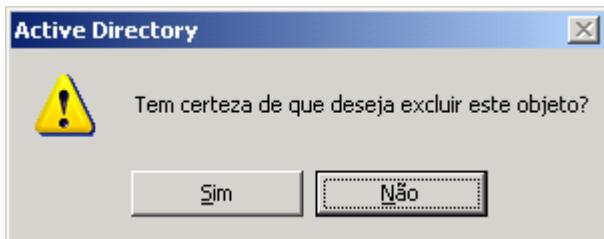
1. Faça o logon com uma conta com permissão para alterar contas de usuários (Administrador ou pertencente ao grupo Oper. de contas).
2. Abra o console Usuários e computadores do Active Directory: Iniciar -> Ferramentas Administrativas -> Usuários e computadores do Active Directory.

**IMPORTANTÍSSIMO: Por que nomes iguais não significam contas iguais?**

**IMPORTANTE: Renomear, neste caso, significa alterar o nome de logon do usuário e não o nome completo.**

**IMPORTANTE: Uma confusão que pode existir é quando você clica com o botão direito do mouse na conta do usuário, na lista de contas, e seleciona a opção Renomear. Ao digitar um novo nome você irá alterar o nome completo do usuário e não o nome de logon, o qual deve ser alterado através da janela Propriedades da conta, na guia Conta, conforme descrito anteriormente.**

3. Clique na opção Users ou acesse a Unidade Organizacional onde está a conta a ser excluída (você aprenderá sobre Unidades Organizacionais mais adiante, neste capítulo).
4. Clique com o botão direito do mouse na conta a ser excluída.
5. No menu de opções que é exibido clique em Excluir.
6. O Windows Server 2003 exibe uma mensagem pedindo confirmação, conforme indicado na Figura 4.27



**Figura 4.27 Confirmando a exclusão da conta.**

7. Clique em Sim para confirmar a exclusão.

O administrador pode desabilitar uma conta de usuário. Ao desabilitar uma conta, o usuário não poderá mais fazer o logon com esta conta. Existem diversas situações práticas onde o administrador pode ter que desabilitar uma conta. Por exemplo, se um funcionário está sob investigação, respondendo a um processo administrativo, o administrador pode desabilitar a conta deste usuário para que ele não tenha acesso a rede. Quando o processo for concluído, se o usuário for absolvido, a conta pode ser habilitada novamente. Se o usuário for condenado a conta pode ser excluída. Outro exemplo de uso desta opção é com estagiários. Vamos supor que um estagiário está deixando a empresa e outro irá assumir as suas funções dentro de 15 dias. Quando o primeiro deixa a empresa, o administrador desabilita a conta que ele utilizava. Quando o novo estagiário assume, o administrador habilita e renomeia a conta, de acordo com o nome de logon escolhido pelo novo estagiário. Como a conta foi apenas renomeada, o novo estagiário, automaticamente, terá acesso aos mesmos recursos que o anterior tinha, o que é bastante coerente, já que o novo estagiário irá desempenhar as mesmas funções do anterior. Se a conta do antigo estagiário fosse excluída, ao invés de ser apenas bloqueada, uma nova conta teria que ser criada para o novo estagiário e todas as permissões de acesso teriam que ser reconfiguradas. Um bom trabalho adicional.

Para desabilitar uma conta de usuário siga os passos indicados a seguir:

1. Faça o logon com uma conta com permissão para alterar contas de usuários (Administrador ou pertencente ao grupo Account Operators).
2. Abra o console Usuários e computadores do Active Directory: Iniciar -> Ferramentas Administrativas -> Usuários e computadores do Active Directory.
3. Clique na opção Users ou acesse a Unidade Organizacional onde está a conta a ser desabilitada (você aprenderá sobre Unidades Organizacionais mais adiante, neste capítulo).
4. Clique com o botão direito do mouse na conta a ser desabilitada.
5. No menu de opções que é exibido clique em Desativar conta.
6. A conta desativada será marcada com um x, conforme indicado na Figura 4.28:

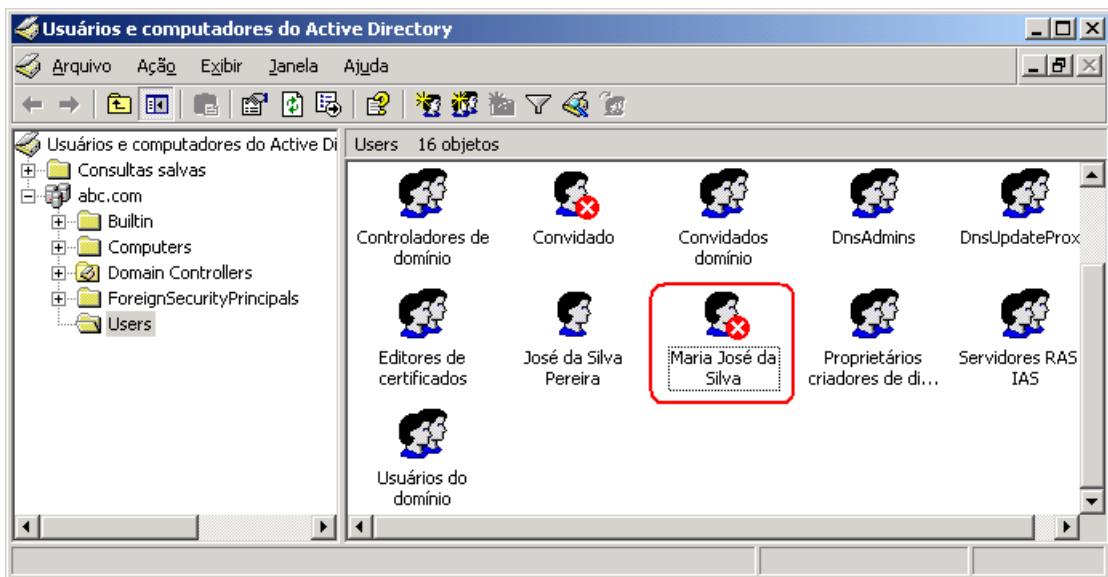


Figura 4.28 Conta desabilitada.

Outra situação que pode acontecer é simplesmente o usuário esquecer a senha da sua conta. Situação que é comum em ambientes de redes com múltiplos diretórios, o que é sinônimo de múltiplas senhas para lembrar, conforme descrito no Capítulo 2. Quando o usuário esquece a senha, o administrador pode definir uma nova senha para a conta do usuário. O administrador deve definir a nova senha, informá-la ao usuário usando os procedimentos definidos nas políticas de segurança da empresa e deve configurar a conta do usuário para que seja solicitada a troca da senha no primeiro logon. Esta última opção é importante para que o usuário possa trocar a sua senha, de tal maneira que somente ele saiba a senha de sua conta (e de preferência não esqueça mais).

Para redefinir a senha de uma conta de usuário, siga os passos indicados a seguir:

1. Faça o logon com uma conta com permissão para alterar contas de usuários (Administrador ou pertencente ao grupo Account Operators).
2. Abra o console Usuários e computadores do Active Directory: Iniciar -> Ferramentas Administrativas -> Usuários e computadores do Active Directory.
3. Clique na opção Users ou acesse a Unidade Organizacional onde está a conta a ter a senha redefinida (você aprenderá sobre Unidades Organizacionais mais adiante, neste capítulo).
4. Clique com o botão direito do mouse na conta a ter a senha redefinida.
5. No menu de opções que é exibido clique na opção Redefinir Senha...
6. Será exibida a janela Redefinir senha. Digite a nova senha duas vezes e marque a opção O usuário deve alterar a senha no próximo logon, conforme indicado na Figura 4.29.
7. Clique em OK. A nova senha será definida e uma mensagem de aviso será exibida, informando que a senha foi redefinida com sucesso. Clique em OK para fechar a janela de aviso.

**IMPORTANTE:** Desabilitar é diferente de bloquear. Uma conta é bloqueada, automaticamente, quando o usuário tenta fazer o logon sem sucesso (por exemplo, digitou a senha incorretamente), um determinado número de vezes (por padrão três vezes) dentro de um período determinado (por padrão uma hora). Nesta situação o Active Directory bloqueia a conta automaticamente. O administrador pode acessar as propriedades de uma conta bloqueada, clicar na guia Conta e desmarcar a opção A conta está bloqueada, para desbloquear a conta. Por padrão a conta será desbloqueada, automaticamente, dentro de 24 horas, caso o administrador não a tenha desbloqueado manualmente.

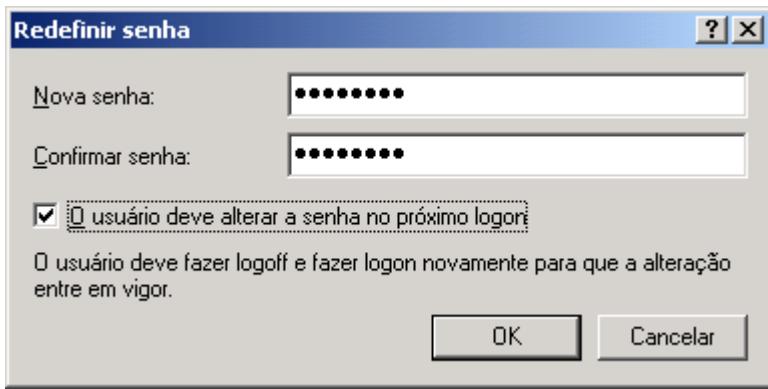


Figura 4.29 Definindo uma nova senha para a conta do usuário.

Sobre contas de usuários, é isso. Você deve ter notado que existem outras guias na janela de propriedades das contas de usuário. Estas guias estão relacionadas a serviços específicos, tais como Terminal Services e Acesso Remoto via RRAS. Estas guias serão estudadas quando os respectivos serviços forem estudados, em capítulos específicos deste livro. Agora é hora de estudarmos, em detalhes, os grupos de usuários.

## Grupos de usuários: Conceitos, tipos e utilização.

Um grupo de usuários é uma coleção de contas de usuários. Por exemplo, podemos criar um grupo chamado Contabilidade, do qual farão parte todos os usuários do departamento de Contabilidade (todas as contas de usuários dos funcionários do departamento de Contabilidade).

A principal função dos grupos de usuários é facilitar a administração e a atribuição de permissões para acesso a recursos, tais como: pastas compartilhadas (Capítulo 6), impressoras de rede (Capítulo 7) e configurações de acesso a serviços diversos.

Ao invés de dar permissões individualmente, para cada um dos usuários que necessitam acessar um determinado recurso, você cria um grupo, inclui os usuários no grupo e atribui permissões para o grupo. Para que um usuário tenha permissão de acesso ao recurso, basta incluir o usuário no grupo, pois todos os usuários de um determinado grupo, herdam as permissões dos grupos aos quais o usuário pertence.

Quando um usuário troca de seção, por exemplo, basta trocar o usuário de grupo. Vamos supor que o usuário jsilva trabalha na seção de contabilidade e pertence ao grupo Contabilidade. Com isso ele tem acesso a todos os recursos para os quais o grupo Contabilidade tem acesso. Ao ser transferido para a seção de Marketing, basta retirar o usuário jsilva do grupo Contabilidade e adicioná-lo ao grupo Marketing. Assim o usuário jsilva deixa de ter as permissões atribuídas ao grupo Contabilidade e passa a ter as mesmas permissões que tem o grupo Marketing. Este exemplo simples já é suficiente para demonstrar o quanto a utilização de grupos pode facilitar a atribuição de permissões. No Capítulo 6 apresentarei um estudo completo sobre o uso de grupos para atribuir permissões de acesso a recursos de diferentes domínios.

Vamos analisar mais um exemplo. Suponha que exista um sistema chamado SEAT, para o qual somente um número restrito de usuários deve ter acesso, sendo que são usuários de diferentes seções (ou até mesmo de diferentes domínios). A maneira mais simples de definir as permissões de acesso ao sistema SEAT é criar um grupo chamado SEAT (poderia ser um outro nome qualquer, tais como Usuários do SEAT, Permissão ao SEAT, etc) e dar permissões

**IMPORTANTE:** O usuário herda as permissões dos grupos aos quais ele pertence. Caso ele pertença a mais de um grupo, as permissões serão cumulativas, conforme será detalhado e exemplificado mais adiante.

de acesso a esse grupo. Assim cada usuário que precisar acessar o sistema SEAT, deve ser incluído no grupo SEAT. Quando o usuário não deve mais ter acesso ao sistema SEAT, basta removê-lo do grupo SEAT. Simples, fácil e muito prático.

Na Figura 4.30 apresento uma ilustração para o conceito de Grupo de usuários. O Grupo Contabilidade possui direito para um recurso compartilhado, o qual pode ser acessado através da rede. Todos os usuários que pertencem ao grupo contabilidade, também possuem permissão para o recurso compartilhado, uma vez que os usuários de um grupo, herdam as permissões do grupo.

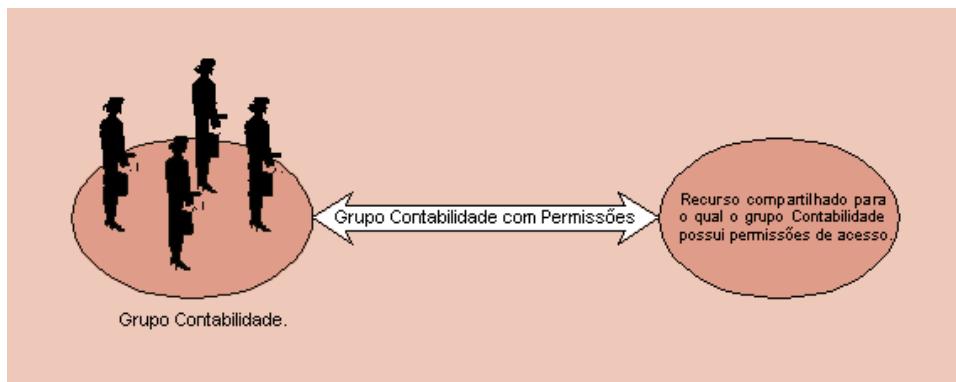


Figura 4.30 O Usuário herda as permissões do grupo.

- ◆ Grupos são uma coleção de contas de usuários.
- ◆ Os membros de um grupo, herdam as permissões atribuídas ao grupo.
- ◆ Os usuários podem ser membros de vários grupos
- ◆ Grupos podem ser membros de outros grupos.
- ◆ Contas de computadores podem ser membros de um grupo (novidade do Windows Server 2003).

**IMPORTANTE:** Quando estiver trabalhando com grupos de usuários, considere os fatos a seguir.

Agora vou falar sobre os tipos de grupos existentes no Windows Server 2003. Os grupos são classificados de acordo com diferentes critérios, tais como: tipo, escopo e visibilidade.

Podemos ter dois tipos de grupos no Windows Server 2003 : Grupos de segurança ( Security Groups) e Grupos de distribuição (Distribution Groups).

## Classificação dos grupos quanto ao tipo:

- ◆ **Grupos de segurança:** Normalmente utilizados para atribuir permissões de acesso aos recursos da rede. Por exemplo, ao criar um grupo Contabilidade (que conterá todas as contas dos funcionários do departamento de contabilidade) o qual será utilizado para atribuir permissões de acesso a uma pasta compartilhada, devo criar este grupo como sendo do tipo Grupo de segurança. Um grupo de segurança também pode ser utilizado como um grupo de distribuição, embora essa não seja uma situação muito comum. Esses grupos, assim como as contas de usuários são armazenados no Banco de dados do Active Directory.
- ◆ **Grupos de distribuição:** São utilizados para funções não relacionadas com segurança (não relacionadas a atribuição de permissões) . Normalmente são utilizados em conjunto com servidores de e-mail, tais como o Exchange Server 2003, para o envio de e-mail para um grupo de usuários. Uma das utilizações típicas para um Grupo de distribuição é o envio de mensagens de e-mail para um grupo de usuários de uma só vez. Somente

programas que foram programados para trabalhar com o Active Directory, poderão utilizar Grupos de distribuição (como é o caso do Exchange Server 2003 citado anteriormente). Provavelmente as novas versões dos principais sistemas de correio eletrônico estarão habilitadas para trabalhar com o Active Directory. Não é possível utilizar grupos de distribuição para funções relacionadas com segurança.

## Classificação dos grupos quanto ao Escopo:

Quando o administrador cria um grupo de usuários, ele deve selecionar um tipo (descrito anteriormente) e um escopo. O Escopo permite que o grupo seja utilizado de diferentes maneiras para a atribuição de permissões. O escopo de um grupo, determina em que partes do domínio ou de uma floresta de domínios, o grupo é visível, ou seja, pode ser utilizado para receber permissões de acesso aos recursos da rede e quais tipos de objetos (grupos e usuários), podem ser inseridos como membros do grupo.

Existem três escopos para grupos de usuários, conforme descrito a seguir: Universal, Global e Local do domínio. Vamos apresentar as diversas características e usos de cada tipo de grupo.

Grupos universais (Universal group):

Como o próprio nome sugere são grupos que podem ser utilizados em qualquer parte de um domínio ou da árvore de domínios e podem conter como membros, grupos e usuários de quaisquer domínios. Em resumo:

- ◆ **Pode conter:** Contas de usuários, outros grupos universais, e grupos globais de qualquer domínio.
- ◆ **Pode ser membro de:** Grupos locais de qualquer domínio ou grupos universais de qualquer domínio.
- ◆ **Pode receber permissões para recursos localizados em qualquer domínio.**
- ◆ Quando o nível de funcionalidade do Domínio está configurado como Windows 2000 Nativo ou Windows Server 2003, os seguintes elementos podem ser incluídos como membros de um grupo universal: Usuários, grupos Globais e grupos Universais de qualquer domínio da floresta.
- ◆ Quando o nível de funcionalidade do Domínio está configurado como Windows 2000 Misto, não é possível criar grupos Universais.
- ◆ Quando o nível de funcionalidade do Domínio está configurado como Windows 2000 Nativo ou Windows Server 2003, um grupo Universal pode ser colocado como membro de um outro grupo Universal e permissões podem ser atribuídas em qualquer domínio.
- ◆ Um grupo pode ser convertido de Universal para Global ou de Universal para Local do domínio. Nos dois casos esta conversão somente pode ser feita se o grupo Universal não tiver como um de seus membros, outro grupo Universal. Não esqueça deste detalhe.

Quando devem ser utilizados grupos universais:

Quando você deseja consolidar diversos grupos globais. Você pode fazer isso criando um grupo Universal e adicionando os diversos grupos globais como membros do grupo Universal.

**IMPORTANTE:** É possível converter um grupo do tipo Segurança para distribuição e vice-versa. Para tal é preciso que o domínio esteja, pelo menos, no modo Windows 2000 Nativo. Para domínios que ainda estejam no modo Windows 2000 Mixed, esta conversão não será possível.

**IMPORTANTE:** Conforme detalhado anteriormente, um domínio baseado no Active Directory pode estar em diferentes modos de funcionalidade (Windows 2000 Nativo, Misto ou Windows Server 2003). Para cada modo existem diferentes possibilidades em relação aos grupos Universais.

## Grupo global:

Um grupo Global é “global” quanto aos locais onde ele pode receber permissões de acesso, ou seja, um grupo Global pode receber permissões de acesso em recursos (pastas compartilhadas, impressoras, etc) de qualquer domínio. Em resumo, considere as afirmações a seguir:

- ◆ Pode conter: Contas de usuários e grupos globais do mesmo domínio, ou seja, somente pode conter membros do domínio no qual o grupo é criado.
- ◆ Pode ser membro de: Grupos universais e Grupos locais, de qualquer domínio.

**IMPORTANTE:** Os grupos Universais devem ser muito bem planejados. Não devem ser feitas alterações freqüentes nos membros de um grupo Universal, uma vez que este tipo de ação causa um volume elevado de replicação no Active Directory.

## Grupos globais do mesmo domínio.

- ◆ Pode receber permissões para recursos localizados em qualquer domínio.

Conforme detalhado anteriormente, um domínio baseado no Active Directory pode estar em diferentes modos (Windows 2000 Nativo, Misto ou Windows Server 2003). Para cada modo existem diferentes possibilidades em relação aos grupos Globais:

- ◆ Quando o nível de funcionalidade do Domínio está configurado como Windows 2000 Nativo ou Windows Server 2003, os seguintes elementos podem ser incluídos como membros de um grupo Global: contas de usuários e grupos globais do mesmo domínio. Por exemplo, se você cria um grupo global chamado WebUsers, no domínio abc.com.br, este grupo poderá conter como membros, grupos globais do domínio abc.com.br e usuários do domínio abc.com.br
- ◆ Quando o nível de funcionalidade do Domínio está configurado como Windows 2000 Misto, somente contas de usuários do próprio domínio é que podem ser membros de um grupo Global. Por exemplo, se você cria um grupo global chamado WebUsers, no domínio abc.com.br e este domínio está no modo Misto, então somente contas de usuários do domínio abc.com.br é que poderão ser membros do grupo WebUsers.
- ◆ Um grupo pode ser convertido de Global para Universal, desde que o grupo Global não seja membro de nenhum outro grupo Global.. Não esqueça deste detalhe.

## Quando devem ser utilizados grupos Globais:

Os grupos Globais devem ser utilizados para o gerenciamento dos objetos que sofrem alterações constantemente, quase que diariamente, tais como contas de usuários e de computadores. As alterações feitas em um grupo Global são replicadas somente dentro do domínio onde foi criado o grupo Global e não através de toda a árvore de domínios (que é o que acontece com os grupos Universais). Por isso que não devemos fazer modificações, constantemente, nos grupos Universais). Com isso o volume de replicação é reduzido, o que permite a utilização de grupos Globais para a administração de objetos que mudam freqüentemente.

## Grupos locais do Domínio(Domain local group):

São grupos que somente podem receber permissões para os recursos do domínio onde foram criados, porém podem ter como membros, grupos e usuários de outros domínios. Em resumo:

- ◆ Pode conter membros de qualquer domínio.
- ◆ Somente pode receber permissões para recursos em servidores do domínio no qual o grupo foi criado.
- ◆ Pode conter: Contas de usuários, grupos universais e grupos globais de qualquer domínio.

## Outros grupos Locais do próprio domínio.

- ◆ Pode ser membro de: Grupos locais do próprio domínio.

Conforme detalhado anteriormente, um domínio baseado no Active Directory pode estar em diferentes modos (Windows 2000 Nativo, Misto ou Windows Server 2003). Para cada modo existem diferentes possibilidades em relação aos grupos Globais:

- ◆ Quando o nível de funcionalidade do Domínio está configurado como Windows 2000 Nativo ou Windows Server 2003, os seguintes elementos podem ser incluídos como membros de um grupo Local: contas de usuários, grupos universais e grupos globais de qualquer domínio. Outros grupos locais do próprio domínio.
- ◆ Um grupo pode ser convertido de Local para Universal, desde que o grupo não tenha como seu membro um outro grupo Local. Não esqueça deste detalhe.

Quando devem ser utilizados grupos Locais:

Os grupos Locais são utilizados para atribuir permissões de acesso aos recursos da rede. Conforme discutirei, em detalhes, no Capítulo 6, a Microsoft recomenda uma estratégia baseada nos seguintes passos, resumidos pela sigla AGLP:

- ◆ Criar as contas de usuários (A = Accounts).
- ◆ Adicionar as contas de usuários a grupos Globais, confere com o que foi dito anteriormente, onde falei que os grupos Globais são utilizados para gerenciar os objetos do dia-a-dia, tais como contas de usuários (G= Global).
- ◆ Adicione os grupos globais ou Universais (se for o caso) como membros dos grupos Locais (L = Local).
- ◆ Atribua permissões de acesso para os grupos Locais (P = Permissions).

Bem, feitas as apresentações teóricas sobre grupos, agora você aprenderá a executar as operações básicas com grupos, tais como criar um novo grupo, adicionar usuários, remover usuários do grupo, renomear grupos, excluir grupos e converter um grupo de um tipo para outro.

---

**IMPORTANTE: Lembre da dica**  
**AGLP – Accounts -> Global Groups**  
**-> Local Groups -> Permissions.**

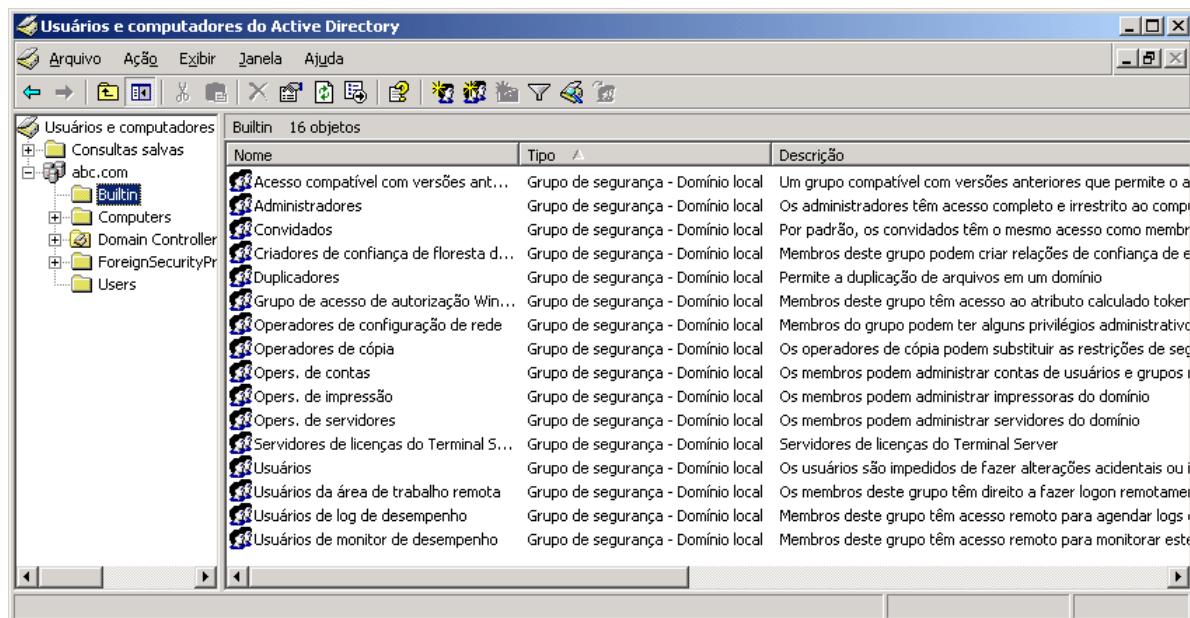
---

## Ações práticas com grupos de usuários.

Neste item você aprenderá sobre os chamados Built-in Groups (Grupos Built-in), que são os grupos criados automaticamente pelo Active Directory quando o domínio é criado. Também aprenderá a executar uma série de ações práticas, relacionadas com grupos.

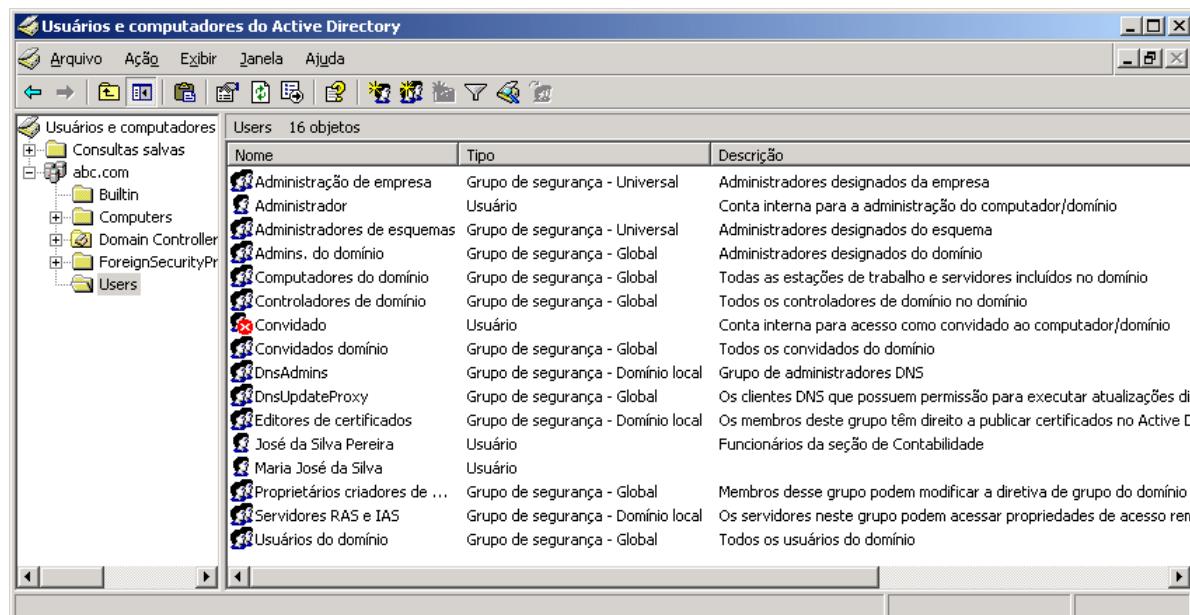
### Built-in Groups.

Quando um domínio é criado (com a instalação do Active Directory no primeiro DC do domínio), uma série de grupos são criados. Estes grupos podem ser acessados usando o console Usuários e computadores do Active Directory. Na opção Built-in são exibidos os grupos locais do domínio, criados automaticamente durante a criação do domínio, conforme indicado na Figura 4.31:



**Figura 4.31 Grupos locais do domínio, criados automaticamente.**

Outros grupos também são criados automaticamente. Estes grupos ficam na opção Users. Nesta opção são criados grupos Locais, Globais e universais, conforme indicado na Figura 4.32:



**Figura 4.32 Grupos locais, globais e universais, criados automaticamente na opção Users.**

A seguir descrevo os diversos grupos que são criados automaticamente pelo Active Directory, os chamados Built-in groups.

Grupos locais criados na opção Builtin:

- ◆ **Account Operators (opers. de conta):** Membros deste grupo podem criar, modificar e excluir contas de usuários, grupos e computadores localizadas nas opções Users e Computers e também localizadas em Unidades

organizacionais do domínio. A exceção são as contas de DCs localizadas na opção Domain Controllers, para as quais somente membros do grupo Administradores tem permissão. Membros do grupo Account Operators não poderão modificar a conta Administrator (Administrador) e nem o grupos Domain Admins (Adminis. do Domínio). Também não tem permissão para modificar as contas que pertencem ao grupo Domain Admins. Observe que o objetivo é impedir que membros deste grupo possam se incluir no grupo Adminis. ou modificar uma conta que já está neste grupo (por exemplo alterando a senha de uma destas contas), para poder fazer o logon com permissão de administrador. Os membros deste grupo podem fazer o logon local nos DCs do domínio e também tem permissão para desligar estes servidores. Membros deste grupo tem um nível de permissão elevado, principalmente pelo fato de poder alterar contas de usuários, por isso a administrador deve ter cuidado ao adicionar membros a este grupo. Por padrão os membros deste grupo também tem os seguintes direitos de usuário: Allow log on locally; Shut down the system.

- ◆ **Administrators (Administradores):** Podem tudo dentro do domínio. Membros deste grupo tem controle e permissão total, em todos os DCs do domínio. Por padrão, o grupo Domain Admins (Adminis. do Domínio) e o grupo Enterprise Admins (“maravilhosamente” traduzido como Administradores de empresa), são membros do grupo local Administrators. A conta Administrator (Administrador) também é membro deste grupo, por padrão. Por padrão os membros deste grupo também tem os seguintes direitos de usuário: Access this computer from the network; Adjust memory quotas for a process; Back up files and directories; Bypass traverse checking; Change the system time; Create a pagefile; Debug programs; Enable computer and user accounts to be trusted for delegation; Force a shutdown from a remote system; Increase scheduling priority; Load and unload device drivers; Allow log on locally; Manage auditing and security log; Modify firmware environment values; Profile single process; Profile system performance; Remove computer from docking station; Restore files and directories; Shut down the system; Take ownership of files or other objects. Como os membros deste grupo tem controle total em todos os DCs do domínio, seja cuidadoso e somente adicione novos membros a este grupo quando realmente for necessário.
- ◆ **Backup Operators (Operadores de Cópia):** Os membros deste grupo podem fazer o backup de pastas e arquivos, mesmo que não tenham permissão de acesso (permissões NTFS – Capítulo 6) as pastas e arquivos. Isso permite que a administração das cópias de segurança (backup) seja realizada centralizadamente, sem que tenha que ser atribuída permissão de acesso para o administrador do backup, em todos os recursos que fazem parte do backup. Por padrão este grupo não tem nenhum membro. O administrador deverá adicionar membros a este grupo. Por padrão os membros deste grupo também tem os seguintes direitos de usuário: Back up files and directories; Allow log on locally; Restore files and directories; Shut down the system
- ◆ **Guests (Convidados):** Por padrão, o grupo Domain Guests (Convidados do Domínio) e a conta Guest (Convidado) são membros deste grupo. Por padrão nenhum direito de usuário é atribuído a este grupo.
- ◆ **Incoming Forest Trust Builders (Criadores de confiança de floresta de entrada):** Membros deste grupo tem permissão para criar relações de confiança one-way (unilateral) com domínio root de outras florestas. Por exemplo, membros deste grupo, pertencente a um domínio da floresta A, podem criar uma relação de confiança one-way (unilateral) com um domínio pertencente a uma floresta X, de tal maneira que as contas do domínio

**IMPORTANTE:** Os direitos de usuários são uma série especial de permissões (tais como fazer o logon localmente, desligar o servidor, incluir um computador no domínio e assim por diante), as quais são atribuídas a grupos e usuários. O administrador pode atribuir diferentes direitos para grupos e usuários.

na floresta A, podem receber permissões de acesso aos recursos do domínio na floresta X, ou seja, o domínio na floresta X, passou a confiar nas contas do domínio da floresta A. Este grupo, por padrão, não tem nenhum membro e também não tem nenhum direito de usuário atribuído ao grupo.

- ◆ **Network Configuration Operators (Operadores de Configurações de Rede):** Membros deste grupo podem fazer alterações nas configurações do TCP/IP nos DCs do domínio e também podem usar o comando ipconfig/renew e o comando ipconfig/release. Por padrão este grupo não tem nenhum membro e nenhum direito de usuário é atribuído a este grupo.
- ◆ **Performance Monitor Users (Usuários do monitor de Desempenho):** Membros deste grupo tem permissão para usar o Console de Desempenho para monitorar os contadores de desempenho dos DCs, tanto localmente quanto a partir de uma estação de trabalho da rede. Estas permissões, por padrão, são atribuídas a este grupo e aos grupos Administrators (Administradores) e Performance Log Users (Usuários dos log de desempenho). Por padrão este grupo não tem nenhum membro e nenhum direito de usuário é atribuído a este grupo.
- ◆ **Performance Log Users (Usuários dos log de desempenho):** Membros deste grupo tem permissão para usar o Console de Desempenho para monitorar os contadores e logs de desempenho, bem como alertas de desempenho nos DCs, tanto localmente quanto a partir de uma estação de trabalho da rede. Estas permissões, por padrão, são atribuídas a este grupo e aos grupos Administrators (Administradores) e Performance Log Users (Usuários de log de desempenho). Por padrão este grupo não tem nenhum membro e nenhum direito de usuário é atribuído a este grupo.
- ◆ **Pre-Windows 2000 Compatible Access (Acesso compatível com versões anteriores ao Windows 2000):** Membros deste grupo tem permissão de acesso de leitura (Read) em todos os objetos do tipo usuários e grupos do domínio. Este grupo é disponibilizado por questões de compatibilidade com estações de trabalho rodando o Windows NT 4.0 ou versão anterior. Por padrão, o objeto Everyone (Todos) é membro deste grupo. Somente adicione usuários a este grupo, se eles estiverem utilizando uma estação de trabalho com o NT 4.0 ou versão anterior. Por padrão os membros deste grupo também tem os seguintes direitos de usuário: Access this computer from the network; Bypass traverse checking.
- ◆ **Print Operators (Operas. de Impressão):** Membros deste grupo tem permissão para gerenciar, criar, compartilhar e excluir impressoras conectadas em DCs do domínio. Eles também tem permissão para gerenciar impressoras que foram publicadas no Active Directory (No Capítulo 7 você aprenderá a publicar e a pesquisar impressoras no Active Directory). Os membros deste grupo também tem permissão para fazer o logon localmente e para desligar os DCs do domínio. Por padrão este grupo não tem nenhum membro. Por padrão os membros deste grupo também tem os seguintes direitos de usuário: Allow log on locally; Shut down the system..
- ◆ **Remote Desktop (Usuários da área de trabalho remota):** Membros deste grupo tem permissão para fazer o logon remotamente nos DCs do domínio. É a mesma funcionalidade de desktop remoto, introduzida inicialmente no Windows XP. Você aprenderá a utilizar esta funcionalidade no Capítulo 12. Por padrão este grupo não tem nenhum membro e nenhum direito de usuário é atribuído a este grupo.
- ◆ **Replicator (Duplicadores):** Este grupo dá suporte as funcionalidades de replicação do Active Directory e é utilizado pelo serviço de replicação de arquivos que roda nos DCs do domínio. Não adicione usuários a este grupo. Por padrão este grupo não tem nenhum membro e nenhum direito de usuário é atribuído a este grupo.
- ◆ **Server Operators (Oper. De Servidores):** Os membros deste grupo podem realizar uma série de operações nos DCs do domínio, tais como: logar localmente, criar e deletar compartilhamentos, inicializar e parar serviços, fazer o backup e o restore de arquivos, formatar um disco rígido e desligar o servidor. Por padrão este grupo não tem nenhum membro. Por padrão os membros deste grupo também tem os seguintes direitos de usuário: Back up files and directories; Change the system time; Force shutdown from a remote system; Allow log on locally; Restore files and directories; Shut down the system.

- ◆ **Users (Usuários):** Os membros deste grupo tem permissão para executar as tarefas mais comuns do dia-a-dia, tais como: executar programas, usar impressoras locais e da rede e bloquear o servidor. Por padrão os seguintes grupos são membros deste grupo: Domain Users (Usuários do domínio), Authenticated Users (Usuários autenticados) e Interactive (Interativo – este é um grupo especial interno do Windows Server 2003, o qual não é exibido no console Active Directory Users and Computers). Com isso qualquer conta do domínio fará parte deste grupo. Por padrão nenhum direito de usuário é atribuído a este grupo.

A seguir descrevo os grupos que são criados, automaticamente, na opção Users. Nesta opção são criados grupos locais, globais e universais, dependendo do modo de funcionalidade do domínio.

Grupos criados na opção Users:

- ◆ **Cert Publishers (Editores de certificados):** Grupo local. Membros deste grupo tem permissões para publicar certificados para contas de usuários e computadores. Por padrão este grupo não tem nenhum membro e nenhum direito de usuário é atribuído ao grupo.
- ◆ **DnsAdmins (em Português o nome também é DnsAdmins):** Grupo local. Este grupo somente é criado quando o DNS é instalado no servidor. Membros deste grupo tem acesso administrativo ao servidor DNS, ou seja, podem executar quaisquer ações nas configurações do servidor DNS. Por padrão este grupo não tem nenhum membro e nenhum direito de usuário é atribuído ao grupo.
- ◆ **DnsUpdateProxy (em Português o nome também é DnsUpdateProxy):** Grupo global. Este grupo somente é criado quando o DNS é instalado no servidor. Membros deste grupo são clientes DNS que podem fazer atualizações dinâmicas em nome de outros clientes, como por exemplo um servidor DHCP. Por padrão este grupo não tem nenhum membro e nenhum direito de usuário é atribuído ao grupo.
- ◆ **Domain Admins (Admins. do domínio):** Grupo global. Membros deste grupo tem controle total nos recursos do domínio. Por padrão, este grupo é membro do grupo local Administrators (Administradores) em todos os DCs, em todas as estações de trabalho e em todos os member servers do domínio. Esta inclusão é feita, automaticamente, quando a estação de trabalho ou o member server é configurado para fazer parte do domínio. Por padrão a conta Administrator (Administrador) faz parte deste grupo. Tenha cuidado ao incluir uma nova conta neste grupo, pois você dará “poderes” totais a esta conta. Por padrão os membros deste grupo também tem os seguintes direitos de usuário: Access this computer from the network; Adjust memory quotas for a process; Back up files and directories: Bypass traverse checking; Change the system time; Create a pagefile; Debug programs; Enable computer and user accounts to be trusted for delegation; Force a shutdown from a remote system; Increase scheduling priority; Load and unload device drivers; Allow log on locally; Manage auditing and security log; Modify firmware environment values; Profile single process; Profile system performance; Remove computer from docking station; Restore files and directories; Shut down the system; Take ownership of files or other objects.
- ◆ **Domain Computers (Computadores do domínio):** Grupo Global. Este grupo contém as contas de todas as estações de trabalho e servidores (member servers) que fazem parte do domínio. Por padrão, qualquer conta de computador criada no domínio, fará parte deste grupo. Por padrão nenhum direito de usuário é atribuído ao grupo.
- ◆ **Domain Controllers (Controladores de domínio):** Grupo Global. Este grupo contém as contas de todos os DCs do domínio. Por padrão nenhum direito de usuário é atribuído ao grupo.

---

**NOTA: No Capítulo 16, do livro Windows Server 2003 – Curso Completo, 1568 páginas, quando você estudar o DNS e o DHCP em detalhes, você encontra uma descrição detalhada desta interação entre o DNS e o DHCP.**

---

- ◆ **Domain Guests (Convidados domínio):** Grupo Global. Este grupo contém a conta Convidado como seu único membro. Por padrão nenhum direito de usuário é atribuído ao grupo.
- ◆ **Domain Users (Usuários do domínio):** Grupo Global. Este grupo contém todos os usuários do domínio. Quando uma nova conta de usuário é criada, ela é automaticamente adicionada a este grupo. Este grupo pode ser utilizado para representar todos os usuários do domínio. Por exemplo, se você quer que todos os usuários do domínio tenham acesso de leitura aos arquivos de uma pasta compartilhada, basta dar permissão de leitura para este grupo. Por padrão nenhum direito de usuário é atribuído ao grupo.
- ◆ **Enterprise Admins (Administração de empresa – este grupo somente é exibido no domínio root de uma árvore de domínios):** Grupo Universal se o modo de funcionalidade do domínio aceita grupos Universais, caso contrário será um grupo Global. Membros deste grupo tem controle total em todos os domínios de uma floresta. Por padrão este grupo é membro do grupo Administrators (Administradores) em todos os DCs da floresta. Por padrão a conta Administrator (Administrador) é membro deste grupo. Existem determinadas operações que somente podem ser realizadas por membros deste grupo, como por exemplo autorizar um servidor DHCP no Active Directory (não esqueça deste importante detalhe). Por padrão, os membros deste grupo também tem os seguintes direitos de usuário: Access this computer from the network; Adjust memory quotas for a process; Back up files and directories; Bypass traverse checking; Change the system time; Create a pagefile; Debug programs; Enable computer and user accounts to be trusted for delegation; Force shutdown from a remote system; Increase scheduling priority; Load and unload device drivers; Allow log on locally; Manage auditing and security log; Modify firmware environment values; Profile single process; Profile system performance; Remove computer from docking station; Restore files and directories; Shut down the system; Take ownership of files or other objects.
- ◆ **Group Policy Creator Owners (Proprietários criadores de diretiva de grupo):** Grupo global. Membros deste grupo podem modificar as políticas de segurança (GPOs) do domínio. Por padrão a conta Administrator (Administrador) é membro deste grupo. Por padrão nenhum direito de usuário é atribuído ao grupo.
- ◆ **IIS\_WPG (somente está disponível quando o IIS é instalado no servidor. Para detalhes sobre o IIS consulte o Capítulo 13):** Este grupo representa o processo de execução do IIS 6.0. Por padrão não tem nenhum membro e nenhum direito de usuário é atribuído a este grupo.
- ◆ **RAS and IAS Servers:** Servidores que são membros deste grupo tem permissão para acessar as propriedades de acesso remoto dos usuários. Por padrão nenhum direito é atribuído a este grupo.
- ◆ **Schema Admins (Administradores de esquemas – somente é exibido no domínio root):** Membros deste grupo podem modificar o esquema do Active Directory. Conforme vimos no Capítulo 2, o esquema é a definição da estrutura de dados do Active Directory. Por padrão a conta Administrator (Administrador) é membro deste grupo. Muito cuidado ao adicionar contas a este grupo, pois modificações indevidas no esquema podem causar verdadeiros desastres em todos os domínios da sua rede. Por padrão nenhum direito é atribuído a este grupo.

Bem, isso encerra a apresentação dos chamados Built-in grupos, ou seja, grupos criados automaticamente no Active Directory.

## Criando novos grupos e adicionando novos membros a um grupo.

Neste item você acompanhará um exemplo prático, onde será criado um grupo chamado GrupoTeste e serão adicionadas algumas contas de usuários como membros deste grupo. O grupo GrupoTeste será um grupo Global.

Exemplo: Como criar um grupo e adicionar membros ao grupo:

1. Faça o logon com uma conta com permissão para alterar contas de usuários (Administrador ou pertencente ao grupo Oper. de contas).
2. Abra o console Usuários e computadores do Active Directory: Iniciar -> Ferramentas Administrativas -> Usuários e computadores do Active Directory.

3. Clique na opção Users ou acesse a Unidade Organizacional na qual você deseja criar o novo grupo (você aprenderá sobre Unidades Organizacionais mais adiante, neste capítulo).
4. Para criar um novo grupo você pode utilizar uma das seguintes opções:
  - ◆ Clicar com o botão direito do mouse em Users e no menu que é exibido clicar em Novo -> Grupo.
  - ◆ Selecionar o comando Ação -> Novo -> Grupo.
  - ◆ Clicar no botão Novo grupo, indicado na Figura 4.33:



Figura 4.33 O botão Novo grupo.

5. Será aberta a janela Novo Objeto – Grupo. No campo Nome do grupo, você digita o nome do grupo. A medida que você digita o nome do grupo, o campo Nome do grupo (anterior ao Windows 2000) é preenchido automaticamente. Se for necessário você pode alterar este campo manualmente. Na parte de baixo da janela você define o escopo do grupo (Domínio local, Global ou Universal) e o tipo do grupo (Segurança ou Distribuição). Marque o escopo Global e o tipo Segurança, conforme indicado na Figura 4.34:



Figura 4.34 Criando um grupo de segurança com escopo global.

6. Clique em OK e pronto, o novo grupo será criado e já será exibido na listagem de grupos, conforme destacado na figura 4.35.

**IMPORTANTE:** Se a opção Universal estiver desabilitada, significa que o domínio ainda está no modo de funcionalidade misto, no qual não são permitidos grupos Universais, conforme descrito anteriormente.

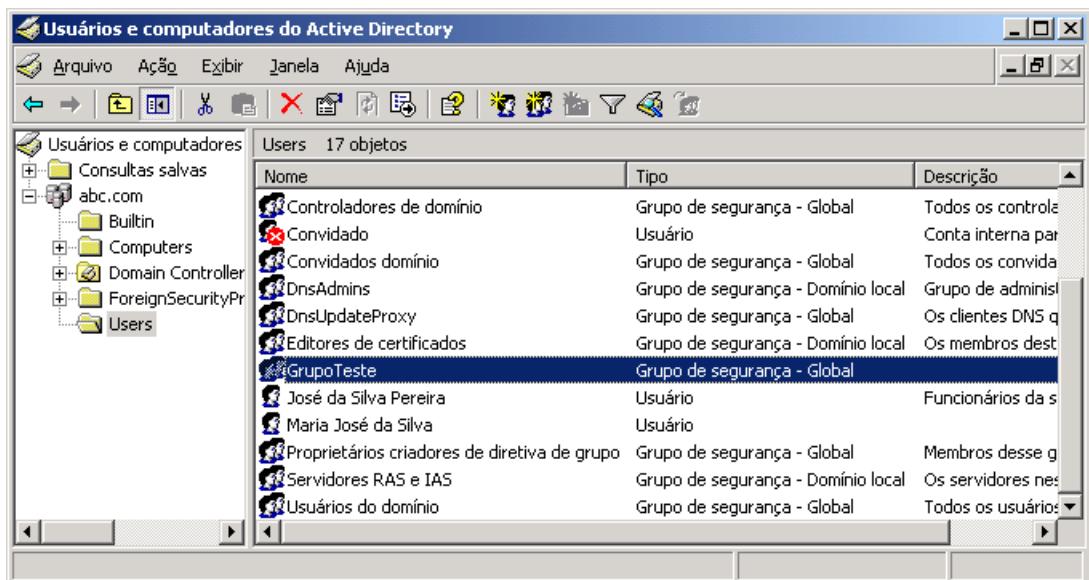


Figura 4.35 O grupo global GrupoTeste, recém criado.

Agora você irá adicionar usuários ao grupo GrupoTeste e aprender a configurar outras propriedades do grupo.

7. Dê um clique duplo no grupo GrupoTeste para exibir as propriedades do grupo.
8. Na guia Geral você pode inserir uma descrição, uma e-mail de contato do responsável pela administração do grupo. Você também pode alterar o tipo e o escopo do grupo e inserir comentários sobre o grupo, conforme exemplo ilustrado na Figura 4.36:

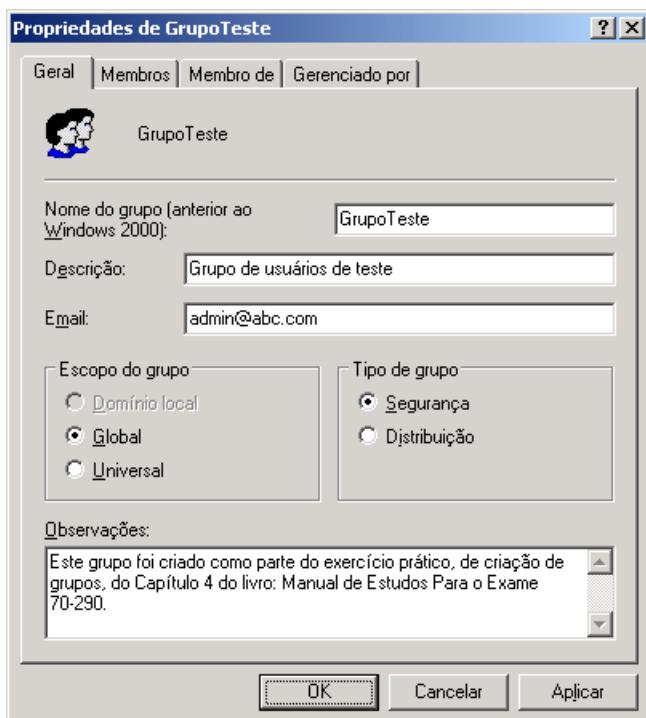
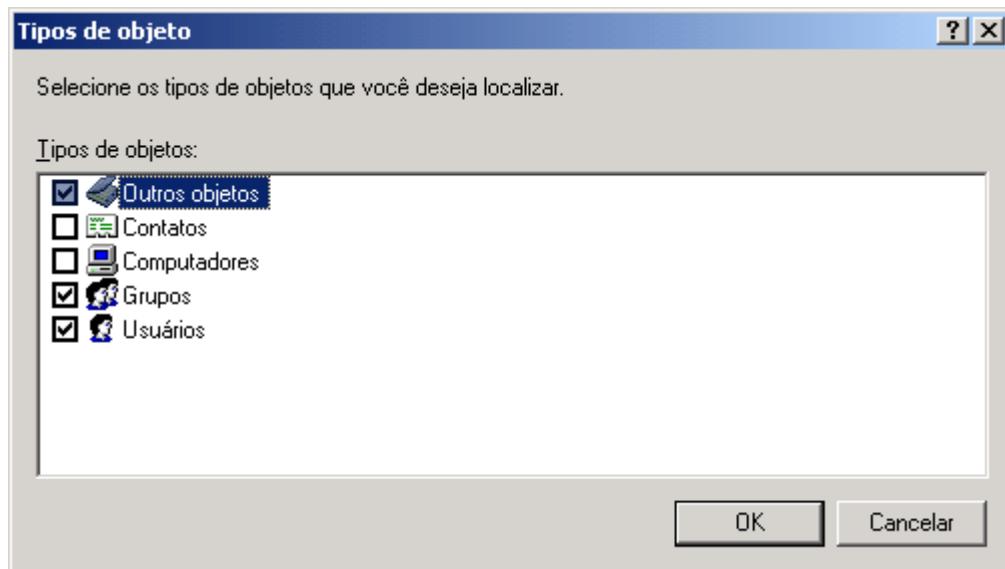


Figura 4.36 Definindo propriedades gerais do grupo.

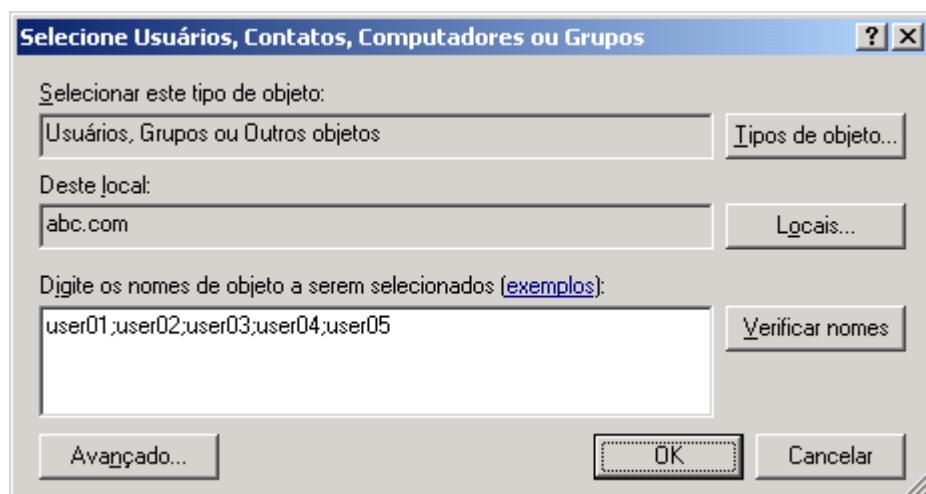
9. Dê um clique na guia Membros. Observe que, por padrão, esta guia está vazia, ou seja, nenhum usuário ou grupo pertence ainda ao grupo GrupoTeste.

10. Para adicionar membros ao grupo dê um clique no botão Adicionar...
11. Será exibida a janela Seleciona Usuários, Contatos, Computadores ou Grupos. Você pode utilizar o botão Tipos de objeto, para limitar os tipos de objetos que serão exibidos na listagem de objetos, conforme indicado na Figura 4.37:



**Figura 4.37 Selezionando os tipos de objetos a serem listados.**

12. Você utiliza o objeto Locais para selecionar o domínio onde estão as contas de usuários e grupos que serão adicionados como membros do grupo GrupoTeste. Por exemplo, você pode adicionar como membros de um grupo local ou universal, usuários e grupos de outros domínios.
13. Se você souber o nome de logon dos usuários que farão parte do grupo, você poderá digitá-los diretamente no campo Digite os nomes de objeto a serem selecionados, separando-os por ponto-e-vírgula, conforme exemplo da figura 4.38.



**Figura 4.38 Digitando o nome dos membros do grupo, separando-os por ponto-e-vírgula.**

14. Porém é pouco provável que você saiba de cor o nome de todos os usuários e grupos da sua rede (imagine uma rede com milhares de usuários e dezenas de grupos). Para exibir uma listagem das contas do domínio clique no botão Avançado... A janela será expandida e será exibido um formulário para pesquisa no Active Directory. Neste formulário você pode definir vários critérios de pesquisa, conforme mostrarei na parte final deste capítulo. Neste momento nos interessa exibir a lista completa de objetos, para selecionar os que queremos adicionar como membros do grupo. Para exibir todos os objetos basta clicar no botão Localizar agora. Como não definimos nenhum critério de pesquisa, todos os objetos serão exibidos, conforme indicado na Figura 4.39:

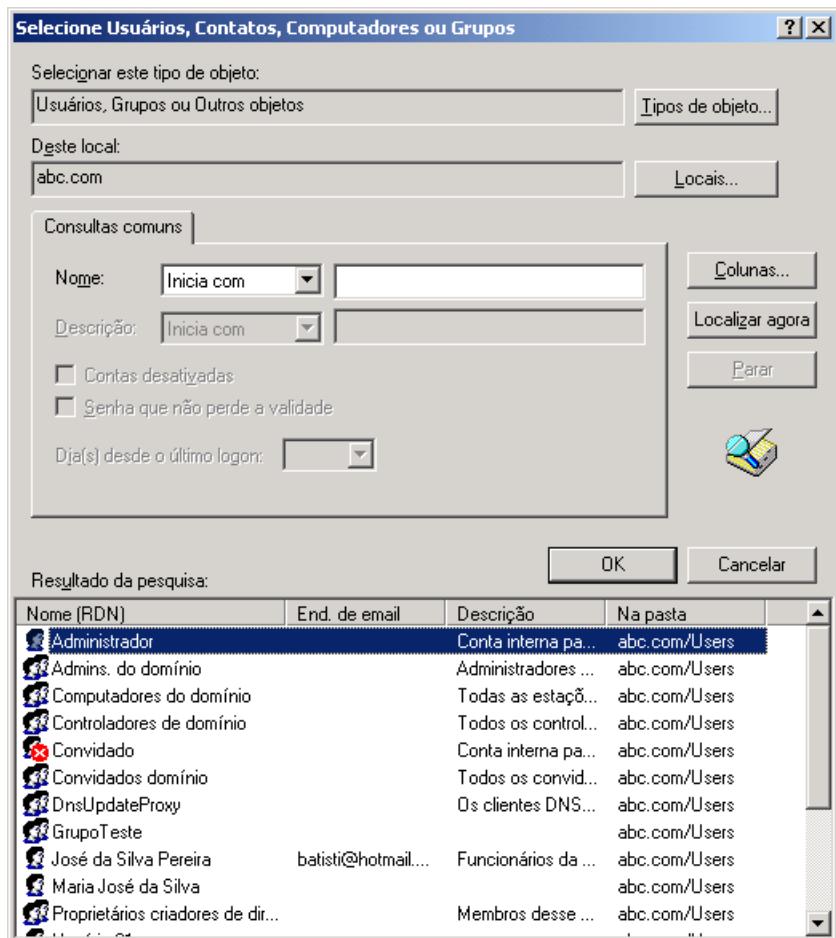


Figura 4.39 Exibindo todos os objetos do domínio abc.com.

15. Agora você deve selecionar os usuários e grupos que serão incluídos como membro do grupo GrupoTeste. Para selecionar objetos nesta janela é como selecionar arquivos no Windows Explorer. Para selecionar vários objetos, intercaladamente, pressione a tecla Ctrl, mantenha-a pressionada e vá clicando nos objetos a serem selecionados. Para selecionar vários objetos em seqüência, clique no primeiro objeto a ser selecionado, libere o botão do mouse, pressione a tecla Shift e mantenha-a pressionada e clique no último objeto da lista. Com isso todos, desde o primeiro até o último serão selecionados. Utilize uma destas técnicas para selecionar os objetos (usuários, grupos, computadores, etc), que farão parte do grupo GrupoTeste. No exemplo da Figura 4.40 selecionei cinco usuários (Usuário 01, Usuário 02 , Usuário 03. Usuário 04, e Usuário 05).

| Nome (RDN)                        | End. de email      | Descrição           | Na pasta      |
|-----------------------------------|--------------------|---------------------|---------------|
| DnsUpdateProxy                    |                    | Os clientes DNS...  | abc.com/Users |
| GrupoTeste                        |                    |                     | abc.com/Users |
| José da Silva Pereira             | batisti@hotmail... | Funcionários da ... | abc.com/Users |
| Maria José da Silva               |                    |                     | abc.com/Users |
| Proprietários criadores de dir... |                    | Membros desse ...   | abc.com/Users |
| Usuário 01                        |                    |                     | abc.com/Users |
| Usuário 02                        |                    |                     | abc.com/Users |
| Usuário 03                        |                    |                     | abc.com/Users |
| Usuário 04                        |                    |                     | abc.com/Users |
| Usuário 05                        |                    |                     | abc.com/Users |
| Usuários do domínio               |                    | Todos os usuári...  | abc.com/Users |

Figura 4.40 Selecionando usuários que farão parte do grupo.

16. Após ter selecionado os objetos que serão incluídos como membros do grupo, clique em OK.
17. Você estará de volta à janela Selecionar Usuários, Contatos, Computadores ou Grupos, com os objetos selecionados já listados. Observe que é listado o nome por extenso do objeto e, entre parênteses o nome de logon mais o domínio, conforme indicado na Figura 4.41. Por exemplo Usuário 01 é o nome por extenso, user01 é o nome de logon e user01@abc.com é o nome completo, incluindo já o domínio.

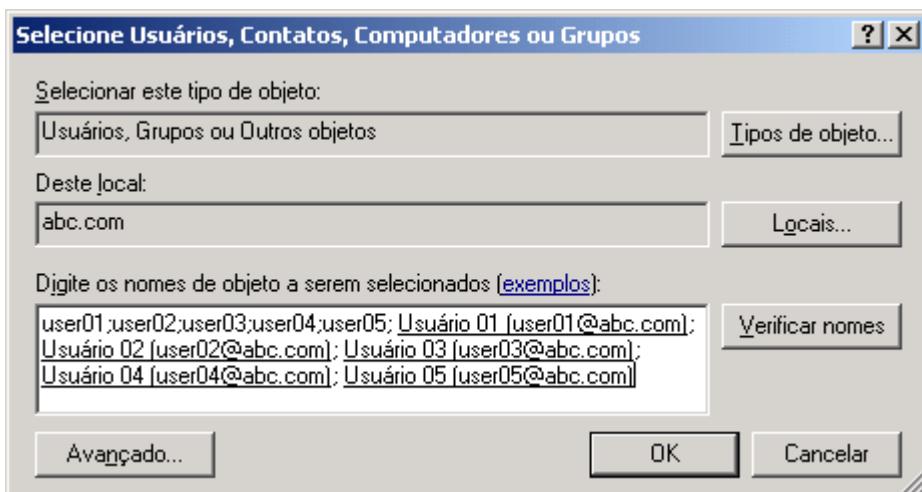
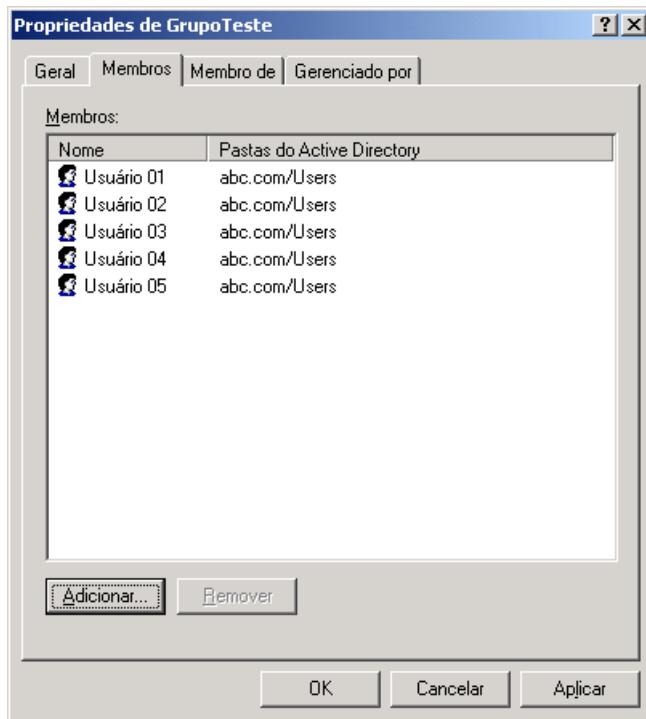


Figura 4.41 Listagem dos objetos selecionados.

18. Clique em OK e pronto, você estará de volta a janela de propriedades do grupo, com os objetos selecionados já listados como membros do grupo, conforme indicado na Figura 4.42.
19. Clique na guia Membro de. Nesta guia são listados em quais grupos o grupo GrupoTeste foi inserido como membro. Em outras palavras, lista a quais grupos pertence o grupo GrupoTeste.
20. Clique na guia Gerenciado por. Neste guia você pode clicar no botão Alterar..., para selecionar quem é o usuário responsável pelo grupo. Ao clicar no botão Alterar, será aberta a janela Selecionar Usuários, Contatos, Computadores ou Grupos, para que você selecione um usuário responsável pelo grupo.
21. Clique em OK e pronto, o grupo foi configurado e novos usuários foram adicionados como membros do grupo.

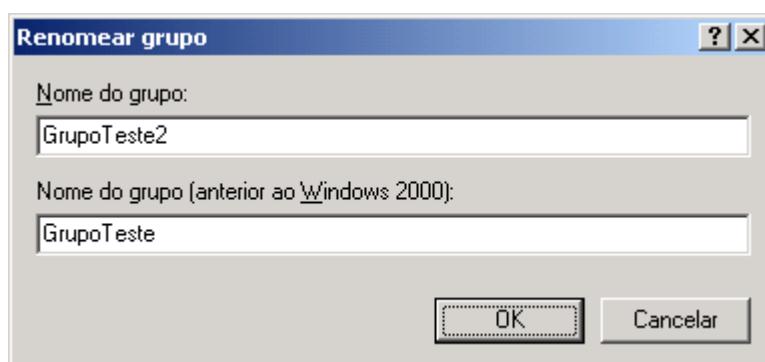
A partir de agora mostrarei como executar outras operações com grupos de usuários, tais como renomear, excluir membros do grupo, alterar o escopo do grupo e excluir um grupo.



**Figura 4.42 Objetos selecionados já inseridos como membros do grupo.**

Para Renomear um grupo siga os passos indicados a seguir:

1. Faça o logon com uma conta com permissão para alterar contas de usuários e grupos (Administrador ou pertencente ao grupo Oper. de contas).
2. Abra o console Usuários e computadores do Active Directory: Iniciar -> Ferramentas Administrativas -> Usuários e computadores do Active Directory.
3. Clique na opção Users ou acesse a Unidade Organizacional onde está o grupo a ser renomeado (você aprenderá sobre Unidades Organizacionais mais adiante, neste capítulo).
4. Clique com o botão direito do mouse no grupo a ser renomeado.
5. No menu que é exibido clique em Renomear. O nome atual será selecionado. Digite o novo nome e pressione Enter. Será exibida a janela Renomaer grupo, para que você possa alterar também o nome Pré Windows 2000, conforme indicado na Figura 4.43:



**Figura 4.43 Alterando o nome Pré – Windows 2000 do grupo.**

6. Altere o nome Pré – Windows 2000 para que fique igual ao nome do grupo e clique em OK. Pronto, o grupo foi renomeado.

Para Excluir um grupo siga os passos indicados a seguir:

1. Faça o logon com uma conta com permissão para alterar contas de usuários e grupos (Administrador ou pertencente ao grupo Oper. de contas).
2. Abra o console Usuários e computadores do Active Directory: Iniciar -> Ferramentas Administrativas -> Usuários e computadores do Active Directory.
3. Clique na opção Users ou accesse a Unidade Organizacional onde está o grupo a ser excluído (você aprenderá sobre Unidades Organizacionais mais adiante, neste capítulo).
4. Clique com o botão direito do mouse no grupo a ser excluído.
5. No menu de opções que é exibido clique em Excluir.
6. O Windows Server 2003 exibe uma mensagem pedindo confirmação, conforme indicado na Figura 4.44:

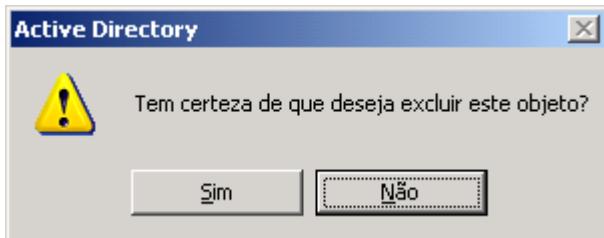


Figura 4.44 Confirmando a exclusão do grupo.

7. Clique em Sim para confirmar a exclusão.

Para excluir membros de um grupo siga os passos indicados a seguir:

1. Faça o logon com uma conta com permissão para alterar contas de usuários e grupos (Administrador ou pertencente ao grupo Oper. de contas).
2. Abra o console Usuários e computadores do Active Directory: Iniciar -> Ferramentas Administrativas -> Usuários e computadores do Active Directory.
3. Clique na opção Users ou accesse a Unidade Organizacional onde está o grupo a ser excluído (você aprenderá sobre Unidades Organizacionais mais adiante, neste capítulo).
4. Dê um clique duplo no grupo a ser alterado para exibir a janela de propriedades do grupo.
5. Clique na guia Membros. A lista de membros do grupo será exibida.
6. Clique no membro a ser excluído do grupo, para seleciona-lo, depois clique no botão Remover.
7. O Windows Server 2003 exibe uma mensagem pedindo que você confirme a exclusão. Clique em Sim e pronto, o objeto selecionado será removido do grupo. Repita a operação para os demais objetos que você deseja remover do grupo. Você pode remover vários objetos de uma só vez. Para isso basta selecionar os vários objetos a serem removidos, usando as teclas Shift ou Ctrl, conforme descrito anteriormente.

Para alterar o tipo ou o escopo de um grupo, siga os passos indicados a seguir:

1. Faça o logon com uma conta com permissão para alterar contas de usuários e grupos (Administrador ou pertencente ao grupo Oper. de contas).

2. Abra o console Usuários e computadores do Active Directory: Iniciar -> Ferramentas Administrativas -> Usuários e computadores do Active Directory.
3. Clique na opção Users ou acesse a Unidade Organizacional onde está o grupo a ser excluído (você aprenderá sobre Unidades Organizacionais mais adiante, neste capítulo).
4. Dê um clique duplo no grupo a ser alterado para exibir a janela de propriedades do grupo.
5. A guia Geral vem selecionada por padrão. Caso esta guia não esteja sendo exibida, dê um clique na guia Geral para exibi-la.
6. Para alterar o escopo do grupo clique em uma das opções de escopo disponíveis. Para alterar o tipo do grupo clique em uma das opções de grupo disponíveis.

---

**IMPORTANTE:** Ao remover uma conta de usuário de um grupo, a conta apenas deixa de ser membro do grupo, a conta não será excluída do Active Directory.

---

## Fundamentos em: Conceito e utilização de Unidades Organizacionais.

Você pode dividir um Domínio em “Unidades Organizacionais”. Uma Unidade Organizacional é uma divisão que pode ser utilizada para organizar os objetos de um determinado domínio em agrupamentos lógicos (tais como por região, cidade, por função ou por outro critério qualquer) para efeitos de administração.

O uso de Unidades Organizacionais resolve uma série de problemas que existiam em redes baseadas no NT Server 4.0. No Windows NT Server 4.0 se um usuário fosse adicionado ao grupo Admins. do Domínio (grupo com poderes totais sobre qualquer recurso do domínio), ele poderia executar qualquer ação em qualquer servidor do domínio. Com a utilização de Unidades Organizacionais, é possível restringir os direitos administrativos apenas a nível da Unidade Organizacional, sem que com isso o usuário tenha poderes sobre todos os demais objetos do Domínio.

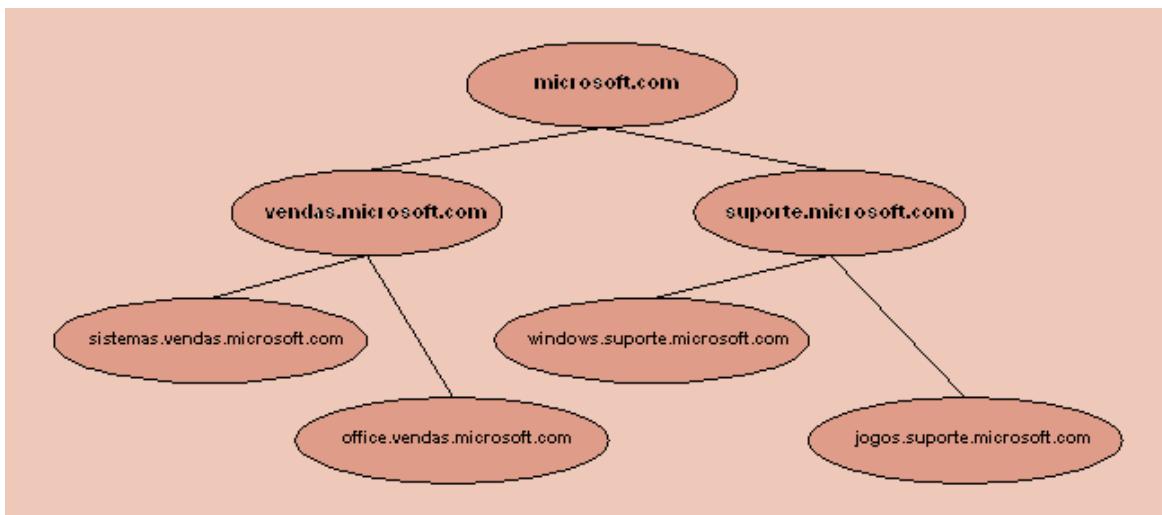
Cada domínio pode implementar a sua hierarquia de Unidades Organizacionais, independentemente dos demais domínios, isto é, os diversos domínios que formam uma árvore de domínios, não precisam ter a mesma estrutura hierárquica de unidades organizacionais. Isto dá uma flexibilidade muito grande, para que o administrador de cada domínio utilize a estrutura de Unidades Organizacionais que for mais adequada.

No exemplo da Figura 4.45, o domínio vendas.microsoft.com, poderia ter uma estrutura hierárquica de Unidades Organizacionais, projetada para atender as necessidades do domínio vendas. Essa estrutura poderia ser completamente diferente da estrutura do domínio suporte.microsoft.com, a qual será projetada para atender as necessidades do domínio suporte. Com isso tem-se uma flexibilidade bastante grande, de tal forma que a árvore de domínios e a organização dos domínios em uma hierarquia de Unidades Organizacionais, possa atender perfeitamente as necessidades de cada divisão da empresa, necessidades estas que podem ser diferentes de uma divisão para outra. A utilização de Unidades Organizacionais não é obrigatória, porém altamente recomendada, conforme mostrarei em alguns exemplos mais adiante.

---

**IMPORTANTE:** O tipo do grupo não poderá ser alterado se o nível de funcionalidade do domínio estiver configurado como Windows 2000 Mixed Mode.

---



**Figura 4.45 Diferentes domínios podem ter diferentes divisões em Unidades Organizacionais.**

Utilize Unidades Organizacionais quando:

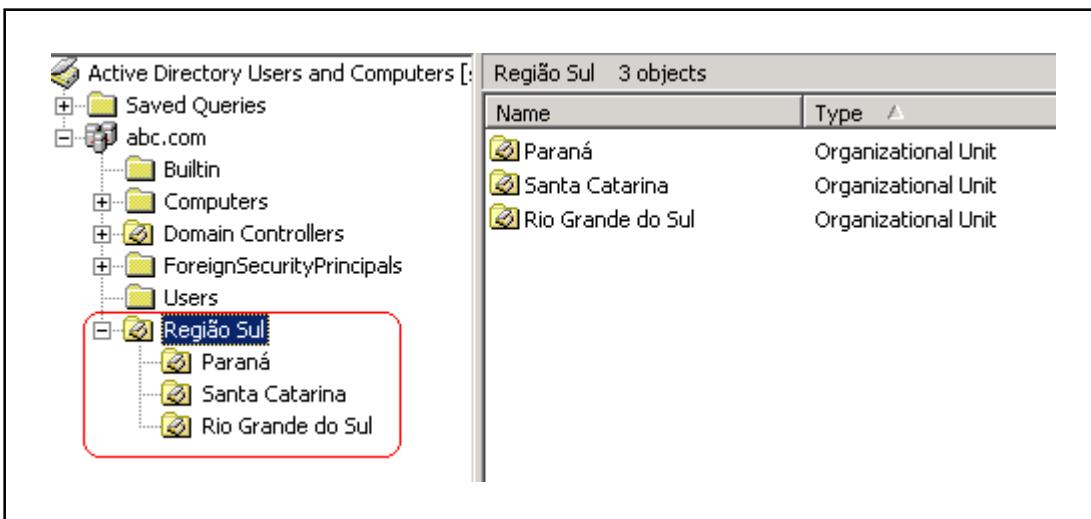
- ◆ Você quiser representar a estrutura e organização (estrutura geográfica ou funcional) da sua companhia em um domínio. Sem a utilização de Unidades Organizacionais, todas as contas de usuários são mantidas e exibidas em uma única lista (na opção Users), independente da localização, departamento ou função do usuário.
- ◆ Você quiser delegar tarefas administrativas sem para isso ter que dar poderes administrativos em todo o Domínio. Com o uso de Unidades Organizacionais, você pode dar permissões para um usuário somente a nível da Unidade Organizacional.
- ◆ Quiser facilitar e melhor acomodar alterações na estrutura da sua companhia. Por exemplo, é muito mais fácil mover contas de usuários entre Unidades Organizacionais do que entre domínios, embora no Windows Server 2003 seja bem mais fácil mover uma conta de um domínio para outro, do que era no Windows 2000 Server.

Com a apresentação destes conceitos, você já está habilitado a aprender as ações práticas de criação de unidades organizacionais e como mover ou criar objetos em uma unidade organizacional.

## Ações práticas com Unidades Organizacionais (OUs).

Neste item você aprenderá a realizar ações práticas com OUs. Primeiro você aprenderá a criar uma nova OU. Conforme mostrarei neste item é possível criar uma OU dentro de outra e assim por diante, como você faz com pastas e subpastas. Porém não é recomendado mais do que quatro níveis de OUs, por questões de desempenho e de replicação do Active Directory. Após criada uma OU, você pode criar novos objetos dentro desta OU, ou mover objetos de outras OUs ou containers (tais como Users, Built-in e assim por diante) para a nova OU. Você também pode excluir OUs. Ao excluir uma OU você deve tomar cuidado, pois todos os objetos que estão dentro da OU a ser excluída, também serão excluídos.

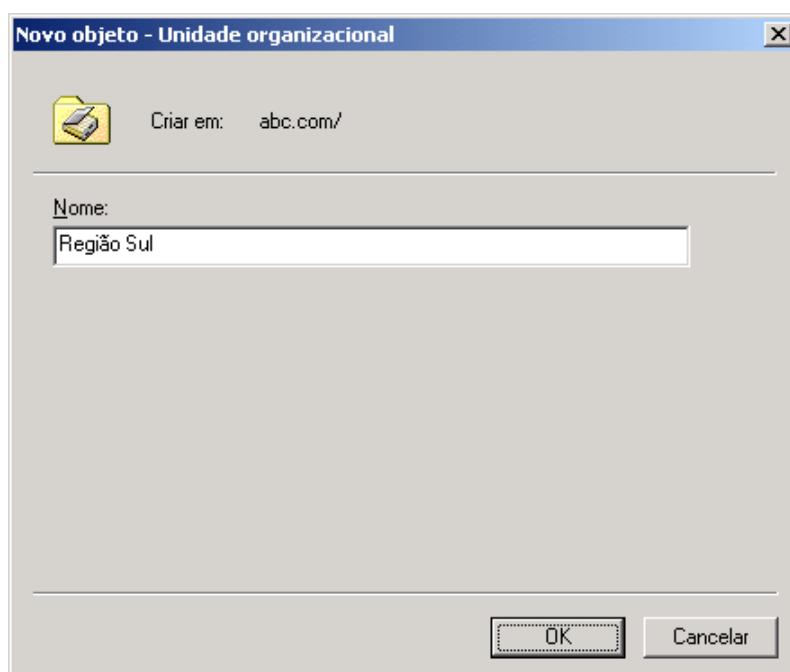
Como criar uma nova OU. Para o exemplo prático a seguir, vou criar a estrutura de OUs indicada na Figura 4.46:



**Figura 4.46 Criando uma estrutura de OUs.**

Para criar as OUs indicadas na Figura 4.46, siga os passos indicados a seguir:

1. Faça o logon com uma conta com permissão para alterar contas de usuários e grupos (Administrador ou pertencente ao grupo Oper. de contas).
2. Abra o console Usuários e computadores do Active Directory: Iniciar -> Ferramentas Administrativas -> Usuários e computadores do Active Directory.
3. Clique com o botão direito do mouse no domínio no qual você quer criar a nova OU.
4. No menu de opções que é exibido clique em Novo -> Unidade organizacional).
5. Será exibida a janela Novo Objeto – Unidade organizacional, solicitando que você digite o nome da nova OU que será criada.
6. Digite Região Sul, conforme indicado na Figura 4.47 e clique em OK.



**Figura 4.47 Informando o nome da nova OU.**

7. Observe que a OU Região Sul já é exibida no painel da esquerda do console Active Directory Users and Computers. Agora é hora de criar as demais OUs do exemplo proposto, as quais serão criadas dentro da OU Região Sul.
8. Clique com o botão direito do mouse na OU Região Sul. No menu de opções que é exibido clique em Novo -> Unidade organizacional. Será exibida a janela Novo Objeto – Unidade organizacional, solicitando que você digite o nome da nova OU que será criada. Digite Paraná e clique em OK. Pronto, a OU Paraná foi criada dentro da OU Região Sul.
9. Clique com o botão direito do mouse na OU Região Sul. No menu de opções que é exibido clique em Novo -> Unidade organizacional. Será exibida a janela Novo Objeto – Unidade organizacional, solicitando que você digite o nome da nova OU que será criada. Digite Santa Catarina e clique em OK. Pronto, a OU Santa Catarina foi criada dentro da OU Região Sul.
10. Clique com o botão direito do mouse na OU Região Sul. No menu de opções que é exibido clique em Novo -> Unidade organizacional. Será exibida a janela Novo Objeto – Unidade organizacional, solicitando que você digite o nome da nova OU que será criada. Digite Rio Grande do Sul e clique em OK. Pronto, a OU Rio Grande do Sul foi criada dentro da OU Região Sul.
11. Muito bem, a estrutura de OUs propostas na Figura 4.46 foi criada. Agora você pode criar contas de usuários, comutadores e grupos dentro destas OUs. Os procedimentos para criar um novo usuário ou grupo dentro de uma OU, são exatamente os mesmos descritos anteriormente, onde você criou um usuário dentro da opção Users.

Para mover um ou mais objetos para dentro de uma OU, siga os passos indicados a seguir:

1. Faça o logon com uma conta com permissão para alterar contas de usuários e grupos (Administrador ou pertencente ao grupo Oper. de contas).
2. Abra o console Usuários e computadores do Active Directory: Iniciar -> Ferramentas Administrativas -> Usuários e computadores do Active Directory.
3. Clique na opção Users ou na Unidade Organizacional onde está o objeto a ser movido.
4. Clique com o botão direito do mouse no objeto a ser movido.
5. No menu de opções que é exibido clique em Mover...
6. Será exibida a janela Mover, com a lista de OUs disponíveis. Acesse a OU de destino, conforme exemplo da Figura 4.48.
7. Clique em OK. Pronto, o objeto (ou os objetos) selecionado no item 4 será movido para a OU selecionada no passo 6, conforme confirmado pela Figura 4.49.

---

**IMPORTANTE:** Agora você aprenderá como mover um usuário ou grupo já existente para dentro de uma OU. Aqui temos mais uma novidade do Windows Server 2003. No console Usuários e Computadores do Active Directory, do Windows Server 2003, você pode arrastar um objeto de uma OU para outra, o que não era possível no Windows 2000 Server. É o mesmo procedimento de arrastar arquivos e pastas usando o Windows Explorer. Aliás você já deve ter notado que a maioria dos consoles de administração do Windows Server 2003 são muito parecidos, em termos de interface e funcionalidade, com o Windows Explorer. Vou apresentar um exemplo prático de como mover objetos para uma OU.

---

**DICA:** Você pode mover vários objetos de uma única vez. Para isso basta selecionar os vários objetos a serem movidos, usando as teclas Shift ou Ctrl, em combinação com o mouse, conforme descrito anteriormente.

---

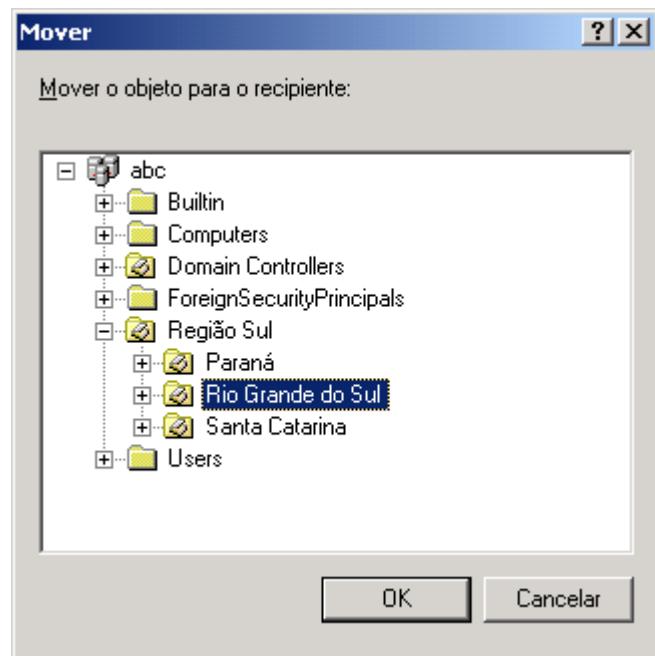


Figura 4.48 Selecionando a OU de destino.

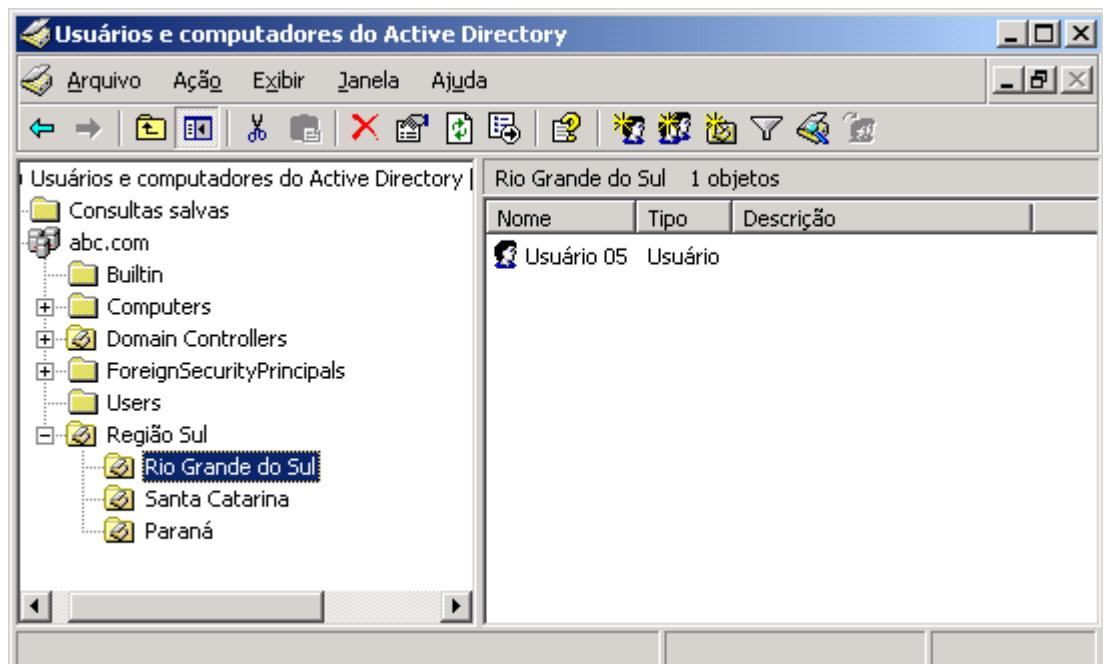


Figura 4.49 O objeto foi movido para a OU selecionada.

A seguir mostrarei os passos para renomear um OU e para excluir uma OU. É importante reforçar o aviso de que, ao excluir uma OU, você também excluirá todos os objetos que estão dentro da OU. Por exemplo, ao excluir a OU Região Sul, criada anteriormente, serão excluídos todos os objetos dentro desta OU, inclusive as OUs Paraná, Santa Catarina, Rio Grande do Sul e os seus respectivos objetos. É o mesmo procedimento que acontece quando você exclui uma pasta do HD. Todos os arquivos e subpastas, dentro da pasta a ser excluída, serão também excluídos.

Para Renomear uma OU siga os passos indicados a seguir:

1. Faça o logon com uma conta com permissão para alterar contas de usuários e grupos (Administrador ou pertencente ao grupo Oper. de contas).
2. Abra o console Usuários e computadores do Active Directory: Iniciar -> Ferramentas Administrativas -> Usuários e computadores do Active Directory.
3. Clique com o botão direito do mouse na OU a ser renomeada.
5. No menu que é exibido clique em Renomear. O nome atual será selecionado. Digite o novo nome e pressione Enter. A OU será renomeada e o novo nome será exibido.

**DICA:** Conforme descrito anteriormente, você pode mover objetos usando os recursos de Arrastar e Soltar. Essa é uma novidade do Windows Server 2003, já que não estava disponível este recurso no Windows 2000 Server.

Para Excluir uma OU siga os passos indicados a seguir:

1. Faça o logon com uma conta com permissão para alterar contas de usuários e grupos (Administrador ou pertencente ao grupo Oper. de contas).
2. Abra o console Usuários e computadores do Active Directory: Iniciar -> Ferramentas Administrativas -> Usuários e computadores do Active Directory.
3. Clique com o botão direito do mouse na OU a ser excluída.
4. No menu de opções que é exibido clique em Excluir.
5. O Windows Server 2003 exibe uma mensagem pedindo confirmação. Clique em Sim para confirmar a exclusão. A OU (e todo o seu conteúdo) será excluída.

Você também pode mover uma OU e todo o seu conteúdo. O procedimento para mover uma OU é o mesmo que para mover outros objetos. Clique com o botão direito do mouse na OU a ser movida. No menu que é exibido clique em Mover.... Será exibida a janela Mover, para que você selecione o destino para onde a OU selecionada será movida. Selecione o destino e clique em OK. Você também pode mover uma OU usando o recurso de Arrastar e soltar.

## Delegando tarefas administrativas a nível de OU:

Conforme descrito nos Capítulo 1 e 2 e “reforçado neste capítulo”, uma das grandes vantagens/utilizações das OUs, é justamente a possibilidade de descentralizar tarefas administrativas, com a possibilidade de delegar permissões para determinados usuários executarem tarefas específicas, apenas nos objetos (usuários, grupos e computadores), contidos dentro de uma determinada OU.

Por exemplo, imagine uma rede onde temos um domínio chamado regiaosul.com.br. Neste domínio temos três redes locais, uma em Curitiba, outra em Florianópolis e outra em Porto Alegre. Você pode montar uma estrutura de tal maneira que apenas um grupo restrito (talvez um ou dois usuários), tenham poderes de Administrador em todo o domínio, isto é, somente um ou dois usuários pertençam ao grupo Admins. do domínio.

Em seguida você pode criar três unidades organizacionais, por exemplo: Curitiba, Florianópolis e Porto Alegre. O próximo passo é mover as contas de usuários, computadores e grupos da rede de Curitiba, para dentro da OU Curitiba; mover as contas de usuários, computadores e grupos da rede de Florianópolis para a OU Florianópolis e, por fim, mover as contas de usuários, computadores e grupos da rede de Porto Alegre para a OU Porto Alegre.

Agora você pode descentralizar algumas tarefas administrativas, dando permissões para que um ou mais usuários possam executar algumas tarefas administrativas nas contas de usuários, grupos e computadores da própria OU. Por exemplo, você pode criar um grupo chamada Administradores da OU Curitiba, dentro da OU Curitiba. Em seguida você pode delegar tarefas para este grupo, em relação a OU Curitiba. Por exemplo, você pode permitir que os membros

do grupo Administradores da OU Curitiba, possam criar novas contas de usuários e editar as contas já existentes somente dentro da OU Curitiba. O mesmo pode ser feito em relação as demais OUs do domínio.

Observe que o com o uso de OUs, na prática, é possível descentralizar uma série de tarefas administrativas, delegando tarefas para que um administrador da própria OU, execute as tarefas mais comuns do dia-a-dia, tais como administração de contas de usuários e de recursos compartilhados, dentro dos recursos da própria OU. A seguir mostrarei um exemplo prático de como delegar permissões para uma OU. No Capítulo 15, nas questões do simulado, você encontrará questões relacionadas ao conceito de delegação de tarefas em OUs.

Exemplo: Para delegar permissões em uma OU, siga os passos indicados a seguir:

1. Faça o logon com uma conta com permissão de administrador.
2. Abra o console Usuários e computadores do Active Directory: Iniciar -> Ferramentas Administrativas -> Usuários e computadores do Active Directory.
3. Clique com o botão direito do mouse na OU na qual você deseja delegar permissões para executar determinadas tarefas. As permissões podem ser delegadas para um ou mais usuários ou grupos. O mais comum é delegar para um ou dois usuários ou para um grupo, no qual estão os usuários que terão permissões para executar tarefas administrativas nos recursos da OU. No menu de opções que é exibido clique em Delegar controle...
4. Será aberto o Assistente para delegação de controle. A primeira etapa do assistente é apenas informativa. Clique em Avançar para seguir para a próxima etapa do assistente.
5. Nesta etapa você irá adicionar os usuários/grupos para os quais você irá delegar permissões em relação a OU. Clique no botão Adicionar...
6. Será aberta a janela Selecionar Usuários, Computadores ou Grupos. Clique no botão Avançado e em seguida clique no botão Localizar agora. Clique no usuário/grupo para o qual você irá delegar permissões e em seguida clique no botão Adicionar. Repita a operação para os demais usuários ou grupos que receberão permissões. Em seguida clique em OK. Você estará de volta a tela do assistente e os usuários/grupos selecionados já serão exibidos, conforme exemplo da Figura 4.50, onde foram adicionados os usuários Usuário 01 e Usuário 02:

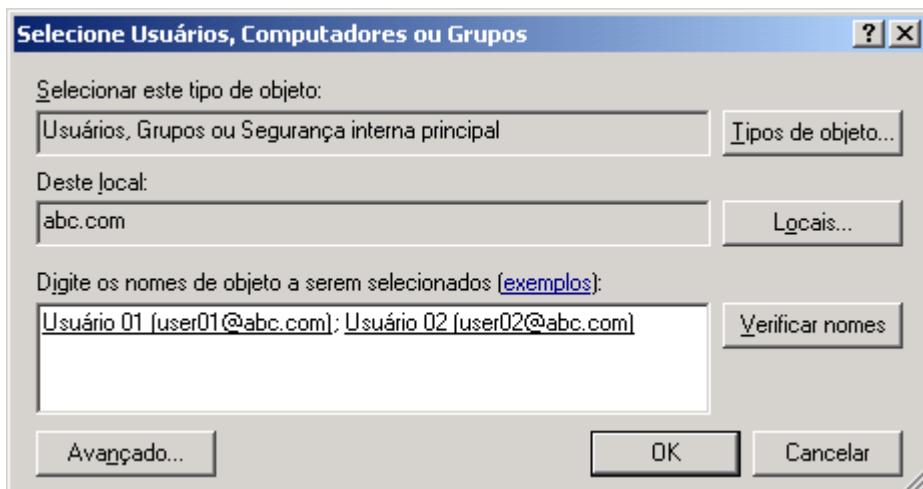


Figura 4.50 Selecionando usuários/grupos.

7. Clique em OK. Você estará de volta ao assistente de delegação de tarefas. Clique em Avançar para seguir para a próxima etapa do assistente.
8. Nesta etapa você deve selecionar quais permissões serão delegadas para os usuários selecionados no passo 6. Estão disponíveis as seguintes opções:
  - ◆ Criar, excluir e gerenciar contas de usuários
  - ◆ Redefinir senhas usuário/forçar alter. senha próx logon
  - ◆ Ler todas as informações do usuário
  - ◆ Criar, excluir e gerenciar grupos
  - ◆ Modificar os membros de um grupo.
  - ◆ Gerenciar vínculos de diretivas de grupo: Esta opção permite que o usuário associe GPOs já existentes a OU
  - ◆ Gerar conjunto de diretivas resultante (planejamento)
  - ◆ Gerar conjunto de diretivas resultante (log)
  - ◆ Criar, excluir e gerenciar contas de inetOrgPerson
  - ◆ Redefinir senhas de inetOrgPerson/forçar alteração senha próx. Logon
  - ◆ Ler todas as informações inetOrgPerson
9. Marque as opções desejadas e clique em Avançar, para seguir para a próxima etapa do assistente.
10. Será exibida a tela final do assistente, com um resumo das opções selecionadas. Você pode utilizar o botão Voltar para fazer quaisquer alterações que sejam necessárias. Clique em Concluir. O assistente será encerrado e serão delegadas as permissões selecionadas para os usuários/grupos que foram adicionados no passo 6.

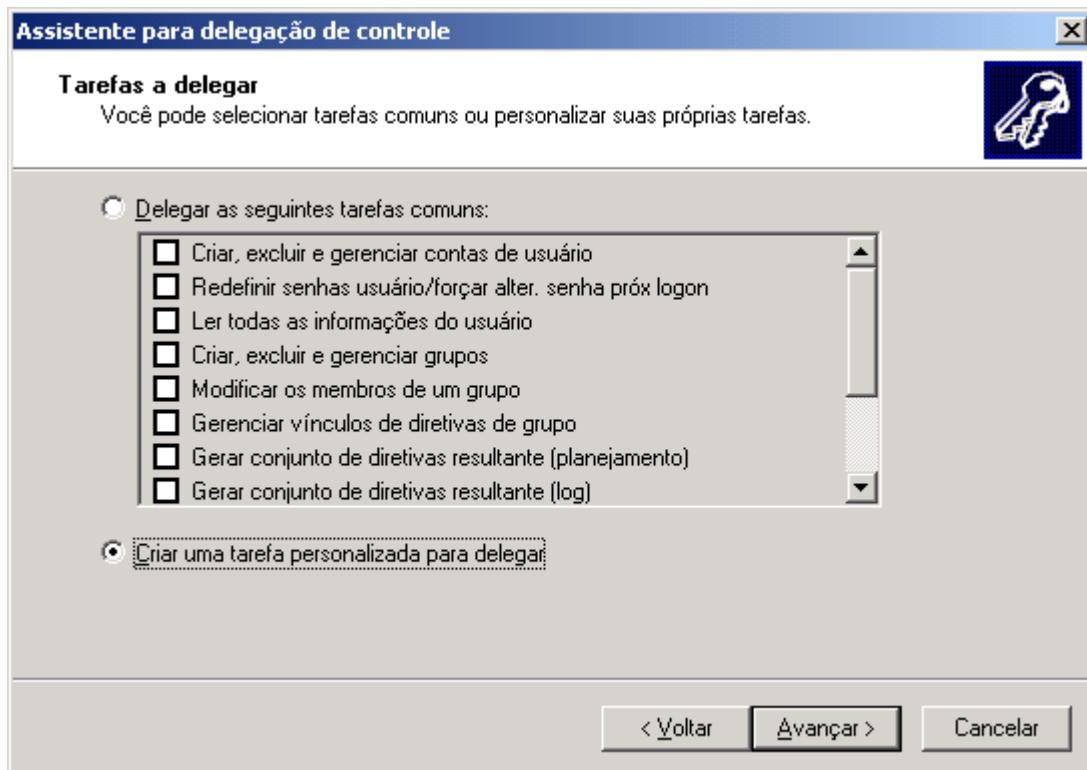
Conforme comentado anteriormente, é possível definir permissões de uma maneira bem mais refinada. Usando o Assistente para delegação de tarefas, você pode definir ações bem específicas que poderão ser executadas pelos usuários. No exemplo a seguir você aprenderá a utilizar o assistente para atribuir permissões para execução de tarefas personalizadas.

Exemplo: Para delegar permissões em uma OU, definindo tarefas personalizadas, siga os passos indicados a seguir:

1. Faça o logon com uma conta com permissão de administrador.
2. Abra o console Usuários e computadores do Active Directory: Iniciar -> Ferramentas Administrativas -> Usuários e computadores do Active Directory.
3. Clique com o botão direito do mouse na OU na qual você deseja delegar permissões para executar determinadas tarefas. As permissões podem ser delegadas para um ou mais usuários ou grupos. O mais comum é delegar para um ou dois usuários ou para um grupo, no qual estão os usuários que terão permissões para executar tarefas administrativas nos recursos da OU. No menu de opções que é exibido clique em Delegar controle...
4. Será aberto o Assistente para delegação de controle. A primeira etapa do assistente é apenas informativa. Clique em Avançar para seguir para a próxima etapa do assistente.
5. Nesta etapa você irá adicionar os usuários/grupos para os quais você irá delegar permissões em relação a OU. Clique no botão Adicionar...
6. Será aberta a janela Selecione Usuários, Computadores ou Grupos. Clique no botão Avançado e em seguida clique no botão Localizar agora. Clique no usuário/grupo para o qual você irá delegar permissões e em seguida

**NOTA:** Você pode definir permissões mais personalizadas do que este grupo de permissões padrão, já existente. Para isso marque a opção Criar uma tarefa personalizada para delegar. Ao marcar esta opção e clicar em Avançar, serão exibidas telas adicionais do assistente, para que você possa definir permissões em um nível bem mais personalizado. Você aprenderá a usar esta opção no próximo exemplo prático.

- clique no botão Adicionar. Repita a operação para os demais usuários ou grupos que receberão permissões. Sem seguida clique em OK. Você estará de volta a tela do assistente e os usuários/grupos selecionados já serão exibidos.
7. Clique em Avançar para seguir para a próxima etapa do assistente.
  8. Nesta etapa, para criar um conjunto de permissões personalizadas, você deve selecionar a opção Criar uma tarefa personalizada para delegar, conforme indicado na Figura 4.51:



**Figura 4.51 Criando uma tarefa personalizada para delegar.**

9. Clique em Avançar para seguir para a próxima etapa do assistente.
10. Nesta etapa você tem duas opções. Você pode criar uma tarefa que se aplica a todos os objetos já existentes na OU e aos novos que serão criados (Esta pasta, objetos existentes nesta pasta e criação de novos objetos nesta pasta) ou pode definir permissões apenas para determinados tipos de objetos (Somente os seguintes objetos na pasta). Ao marcar a opção Somente os seguintes objetos na pasta você poderá marcar um ou mais dos diversos tipos de objetos, sobre os quais se aplicará a tarefa personalizada que está sendo criada. Por exemplo, se você quer delegar permissões que se relacionam apenas a objetos do tipo contas de computadores, marque a opção Somente os seguintes objetos na pasta e, na lista de objetos, marque a opção Computador objetos, conforme exemplo da Figura 4.52.
11. Marque as opções indicadas na Figura 4.52 e clique em Avançar, para seguir para a próxima etapa do assistente.
12. Nesta etapa é exibida uma extensa lista de permissões relacionadas com os objetos selecionados na etapa anterior. No nosso exemplo, com objetos do tipo Computadores. Por exemplo, existem permissões tais como Controle total, Ler, Gravar, Criar todos os objetos filho e assim por diante. Defina as permissões que serão delegadas e clique em Avançar, para seguir para a próxima etapa do assistente.
13. Será exibida a tela final do assistente, com um resumo das opções selecionadas. Você pode utilizar o botão Voltar para fazer quaisquer alterações que sejam necessárias. Clique em Concluir. O assistente será encerrado e serão delegadas as permissões que forem especificadas, para os usuários/grupos que foram adicionados no passo 6.

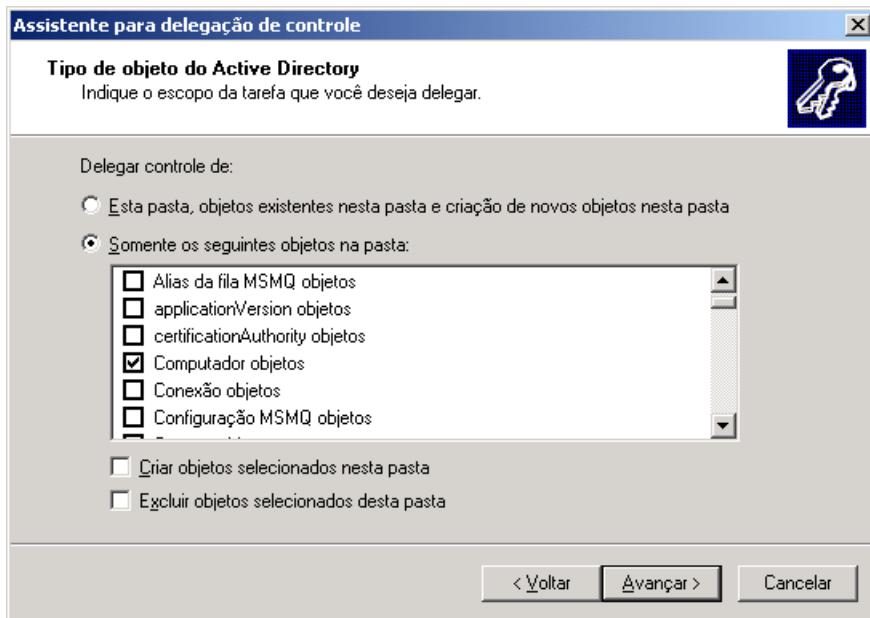
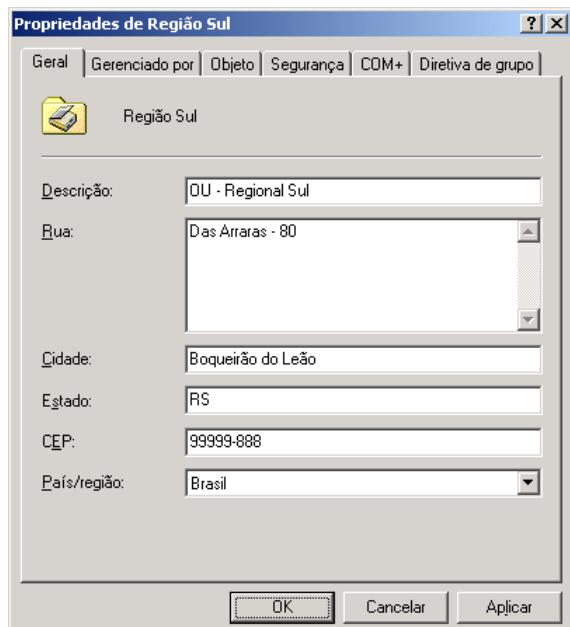


Figura 4.52 Delegando tarefas relacionadas a objetos do tipo Computadores.

## Propriedades e Permissões de Segurança em Unidades Organizacionais.

Todos os objetos do Active Directory (usuários, grupos, computadores, Unidades Organizacionais e assim por diante) tem um conjunto de propriedades e uma lista de permissões associadas. Neste item mostrarei as principais propriedades de uma OU e as configurações de segurança associadas.

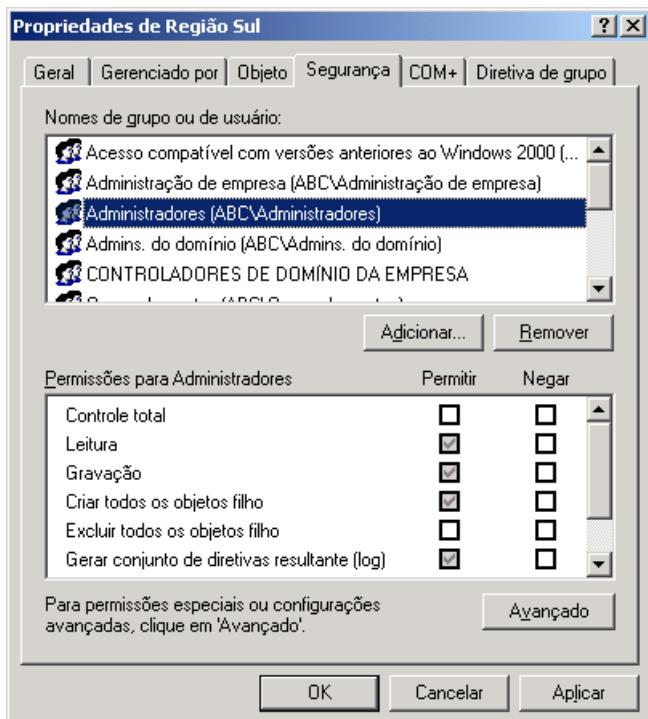
Para acessar as propriedades de uma OU, basta abrir o console Usuários e Computadores do Active Directory, localizar a OU desejada, clicar com o botão direito na OU e, no menu de opções que é exibido, clicar em Propriedades. Será exibida a janela de Propriedades da OU, com a guia Geral selecionada por padrão, conforme indicado na Figura 4.53:



**DICA:** Para que todas as opções da janela de propriedades de um objeto do Active Directory estejam disponíveis, você deve fazer com que as opções avançadas sejam exibidas. Para tal basta usar o comando Exibir -> Recursos avançados, no console Usuários e Computadores do Active Directory. Execute este comando antes de seguir adiante.

Figura 4.53 A janela de propriedades da OU.

Na guia Geral são exibidas informações sobre a OU, tais como Cidade, país, etc. Na guia Gerenciado por você pode selecionar um usuário que será o contato e o responsável pelo gerenciamento da OU. Normalmente é o usuário que recebeu permissões para gerenciar os objetos da OU, através do uso do assistente para Delegação de controle, descrito anteriormente. Clique na guia Segurança. Será exibida uma lista de usuários e grupos, com permissões de acesso a OU e aos objetos da OU. Este é uma lista de permissão de segurança igual a tantas outras utilizadas no Windows Server 2003, como por exemplo uma lista de permissões NTFS de acesso a pastas e arquivos (Capítulo 6), conforme exemplo da Figura 4.54:



**Figura 4.54 Permissões básicas de segurança para a OU.**

Além das permissões básicas, tais como Controle total, Leitura, Gravação, Criar todos os objetos filho e Excluir todos os objetos filho, você pode definir permissões bem mais refinadas. Para isso clique no botão Avançado. Será exibida a janela de Configurações de controle de acesso. Para definir uma grande variedade de permissões para um determinado usuário ou grupo, clique no respectivo usuário ou grupo para selecioná-lo e em seguida clique no botão Exibir/editar... Será aberta a janela Entrada de permissão, na qual você tem um grande número de permissões, conforme indicado na Figura 4.55, na próxima página.

Na lista aplicar em você ainda pode selecionar um determinado tipo de objeto. Ao selecionar um tipo de objeto, serão exibidas apenas as permissões relacionadas ao tipo de objeto selecionado. Após ter definido as permissões desejadas clique em OK. Você estará de volta à janela de Configurações de controle de acesso. Clique em OK para fechá-la. Você estará de volta à janela de propriedades da OU, com a guia Segurança selecionada. Clique em OK para fechá-la.

Pronto, agora você já sabe como delegar tarefas básicas, tarefas personalizadas, como definir permissões básicas de segurança e permissões personalizadas para OUs.

## Contas de computadores – Conceito e Prática

Todos os computadores que executam o Windows NT, o Windows 2000, o Windows XP ou um servidor que executa Windows Server 2003 que se associa a um domínio têm uma conta de computador. Semelhantes a contas de usuário,

as contas de computador fornecem um meio de autenticar e auditar o acesso do computador à rede e aos recursos de domínio. Cada conta de computador deve ser exclusiva, isto é, não podem haver duas contas, com o mesmo nome, no mesmo domínio.

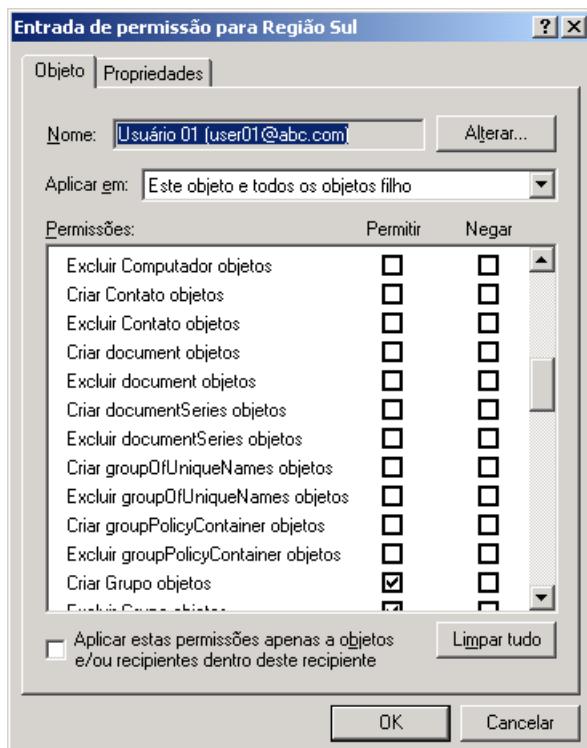


Figura 4.55 Diversas permissões de segurança para a OU.

As contas de usuário e computador são adicionadas, desabilitadas, redefinidas e excluídas usando o console Usuários e computadores do Active Directory. Uma conta de computador também pode ser criada quando você inclui um computador em um domínio. Uma conta de computador é mais um tipo de objeto, armazenado no Active Directory. Quando um administrador configura uma estação de trabalho, para fazer parte de um domínio, será criada no Active Directory, uma conta para o computador que está ingressando no domínio. O nome da conta terá o mesmo nome do computador.

Todo computador que faz parte de um domínio (com exceção de computadores com o Windows 95/98/Me), tem uma conta de computador criada no Active Directory. Além da conta é criada também uma senha, porém esta senha é gerada, automaticamente, pelo Active Directory. Esta senha também é alterada, periodicamente, pelo Active Directory.

Ao instalar o Windows Server 2003 em um servidor ou em uma estação de trabalho, o padrão é que o computador seja configurado para fazer parte de um Workgroup. Para que o computador faça parte de um domínio, baseado no Active Directory, você deve executar os seguintes passos:

- ◆ Criar uma conta de computador, com o mesmo nome do computador.
- ◆ Configurar o computador para fazer parte do domínio.

A seguir apresentarei dois exemplos práticos, onde serão executados estes passos.

---

**IMPORTANTE:** Computadores executando Windows 95 e Windows 98 não têm recursos de segurança avançados e não têm contas de computador atribuídas a eles.

---

**IMPORTANTE:** Quando o nível funcional de domínio foi definido como Windows Server 2003, um novo atributo `lastLogonTimestamp` é usado para rastrear o último horário de logon de uma conta de usuário ou computador. Este atributo é replicado no domínio e pode fornecer informações importantes sobre o histórico de um usuário ou computador.

---

## Criando uma conta de computador no Active Directory.

Você pode criar uma conta de computador, usando o console Usuários e computadores do Active Directory ou usando o comando dsadd computer. A seguir mostro estas duas maneiras de criar uma conta de computador.

### Criando uma conta de computador com o console Usuários e computadores do Active Directory:

Para criar uma conta de computador no Active Directory, siga os passos indicados a seguir:

1. Faça o logon como Administrador, com uma conta com permissão de Administrador ou com uma conta pertencente ao grupo Operadores de contas (Account Operators).
2. Abra o console Usuários e computadores do Active Directory: Iniciar -> Ferramentas Administrativas -> Usuários e computadores do Active Directory.
3. Clique com o botão direito do mouse na opção Computers ou na OU onde será criada a conta de computador.
4. No menu de opções que é exibido, clique em Novo -> Computador.
5. Será aberta a janela Novo objeto – Computador. Preencha os campos, conforme exemplo da Figura 4.56, onde estou criando uma conta para o computador micro-01:

**IMPORTANTE:** Para criar uma conta de computador, você deve ser um membro do grupo Operadores de contas, Administradores do domínio ou do grupo Administração de empresa, no Active Directory ou ter recebido a delegação adequada.

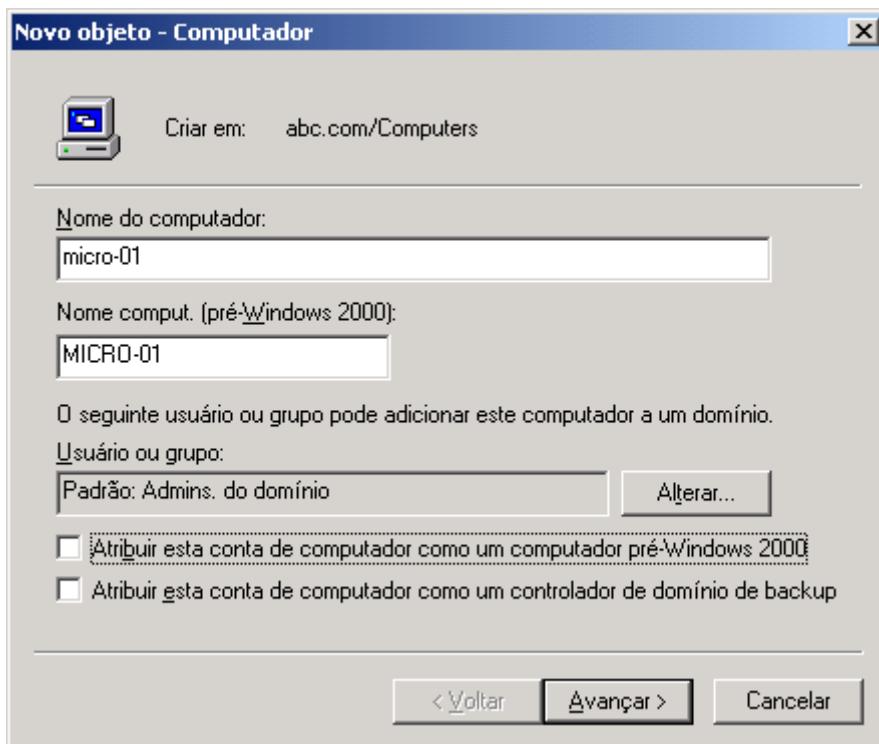


Figura 4.56 Criando uma conta de computador.

6. Nesta etapa você deve informar se a conta que está sendo criada é ou não uma conta de computador gerenciado. Conta de computador gerenciado, tem a ver com o serviço de instalação remota do Windows Server 2003 – RIS (Remote Installation Services). Para mais detalhes sobre este item, consulte o item sobre RIS, na Ajuda do Windows Server 2003. Para o nosso exemplo, não marque esta opção.

- Clique em Avançar para seguir para a próxima etapa do assistente.
- Será exibida a tela final do assistente. Clique em Concluir e pronto, a conta de computador será criada, conforme pode ser comprovado na Figura 4.57:



Figura 4.57 Criação da conta de computador.

### Criando uma conta de computador usando o comando `dsadd computer`:

Você pode criar uma conta de computador, usando o comando `dsadd computer`. A forma mais simples deste comando, está descrita a seguir:

```
dsadd computer NDComputador
```

- ◆ **NDComputador:** É Obrigatório. Especifica o nome distinto do computador a ser adicionado. Se o nome distinto for omitido, ele será retirado da entrada padrão (stdin).

### Configurando uma estação de trabalho, para fazer parte de um domínio

A seguir mostrarei um exemplo prático, onde uma estação de trabalho, com o Windows XP instalado, é configurada para fazer parte de um domínio.

A exemplo do que já acontecia com o Windows 2000 Professional, o Windows XP Professional, como seu sucessor, é o sistema operacional recomendado pela Microsoft, para ser instalado nas estações cliente, em uma rede baseada no Windows 2000 Server, onde é implementada uma estrutura de rede baseada no Active Directory.

Muitas das funcionalidades e facilidades administrativas do Windows Server 2003, somente poderão ser utilizadas com clientes Windows 2000 Professional ou Windows XP Professional. Embora seja possível fazer com que um cliente com o Windows 95/98/Me instalado, faça parte de um domínio, muitas das facilidades administrativas e de segurança, disponibilizadas pelo Active Directory, não poderão ser implementadas.

---

**DICA:** Outro comando que pode ser utilizado para criar uma conta de computador é o comando `NETDOM`, o qual está contido no arquivo `Support.cab`, da pasta `Support\Tools`, do CD de instalação do Windows Server 2003.

---

Com a utilização do Windows 2000 Professional ou do Windows XP Professional nos clientes, o Administrador da rede pode utilizar todos os recursos disponibilizados pelo Windows Server 2003. O Windows XP Professional vai um passo adiante, disponibilizando funcionalidades como o Desktop Remoto e outras novidades que facilitam a administração.

A seguir você aprenderá a configurar um computador com o Windows XP Professional, para que este ingresse em um domínio baseado no Windows Server 2003. Para que você possa fazer a inclusão de um computador em um domínio, você deve ter acesso a uma conta com permissão de Administrador no domínio. Veja bem, não é a conta de Administrador local, no computador que será adicionado ao domínio e sim a conta de Administrador ou pertencente ao grupo Administradores do domínio.

No exemplo que faremos logo em seguir, farei a inclusão de um computador chamado microxp01 em um domínio chamado groza.com. Substitua os nomes utilizados no exemplo, pelos nomes com os quais você está trabalhando.

Exemplo: Incluindo um computador com o Windows XP Professional em um domínio.

1. Faça o logon no computador que será incluído no domínio. Utilize a conta Administrador ou uma conta do tipo Administrador do computador.
2. Clique no menu Iniciar e nas opções que são exibidas, clique com o botão direito do mouse no Meu computador. No menu de opções que é exibido, dê um clique em Propriedades.
3. Será aberta a janela Propriedades do sistema. Dê um clique na guia Nome do computador. Será exibida a janela indicada na Figura 4.58:

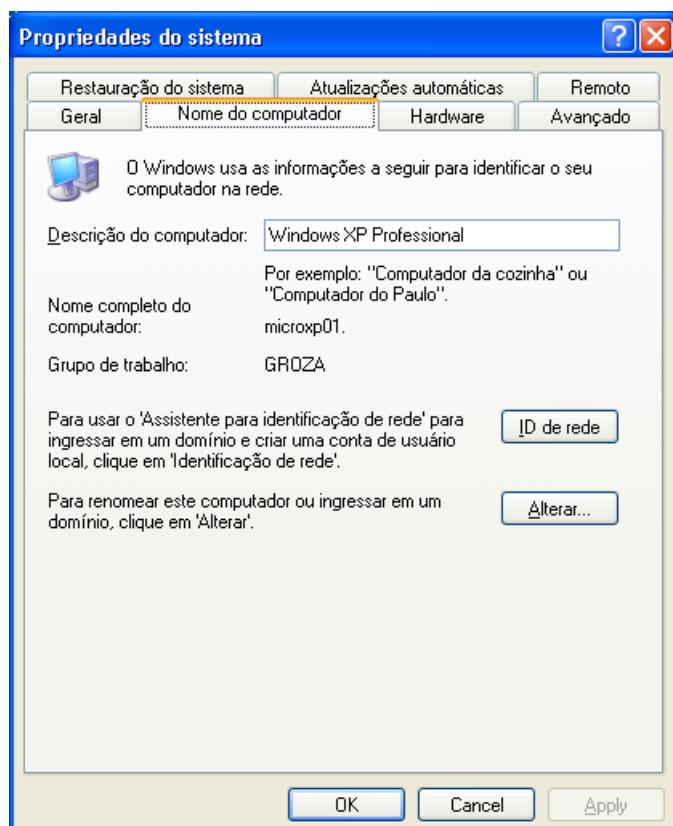


Figura 4.58 A guia Nome do computador.

**IMPORTANTE: Não é possível fazer com que um computador com o Windows XP Home instalado, faça parte de um domínio baseado no Windows 2000 Server ou no Windows Server 2003 e no Active Directory. Este é um aceno claro da Microsoft no sentido de que o Windows XP Home é para uso residencial e o Windows XP Professional, para uso empresarial.**

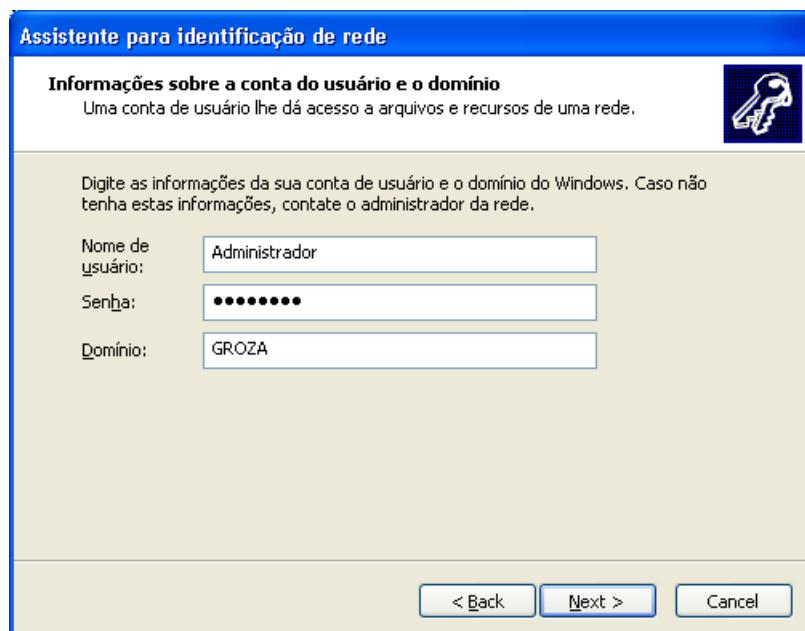
4. Dê um clique no botão ID de rede. Será aberto o Assistente para identificação de rede.
5. A primeira tela do assistente é apenas informativa. Dê um clique no botão Avançar, para ir para a próxima etapa do assistente.

Na segunda etapa do assistente devemos selecionar uma das seguintes opções:

- ◆ **Este computador faz parte de uma rede corporativa e o utilizo para conectar-me a outros computadores no trabalho:** Esta opção é utilizada quando estamos incluindo o computador em um Domínio baseado no Windows Server 2003 e no Active Directory.
  - ◆ **Este computador é usado em casa e não faz parte de uma rede corporativa:** Este opção é utilizada quando temos um computador residencial ou estamos utilizando-o em uma pequena rede do tipo Workgroup.
6. Certifique-se de que a opção “Este computador faz parte de uma rede corporativa e o utilizo para conectar-me a outros computadores no trabalho” esteja marcada e dê um clique no botão Avançar, para ir para a próxima etapa do assistente.
  7. Nesta etapa informamos se a rede é baseada no conceito de Domínio ou não. Certifique-se de que a opção “Minha empresa usa uma rede com um domínio” esteja marcada e dê um clique no botão Avançar, para seguir para a próxima etapa do assistente.

Surge uma tela informando que para conectar o computador a um domínio, você precisa das seguintes informações:

- ◆ Nome do usuário: uma conta com permissões de administrador no domínio.
  - ◆ Senha do usuário
  - ◆ Nome do domínio
8. Dê um clique no botão Avançar, para ir para a próxima etapa do assistente.
  9. Na próxima tela é solicitado o nome de uma conta de administrador no domínio, a respectiva senha e o nome do domínio, conforme indicado na Figura 4.59. Informe os dados solicitados e dê um clique no botão Avançar, para ir para a próxima etapa do assistente.



**Figura 4.59** Informações necessárias para ingressar no domínio.

Todo computador que faz parte de um domínio deve ter uma conta de computador, criada no domínio. Esta conta pode ser criada antecipadamente, pelo Administrador do domínio, ou pode ser criada no momento do ingresso do computador no domínio. Se a conta ainda não tiver sido criada pelo Administrador, será exibida uma janela solicitando o nome da conta a ser criada e o nome do domínio, conforme indicado na Figura 4.60.

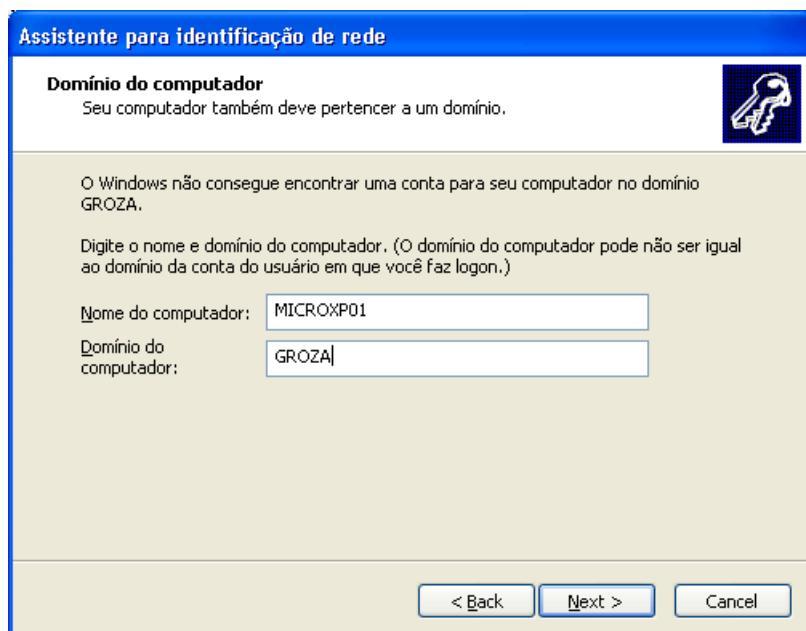


Figura 4.60 Informações necessárias para a criação da conta do computador no domínio.

10. Digite as informações solicitadas e dê um clique no botão Avançar, para seguir para a próxima etapa do assistente.
11. Será exibida a janela Nome de usuário e senha para o domínio. Nesta janela você deve informar o nome de uma conta com permissão de administrador no domínio, a respectiva senha e confirmar o nome do domínio, conforme indicado na Figura 4.61.

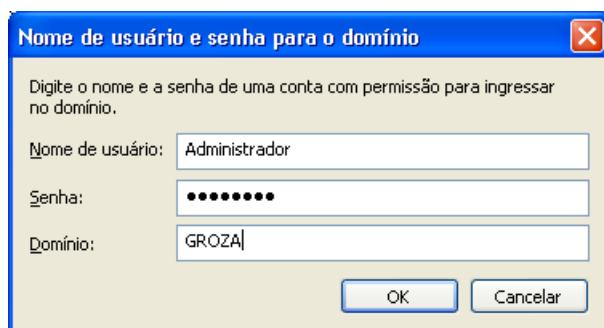


Figura 4.61 Confirmando informações sobre uma conta de Administrador no domínio.

O processo de inclusão no domínio pode demorar alguns minutos.

Ao finalizar o processamento da inclusão no domínio, será exibida uma janela perguntando se você deseja adicionar algum usuário do domínio. O nível de acesso deste usuário será definido na próxima etapa. Por padrão é sugerido que seja adicionado o usuário Administrador, de tal forma que este usuário possa ter acesso administrativo a todos os computadores da rede. A inclusão ou não deste usuário,

**IMPORTANTE:** Se você tiver qualquer conexão com o servidor que é um DC – Domain Controller, como por exemplo uma drive de rede mapeado, a inclusão no domínio irá falhar e uma

depende das políticas de segurança definidas pela empresa. Para o nosso exemplo, vamos incluir o usuário Administrador do domínio, como administrador no computador local, conforme indicado na Figura 4.62:

mensagem será emitida, avisando que antes de fazer a inclusão, você deve fechar todas as conexões existentes.

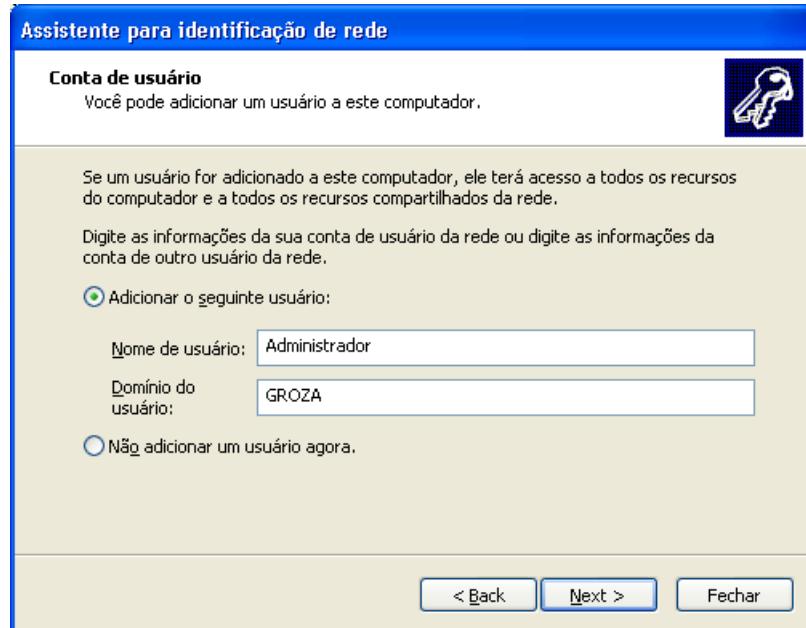


Figura 4.62 Incluindo permissões para o usuário Administrador do domínio.

12. Digite o nome do usuário e o nome do domínio e dê um clique no botão Avançar, para ir para a próxima etapa do assistente.

Nesta etapa você definirá o nível de acesso que o usuário adicionado na etapa anterior, terá ao computador local. Por padrão é sugerida a inclusão do usuário no grupo Usuários avançados. Outras opções são Usuário restrito e Outro, na qual podemos personalizar o nível de acesso.

13. Vamos definir um nível de acesso Administrador, ou seja, o usuário Administrador, do domínio GROZA, representado como GROZA\Administrador, terá acesso de Administrador ao computador que estamos incluindo no domínio. Clique na opção Outro e na lista de opções selecione Administrador, conforme indicado na Figura 4.63 e dê um clique no botão Avançar, para ir para a etapa final do assistente.
14. Na etapa final é apresentado um resumo das opções selecionadas. Você pode utilizar o botão Voltar, para fazer as alterações necessárias.
15. Clique no botão Concluir para encerrar o assistente.
16. Surge uma mensagem informando que você deve Reiniciar o computador para que as alterações tenham efeito. Clique em OK para fechar a mensagem.
17. Você estará de volta a guia Nome do computador. Observe que na parte de baixo da janela aparece um ponto de exclamação, dentro de um triângulo amarelo, com a seguinte mensagem: As alterações terão efeito depois que você reiniciar o computador. Dê um clique em OK. Uma mensagem será exibida perguntando se você deseja reiniciar o computador. Clique em Sim e o computador será reinicializado.

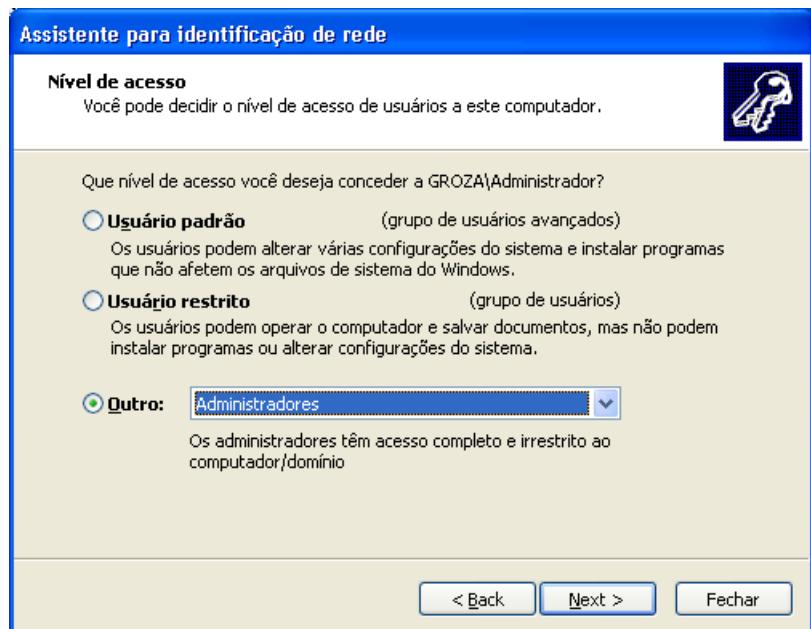


Figura 4.63 Definindo o nível de permissão para a conta do domínio.

Ao reiniciar o computador você já nota a primeira diferença. A tela tradicional de logon, onde era exibida a lista de usuários cadastrados no computador local, não é mais exibida. Ao invés disso é exibida a tela de logon tradicional, onde você deve informar o nome do usuário, a senha e também o nome do domínio, conforme exemplo da Figura 4.64.



Figura 4.64 A tela tradicional de logon.

Ainda é possível fazer o logon usando as contas locais. Para isso basta informar o nome de logon de um usuário local (jsilva, mariax, user1, etc.), a respectiva senha e, no campo Fazer logon em: selecionar a opção que corresponde ao nome do computador. Ao fazer o logon local, o usuário não terá acesso aos recursos do domínio, como por exemplo pasta e impressoras compartilhadas nos servidores do domínio. É interessante observar que, todas as contas locais foram mantidas. Se no futuro, o computador for retirado do domínio, a tela de logon do Windows XP, com a lista de usuários voltará a ser exibida. Em resumo, ao ingressar no domínio passamos a ter duas opções de logon: Fazer o logon no domínio ou fazer o logon localmente.

Com isso concluímos a inclusão do computador no domínio. A partir deste momento, todas as políticas de segurança e demais configurações administrativas, configuradas no domínio, passarão a ser aplicadas ao computador, enquanto ele fizer parte do domínio. Por exemplo, o Administrador pode aplicar políticas de segurança, restringindo o acesso a determinadas opções de configuração, como por exemplo o acesso às configurações de rede. Estas políticas serão aplicadas a todos os computadores e usuários que fizerem parte do domínio. Contudo é importante salientar, conforme já descrito anteriormente, que ainda é possível fazer o logon localmente. Por exemplo, a conta Administrador local continua existindo. Sempre que você precisar executar alguma ação com permissões de Administrador, como por exemplo instalar um driver de Hardware, poderá utilizar a conta Administrador local.

- ◆ **Deixar que o assistente crie a conta de computador:** Você pode deixar que o assistente de ingresso no domínio, crie a conta de computador no Active Directory. Neste caso, a conta será criada, na opção Computers. Fazendo isso, você terá um passo a mais, que será mover a conta da opção Computers para a OU onde a conta deverá ficar em definitivo. Você pode mover contas de computador, da mesma maneira que move uma conta de usuário, usando o console Computadores e usuários do Active Directory. Você também pode mover uma conta de computador, usando o comando DSMOVE.
- ◆ **Criar a conta de computador, antes de configurar o computador para ingressar no domínio:** Com esta abordagem, você pode criar a conta de computador, diretamente na OU onde a conta ficará em definitivo. Depois, é só configurar a estação de trabalho para ingressar no domínio, conforme descrito no exemplo prático anterior. Com esta abordagem, o administrador “poupa” o serviço de mover a conta de computador da opção Computers para a OU onde ficará a conta, em definitivo.

**IMPORTANTE:** Sempre é importante reforçar que não é possível configurar um computador com o Windows XP Home Edition, para que ele faça parte de um domínio.

**IMPORTANTE:** Dependendo das políticas de segurança da empresa, pode ser definido que os usuários não tenho acesso a senha de Administrador local, a qual fica disponível apenas para os administradores do domínio. Na prática, não é informado para o usuário da máquina, qual a senha da conta Administrador local. A definição de um política de segurança é de fundamental importância para a implementação de um ambiente com um nível razoável de segurança. Na política são definidas uma série de questões, tais como responsabilidades, configurações de segurança e dos equipamentos de comunicação e, principalmente, estratégias e ações para a educação dos usuários. De nada adianta ter os mais modernos equipamentos e programas, se não for feito investimento adequado em treinamento e educação contínua. As estatísticas comprovam que a

## Políticas de Senha para o Domínio

Ao criar um domínio, com a instalação do Active Directory no primeiro DC do domínio, por padrão são definidas algumas políticas de segurança relacionadas com as senhas dos usuários. Por exemplo, por padrão é definido que a senha deve ter no mínimo 7 caracteres e que deve ser trocada a cada 42 dias, dentre outras definições. O administrador do sistema pode alterar estas políticas de segurança, para adequá-las as necessidades da sua rede.

As políticas de segurança são definidas para o domínio como um todo, ou seja, uma vez definidas elas passam a valer em todo o domínio. Aliás esta é um das características determinantes de um domínio, ou seja, o compartilhamento de um conjunto único de políticas de segurança.

Neste item você aprenderá a configurar as políticas de segurança relacionadas com a senha do usuário. Estas políticas estão divididas em três grupos, conforme descrito a seguir:

- ◆ **Password Policy (Políticas de Senha):** Estas políticas definem as características que as senhas devem ter. Por exemplo: qual o número mínimo de caracteres, devem ser trocadas de quantos em quantos dias, devem ou não atender a critérios de complexidade e assim por diante.

- ◆ **Account Lockout Policy (Políticas para Bloqueio de Senha):** Estas políticas definem quando uma conta será bloqueada, com base em um número de tentativas de logon sem sucesso. Por exemplo, o administrador pode definir que se o usuário tentar fazer três logons sem sucesso (por exemplo digitando uma senha incorreta para a sua conta) dentro do período de uma hora, que a conta seja bloqueada. Estas políticas são utilizadas para evitar que um usuário mal intencionado tente sucessivamente fazer o logon, usando diferentes senhas, em um tentativa de “adivinar” a senha do usuário.
- ◆ **Kerberos Policy (Políticas do Kerberos):** O Kerberos é um protocolo de autenticação utilizado por muitos sistemas operacionais, como por exemplo o Windows 2000 Server, Windows Server 2003 e muitas versões do UNIX. É um protocolo padrão e muito utilizado. Existem algumas políticas de segurança relacionadas ao protocolo Kerberos que podem ser definidas pelo administrador.

**grande maioria dos problemas com segurança, na maioria dos casos mais de 70% dos problemas, tem origens e causas internas, ou seja, são resultantes de ações dos próprios funcionários da empresa. Nem sempre são ações de má fé, ou seja, com a intenção de provocar algum dano ou acessar informações sigilosas; muitas vezes os problemas ocorrem por falta de orientação e treinamento adequados.**

Estas políticas são configuradas usando o console Diretiva de segurança de domínio, o qual é acessado Iniciar -> Ferramentas Administrativas.

Ao abrir o console Diretiva de segurança de domínio serão exibidas diversas opções de configurações de políticas de segurança do domínio. Clique no sinal de +, ao lado da opção configurações de segurança. Serão exibidas várias opções. A primeira opção, no painel da esquerda, é: Diretivas de conta. Ao clicar no sinal de + ao lado desta opção, são exibidas as opções Diretivas de senha, Diretivas de bloqueio de conta e Diretivas do Kerberos, conforme indicado na Figura 4.65:

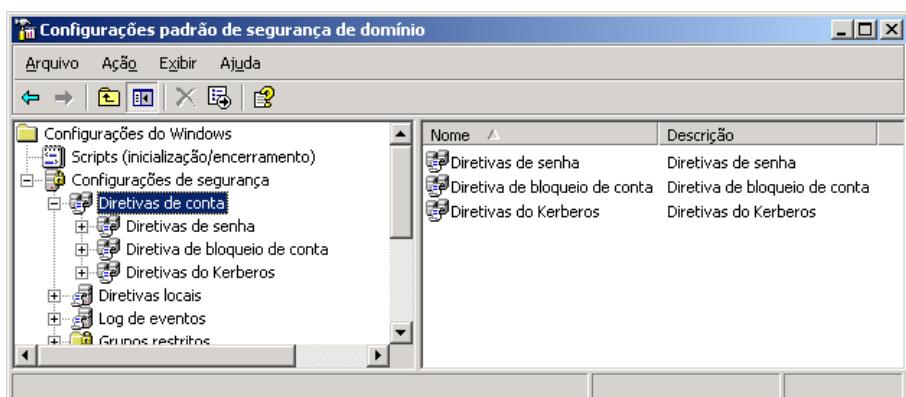


Figura 4.65 As opções de diretivas de contas do domínio.

Ao clicar em uma das opções, por exemplo Diretivas de senha, as diversas diretivas da opção selecionada serão exibida no painel da direita, conforme indicado na Figura 4.66.

Para alterar uma diretiva basta dar um clique duplo na respectiva diretiva. Por exemplo, dê um clique duplo na diretiva Tempo de vida máximo da senha. Por padrão é definido o valor de 42 dias para esta diretiva. Ao dar um clique duplo nesta diretiva será aberta uma janela onde são exibidas as configurações atuais da diretiva e onde você pode fazer as alterações necessárias, conforme exemplo da Figura 4.67 onde são exibidas as configurações da diretiva Tempo de vida máximo de senha.

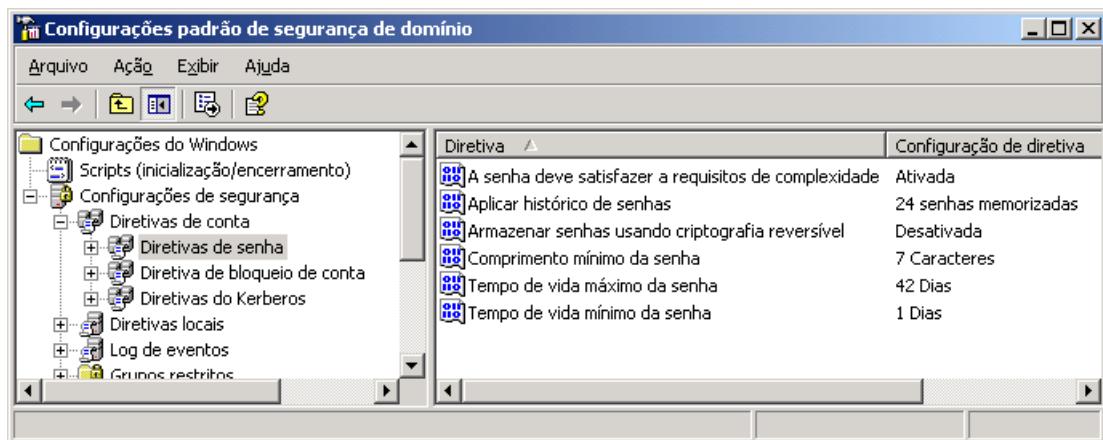


Figura 4.66 Diretivas da opção Diretivas de senha.

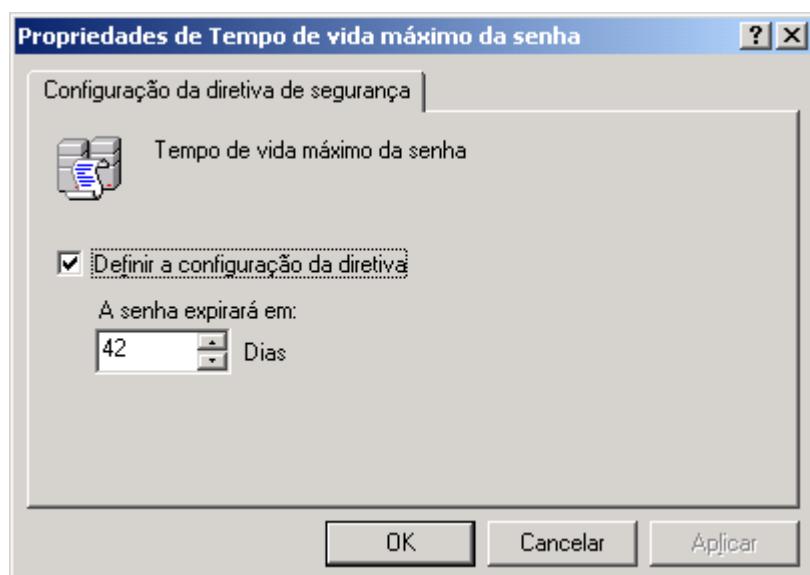


Figura 4.67 Configurando os valores da diretiva Tempo de vida máximo de senha.

Após ter definido as configurações desejadas é só clicar em OK. Observe a opção Definir a configuração da diretiva. Você pode desabilitar uma diretiva, fazendo com que ela deixe de ser aplicada, simplesmente desmarcando esta opção.

A seguir descrevo as diretivas dos grupos Diretivas de senha e Diretivas de bloqueio de senha. Estas são as diretivas cobradas no Exame 70-290.

## Descrição das diretivas do grupo Diretivas de senha: No Windows Server 2003, por padrão, são definidas as seguintes políticas de segurança em relação as senhas de usuários:

- ◆ Quando o usuário vai trocar a senha, não pode ser utilizada uma senha igual as 24 últimas (haja criatividade para inventar senhas).
- ◆ A senha expira (isto é, deve ser alterada) a cada 42 dias.
- ◆ O tempo mínimo de vida de senha é um dia. Ou seja, você trocou a senha hoje, não poderá trocá-lo novamente daqui a uma ou duas horas, somente após um dia.
- ◆ Tamanho mínimo de sete caracteres.

- ◆ A opção “A senha deve atender critérios de complexidade (Password must meet complexity requirements) é habilitada por padrão”.

Com a opção A senha deve atender critérios de complexidade (Password must meet complexity requirements) habilitada por padrão, uma série de requisitos devem ser atendidos para que a senha seja aceita. A seguir descrevo estes critérios:

- ◆ A senha não pode conter parte ou todo o nome da conta. Por exemplo, se o nome da conta for jsilva, a senha não poderá conter a sílaba “sil” ou a palavra “silva”.
- ◆ Ter pelo menos seis caracteres. O número mínimo de caracteres pode ser aumentado, configurando-se as políticas de segurança para senhas, conforme mostrarei mais adiante.
- ◆ Deve conter caracteres de pelo menos três dos quatro grupos a seguir: letras maiúsculas de A até Z, letras minúsculas de a até z, dígitos de 0 a 9 ou caracteres especiais (:, !, @, #, \$, %, etc.).

Estes requisitos de complexidade são verificados quando a senha é criada pela primeira vez, durante o cadastramento do usuário e toda vez que a senha for alterada. Com estes requisitos definidos, as senhas a seguir seriam válidas:

**AbCsenha1**

**AbcSenha#**

**Abc123**

**Abc ; ; senha**

Já as senhas a seguir não seriam válidas:

- ◆ **abcsenha123:** (contém somente caracteres de dois dos quatro grupos: letras minúsculas e números).
- ◆ **abc;senha:** (contém somente caracteres de dois dos quatro grupos: letras minúsculas e caracteres especiais).

Todas estas configurações de senha são definidas pelas diretivas de segurança do grupo Diretivas de senha, as quais estão descritas a seguir:

- ◆ **Aplicar histórico de senhas:** Nesta diretiva o administrador informa o número de senhas que serão gravadas no histórico de senhas do usuário. Por exemplo, se esta diretiva estiver definida com um valor 5, significa que ao trocar a senha, o usuário não poderá utilizar uma das últimas cinco senhas que ele utilizou. Esta diretiva é utilizada para evitar que o usuário possa repetir sempre as mesmas senhas. Por padrão ela tem o seu valor definido como 24, ou seja, ao trocar a senha, o usuário não poderá utilizar uma senha igual a uma das últimas 24 que ele utilizou.
- ◆ **Tempo de vida máximo da senha:** Esta diretiva define um tempo máximo de duração da senha. Uma vez transcorrido este período o usuário é obrigado a alterar a senha. Esta diretiva aceita valores na faixa entre 1 e 999. Se você definir um valor 0 para este diretiva, equivale a definir que as senhas nunca expiram (embora não seja nada recomendado definir que as senhas nunca expiram). Se o valor desta diretiva for definido na faixa entre 1 e 999, o valor da diretiva Minimum password age (Tempo de vida mínimo da senha), deve ser menor do que o valor definido na diretiva Maximum password age (Tempo de vida máximo da senha). Em outras palavras, o tempo mínimo de vida deve ser menor do que o tempo máximo, o que faz sentido evidentemente. O valor padrão para esta diretiva é de 42 dias. É recomendado um valor entre 30 e 45 dias para esta diretiva.

**IMPORTANTE:** Para as senhas, o Windows Server 2003 distingue letras maiúsculas de minúsculas. Por exemplo a senha “Abc123” é diferente da senha “abc123”.

**NOTA:** O valor de 24 para este diretiva é o padrão em DCs do domínio. Em member servers o valor padrão é zero, ou seja, sem histórico de senha. Para que esta diretiva tenha efeito, ele deve ser utilizada em conjunto com a diretiva Minimum password age (Tempo de vida mínimo da senha). Se não houver um tempo mínimo de vida para a senha, o usuário poderia trocar a senha 24

◆ **Tempo de vida mínimo da senha:** Esta diretiva define o tempo mínimo, em dias, pelo qual a senha deve ser utilizada, antes que ele possa ser novamente alterada. Por exemplo, se esta diretiva estiver definida com um valor igual a 5 e o usuário alterar a sua senha hoje, significa que ele somente poderá alterar novamente esta senha daqui a cinco dias. Este diretiva, conforme descrito anteriormente, deve ser utilizada em conjunto com a diretiva Enfore password history (Aplicar histórico de senhas), para efetivamente forçar que seja mantido um histórico de senhas e que o usuário não possa utilizar uma senha igual as últimas x senhas, sendo o valor x definido na diretiva Enfore password history (Aplicar histórico de senhas). O valor desta diretiva pode estar na faixa de 1 a 998. Um valor 0 significa que não existe tempo de vida mínimo da senha, ou seja, o usuário pode alterar a senha a qualquer momento e repetidamente. Por padrão é definido o valor 1 nos DCs e 0 nos member servers. Uma regra normalmente utilizada é definir esta diretiva com um valor correspondente a um terço do valor definido na diretiva Maximum password age (Tempo de vida máximo da senha).

vezes no mesmo dia. Com isso ele poderia simplesmente continuar utilizando sempre a mesma senha.

---

◆ **Comprimento mínimo da senha:** Esta diretiva define o número mínimo de caracteres que deve ter a senha. Você pode definir um valor entre 1 e 14. Para definir que não é exigido um comprimento mínimo, defina esta diretiva com o valor 0. Por padrão é definido o valor 7 nos DCs e 0 nos member servers.

◆ **A senha deve satisfazer a requisitos de complexidade:** Esta diretiva é habilitada por padrão. Com isso, uma série de requisitos devem ser atendidos para que a senha seja aceita. A seguir descrevo estes critérios:

- ◆ A senha não pode conter parte ou todo o nome da conta. Por exemplo, se o nome da conta for jsilva, a senha não poderá conter a sílaba “sil” ou a palavra “silva”.
- ◆ Ter pelo menos seis caracteres. O número mínimo de caracteres pode ser aumentado, configurando-se as políticas de segurança para senhas, conforme mostrarei mais adiante.
- ◆ Deve conter caracteres de pelo menos três dos quatro grupos a seguir: letras maiúsculas de A até Z, letras minúsculas de a até z, dígitos de 0 a 9 ou caracteres especiais (:, !, @, #, \$, %, etc.).

Estes requisitos de complexidade são verificados quando a senha é criada pela primeira vez, durante o cadastramento do usuário e toda vez que a senha for alterada. Com estes requisitos definidos, as senhas a seguir seriam válidas:

**AbCsenha1**

**AbcSenha#**

**Abc123**

**Abc ; ; senha**

Já as senhas a seguir não seriam válidas:

- ◆ **abcsenha123:** (contém somente caracteres de dois dos quatro grupos: letras minúsculas e números).
- ◆ **abc;senha:** (contém somente caracteres de dois dos quatro grupos: letras minúsculas e caracteres especiais).
- ◆ **Armazenar senhas usando criptografia reversa:** Esta diretiva somente deve ser habilitada quando houver aplicações que necessitam deste padrão de senhas. Mais especificamente são aplicações que precisam conhecer a senha do usuário por questões de autenticação. Esta diretiva, em termos de segurança, é muito semelhante a armazenar a

**IMPORTANTE:** Para as senhas, o Windows Server 2003 distingue letras maiúsculas de minúsculas. Por exemplo a senha “Abc123” é diferente da senha “abc123”.

---

senha como texto sem criptografia, ou seja, não é recomendada em termos de segurança e somente deve ser habilitada quando realmente houver necessidade por questões de compatibilidade com algum sistema de aplicação crítica para a empresa. Esta diretiva é requerida também em algumas situações específicas, por exemplo, quando é utilizado o protocolo CHAP para autenticação através do RRAS ou do IAS. Também é requerida quando for usada a autenticação do tipo Digest Authentication com o IIS. Por padrão esta diretiva está desabilitada.

## Descrição das diretivas do grupo Diretivas de bloqueio de conta

A seguir descrevo as diretivas deste grupo, as quais são utilizadas para definir quando uma conta deve ser bloqueada, após sucessivas tentativas de logon sem sucesso.

- ◆ **Límite de bloqueio de conta:** Esta diretiva define o número de tentativas de logon sem sucesso que serão necessárias para que a conta seja bloqueada. Este número de tentativas deve ocorrer dentro do período definido pela diretiva Zerar contador de bloqueios de conta após. Vamos supor que a diretiva Límite de bloqueio de conta esteja definida com o valor três e que a diretiva Zerar contador de bloqueios de conta após esteja definida com o valor 60 minutos. Isso significa que se o usuário fizer três tentativas de logon sem sucesso, dentro de uma hora, a sua conta será bloqueada. Esta diretiva pode ter um valor entre 1 e 999. Um valor igual a 0 significa sem bloqueio, ou seja, o usuário poderá fazer quantas tentativas quiser, que a conta não será bloqueada.
- ◆ **Zerar contador de bloqueios de conta após:** Esta diretiva define o período dentro do qual as tentativas de logon sem sucesso devem ser feitas para que a conta seja bloqueada. Por exemplo, vamos imaginar que esta diretiva estiver definida como 60 minutos e o usuário tenha feito duas tentativas de logon sem sucesso. Se ele fizer mais uma tentativa nos próximos sessenta minutos, a conta será bloqueada. Se transcorrer 60 minutos sem nenhuma tentativa sem sucesso, o contador será zerado. Esta diretiva pode conter valores na faixa de 1 a 99999 minutos. Esta diretiva somente pode ser habilitada quando a diretiva Límite de bloqueio de conta, estiver habilitada.
- ◆ **Duração do bloqueio de conta:** Esta diretiva define o tempo, em minutos, pelo qual a conta permanecerá bloqueada, uma vez que tenha sido bloqueada por sucessivas tentativas de logon sem sucesso. O valor pode variar de 1 a 99999. Um valor 0 significa que a conta não será desbloqueada automaticamente. Com esta configuração o Administrador terá que desbloquear a conta do usuário. Esta diretiva somente terá efeito quando a diretiva Límite de bloqueio de conta tiver sido definida.

**IMPORTANTE:** Tentativas de desbloqueio de estações de trabalho e member servers, sem sucesso, também contam para o número de tentativas sem sucesso.

A seguir apresento uma série de recomendações em relação ao uso de senhas e à definição de políticas de senha para um domínio do Windows Server 2003.

1. Eduque seus usuários e faça campanhas permanentes com orientações sobre segurança. Quando eu faço uma palestra sobre segurança tem uma frase que eu adoro repetir: “Em segurança você pode trabalhar 20 anos sem ter um problema, porém o primeiro que acontecer é problema para mais vinte anos.” O que eu quero dizer com isso? Quem em termos de segurança o melhor mesmo é prevenir. E a melhor maneira de prevenir problemas é através da educação dos usuários. Oriente os usuários da sua rede a proteger suas senhas, a escolher senhas que não sejam óbvias e assim por diante. Esta campanha de educação tem que ser permanente, através do e-mail da empresa, crie cartilhas com orientações sobre segurança, faça palestras de dois em dois meses e não baixe a guarda nunca. Claro que é difícil pedir que o usuário não utilize senhas óbvias, se a rede da empresa tem vários sistemas em funcionamento, cada sistema em um ambiente diferente e exigindo uma senha diferente. A seguir algumas ações e orientações para incentivar os usuários a utilizarem senhas “fortes”, isso é, não óbvias, difíceis de serem “adivinhadas” ou quebradas.

- ◆ Mantenha habilitada a diretiva Password must meet complexity requirements (Senhas devem satisfazer a requisitos de complexidade), para exigir que as senhas atendam certos requisitos de complexidade, conforme descrito anteriormente.
  - ◆ Se a política de segurança da empresa define que certas senhas institucionais, como a senha do usuário Administrator (Administrador) dos member servers deva estar registrada em papel, certifique-se de que os envelopes contendo estas senhas sejam armazenados em um local seguro, tal como um cofre a prova de foto.
  - ◆ Jamais permita o compartilhamento de senhas. Cada usuário deve ter a sua própria conta. Se mais de uma pessoa trabalha como administrador, cada uma deve ter a sua própria conta e ser cadastrada no grupo Domain Admins (Admins. do Domínio) para ter permissão de Administrador.
  - ◆ Providencie a alteração da senha da sua conta imediatamente se você desconfia que alguém tentou descobrir ou quebrar a senha. Para alterar a senha basta pressionar Ctrl+Alt+Del. Será exibida a janela Windows Security (Segurança do Windows). Clique no botão Change Password... (Alterar senha...). A janela Change Password (Alterar Senha) será exibida. Digite a senha atual e a nova senha duas vezes para confirmar. Clique em OK. Pronto, a senha foi alterada.
  - ◆ Seja cuidadoso com as janelas de aviso que pedem para salvar a senha no seu computador. Estas janelas são exibidas quando o usuário faz uma conexão remota ou quando o usuário tem que fornecer um login e senha para acessar áreas restritas da Intranet da empresa, de uma aplicação Web ou áreas restritas de um site da Internet. Existem programas que tentam descobrir a senha do usuário, lendo os arquivos de informação onde as senhas são gravadas no computador. Por padrão oriente os usuários a não salvar as senhas localmente.
2. Utilize o utilitário Syskey em todos os computadores da rede. Este utilitário usa técnicas adicionais de criptografia forte para garantir a segurança das senhas armazenadas na base de dados dos computadores. Por exemplo, computadores com o Windows 2000 Professional ou XP Professional ou members servers do domínio, tem uma base local de usuários, a qual é armazenada em uma base conhecida como Security Accounts Manager (SAM) database. Para executar o utilitário Syskey basta ir para o prompt de comando e executar o comando Syskey. Será exibida uma janela pedindo se você deseja habilitar a criptografia forte, conforme indicado na Figura 4.68:

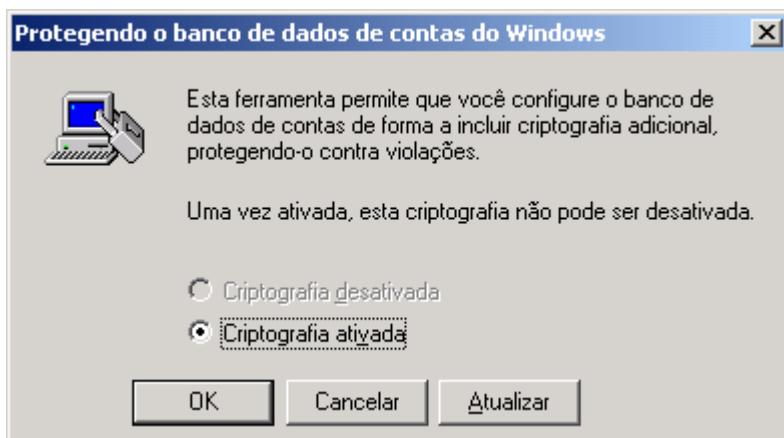


Figura 4.68 Utilizando o utilitário Syskey.

- ◆ Defina uma política de segurança para a empresa como um todo, dentro da qual está a definição das políticas de senha. A política de segurança deve ser constantemente revisada e atualizada e o mais importante, divulgada para todos na empresa.

**IMPORTANTE:** A seguir apresento algumas recomendações (conforme ajuda do Windows Server 2003) sobre os valores a serem definidos

- ◆ Habilite sempre as políticas para bloqueio de conta, de tal maneira que após um número determinado de tentativas de logon sem sucesso a conta do usuário seja bloqueada. Em ambientes em que a segurança é um fator crítico, defina também que somente o Administrador pode desbloquear contas. Normalmente utiliza-se o valor de três tentativas de logon sem sucesso em uma hora como limite para o bloqueio das contas.
- ◆ Habilite a diretiva para tempo máximo e tempo mínimo de senha, conforme descrito anteriormente. Em conjunto com estas políticas defina a política que define o historiograma de senhas a ser armazenado no Active Directory. Valores normalmente utilizados para estas diretivas são um tempo máximo de 30 dias, um tempo mínimo de 10 dias e um histórico de cinco senhas. Com estas diretivas significa que o usuário deve alterar a sua senha a cada trinta dias, uma vez alterada a senha ele poderá alterá-la novamente somente daqui a 10 dias e ao alterar a senha o usuário não poderá utilizar uma senha que seja igual a uma das cinco últimas que ele utilizou.
- ◆ Defina um número mínimo de caracteres para a senha (diretiva Minimum password length (Comprimento mínimo da senha)). Um valor normalmente utilizado é de 8 caracteres para ambientes empresariais e 10 caracteres para redes de segurança crítica. O máximo que você pode definir como tamanho mínimo é de 14 caracteres. A senha pode conter mais do que 14 caracteres, o que não é possível é definir que as senhas devem ter um tamanho mínimo superior a 14 caracteres.

## Administração do “Schema” do Active Directory.

A definição de todos os objetos do Active Directory e demais informações está contida no que é conhecido como Schema do Active Directory. O Active Directory utiliza um modelo de banco de dados hierárquico, diferente do Modelo Relacional de Dados com o qual estamos mais habituados. Mas, me permitam esta analogia, o Schema é como se fosse (na verdade é) a definição da estrutura do banco de dados do Active Directory. Por exemplo, a definição do objeto usuário, quais atributos tem este objeto, o tipo de cada atributo e demais informações sobre o objeto usuário, estão todas contidas no Schema. A definição de cada objeto, de cada atributo, está contida no Schema.

O Schema contém a definição para todos os objetos do Active Directory. Quando você cria um novo objeto, as informações fornecidas são validadas com base nas definições contidas no Schema, antes que o objeto seja salvo na base de dados do Active Directory. Por exemplo, se você preencheu um atributo do tipo número, com valores de texto, o Active Directory não irá gravar o objeto no Active Directory e uma mensagem de erro será exibida.

O Schema é feito de objetos, classes e atributos. O Schema definido por padrão com o Active Directory, contém um número de classes e atributos, os quais atendem as necessidades da maioria das empresas. Porém o Schema pode ser modificado, o Administrador pode modificar as classes existentes ou adicionar novas classes ou atributos. Qualquer alteração no Schema deve ser cuidadosamente planejada, pois alterações feitas no Schema afetam toda a árvore de domínios. Todos os domínios de uma árvore tem que utilizar o mesmo Schema, ou seja, não podem ser utilizados diferentes esquemas para os diferentes domínios de uma árvore de domínios.

Como os objetos do Active Directory são definidos no Schema:

No Schema, uma classe de objetos representa uma categoria de objetos do Active Directory, como por exemplo contas de usuários, contas de computadores, impressoras ou pastas compartilhadas publicadas no Active Directory e assim por diante. Na definição de cada classe de objetos do Active Directory, está contida uma lista de atributos que podem ser utilizadas para descrever um objeto da referida classe. Por exemplo, um objeto usuário contém atributos tais como: nome, senha, validade da conta, descrição, etc. Quando um novo usuário é criado no Active Directory, o usuário torna-se uma nova instância da classe User do Schema e as informações que você digita sobre o usuário, tornam-se instâncias dos atributos definidos na classe user.

Como o Schema é armazenado no Active Directory:

Cada floresta pode conter um único Schema, ou seja, o Schema tem que ser único ao longo de todos os domínios de uma floresta. O Schema é armazenado nas partições de schema do Active Directory. A partição de schema do Active Directory, bem como a partição de definição do Active Directory, são replicadas para todos os DCs da floresta. Porém um único DC controla a estrutura do Schema, DC este conhecido como Schema Master. Ou seja, somente no DC configurado como Schema Master é que o Administrador poderá fazer alterações no Schema.

Cache do Schema.:

Cada DC mantém uma cópia do Schema na memória do servidor (bem como uma cópia em disco), para melhorar a performance das operações relacionadas ao Schema, tais como validação de novos objetos. A versão armazenada no Cache do servidor é automaticamente atualizada (em intervalos de tempos definidos) cada vez que o Schema é atualizado (o que não ocorre com frequência, na verdade é muito raro fazer alterações no Schema).

Quem tem autorização para modificar o Schema:

A definição do Schema é protegida por permissões de acesso. Por padrão, somente membros do grupo Schema Admins (Administradores de esquemas) têm permissão de leitura no Schema. Para que um administrador possa alterar o Schema (operação conhecida como estender o Schema), a sua conta deve fazer parte do grupo Schema Admins (Administradores de esquemas). Por padrão somente a conta Administrator (Administrador) do domínio root (em uma árvore de domínios) faz parte do grupo Schema Admins (Administradores de esquemas). Evidentemente que o acesso a este grupo deve ser rigorosamente limitado, pois ao adicionar um usuário a este grupo, você dá ao usuário permissões para alterar o Schema. Alterações indevidas (ou má intencionadas) no Schema podem simplesmente paralisar toda a rede, em situações mais graves, fazendo que todos os servidores tenham que ser reinstalados, causando possíveis perdas de dados, enfim: um verdadeiro desastre.

Para alterar o Schema você deve ter acesso ao servidor que atua como Schema Master. O Schema Master normalmente é o primeiro DC instalado no domínio root, embora esta função possa ser delegada a qualquer outro DC do domínio. A seguir descrevo um exemplo de utilização do Snap-in para administração do Schema.

Exemplo: Como utilizar o console de administração do Schema: Você deve estar no servidor que está executando a função de Schema Master. Em todo o diretório existe um único servidor no qual existe uma cópia do Schema habilitada para alterações. Este servidor é conhecido como Schema Master e normalmente é o primeiro DC instalado no domínio root de uma árvore de domínios.

Para abrir o console de administração do Schema, siga os passos indicados a seguir:

1. Faça o logon com uma conta com permissão de Administrador, no DC que está executando a função de Schema Master.
2. Selecione o comando Iniciar -> Executar.
3. Na janela que surge, no campo Abrir, digite mmc e dê um clique em OK.
4. Será aberto o MMC sem nenhum Snap-In Carregado.
5. Com o MMC carregado anteriormente, selecione o comando Arquivo -> Adicionar/remover snap-in .. Será exibida a janela Adicionar/remover snap-in. Observe que não existe nenhum snap-in adicionado e a lista está vazia.
6. Na janela Adicionar/remover snap-in, dê um clique no botão Adicionar.
7. Será exibida a janela Adicionar snap-in autônomo. Nesta janela é exibida uma listagem com todos os snap-ins disponíveis, isto é, instalados no computador.

**IMPORTANTE:** Antes de poder ter acesso ao console de gerenciamento do Schema, você tem que executar o comando: `regsvr32 schmmgmt.dll`, para instalar o Snap-in de gerenciamento do Schema. Abra um prompt de comando e execute o comando: `regsvr32 schmmgmt.dll`. É exibida uma mensagem informando que o registro foi efetuado com sucesso. Clique em OK para fechá-la.

8. Localize na listagem o seguinte snap-in: Esquema do Active Directory, conforme indicado na Figura 4.69 e dê um clique sobre ele para selecioná-lo.

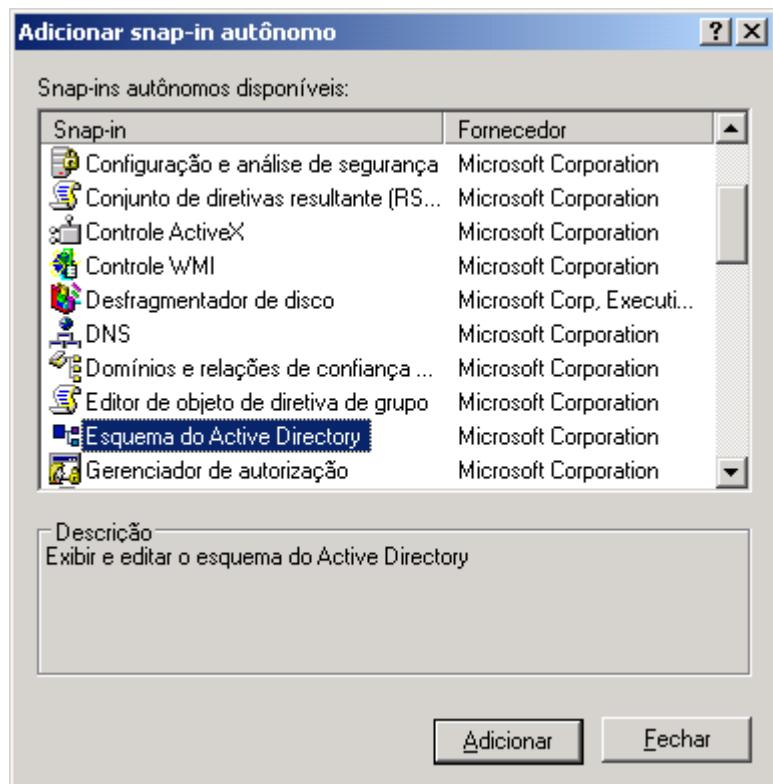


Figura 4.69 Adicionando o snap-in Esquema do Active Directory.

9. Dê um clique no botão Adicionar.  
10. Clique no botão Fechar.  
11. Você estará de volta a janela Adicionar snap-in autônomo e o snap-in Esquema do Active Directory já é exibido na lista. Caso você queira será possível adicionar outros snap-ins. Como não será adicionado mais nenhum snap-in, dê um clique no botão OK.  
12. Você estará de volta ao MMC, agora com o snap-in Esquema do Active Directory já carregado, conforme indicado pela Figura 4.70.

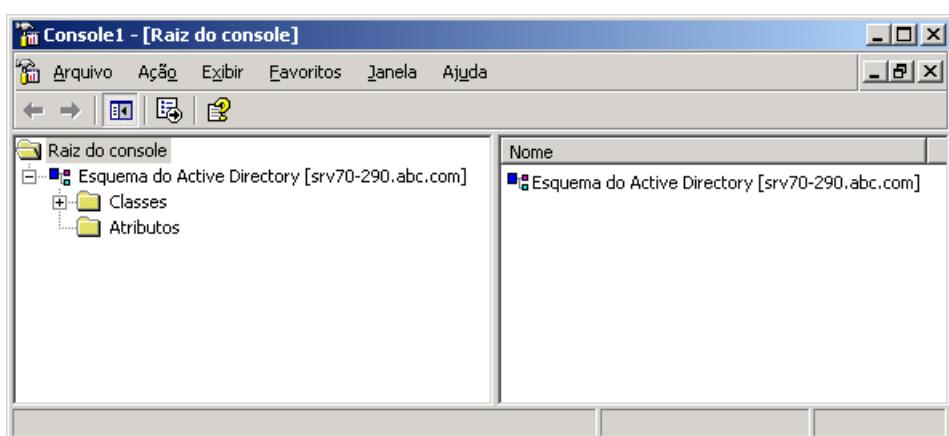
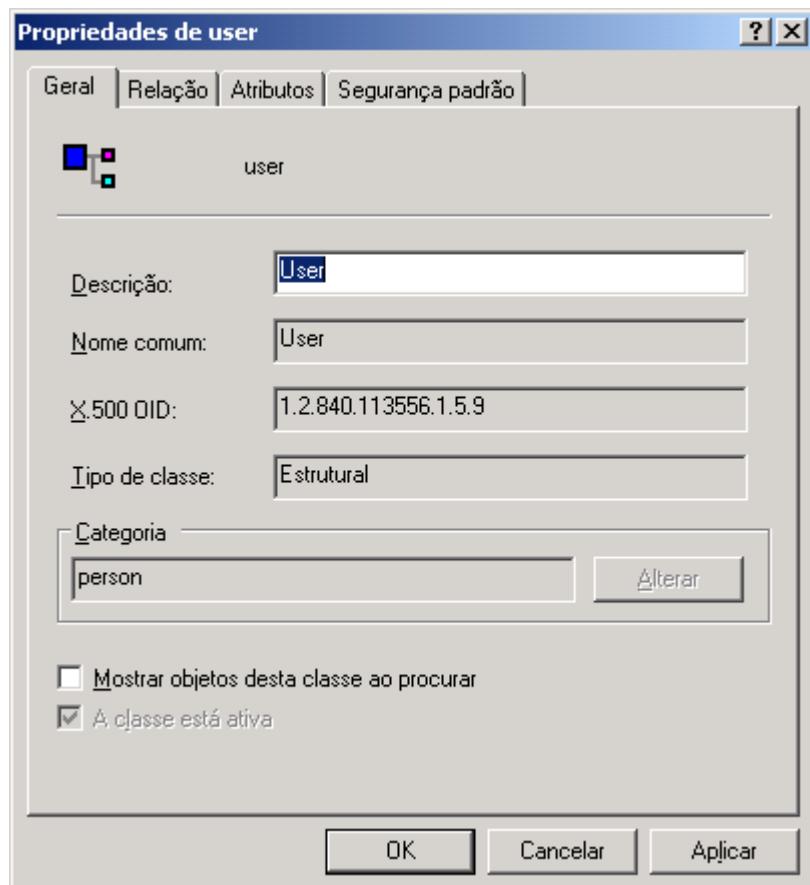


Figura 4.70 Console com o snap-in Esquema do Active Directory, já carregado.

13. Clique no sinal de mais ao lado da opção Esquema do Active Directory [nome do servidor]. Serão exibidas as opções Classes e Atributos.
14. Clique na opção Classes.
15. No painel da direita serão exibidas as dezenas de classes que formam a estrutura do banco de dados do Active Directory.
16. Localize a classe User (as classes estão em ordem alfabética) e dê um clique duplo nesta classe. Serão exibidas as propriedades da classe, conforme indicado na Figura 4.71:



**Figura 4.71 Propriedades da classe User.**

17. Clique na guia Atributos da janela de propriedades da classe User.
18. Serão exibidos os vários atributos da classe User. Clique em alguns dos tributos e observe que para alguns tributos o botão Remover é habilitado. Os tributos para os quais o botão Remover é habilitado são atributos que podem ser retirados da classe, não são obrigatórios. O administrador do Esquema pode utilizar o botão Adicionar para adicionar novos atributos a uma determinada classe. Esta operação é conhecida como estender o Esquema. Por exemplo, você poderia adicionar um atributo CPF ou Número da matrícula à classe User.
19. Clique em OK para fechar as propriedades da classe User.
20. Feche o MMC. Será emitida uma mensagem perguntando se você deseja salvar as alterações no console, clique em Não.

Nunca é demais lembrar que toda e qualquer alteração no schema deve ser cuidadosamente planejada.

# Conclusão

Neste capítulo você aprenderá sobre uma série de assuntos relacionados com a administração de dois elementos básicos do Active Directory: contas de usuários e grupos de usuários. Foram abordados os seguintes assuntos:

- ◆ O conceito de contas de usuários, contas de computadores e grupos de usuários.
- ◆ Criação e administração de contas de usuários e de computadores.
- ◆ Criação e administração de grupos de usuários.
- ◆ Criação e administração de Unidades Organizacionais.
- ◆ O modelo de permissões do Windows Server 2003.
- ◆ Ferramenta para administração do Esquema do Active Directory.
- ◆ Políticas de contas e senhas para o domínio.

A conta de usuário é a identidade do usuário A partir da conta que o usuário utilizou para fazer o logon na rede é que o Windows Server 2003 consegue identificar o usuário. Cada usuário que precisa de acesso a rede deve ter sua própria conta e senha que seja somente de seu próprio conhecimento.

Entendidos os conceitos de contas de usuários e grupos de usuários, parti para a explicação sobre Unidades Organizacionais (OUs). Mostrei o que é uma Unidade organizacional, como ela difere de um domínio, quando usar Unidades Organizacionais e quando utilizar domínios. Também mostrei a parte prática de criação e administração de Unidades Organizacionais, bem como operações de mover contas de usuários e grupos de uma unidade organizacional para outra.

Também falei sobre as políticas de segurança relacionadas com a definição de senhas e com o bloqueio de contas do domínio. Você aprendeu sobre as diversas políticas disponíveis e a função de cada uma. O uso destas políticas é de fundamental importância para que se tenha um ambiente mais seguro, onde sejam utilizadas senhas chamadas senhas “fortes”, ou seja, dificeis (eu nunca uso o termo “impossíveis”) de serem quebradas.

Para encerrar o capítulo apresentei mais uma ferramenta de administração do Active Directory: a ferramenta para gerenciamento do Esquema (lembrando do Capítulo 2, o Esquema é a definição da estrutura do banco de dados do Active Directory). Falarei da importância e da função do Esquema e irei ressaltar que toda e qualquer alteração no Esquema deve ser cuidadosamente (eu diria cuidadosamente ao quadrado) planejada e testada em laboratório, antes de ser implementada em um ambiente de produção. Erros nas alterações do Esquema podem causar verdadeiros desastres.

Com certeza os conceitos apresentados neste capítulo representam um bom percentual do trabalho diário do administrador. Administrar contas de usuários e grupos, juntamente com a atribuição de permissões de acesso a pastas (Capítulo 6) e Impressoras da rede (Capítulo 7), representa grande parte do dia de trabalho do administrador.

No próximo capítulo você aprenderá a gerenciar discos e volumes no Windows Server 2003.

# Introdução

Neste capítulo apresentarei os conceitos de armazenamento básico e armazenamento dinâmico, bem como a diferença entre ambos. Depois você aprenderá as tarefas mais comuns no que diz respeito a gerenciamento de discos e volumes, tais como adicionar um novo disco, criar partições ou volumes e formatá-las para que estas possam ser utilizadas pelo Windows Server 2003.

Vou iniciar o capítulo com uma apresentação teórica dos conceitos de armazenamento básico e armazenamento dinâmico. Mostrarei as vantagens do armazenamento dinâmico e como existem diferentes terminologias para os volumes (criados nos discos de armazenamento dinâmico) e para as partições (criadas nos discos de armazenamento básico). Mostrarei que os discos de armazenamento dinâmico oferecem uma série de vantagens em relação ao sistema mais antigo, baseado em partições, sistema este usado nos discos de armazenamento básico.

Em seguida passarei a falar dos diferentes tipos de partições que podem ser criadas nos discos de armazenamento básico e dos diferentes tipos de volumes que podem ser criados nos discos de armazenamento dinâmico. Você verá que é possível implementar tolerância á falhas usando somente as configurações de software fornecidas pelo Windows Server 2003.

Na seqüência partirei para a parte prática. O gerenciamento de discos e volumes no Windows Server 2003 pode ser feito pela opção Gerenciamento de Disco do console Gerenciamento do computador. Mas para facilitar o acompanhamento dos exemplos práticos deste capítulo, o primeiro passo será criar um console personalizado apenas com o Snap-in de administração de discos.

Criado o console personalizado, mostrarei como criar os diversos tipos de volumes possíveis em um disco dinâmico. Também mostrarei como alterar, formatar e excluir estes volumes. Você também aprenderá a converter um disco de armazenamento básico para armazenamento dinâmico.

Em seguida Falarei sobre as ferramentas para manutenção preventiva de volumes e partições. Você aprenderá sobre o conceito de fragmentação de discos e aprenderá a utilizar o utilitário de desfragmentação, o qual está bem mais eficiente no Windows Server 2003 em relação ao utilitário de desfragmentação do Windows 2000 Server. Você também aprenderá sobre os utilitários de linha de comando disponíveis para o gerenciamento de discos e volumes.

Na seqüência passarei a falar sobre uma das características que é exclusiva do sistema de arquivos NTFS: Criptografia de Arquivos. Quando uma pasta ou um arquivo é criptografado, o usuário continua trabalhando com o arquivo normalmente, da mesma maneira que em outros arquivos e pastas. A criptografia é “transparente” para o usuário que criptografou o arquivo. Isso significa que você não precisa descriptografar manualmente o arquivo criptografado para poder usá-lo. Você pode abrir e alterar o arquivo da maneira habitual. Já quando outro usuário, que não o usuário que criptografou o arquivo, tenta acessar o arquivo criptografado, este outro usuário receberá uma mensagem de acesso negado.

CAPÍTULO

5

Administrando discos  
e volumes no Windows  
Server 2003

A tecnologia de criptografia do Windows Server 2003 é baseada no EFS – Encrypted File System (Sistema de arquivos criptografados). O EFS fornece todo o suporte necessário para trabalhar com arquivos criptografados. Somente arquivos e pastas em volumes NTFS podem ser criptografados. Esta, aliás, é uma das tantas vantagens do sistema de arquivos NTFS em relação ao sistema FAT/FAT32. Estas diferenças serão discutidas em detalhes no Capítulo 6.

## Conceitos que Você Precisa Conhecer

Existem alguns conceitos, termos e definições que você precisa conhecer, antes de partirmos para o estudo prático do gerenciamento de discos e volumes, no Windows Server 2003. Por exemplo, é fundamental que você saiba a diferença entre um Disco físico e um Volume lógico. Neste tópico vou apresentar os diversos termos relacionados com o gerenciamento de discos e volumes no Windows Server 2003.

### Disco físico

Chamamos de Disco Físico, a cada HD (antigamente mais conhecido por Winchester) instalado no computador. O primeiro HD instalado é denominado de Disco 0, o Segundo HD é chamado de Disco 1 e assim por diante. Um disco físico pode ser configurado como Disco Básico ou Disco Dinâmico. Mais adiante você entenderá 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. Você aprenderá o conceito de disco dinâmico e básico, bem como as ações práticas relacionadas, neste capítulo.
- ◆ Em servidores, onde é utilizada uma placa da RAID por hardware (você aprenderá mais sobre RAID neste capítulo), pode acontecer de um conjunto de três ou mais discos físicos, que fazem parte do RAID, “aparecerem” para o Windows Server 2003. Por exemplo, pode acontecer de você ter cinco discos de 50 GB formando o RAID, e estes discos aparecerem como um único disco físico, de 160 GB (eu não errei na soma não, quando estudarmos RAID, você entenderá o porquê 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. Por exemplo, você pode criar o C: com 40 GB, onde será instalado o Windows Server 2003 e os aplicativos, pode criar um D: com 20 GB, onde serão gravados arquivos de log do Sistema Operacional, o banco de dados do Active Directory e arquivos de log de outros serviços, como por exemplo os arquivos de Log de Transações do SQL Server 2000 e, finalmente, um E:, com os 20 GB restantes, onde serão gravados arquivos dos usuários. Observe que neste exemplo temos um disco físico (Disco 0), o qual foi dividido em três Volumes Lógicos (C:, D: e E:).

A definição oficial de volume, contida na Ajuda do Windows Server 2003 é a seguinte:

“Volume é uma área de armazenamento em um disco rígido (disco físico). Um volume é formatado usando um sistema de arquivos, tais como FAT ou NTFS, e tem uma letra de unidade atribuída a ele. Você pode visualizar o

conteúdo de um volume clicando em seu ícone no Windows Explorer ou em Meu computador. Um único disco rígido pode ter vários volumes, que também podem abranger vários discos”.

A última parte da definição é que pode parecer um pouco esquisita: “...que podem abranger vários discos”. Você verá, neste capítulo, que determinados tipos de volumes, podem ocupar áreas em dois ou mais discos.

## 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 (a exemplo do que acontece no Windows 2000 Server) é possível optar entre dois tipos de armazenamento: Armazenamento básico ou o Armazenamento dinâmico. A seguir descreverei estes dois tipos de armazenamento em detalhes.

### Armazenamento básico

É o tipo de armazenamento que vem sendo utilizado desde a época do bom e velho (talvez não tão bom) MS-DOS. É utilizado por sistemas como o Windows 95, Windows 98, Windows NT Server 4.0 e Windows NT Workstation 4.0. 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. 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 prática se comportam como se fossem dois discos de 2GB independentes. Em um disco com armazenamento básico, é possível ter Partições primárias, partições estendidas e Drivers lógicos. Mostrarei mais detalhes sobre estes elementos, bem como exemplos de utilização de cada um deles.

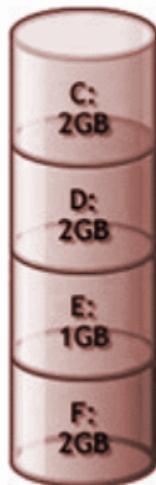
Partição primária: O Windows Server 2003 pode utilizar uma partição primária, para inicializar o computador, sendo que somente partições primárias podem ser marcadas como ativas. Uma partição ativa é onde o computador procura pelos arquivos de inicialização para efetuar o processo de boot do Sistema Operacional. Um disco básico somente pode possuir uma partição marcada como ativa. Um disco básico pode conter no máximo quatro partições primárias. Considere o exemplo da Figura 5.1, onde um disco de 7 GB foi dividido em quatro partições primárias. Três de 2 GB e uma de 1GB. Observe que para cada partição primária é atribuída uma letra de unidade: C; D; e assim por diante.

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

**NOTA:** Neste capítulo utilizarei a palavra **disco** como sendo sinônimo de **um disco rígido**, ou seja, **um disco físico**. Então sempre que você encontrar uma referência a **disco**, entenda como sendo **um disco rígido** e não **um disquete** ou **outro tipo de mídia**. Também é importante salientar que uso a palavra **disco** em referência ao **disco físico**, o qual pode ser dividido em várias partições (no caso de **armazenamento básico**) ou vários volumes (no caso de **armazenamento dinâmico**).

**IMPORTANTE:** É importante salientar que **um disco** somente pode ser configurado para **um tipo de armazenamento**. Não é possível, por exemplo, ter **uma parte do disco configurada como armazenamento básico e o restante como armazenamento dinâmico**.

que cada segmento representará um drive lógico. Deve ser atribuída uma letra para cada drive lógico e este deve ser formatado com um sistema de arquivos – FAT, FAT32, NTFS ou NTFS 5 (nova versão do NTFS disponível a partir do Windows 2000). Com o uso de uma partição estendida e drivers lógicos, é possível superar o limite de quatro unidades por disco, que é imposto quando se utiliza apenas partições primárias.



**Figura 5.1** No máximo podem ser criadas quatro partições primárias em um disco básico.

Considere o exemplo da Figura 4.2, onde é exibido um disco com três partições primárias (C; D; e E;), e um volume estendido, no qual foram criados dois drivers lógicos (F; e G;).

(FIG10-2.TIF) – Do livro de Windows Server 2003



**Figura 5.2** Utilizando partições estendidas.

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 Partição de 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 do Sistema e a Partição de boot, estão na mesma partição, tipicamente no drive C:

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 do Sistema:** Contém os arquivos necessários para o boot do Windows Server 2003.
- ◆ **Partição de boot:** Contém os arquivos do Windows Server 2003, tipicamente em uma pasta WINNT ou WINDOWS.
- ◆ **Volume set:** Para criar um Volume set é usado o espaço de duas ou mais partições, no mesmo disco ou em discos diferentes, de tal forma que estas partições apareçam, para o Windows Server 2003 como uma única unidade. Por exemplo posso combinar uma partição de 1 GB com outra de 4 GB, para formar uma unidade de 5 GB. Posso aumentar o tamanho de um Volume set (operação chamada de estender o Volume set), porém não posso reduzir 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 da segunda e assim por diante. Se uma das partições apresentar problemas, todo o Volume set será perdido. Posso juntar partições de tamanhos diferentes. Um Volume set não pode conter a Partição do sistema, nem a Partição de boot.
- ◆ **Stripe set:** Para criar um Stripe set combina-se espaços iguais de dois ou mais discos. Não podem ser utilizadas duas partições do mesmo disco. Posso utilizar 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 às gravações simultâneas em mais de um disco. Não pode conter a Partição do 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 do 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 (2 GB 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.

**IMPORTANTE:** Não esqueça que a partição do sistema e a partição de boot, não pode ser uma partição do tipo Volume set, Stripe set sem paridade ou Stripe Set com Paridade (RAID-5). Ou de uma maneira mais simples, as partições do sistema e de boot, somente podem ser do tipo partição simples ou do tipo Mirror set.

## 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 disco dinâmico, diretamente, sem perda de dados. Existem diferentes tipos de volumes. O tipo de volume a ser utilizado, é determinado por fatores tais 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 de comprometimento de um disco ou volume.

Em discos de volume dinâmico 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 criado usando duas ou mais partes de um mesmo disco dinâmico. Não fornece nenhum 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 do sistema. Ao estender um volume simples, usando porções de dois ou mais discos, ele torna-se um Spanned volume (Volume estendido). Mais adiante irei detalhar o conceito de volume estendido.
- ◆ **Volume estendido:** Pode incluir 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 10 GB você precisará de um espaço adicional de 10 GB em outro disco rígido. Ou seja, para 10 Gb de informações você utiliza 20 GB, sendo os 10 GB adicionais para o espelhamento.
- ◆ **Striped Volume:** Podem ser combinadas áreas de espaço livre de até 32 discos. Não apresenta 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 Striped volume, 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 reconstituída a partir das informações de paridade, contida nos demais discos. O disco defeituoso pode ser substituído e a informação nele contida pode ser recriada a partir da informação de paridade gravada 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 à falhas restringe-se a falha de um dos discos do volume, se dois discos falharem ao mesmo tempo, não será possível recuperar os dados

---

**NOTA: Dispositivos de armazenamento removíveis, com um Zip drive, somente suportam armazenamento básico e somente podem ter partições primárias. Além disso uma partição primária deste tipo de dispositivo, não pode ser marcada como ativa, para que seja possível dar o boot a partir desta partição.**

---

Existem mais alguns detalhes importantes que devem ser conhecidos:

OBS. : É muito importante lembrar, que o armazenamento dinâmico somente é suportado pelo Windows 2000 (Professional e Server e também pelo Windows XP) e pelo Windows Server 2003, sendo que discos dinâmicos não serão reconhecidos por outros sistemas operacionais como o Windows NT Server 4.0, Windows 95, Windows 98 e Windows NT Workstation 4.0.

Conhecendo estes aspectos básicos sobre o armazenamento de informações do Windows Server 2003, é hora de ir para a parte prática, onde você aprenderá a realizar as tarefas de gerenciamento de discos, utilizando o Snap-in especialmente projetado para esse fim.

## Operações Práticas no Gerenciamento de Discos e Volumes

Neste tópico (o mais extenso do capítulo) você aprenderá uma série de tarefas relacionadas com a criação, administração, alteração e exclusão de discos e volumes no Windows Server 2003. Todas estas tarefas podem ser executadas utilizando a opção Gerenciamento de disco, do console administrativo Gerenciamento do computador. Porém, para facilitar o trabalho, você iniciará o tópico criando um console personalizado, somente com o Snap-in Gerenciamento de disco. Nos exemplos práticos deste tópico você utilizará o console personalizado.

### Criando um console personalizado para gerenciamento de discos e volumes

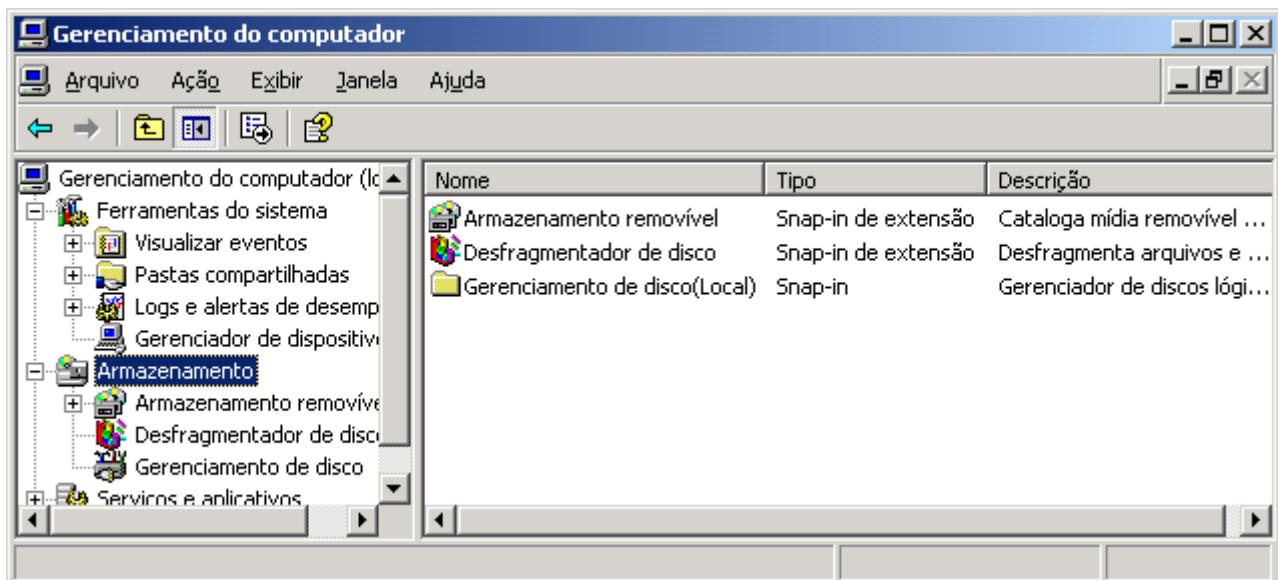
Neste item você aprenderá a acessar o console padrão para gerenciamento de discos, o qual é acessado através do console Gerenciamento do computador, do menu Ferramentas administrativas. Observe que não existe mais uma ferramenta chamada Disk administrator, como existia no Windows NT Server 4.0. Por isso você aprenderá a criar um console personalizado, onde será adicionado somente o Snap-in para Gerenciamento de disco.

A criação de um console personalizado, possibilita que a administração de um servidor seja, mais facilmente dividida entre vários administradores, conforme discutido no Capítulo 3. Por exemplo, você pode ter um administrador responsável por administrar contas de usuários, outro por administrar discos e assim por diante. Com o console personalizado, o administrador recebe um console onde é carregado apenas o Snap-in que tem a ver com a sua função. Com uma interface mais simples, o aprendizado é mais rápido.

Exemplo: Para acessar o gerenciamento de discos através do console Gerenciamento do computador, siga os passos indicados a seguir.

1. Faça o logon com a conta Administrador ou com uma conta com permissão de administrador.
2. Abra o console Gerenciamento do Computador: Iniciar -> Ferramentas Administrativas -> Gerenciamento do Computador.
3. Este console dá acesso a diversas tarefas de administração do Windows Server 2003, tais como auditoria, configuração e criação de contas de usuários e grupos locais e assim por diante.
4. Dê um clique no sinal de + ao lado da opção Armazenamento, caso ela não esteja aberta.
5. Serão exibidas três opções, conforme indicado na Figura 5.3:

**IMPORTANTE:** Para acompanhar os exemplos deste capítulo, você deve dispor de um disco o qual possa ser formatado, criadas partições, etc. Cabe lembrar que todas as informações do disco serão perdidas. Por isso não utilize um disco que contém informações importantes e que não possam ser apagadas. Para acompanhar os exemplos de criação de volumes do tipo Striped Volume ou Volume do tipo RAID-5 você deve ter um servidor com espaço livre em, pelo menos, três discos rígidos diferentes.



**Figura 5.3 Opções de Armazenamento.**

6. Abaixo de Armazenamento são exibidas opções para administração do Armazenamento removível, opção para o utilitário de desfragmentação de discos (Desfragmentador de disco) e opção para o gerenciamento de discos e volumes (Gerenciamento de disco).
7. Feche o console Gerenciamento do computador.

Agora você irá criar um console personalizado, no qual irá adicionar somente o Snap-in para Gerenciamento de disco. Em seguida você irá salvar este console com o nome de Gerenciamento de disco. O console personalizado será salvo na Área de trabalho, para facilitar a sua utilização.

Exemplo: Para criar um console personalizado e salvá-lo com o nome de Gerenciamento de discos, siga os seguintes passos:

1. Faça o logon com a conta Administrador ou com uma conta com permissão de administrador.
2. Clique em Iniciar -> Executar.
3. Na janela que surge, no campo Abrir digite mmc e dê um clique em OK.

Será aberta uma janela que mostra o MMC sem nenhum Snap-In Carregado.

4. Com o MMC carregado, dê um clique no menu Arquivo e escolha a opção Adicionar/remover Snap-in ... Será exibida a janela Adicionar/Remover Snap-in.
5. Na janela Adicionar/Remover Snap-in dê um clique no botão Adicionar.
6. Será exibida a janela Adicionar snap-in autônomo. Nesta janela é exibida uma listagem com todos os snap-ins disponíveis no servidor que você está utilizando.
7. Localize na listagem o seguinte snap-in: Gerenciamento de disco, conforme indicado na Figura 5.4 e dê um clique sobre ele para selecioná-lo.
8. Dê um clique no botão Adicionar.
9. Surge a janela Selecionar computador. Essa janela permite que você defina de qual computador você quer gerenciar os discos. Neste momento você pode gerenciar discos de um computador remoto, desde que você tenha permissão para isso. Essa é uma das novidades introduzidas no Windows 2000 Server e que está presente também no Windows Server 2003, já que em versões anteriores, (NT Server 4.0 ou anterior) somente era possível gerenciar discos estando localmente logado no servidor.

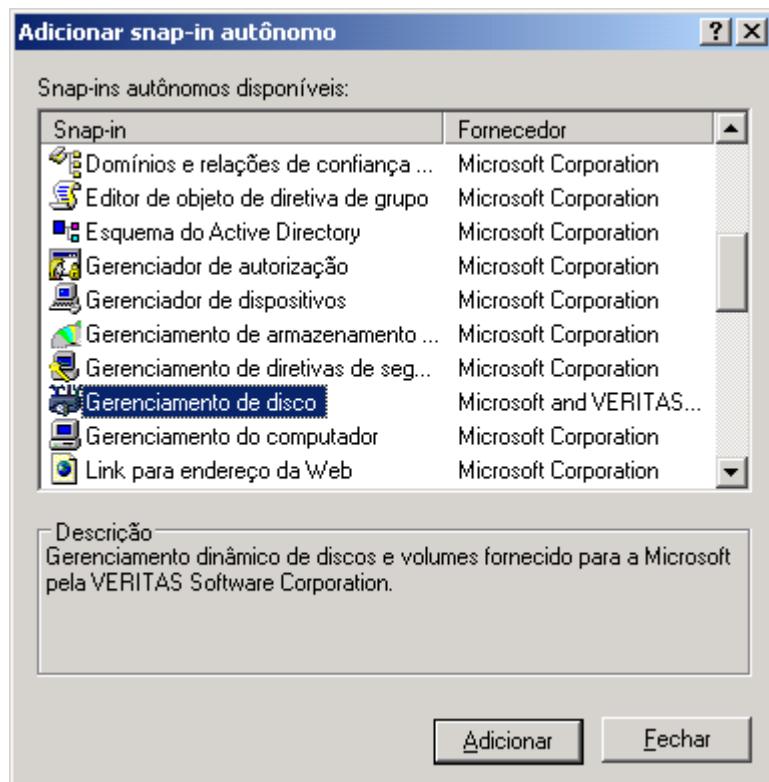


Figura 5.4 Selecionando o snap-in de gerenciamento de discos e volumes.

10. Por padrão vem selecionado o servidor local Este computador. Aceite esta seleção e dê um clique no botão Concluir.
11. Você estará de volta a janela Adicionar snap-in autônomo.
12. Como você não irá adicionar mais nenhum snap-in, dê um clique no botão Fechar.
13. Você estará de volta à janela Adicionar/remover snap-in. Observe que o snap-in Gerenciamento de disco (local), já aparece na listagem.
14. Dê um clique em OK para fechar a janela Adicionar/remover snap-in.
15. Você estará de volta ao MMC, agora com o snap-in Gerenciamento de disco já carregado, conforme indicado pela Figura 5.5.

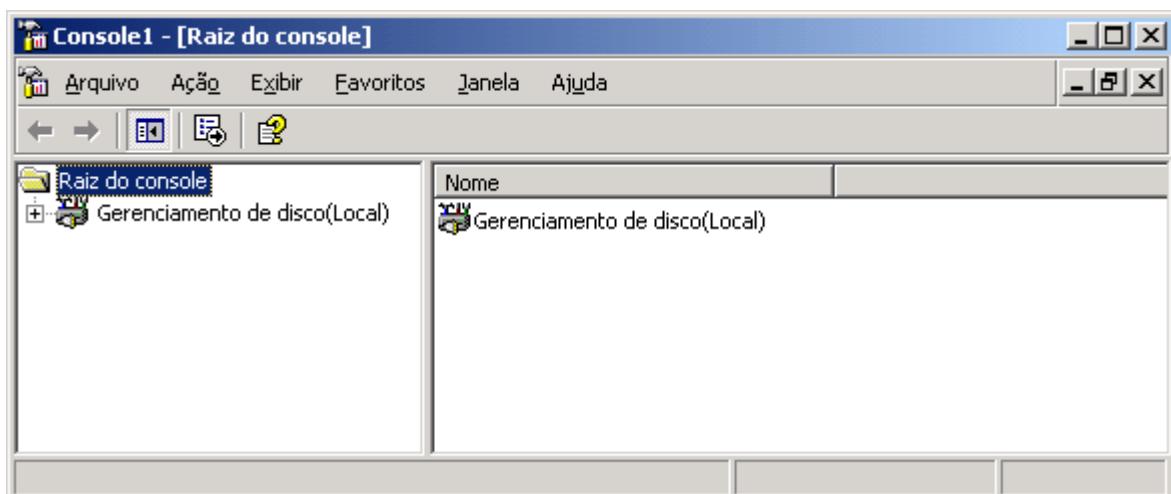


Figura 5.5 O Snap-In Disk Management já carregado.

16. Selecione o comando Arquivo -> Salvar.
17. Na janela Salvar como, no campo Nome do arquivo digite Gerenciamento de disco.
18. Nas opções do lado esquerdo da janela Salvar como) clique na opção Desktop.
19. Dê um clique no botão Salvar.
20. Feche o MMC.
21. Verifique que na área de trabalho foi criado o arquivo Gerenciamento de disco.msc (dependendo das configurações de pasta que você está utilizando pode ser que a extensão .msc não esteja sendo exibida). Este arquivo é o console personalizado, para gerenciamento de discos, que utilizarei nos exemplos práticos deste capítulo. No início de cada exemplo usarei a frase: “Abra o console personalizado para Gerenciamento de discos, criado anteriormente.”. Para abrir este console basta dar um clique duplo no respectivo arquivo (Gerenciamento de disco.msc), na área de trabalho.

Agora temos um console somente com o Snap-in para Gerenciamento de disco carregado. Este console pode ser utilizado por um administrador com funções específicas de gerenciar discos. É um console que possui apenas as opções necessárias para a tarefa em questão – Gerenciar discos.

Nos demais itens deste tópico, utilizarei o console Gerenciamento de disco, para os exemplos práticos que serão apresentados. Para acompanhar os exemplos deste tutorial, você precisa estar logado como Administrador, ou a sua conta de usuário deve ter permissões de administrador, pois você irá executar uma série de tarefas, tais como criar novos volumes, excluir volumes, formatar volumes e assim por diante, tarefas estas que exigem permissão de administrador.

## Reativando discos que ainda não foram completamente reconhecidos pelo Windows Server 2003

Pode acontecer de após o administrador ter instalado, fisicamente o disco e inicializado o servidor, de o disco ter sido reconhecido no Setup do computador, porém ainda não estar disponível para uso no Windows Server 2003. Nestas situações o disco pode apresentar diferentes Status, dependendo de o disco já estar sendo utilizado em outro servidor, de estar ou não formatado, de fazer ou não parte de um volume set ou de um volume RAID-5 e assim por diante. No próximo exemplo mostrarei uma situação onde dois novos discos foram instalados no servidor. O Windows Server 2003 reconheceu a presença destes discos, porém marcou-os com o Status Foreign (Externo). Este status, normalmente, indica discos que estavam sendo utilizados em outros computadores e foram instalados no servidor no qual você está trabalhando. No exemplo a seguir mostrarei como tornar estes discos disponíveis para o Windows Server 2003. Você irá, primeiro, importar os discos.

Exemplo: Para tornar disponíveis discos com o status Foreign (Externo), siga os passos indicados a seguir:

1. Faça o logon como Administrador ou com uma conta com permissões de administrador.
2. Abra o console personalizado para Gerenciamento de Discos, criado anteriormente.
3. Clique na opção Gerenciamento de disco.
4. Em alguns instantes são exibidos os discos disponíveis no computador. No exemplo da Figura 5.6 são exibidos dois discos com o status Foreign (Externo). Neste exemplo você irá importar estes discos e depois irá excluir os volumes (ou volume) neles existentes.

Observe que o Disco 2 e o Disco 3 estão com o status Foreign (Externo). O Windows Server 2003 numera os discos a partir do zero. No servidor da Figura 5.6 existem 4 discos instalados (Disco 0, Disco 1, Disco 2 e Disco 3). Você irá importar os discos 2 e 3, os quais estão com o status Foreign (Externo).

5. Clique com o botão direito do mouse próximo ao ponto de exclamação, ao lado de Disco 2. No menu de opções que é exibido clique na opção Import Foreign Disks... (Importar discos externos).

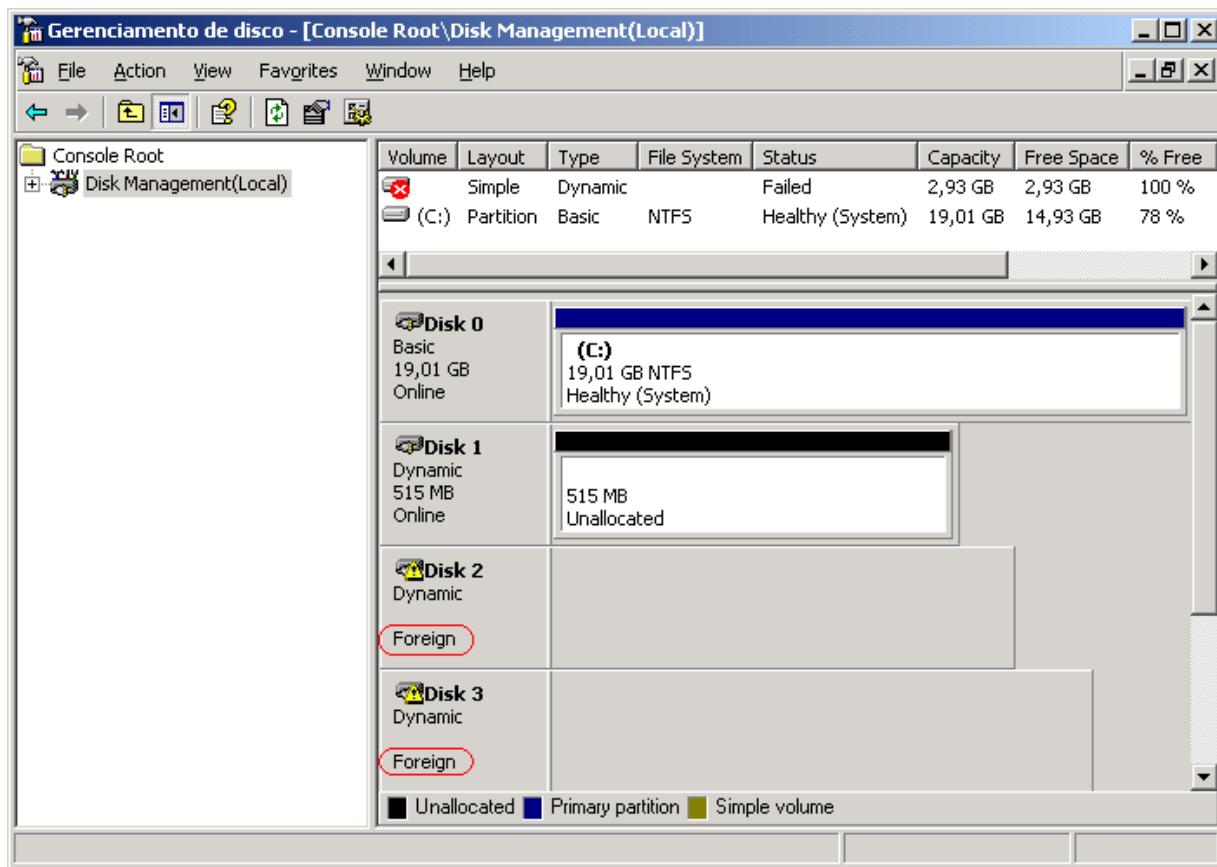


Figura 5.6 Discos com o status Foreign.

6. Será exibida a janela Import Foreign Disks (Importar discos externos). Nesta janela já vem selecionado o disco no qual você clicou com o botão direito do mouse, conforme indicado na Figura 5.7. Se você clicar no botão Disks... (Discos) será exibido o disco no qual você clicou com o botão direito do mouse. Nesta janela somente pode ser selecionado um disco por vez, ou seja, não é possível importar mais de um disco ao mesmo tempo.

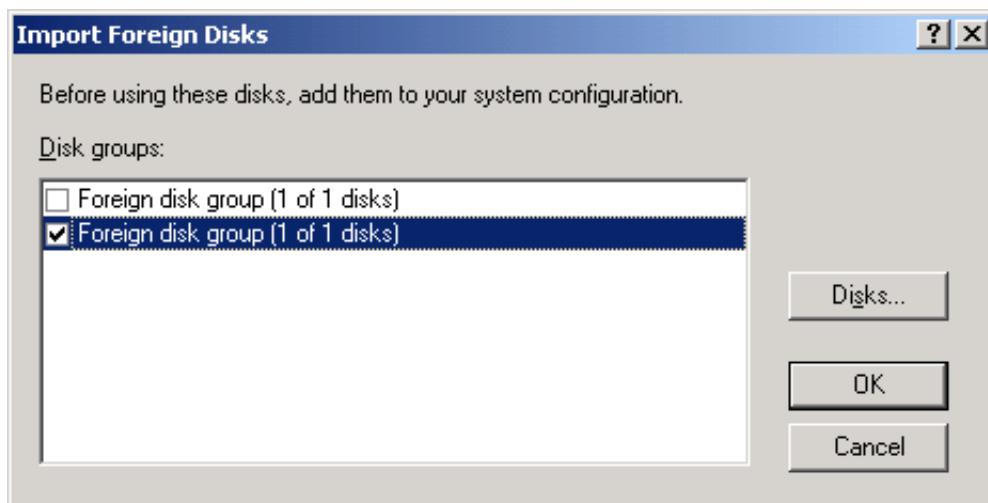


Figura 5.7 Discos com o status Foreign (Externo).

7. Clique em OK e pronto, o disco será importado. Observe que o disco que você acabou de importar já está disponível para uso.

8. Agora clique com o botão direito do mouse no outro disco a ser importado. Selecione o comando Import Foreign Disks... (Importar discos externos...)
9. A janela Import Foreign Disks (Importar discos externos) será exibida. Clique em OK. Se houver algum volume que possa ser utilizado no Windows Server 2003, disponível no disco que está sendo importado, será exibida a janela Foreign Disk Volumes (Volumes do disco externo).
10. Clique em OK para fechar esta janela.
11. Pronto, o disco foi importado e está disponível para uso, conforme indicado na Figura 5.8, onde não existe mais nenhum disco com o status Foreign (externo). Todos os discos estão com o status Online. Observe que no último disco que foi importado (Disco 3) existe um volume simples (formado por duas porções do disco, uma de 2 GB e outra de 512 MB e um espaço não alocado de 1,51 GB).

|        |   |                                 |                        |
|--------|---|---------------------------------|------------------------|
| Disk 0 | (C:)<br>19,01 GB NTFS<br>Healthy (System) |                                 |                        |
| Disk 1 | 515 MB<br>Unallocated                     |                                 |                        |
| Disk 2 | 1,19 GB<br>Unallocated                    |                                 |                        |
| Disk 3 | Dados<br>2,00 GB NTFS<br>Healthy          | Dados<br>512 MB NTFS<br>Healthy | 1,51 GB<br>Unallocated |

Figura 5.8 Volumes existentes no disco que foi importado.

A seguir apresenta uma descrição de cada um dos possíveis Status que podem ser exibidos para um disco, no console Gerenciamento de disco.

#### Status Externo:

O status Externo ocorre quando você move um disco dinâmico de um computador que esteja executando o Windows 2000, Windows XP Professional, ou a família de sistemas operacionais Windows Server 2003 para o computador local. O status Externo também pode ocorrer em computadores executando o Windows XP Home Edition que estejam configurados como multi boot, com outro sistema operacional que use discos dinâmicos (como o Windows 2000 Professional ou o Windows XP Professional). Não há suporte para discos dinâmicos no Windows XP Home Edition ou em notebooks. Um ícone de aviso é exibido nos discos que exibem o status Externo.

Para acessar os dados no disco, você deve adicionar o disco à configuração de sistema do computador. Para adicionar um disco à configuração de sistema do computador, importe o disco externo (conforme descrito no exemplo anterior).

**IMPORTANTE:** No entanto, você não poderá acessar dados no disco se estiver executando o Windows XP Home Edition. Para usar o disco no Windows XP Home Edition, é necessário convertê-lo em disco básico, o que destrói todos os dados contidos nele. Também é importante salientar, que computadores móveis, como Notebooks, não tem suporte a discos dinâmicos.

Todos os volumes existentes no disco externo se tornam visíveis e acessíveis quando você importa o disco.

Em alguns casos, um disco que foi previamente conectado ao sistema pode exibir o status Externo. Os dados de configuração dos discos dinâmicos são armazenados em todos os discos dinâmicos. Portanto, as informações sobre quais discos pertencem ao sistema se perdem quando todos os discos dinâmicos falham.

#### Status Inicializando:

O status Inicializando é um status temporário que ocorre quando você converte um disco básico em dinâmico. Quando a inicialização termina, o status do disco é alterado para On-line.

#### Status Faltando:

O status Faltando ocorre quando um disco dinâmico é corrompido, desligado ou desconectado. Em vez de ser exibido na coluna de status, o status Faltando é exibido como nome de disco. Após reconectar ou ligar o disco ausente, abra o console Gerenciamento de disco, clique com o botão direito do mouse no disco ausente e, em seguida, clique em Reativar disco. Se houver mais de um disco faltando no grupo, o Gerenciamento de disco tentará reativar todos os discos.

#### Status Não inicializado:

O status Não inicializado ocorre quando um disco não contém uma assinatura válida. Depois que você instala um novo disco, o Windows XP Professional ou a família de sistemas operacionais Windows Server 2003 deve gravar um registro de inicialização principal (MBR) ou uma tabela de partição GUID (GPT) para que seja possível criar partições no disco. Quando você iniciar o Gerenciamento de disco pela primeira vez após a instalação de um novo disco, será exibido um assistente que fornece uma lista dos novos discos detectados. Se você cancelar o assistente antes que a assinatura de disco seja gravada, o status do disco permanecerá como Não inicializado até que você clique com o botão direito do mouse no disco e, em seguida, clique em Inicializar disco. O status do disco se altera brevemente para Inicializando e, em seguida, para On-line.

#### Status On-line:

O status On-line ocorre quando um disco básico ou dinâmico pode ser acessado e aparenta não ter nenhum problema. Este é o status normal de um disco. Não é necessária nenhuma ação do usuário.

#### Status On-line (erros):

O status On-line (erros) ocorre quando os erros de E/S (entrada e saída) são detectados em uma região de um disco dinâmico. Um ícone de aviso é exibido no disco dinâmico com erros.

Se os erros de E/S forem temporários, (por exemplo, devido a um fio solto que já esteja no lugar) o disco retornará para o status On-line quando você reativá-lo.

#### Status Off-line:

O status Off-line ocorre quando um disco dinâmico não pode ser acessado. O disco dinâmico pode estar corrompido ou temporariamente não disponível. Um ícone de erro é exibido no disco dinâmico off-line.

Se o status do disco for Off-line e o nome do disco for alterado para Faltando, é sinal de que o disco estava recentemente disponível no sistema, mas não pode mais ser localizado ou identificado. O disco ausente pode estar corrompido, desligado ou desconectado.

**IMPORTANTE: Não converta um disco dinâmico em básico, a menos que você tenha certeza de que não precisará mais dos dados contidos nesse disco. A conversão de um disco dinâmico em básico destruirá todos os dados do disco.**

### **Colocando um disco que está off-line e ausente novamente on-line:**

Repare qualquer disco, controlador ou problema de cabo e certifique-se de que o disco físico está ligado, conectado à fonte de energia e instalado no computador. No Gerenciamento de disco, clique com o botão direito do mouse no disco e, em seguida, clique em Reativar disco para colocar o disco novamente on-line.

Se o status do disco permanecer Off-line, o nome do disco continuar como Faltando e você determinar que o disco está com um problema que não pode ser reparado, remova o disco do sistema (usando o comando Remover disco). Entretanto, antes de remover o disco, exclua todos os volumes (ou espelhos) do disco. Você pode salvar todos os volumes espelhados do disco removendo o espelho, em vez de remover todo o volume. A exclusão de um volume destruirá os dados do volume. Portanto, você deve remover um disco somente se estiver absolutamente certo de que o disco está definitivamente danificado ou inutilizado.

### **Colocando um disco que está off-line e ainda é chamado de Disco nº (não ausente) novamente on-line:**

No Gerenciamento de disco, clique com o botão direito do mouse no disco e, em seguida, clique em Reativar disco para colocar o disco novamente on-line. Se o status do disco continuar Off-line, verifique os cabos e o controlador do disco, e certifique-se de que o disco físico está íntegro. Corrija quaisquer problemas e tente reativar o disco novamente. Se a reativação do disco tiver êxito, todos os volumes do disco retornarão automaticamente ao status Íntegro.

### **Status Ilegível:**

O status Ilegível ocorre quando um disco básico ou dinâmico não pode ser acessado. O disco pode estar com uma falha de hardware, corrompido ou com erros de E/S. A cópia do banco de dados de configuração de disco do sistema pertencente ao disco pode estar corrompida. Um ícone de erro é exibido nos discos que exibem o status Ilegível.

Os discos podem exibir o status Ilegível enquanto estão girando ou quando o Gerenciamento de disco está examinando novamente todos os discos do sistema. Em alguns casos, um disco ilegível apresenta falha e não pode ser recuperado. Nos discos dinâmicos, o status Ilegível é geralmente provocado por danos e erros de E/S em parte do disco, e não por falhas no disco inteiro. Você pode examinar novamente os discos (clique em Ação e, em seguida, clique em Examinar discos novamente) ou reiniciar o computador para ver se o status do disco foi alterado.

Nos próximos exemplos você aprenderá a criar, formatar e a gerenciar os diversos tipos de volumes disponíveis no Windows Server 2003.

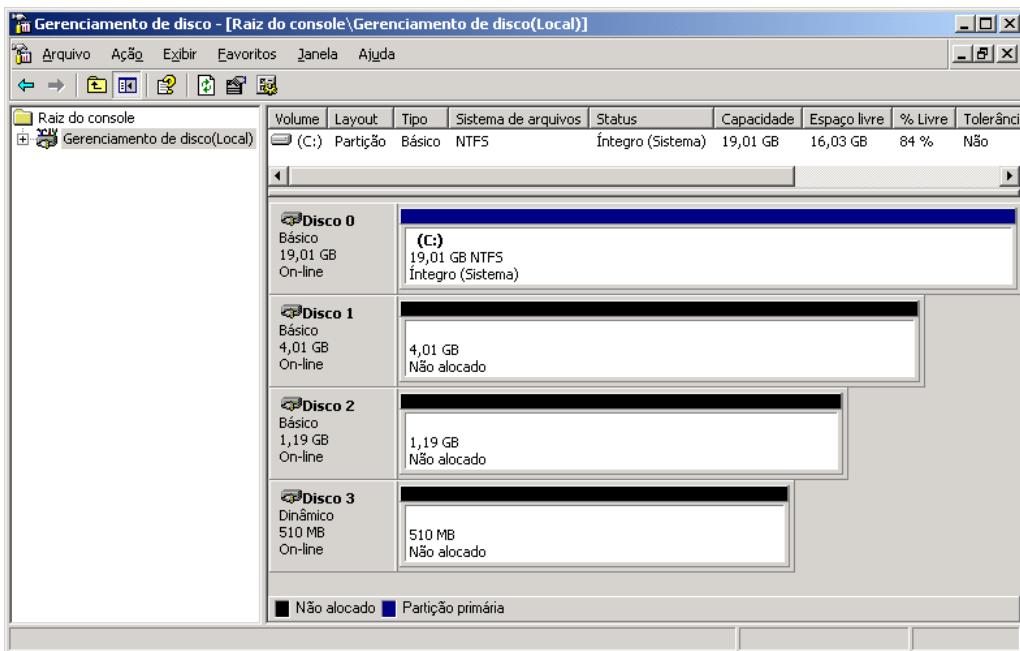
## **Acessando informações sobre os discos do seu servidor**

Neste item detalharei um pouco mais o console Gerenciamento de disco. Além de abrir o console personalizado, criado anteriormente, você irá acessar informações sobre os discos instalados no sistema e aprender a interpretar estas informações. Também aprenderá a fazer a conexão com um outro computador da rede, para que seja possível gerenciar os discos deste computador remotamente. Conforme citado anteriormente, a possibilidade de gerenciamento remoto de discos é uma novidade que foi introduzida a partir do Windows 2000 Server, e se encaixa na filosofia de facilitar a administração centralizada dos recursos do sistema.

Exemplo: Para acessar as informações sobre os discos instalados no seu servidor, siga os seguintes passos indicados a seguir:

1. Faça o logon como Administrador ou com uma conta com permissões de administrador.
2. Abra o console personalizado para Gerenciamento de discos, criado anteriormente.
3. Clique na opção Gerenciamento de disco.

4. Em poucos instantes o Windows Server 2003 exibirá informações sobre os diversos discos e as partições criadas em cada um deles, conforme exemplo mostrado na Figura 5.9:



**Figura 5.9** Informações sobre os discos instalados e os respectivos volumes.

5. Observe na legenda (parte de baixo do console), que Partições primárias são exibidas com a barra de título em Azul escuro, volumes simples em verde, e espaço Não alocado em preto. Outros tipos de volumes são exibidos com diferentes cores.
  6. Observe também que o Primeiro disco é chamada de Disk 0 (Disco 0), o segundo de Disk 1 (Disco 1) e assim por diante.
  7. No exemplo da Figura 5.9, no Disco 0, existe um único volume de 19,01 GB, (C:) formatada com NTFS, a qual é a partição do Sistema, conforme indicado pela palavra Sistema entre parênteses. Este é um disco básico e contém os arquivos de boot (partição do sistema), bem como os arquivos do sistema operacional (partição de boot).
  8. Da mesma forma você pode observar que o Disco 3 é um disco de 510 MB (bem antigo, na verdade é o HD que utilizei em meu primeiro computador, um 486 DX2 66) o qual não está sendo utilizado, ou seja, nenhum volume foi criado neste disco. Na verdade ele ainda está como disco básico. Para que você possa criar volumes neste disco ele deve ser convertido para disco dinâmico (conforme você aprenderá mais adiante).
  9. Na parte de cima da janela, existe uma listagem com todas as partições/volumes configuradas no computador. São exibidas informações tais como o espaço ocupado, o espaço livre, a porcentagem do espaço livre, o sistema de arquivos, etc. Observe que a segunda coluna informa o Layout, o qual é Partição para discos básicos e o tipo de volume para discos dinâmicos. A terceira coluna informa o tipo de armazenamento se básico ou dinâmico.
  10. Você pode configurar quais informações são exibida no painel de cima do console (lista de discos, lista de volumes ou uma visualização gráfica dos discos). Para configurar o tipo de visualização do painel de cima, selecione um dos seguintes comandos: Exibir -> Superior -> Lista de disco, para exibir uma lista dos discos do sistema; Exibir -> Superior -> Lista de volume, para exibir uma lista dos volumes configurados no sistema ou Exibir -> Superior -> Visualização gráfica), para exibir um listagem gráfica dos discos instalados no sistema.

11. Você pode configurar quais informações são exibida no painel de baixo do console (lista de discos, lista de volumes ou uma visualização gráfica dos discos). Para configurar o tipo de visualização do painel décima selecione um dos seguintes comandos: Exibir -> Inferior -> Lista de discos, para exibir uma lista dos discos do sistema; Exibir -> Inferior -> Lista de volume, para exibir uma lista dos volumes configurados no sistema; Exibir -> Inferior -> Visualização gráfica, para exibir um listagem gráfica dos discos instalados no sistema ou Exibir -> Inferior -> Ocultar, para ocultar o painel de baixo, onde por padrão é exibida uma listagem gráfica dos discos do sistema.
12. Feche o console personalizado Gerenciamento de discos.

## Trabalhando com partições em um disco de armazenamento básico

Neste item você aprenderá a realizar algumas operações básicas com partições em um disco de armazenamento básico. Mostrarei como criar uma nova partição, formatá-la com um sistema de arquivos e excluir uma partição que não seja mais necessária. Ao excluir uma partição, o espaço que era ocupado pela partição será liberado e aparece como espaço não alocado, isto é, espaço disponível para ser utilizado por outras partições.

Exemplo: Para criar e formatar uma nova partição a partir de um espaço não alocado, em um disco básico, siga os seguintes passos:

1. Faça o logon como Administrador ou com uma conta com permissões de administrador.
2. Abra o console personalizado para Gerenciamento de disco, criado anteriormente.
3. Clique na opção Gerenciamento de disco. Localize um disco que contenha espaço não alocado, normalmente indicado pela expressão Não alocado e pela barra de título na cor preta.
4. Para criar uma nova partição no espaço não alocado, dê um clique com o botão direito neste espaço. No menu que surge, dê um clique na opção Nova partição...
5. Será iniciado o Assistente para criação de novas partições.

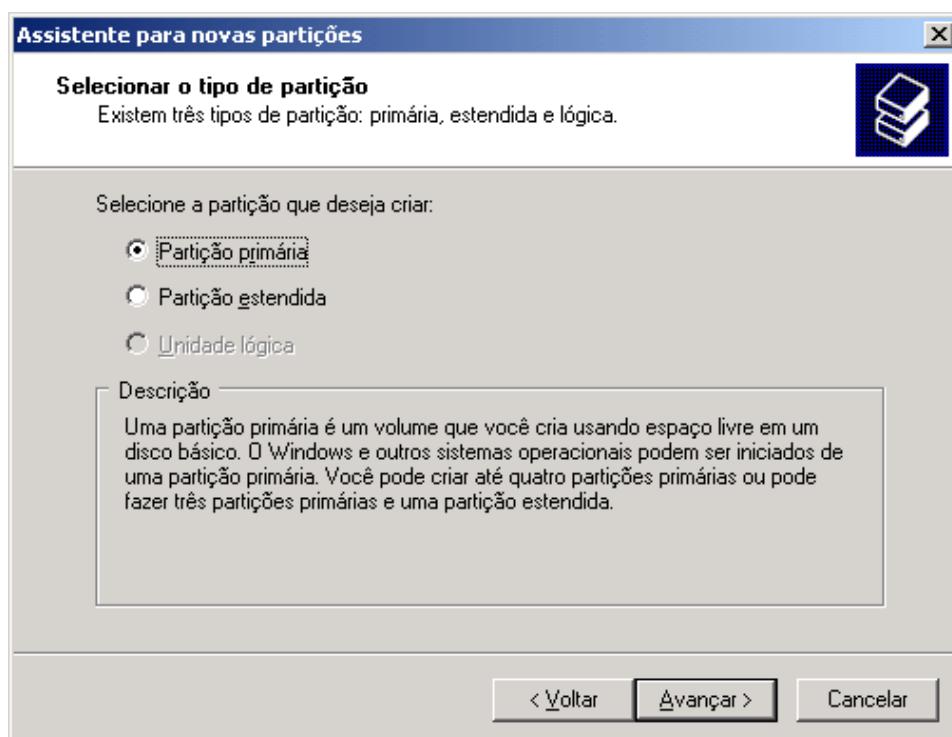
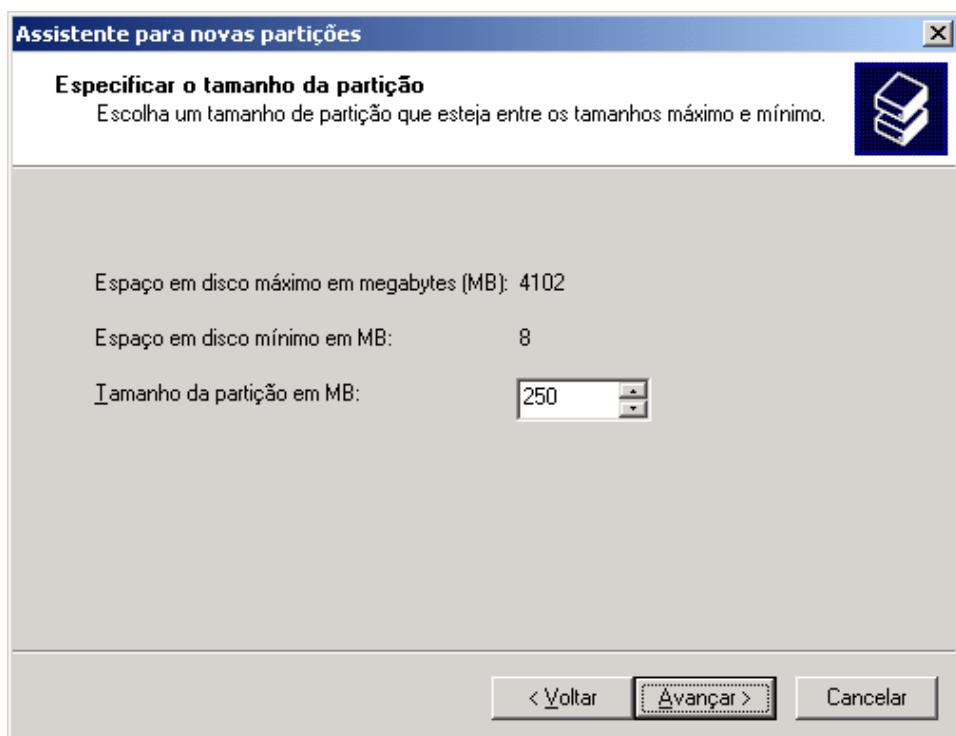


Figura 5.10 Criando uma partição primária em um disco básico.

6. A tela inicial é simplesmente uma mensagem informativa. Dê um clique no botão Avançar para ir para a próxima etapa do assistente.
7. Na segunda tela do assistente, você tem que definir o tipo de partição que está sendo criada. Dependendo da partição, uma ou mais opções podem estar desabilitadas. Escolha Partição primária, conforme indicado na Figura 5.10. A opção Partição primária é utilizada para a primária partição criada em um disco básico. A segunda partição deve ser criada como partição estendida e depois, em cima da partição estendida, criam-se drivers lógicos, conforme descrito no início deste capítulo.
8. Dê um clique no botão Avançar para ir para a próxima tela do assistente.
9. Nesta etapa você define o tamanho, em MB, que a nova partição irá utilizar. No campo Tamanho da partição em MB, especifique o tamanho da nova partição, conforme exemplo da Figura 5.11.



**Figura 5.11 Definindo o tamanho da nova partição que está sendo criada.**

10. Dê um clique no botão Avançar para ir para a próxima tela do assistente.
11. Na quarta tela do assistente estão disponíveis diversas opções. Você pode definir a letra de unidade que será associada com esta partição. Por padrão o Windows Server 2003 sugere a primeira letra que estiver disponível para uso. Na lista Atribuir uma letra de unidade, selecione a letra desejada, conforme exemplo da Figura 5.12 e dê um clique no botão Avançar para ir para a próxima tela do assistente.
12. Dê um clique no botão Avançar, para ir para a próxima tela do assistente.
13. Nesta etapa você define uma série de detalhes a respeito da partição. Você define se irá formatá-la agora ou não, Qual o sistema de arquivos a ser utilizado. Se vai ou não utilizar compressão de arquivos. Pode ser definido um nome para a partição. Na Figura 5.13 mostro um exemplo onde a partição será formatada, com o sistema de arquivos NTFS, foi mantido o tamanho padrão de unidade de alocação, o nome da unidade foi definido como Exemplo-01, foi escolhida uma formatação rápida (Executar uma formatação rápida) e foi habilitada a compactação de arquivos (Ativar compactação de arquivos e pastas).

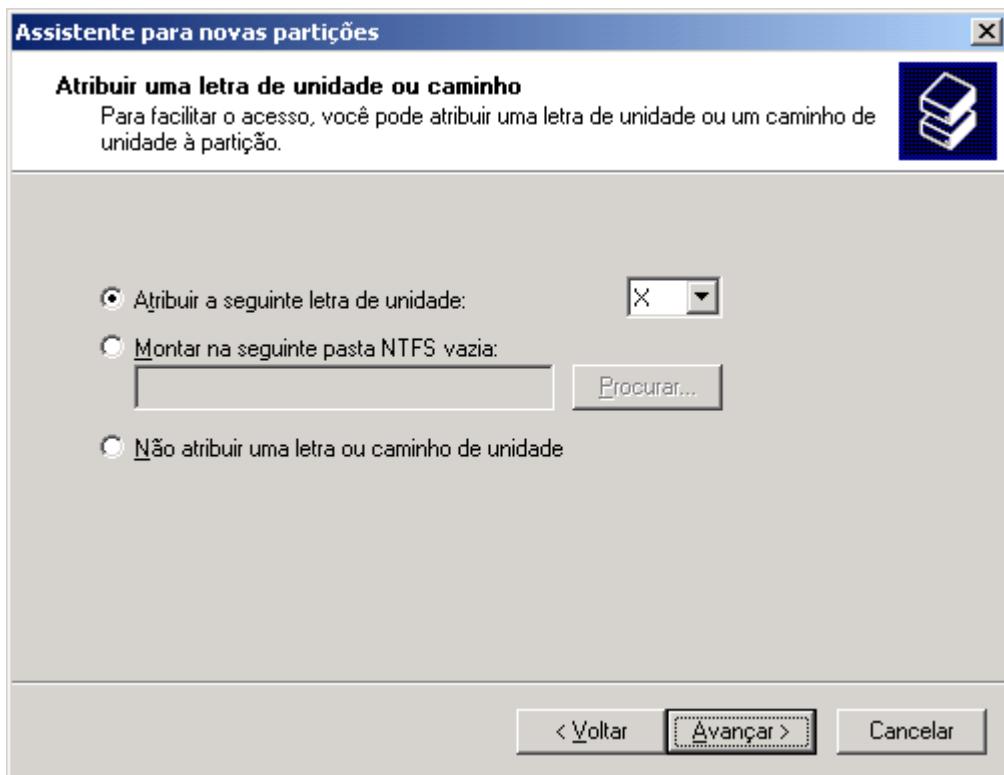


Figura 5.12 Selecionando a letra a ser associada com a nova partição.

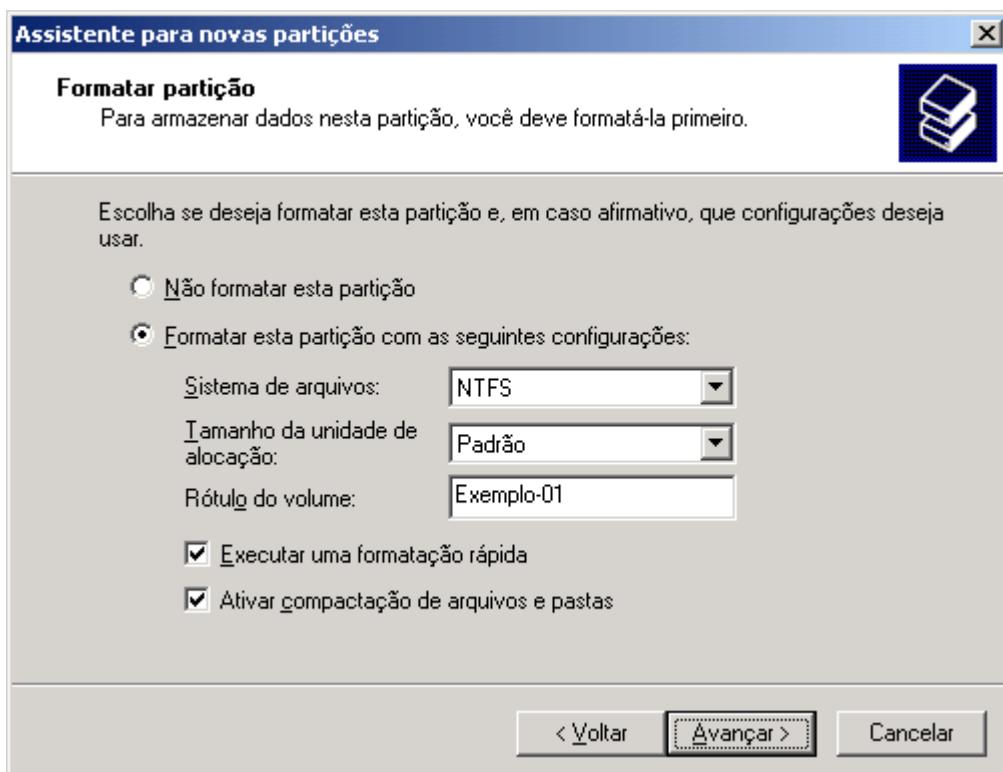


Figura 5.13 Especificando as informações para a formatação da partição.

14. Dê um clique no botão Avançar para ir para a tela final do assistente. Nesta tela é exibido um resumo com as opções que você escolheu nos diversos passos do assistente. Caso você queira alterar alguma informação, basta utilizar o botão Voltar.
15. Dê um clique no botão Concluir para finalizar a criação e formatação da partição.
16. Na figura 5.14, é exibida a partição X:, com 250 MB, formatada com o sistema de arquivos NTFS e com o nome de Exemplo-01, criada neste exemplo

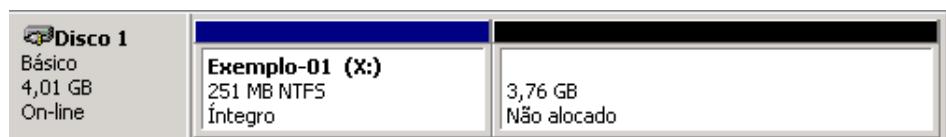


Figura 5.14 Partição Exemplo-01 com 250 MB, recém criada.

17. Observe ainda, que somente restaram 3,76 GB (4,01 GB – 250 MB), não alocados no Disco 1, onde a partição foi criada. Se você abrir o Meu computador ou o Windows Explorer, na listagem de drivers já estará sendo exibido o drive X: (Exemplo-01), com 250 MB de espaço disponível.
18. Feche o console Gerenciamento de disco. Caso o Windows Server 2003 peça para salvar as alterações, dê um clique em Sim.

Agora você aprenderá a excluir uma partição criada em um disco básico. Você irá excluir a partição Exemplo-01, recém criada.

Exemplo: Para excluir uma partição siga os seguintes passos:

1. Faça o logon como Administrador ou com uma conta com permissões de administrador.
2. Abra o console personalizado para Gerenciamento de disco, criado anteriormente.
3. Clique na opção Gerenciamento de disco.
4. Localize a partição a ser excluída e dê um clique com o botão direito do mouse sobre a ela. Por exemplo, localize a partição X: criada no exemplo anterior e dê um clique com o botão direito do mouse nesta partição. No menu que surge dê um clique na opção Excluir partição...
5. O Windows Server 2003 emite um aviso de que todos os dados da partição serão perdidos e pede confirmação para a exclusão da partição, conforme indicado na Figura 5.15:

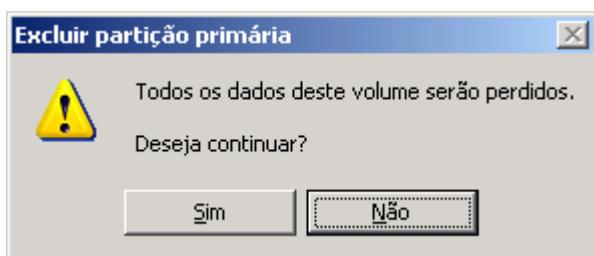


Figura 5.15 Pedindo confirmação para a exclusão da partição.

**NOTA:** Caso você não formate a partição no momento de criação, é possível formatá-la facilmente depois. Para isso basta abrir o Meu computador e clicar com o botão direito do mouse no drive correspondente a partição não formatada e no menu que surge, dê um clique na opção Formatar. Surge uma janela com as opções de formatação onde você pode especificar os detalhes para a formatação.

6. Dê um clique em Sim para confirmar a exclusão.
7. O espaço que era ocupado pela partição, agora fica sendo exibido como espaço não alocado.
8. Feche o console Gerenciamento de disco.

## Eliminando um volume set, disk mirror, stripe set e stripe set com paridade em discos de armazenamento básico

Exemplo: Para eliminar qualquer tipo de volume em um disco básico, siga os passos indicados a seguir:

1. Faça o logon como Administrador ou com uma conta com permissões de administrador.
2. Abra o console personalizado para Gerenciamento de disco, criado anteriormente.
3. Clique na opção Gerenciamento de disco.
4. Localize a partição a ser excluída e dê um clique com o botão direito do mouse sobre a ela. No menu que surge dê um clique na opção Excluir partição...
5. O Windows Server 2003 emite um aviso de que todos os dados da partição serão perdidos e pede confirmação para a exclusão da partição.
6. Dê um clique em Sim para confirmar a exclusão.
7. O espaço que era ocupado pela partição, agora fica sendo exibido como espaço não alocado.
8. Feche o console Gerenciamento de disco.

**IMPORTANTE:** Quando é feita a migração do Windows NT Server 4.0 para o Windows Server 2003, qualquer Volume set ou disk mirror existente será mantido. O Windows Server 2003 também mantém qualquer Stripe set ou Stripe set com paridade. Porém uma vez instalado o Windows Server 2003, não é possível criar novos volumes do tipo Volume set, disk mirror, Stripe set ou Stripe set com paridade, em discos de armazenamento básico. Somente é possível criar estes tipos de volumes em discos de armazenamento dinâmico. Isso acontece porque o Windows Server 2003 dá preferência a que seja utilizado o Armazenamento dinâmico, sendo que o suporte a Volume set, disk mirror, Stripe set e Stripe set com paridade em partições de armazenamento básico, somente é mantido por questões de compatibilidade com versões anteriores do Windows. Você pode criar estes diversos elementos, apenas em discos de armazenamento dinâmico, conforme mostrarei nos próximos itens.

## Convertendo um disco de Armazenamento básico para Armazenamento dinâmico

Conforme descrito no início deste capítulo, é possível converter um disco de Armazenamento básico para Armazenamento dinâmico, sem perda de dados. Para efetuar a conversão para Armazenamento dinâmico, deve haver pelo menos 1 MB de espaço não alocado, no disco a ser convertido, para que a conversão possa ser feita com sucesso. O console de Gerenciamento de disco, automaticamente reserva este espaço ao criar partições ou volumes em um disco. Porém discos com partições ou volumes criados por outros sistemas operacionais, podem não ter este espaço não alocado, disponível. Um disco com Armazenamento dinâmico não terá partições ou drivers lógicos, ao invés disso o disco é dividido em volumes, conforme detalhado no início deste capítulo.

Converter um disco de Armazenamento dinâmico de volta para Armazenamento básico diretamente, não é possível, sem perda de dados. Primeiro você deve excluir todos os volumes existentes no disco de Armazenamento dinâmico, para depois revertê-lo para armazenamento básico. Porém isso causa a perda de toda a informação armazenada no disco, a qual deve ser restaurada a partir de uma cópia de segurança (backup).

Quando você converte um disco de Armazenamento básico para Armazenamento dinâmico, o Windows Server 2003 efetua o mapeamento das partições existentes para os tipos de volume indicados na tabela 5.1.

**Tabela 10.1 Conversão de armazenamento básico para dinâmico.**

| Disco Básico            | Disco Dinâmico  |
|-------------------------|---|
| Partição do sistema     | Volume simples  |
| Partição do boot        | Volume simples  |
| Partição primária       | Volume simples  |
| Partição estendida      | Um volume simples para cada drive lógico e qualquer espaço não alocado restante |
| Drive lógico            | Volume simples  |
| Volume set              | Spanned volume  |
| Stripe set              | Striped volume  |
| Disk mirror             | Mirrored volume   |
| Stripe set com paridade | Volume RAID-5   |

Caso programas instalados no disco a ser atualizado, estejam abertos, estes devem ser fechados antes que a atualização possa ser feita.

As partições de boot e do sistema somente são convertidas após uma reinicialização do computador. Todas as outras partições serão atualizadas imediatamente.

No próximo exemplo você aprenderá os passos para a conversão de um disco básico para disco dinâmico.

Exemplo: Para converter um disco básico para Armazenamento dinâmico siga os seguintes passos:

1. Faça o logon como Administrador ou com uma conta com permissões de administrador.
2. Abra o console personalizado para Gerenciamento de disco, criado anteriormente.
3. Clique na opção Gerenciamento de disco.
4. Em poucos instantes o Windows Server 2003 exibe as informações sobre os discos instalados no seu computador.
5. Localize o disco a ser atualizado para Armazenamento dinâmico, dê um clique com o botão direito do mouse sobre o disco (Disco 0, Disco 1, etc), e no menu que surge dê um clique na opção Converter em disco dinâmico...
6. Surge uma janela perguntando quais discos que você deseja atualizar. Certifique-se que apenas o disco que você quer atualizar está marcado, conforme indicado pela Figura 5.17, onde esta sendo atualizando o Disco 1.

**IMPORTANTE:** Se um disco básico possui parte de uma partição que se estende por mais de um disco (Volume set, Stripe set, Disk mirror ou Stripe set com paridade), todos os discos que contém as partes da partição devem ser convertidos ao mesmo tempo. Todos os discos devem conter, pelo menos, 1 MB de espaço não alocado, caso contrário a conversão irá falhar. Este espaço de 1 MB pode existir mesmo que não seja visível no Snap-in de Gerenciamento de disco, conforme descrito anteriormente.

**IMPORTANTE:** Clique na parte da esquerda, onde está escrito Disco n, onde n é o número do Disco a ser convertido para dinâmico, conforme destacado na Figura 5.16. Se você clicar em uma das partições ou no espaço não alocado, não surgirá a opção Converter em disco dinâmico...

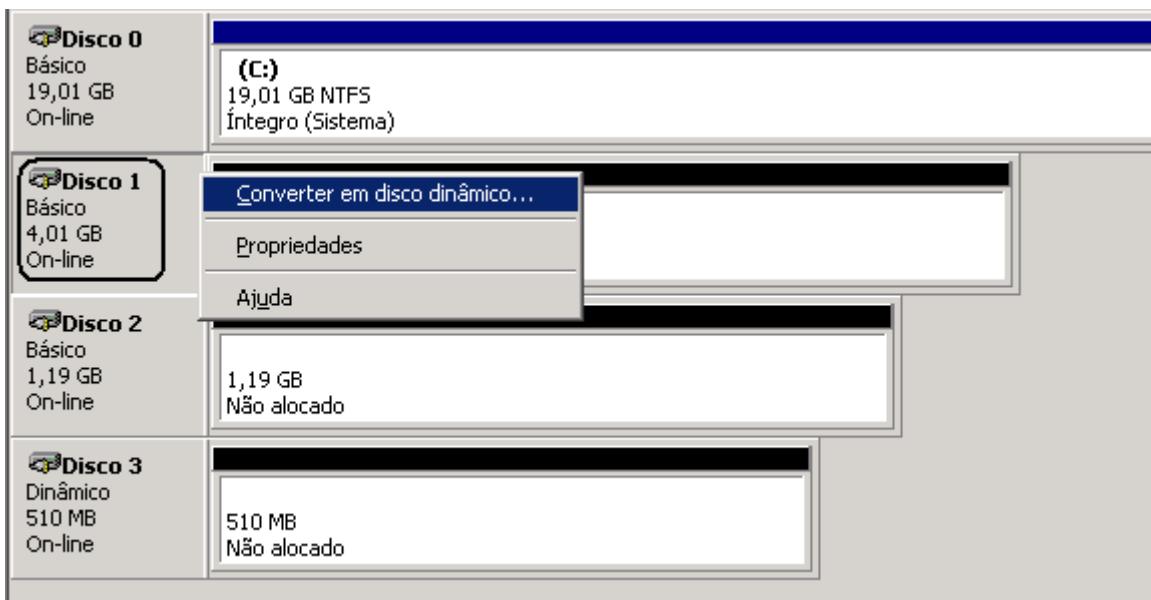


Figura 5.16 Clique com o botão direito na parte destacada na figura.

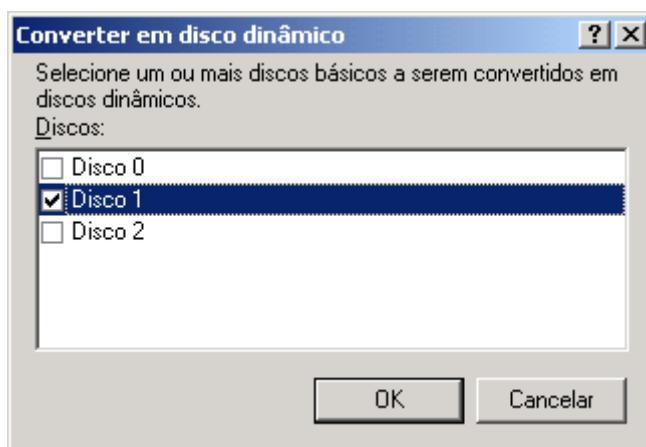


Figura 5.17 Marque apenas o disco (ou discos) a ser atualizado.

7. Dê um clique no botão OK e aguarde. Em poucos instantes o Windows Server 2003 já mostra no console de Gerenciamento do computador, que o disco foi convertido para Armazenamento dinâmico, conforme indicado pela Figura 5.18.



Figura 5.18 Disco 1 já convertido para Armazenamento dinâmico.

8. Feche o console de Gerenciamento de disco.

## Criando e expandindo um Volume simples

Neste item você aprenderá a criar e a expandir um volume simples. É possível criar um Volume simples, em qualquer espaço não alocado de um disco de Armazenamento dinâmico. Um Volume simples pode conter espaço não alocado de um único disco, possui uma letra de unidade atribuída ao Volume, pode ser formatado com FAT, FAT32 ou NTFS. Após criado, um Volume simples pode ser expandido somente com espaço do mesmo disco e somente se tiver sido formatado com NTFS. Um Volume simples, aparece para o Windows Server 2003 como um drive. Por exemplo F:, G:, etc.

É importante lembrar que um volume simples não apresenta nenhum tipo de mecanismo a falha, ou seja, se houver algum problema com o volume ou com o disco no qual o volume foi criado, todos os dados serão perdidos e a única maneira de recuperá-los é utilizando uma cópia de segurança (backup), supondo, evidentemente, que você, como bom administrador que é, tenha cópias de segurança sempre atualizadas e confiáveis.

Nos próximos exemplos práticos você continuará a usar o console personalizado Gerenciamento de disco, criado no início deste tópico. Ao invés deste console você poderia também utilizar o console Gerenciamento do computador. No console Gerenciamento do computador, basta acessar a opção Gerenciamento de disco, dentro do grupo Armazenamento.

Exemplo: Para criar um Volume simples siga os seguintes passos:

1. Faça o logon como Administrador ou com uma conta com permissões de administrador.
2. Abra o console personalizado para Gerenciamento de disco, criado anteriormente.
3. Clique na opção Gerenciamento de disco.
4. Em poucos instantes o Windows Server 2003 exibe as informações sobre os discos instalados no seu computador.
5. Localize um disco de Armazenamento dinâmico que possua espaço não alocado.
6. Dê um clique com o botão direito do mouse em qualquer parte do espaço não alocado. No menu que surge dê um clique na opção Novo volume...
7. O Windows Server 2003 abre o Assistente para criação de volumes.
8. A primeira tela é simplesmente informativa. Dê um clique no botão Avançar para ir para a segunda tela do assistente.
9. Na segunda etapa você deve selecionar o tipo de volume que será criado. Marque a opção Simples, conforme indicado na Figura 5.19:
10. Dê um clique no botão Avançar para ir para a terceira tela do assistente.
11. Na terceira etapa, o Windows Server 2003 exibe o disco no qual será criado o Volume, e também o tamanho máximo disponível. Nesta tela, caso existam outros discos dinâmicos, com espaço livre, é possível alterar o disco no qual será criado o Volume simples. Para isto basta marcar o disco desejado e utilizar o botão Adicionar para incluir o disco desejado.
12. No exemplo da Figura 5.20, está sendo criado um volume simples o qual ocupa 200 MB dos 4103 MB disponíveis no Disco 1.

**IMPORTANTE:** Embora seja possível usar FAT ou FAT32 como sistema de arquivos, é recomendado o uso do sistema NTFS, principalmente em servidores da rede. O sistema de arquivos NTFS apresenta uma série de vantagens relacionadas à segurança, conforme descreverei mais adiante.

**IMPORTANTE:** Algumas das opções nesta etapa podem estar desabilitadas. Por exemplo, se não houver espaço não alocado em, pelo menos, três discos diferentes, a opção RAID-5 estará desabilitada.

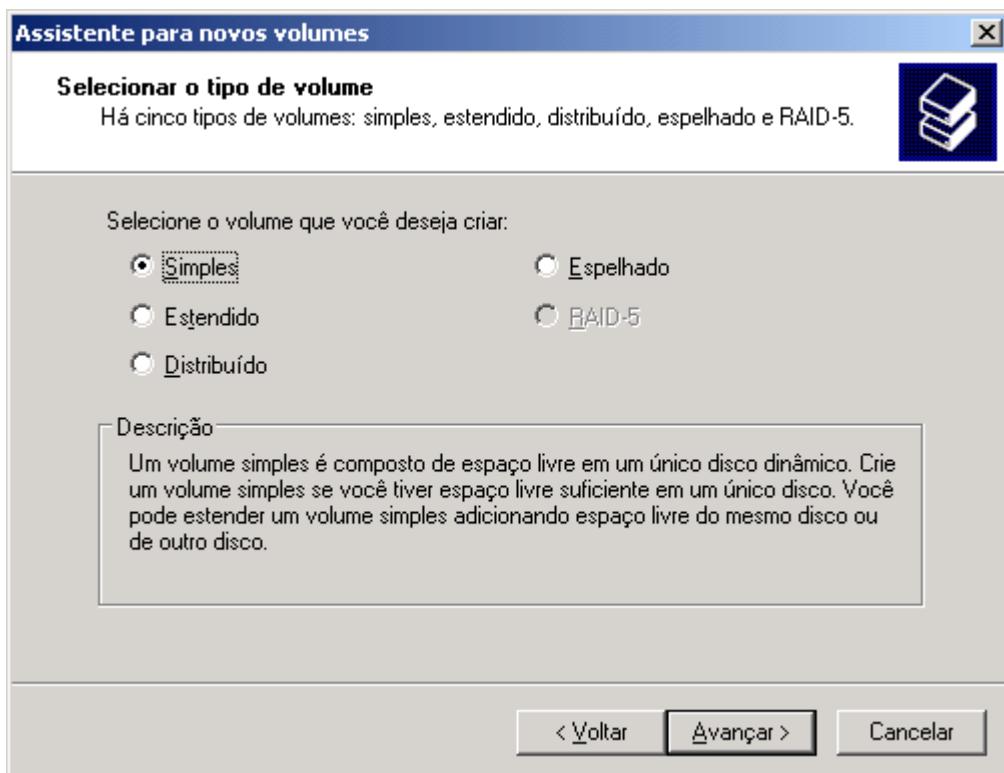


Figura 5.19 Criando um Volume simples.

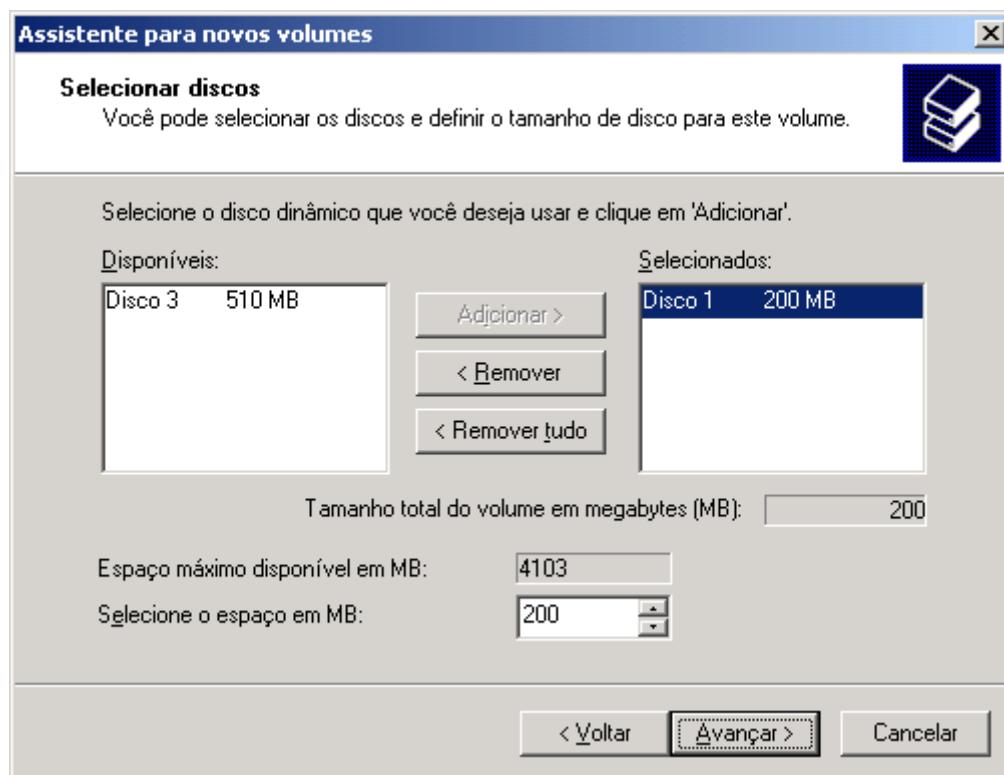
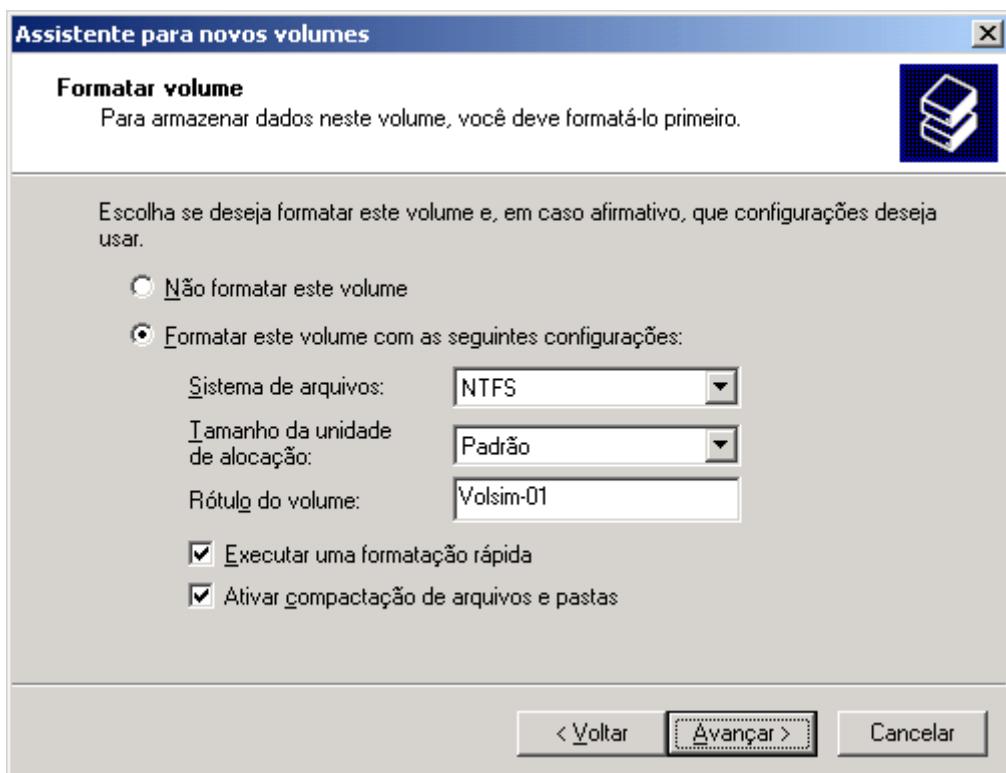


Figura 5.20 Criando um Volume simples de 200 MB no Disco 1.

13. Especifique um tamanho para o volume a ser criado e dê um clique no botão Avançar para ir para a próxima etapa do assistente.

14. Nesta etapa você define uma letra de unidade a ser associada com o volume que está sendo criado. Por padrão o Windows Server 2003 sugere a primeira letra disponível.
15. Aceita a sugestão do Windows Server 2003 e dê um clique no botão Avançar para ir para próxima etapa do assistente.



**Figura 5.21** Especificando as informações para a formatação do volume simples.

16. Nesta etapa você define uma série de detalhes a respeito do volume simples que está sendo criado. Você define se irá formatá-la agora ou não, Qual o sistema de arquivos a ser utilizado. Se vai ou não utiliza compressão de arquivos. Pode ser definido um nome para o volume. Na Figura 5.21 mostro um exemplo onde a partição será formatada, com o sistema de arquivos NTFS, foi mantido o tamanho padrão de unidade de alocação, o nome da unidade foi definido como Volsim-01, foi escolhida uma formatação rápida (Executar uma formatação rápida) e foi habilitada a compactação de arquivos (Ativar compressão de arquivos e pastas).
17. Defina as opções de formatação e dê um clique no botão Avançar, para ir para a tela final do assistente.
18. Na etapa final é exibido um resumo das escolhas feitas nas etapas anteriores. Caso você queira alterar alguma opção, utilize o botão Voltar, para voltar as etapas anteriores e fazer as correções necessárias.
19. Dê um clique no botão Concluir e pronto. Em poucos instantes o Windows Server 2003 terá criado um Volume simples com as opções especificadas, conforme indicado na Figura 5.22:

**NOTA:** Caso você não formate o volume simples no momento de sua criação, é possível formatá-lo facilmente depois. Para isso basta abrir o Meu computador e clicar com o botão direito do mouse na letra do drive associado com o volume não formatado e, no menu que surge, dar um clique na opção Formatar. Surge uma janela com as opções de formatação onde você pode especificar os detalhes para a formatação.

|                |                                     |                        |
|----------------|-------------------------------------|------------------------|
| <b>Disco 1</b> | <b>(D:)</b><br>200 MB<br>Formatação | 3,81 GB<br>Não alocado |
|----------------|-------------------------------------|------------------------|

Figura 5.22 Volume simples de 200 MB, formatado com NTFS.

20. Mantenha o console para Gerenciamento de disco aberto, pois você irá utilizá-lo nos próximos exemplos práticos.

Exemplo: Neste exemplo você aprenderá a expandir um Volume. Expandir o volume significa aumentar o espaço total do volume simples, acrescentando espaços de áreas não alocadas no mesmo disco ou em outros discos disponíveis. Se você expandir o volume simples, através da adição de áreas não alocadas em outro disco, o volume simples torna-se um Spanned Volume (volume expandido que ocupa espaços em dois ou mais discos).

Para expandir um volume simples siga os seguintes passos:

1. Com o console para Gerenciamento de disco ainda aberto, dê um clique com o botão direito do mouse sobre o volume a ser estendido. No menu que surge dê um clique na opção Estender Volume...
2. Será aberto o Assistente para extensão de volumes.
3. A primeira tela é simplesmente informativa, dê um clique no botão Avançar para ir para a próxima etapa do assistente.
4. Na segunda etapa, o Windows Server 2003 exibe informações sobre o espaço não alocado disponível em cada disco do sistema. Por padrão vem adicionado apenas o disco onde está o volume a ser estendido. Você pode adicionar espaço de outros discos disponíveis (Disco 3, na Figura 5.23), usando o botão Adicionar. Porém lembre que, ao usar espaços de outros discos, você transforma o volume simples em um volume do tipo Spanned Volume. Outro detalhe importante é que só são listados os discos dinâmicos. Neste exemplo, não é listado o Disco 2, pois ele ainda é um disco básico. Conforme exemplo da Figura 5.23 estou adicionando mais 150 MB de espaço não alocado.

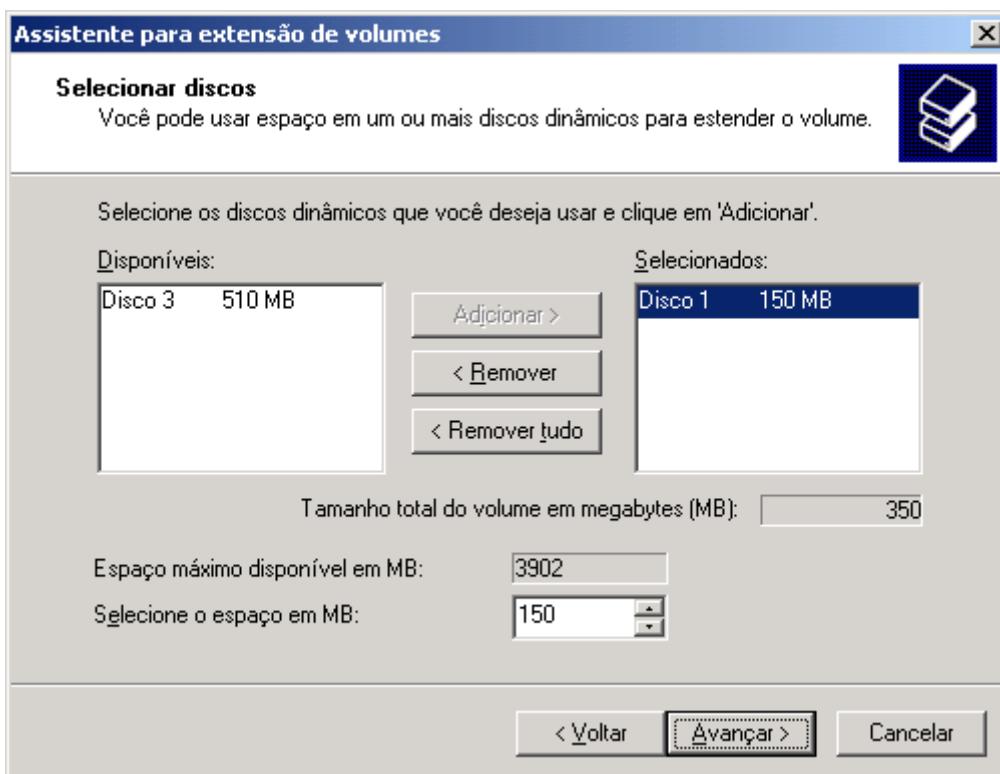


Figura 5.23 Estendendo o volume em mais 150 MB

5. Selecione as opções desejadas e dê um clique no botão Avançar para ir para a tela final do assistente.
6. Na tela final, o Windows Server 2003 exibe as opções escolhidas nos passos anteriores. Caso deseje alterar alguma opção, utilize o botão Voltar.
7. Dê um clique no botão Concluir para estender o volume em mais 150 MB (ou pelo valor que você definiu no passo 4). Com isso o Volume simples (do nosso exemplo) deve estar com 350 MB, 200 da criação original mais 150 MB que foram adicionados, conforme indicado na Figura 5.24:

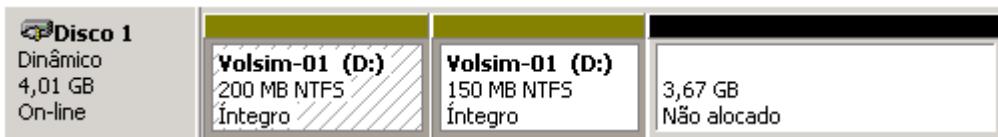


Figura 5.24 Volume Volsim-01 com 350 MB.

8. Feche o console Gerenciamento do computador.

## Criando um volume estendido

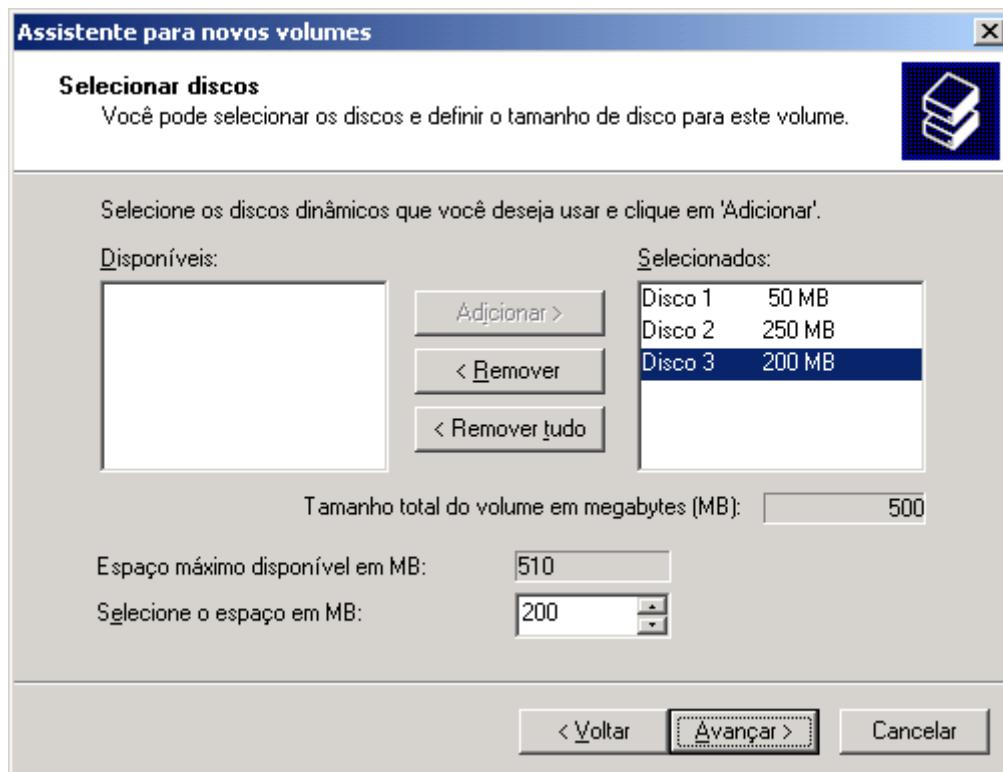
Um Volume estendido em discos de Armazenamento dinâmico, é similar a um Volume set nos discos de Armazenamento básico. Consiste de no mínimo duas e no máximo 32 áreas não de espaço não alocado, em discos diferentes. Pode combinar áreas de diferentes tamanhos. O Windows Server 2003 grava na primeira área até preenchê-la, depois passa para a segunda e assim por diante. Não apresenta tolerância a falhas, pois se uma das áreas apresentar problemas, todo o Volume estendido estará comprometido.

Você pode criar Volumes estendidos através do console Gerenciamento do computador, na opção Armazenamento – Gerenciamento de disco. Para que a opção Volume estendido esteja habilitada, deve existir espaço livre, em pelo menos dois discos de Armazenamento dinâmico.

Exemplo: Para criar um Volume estendido siga os seguintes passos:

1. Faça o logon como Administrador ou com uma conta com permissões de administrador.
2. Abra o console personalizado para Gerenciamento de disco, criado anteriormente.
3. Clique na opção Gerenciamento de disco.
4. Em poucos instantes o Windows Server 2003 exibe as informações sobre os discos instalados no seu computador.
5. Certifique-se de que você possui espaço não alocado em pelo menos dois discos de Armazenamento dinâmico.
6. Clique com o botão direito do mouse em um dos espaços não alocados, e na opção que surge dê um clique em Novo volume...
7. O Windows Server 2003 exibe o Assistente para criação de volumes. A primeira etapa é simplesmente informativa. Dê um clique no botão Avançar para ir para a segunda etapa do Assistente.
8. Na segunda etapa você deve selecionar o tipo de volume a ser criado. Dê um clique na opção Estendido para marca-la. Se não estiver disponível espaço não alocado em, pelo menos, dois discos dinâmicos diferentes, a opção Estendido não estará habilitada. Dê um clique no botão Avançar, para ir para a terceira etapa do Assistente.
9. Nesta tela são exibidos os discos com Armazenamento dinâmico que possuem espaço não alocado, os quais podem ser utilizados para criar o Volume estendido. Você pode utilizar todo o espaço não alocado de cada disco, bem como somente parte dele. Esta tela é dividida em duas colunas. Na coluna da direita estão os discos a partir dos quais você utilizará espaço não alocado. Observe que o disco no qual você clicou com o botão direito do mouse antes de iniciar o assistente, já aparece na coluna Selecionados. Observe também, que existem mais dois

discos com espaço não alocado, os quais podem ser utilizados para criação do Volume estendido. Para adicionar espaço de outros discos basta clicar no disco, na coluna Disponíveis e depois clicar em Adicionar, para incluir o disco na lista Selecionados. Em seguida clique no disco na lista Selecionados para selecioná-lo e defina o espaço que será utilizado deste disco. O espaço é informado no campo Selecione o espaço em MB. Você deve repetir esta operação para definir o espaço a ser utilizado em cada um dos discos que farão parte do Volume expandido. Você pode utilizar diferentes espaços de cada disco. No exemplo da Figura 5-25 vou criar um Volume de 500 MB, no qual utilizo 50 MB do disco 1, 250 do disco 2 e 200 do disco 3.



**Figura 5.25 Especificando as configurações para o Volume estendido de 500 MB.**

10. Dê um clique no botão Avançar, para ir para a próxima etapa do Assistente.
11. Nesta etapa você define a letra que será associada com o volume. Selecione uma das letras disponíveis e dê um clique no botão Avançar, para ir para a próxima etapa do assistente.
12. Nesta etapa você define uma série de detalhes a respeito do volume que está sendo criado. Você define se irá formatá-la agora ou não, Qual o sistema de arquivos a ser utilizado. Se vai ou não utilizar compressão de arquivos. Pode ser definido um nome para o volume. Na Figura 5.26 mostro um exemplo onde o volume será formatado com o sistema de arquivos NTFS, foi mantido o tamanho padrão de unidade de alocação, o nome da unidade foi definido como VolEsp-01, foi escolhida uma formatação rápida e foi habilitada a compactação de arquivos e pastas.
13. Defina as opções de formatação e clique no botão Avançar, para seguir para a próxima etapa do assistente.
14. Será exibida a tela da última etapa do assistente, onde é apresentado um resumo das opções selecionadas. Caso alguma opção esteja incorreta, utilize o botão Voltar.
15. Dê um clique em Concluir para criar o Volume estendido.
16. Em poucos instantes o Windows Server 2003 criará e formatará o Volume, conforme indicado na Figura 5.27:

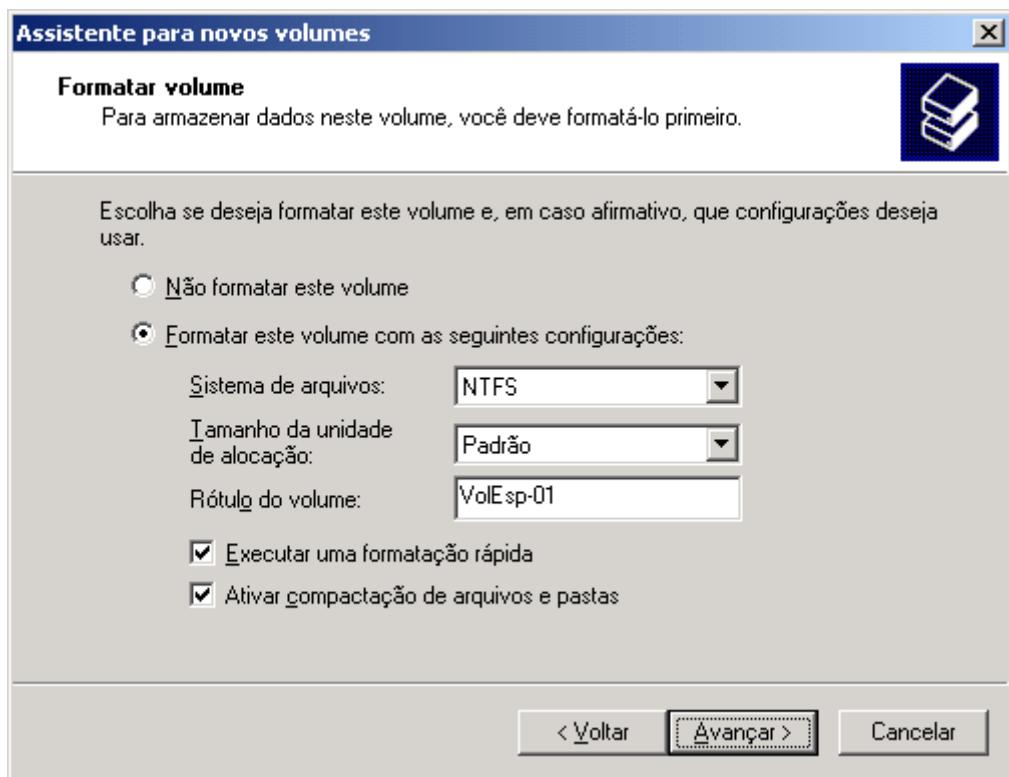


Figura 5.26 Definindo as opções de formatação e a letra de unidade para o volume.

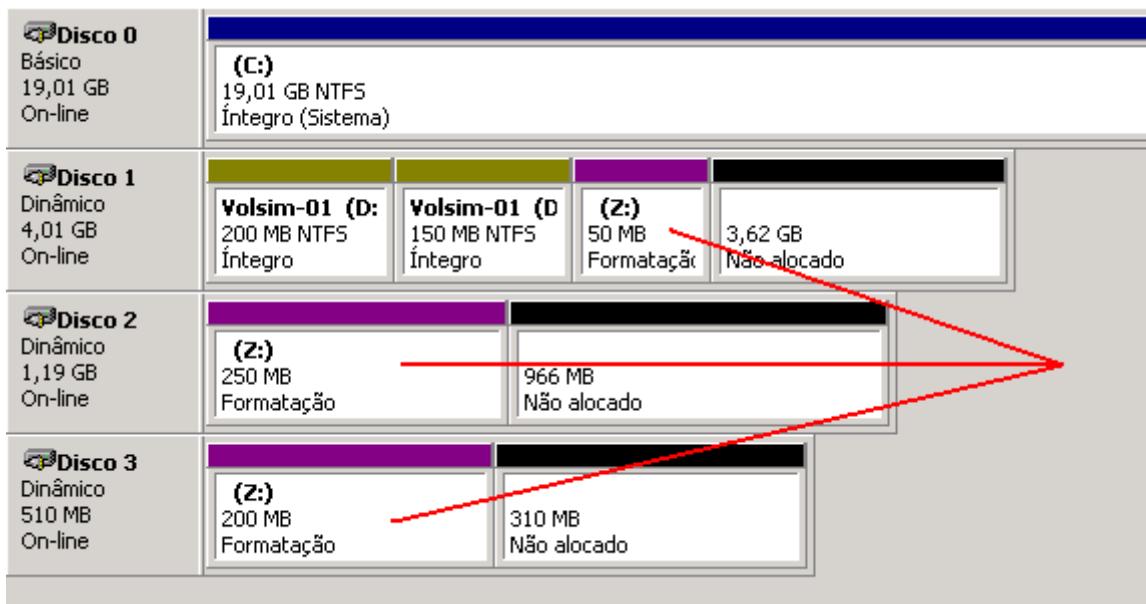


Figura 5.27 Volume estendido (Z:), ocupando espaço em três discos diferentes.

## Criando um striped volume (volume distribuído)

Um Striped volume em discos de Armazenamento dinâmico, é similar a um Striped set sem paridade, nos discos de Armazenamento básico. Consiste de no mínimo duas e no máximo 32 áreas não de espaço não alocado, em discos diferentes. Todas as áreas devem ser do mesmo tamanho (diferente do Spanned Volume, onde podem ser áreas de tamanhos

diferentes). Por exemplo se você tiver 200 MB em um disco e 150 MB em outro disco, o Striped volume somente poderá utilizar 150 MB de cada disco (menor espaço disponível entre os discos participantes). Utilizando 150 MB de cada um dos dois discos, o total ficará em 300 MB. Não apresenta tolerância a falhas, pois se uma das áreas apresentar problemas, todo o Striped volume estará comprometido. Neste caso o volume deve ser excluído, o disco com problemas substituído, o volume deve ser recriado e os dados restaurados a partir de uma cópia de segurança (Backup).

Você pode criar Volumes estendidos através do console Gerenciamento do computador, na opção Armazenamento – Gerenciamento de disco ou diretamente através do console personalizado que foi criado no início deste item. Para que a opção Striped volume esteja habilitada, devemos ter espaço livre, em pelo menos dois discos de Armazenamento dinâmico.

Exemplo: Para criar um Striped volume siga os seguintes passos:

1. Faça o logon como Administrador ou com uma conta com permissões de administrador.
2. Abra o console personalizado para Gerenciamento de disco, criado anteriormente.
3. Clique na opção Gerenciamento de disco.
4. Em poucos instantes o Windows Server 2003 exibe as informações sobre os discos instalados no seu computador.
5. Certifique-se de que você possui espaço não alocado em pelo menos dois discos de Armazenamento dinâmico.
6. Clique com o botão direito do mouse em um dos espaços não alocados, e na opção que surge dê um clique em Novo Volume...
7. O Windows Server 2003 exibe o Assistente para criação de volumes. A primeira tela é somente informativa. Dê um clique no botão Avançar para ir para a segunda tela do Assistente.
8. Na tela que surge, marque a opção Distribuído, depois dê um clique no botão Avançar, para ir para a próxima etapa do Assistente.

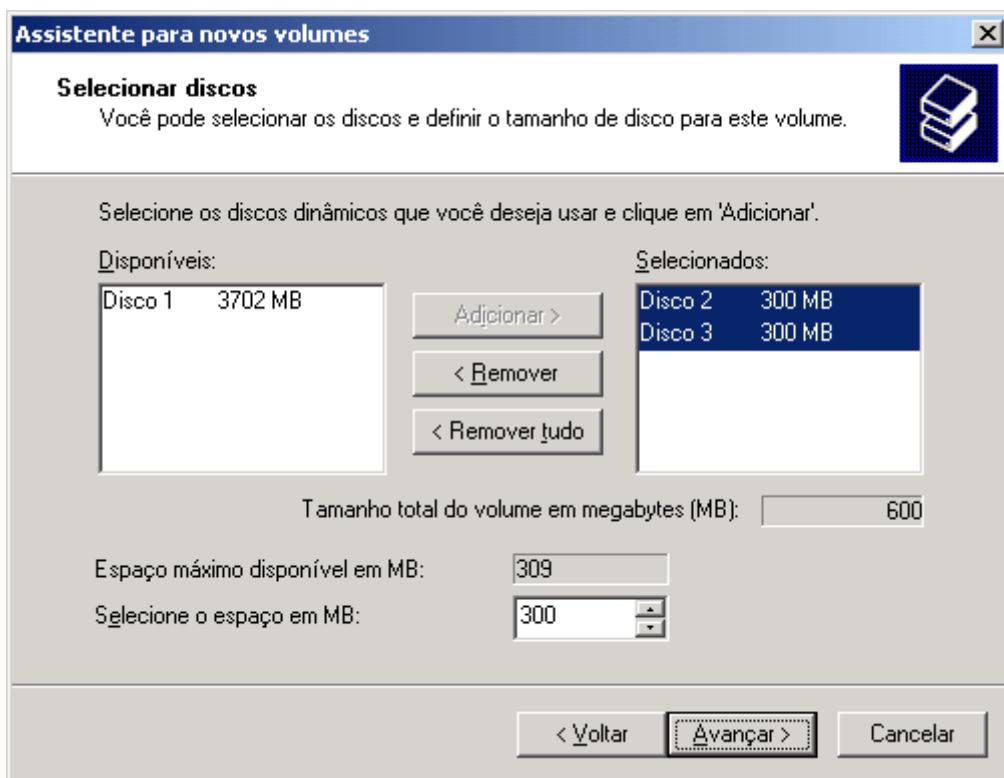
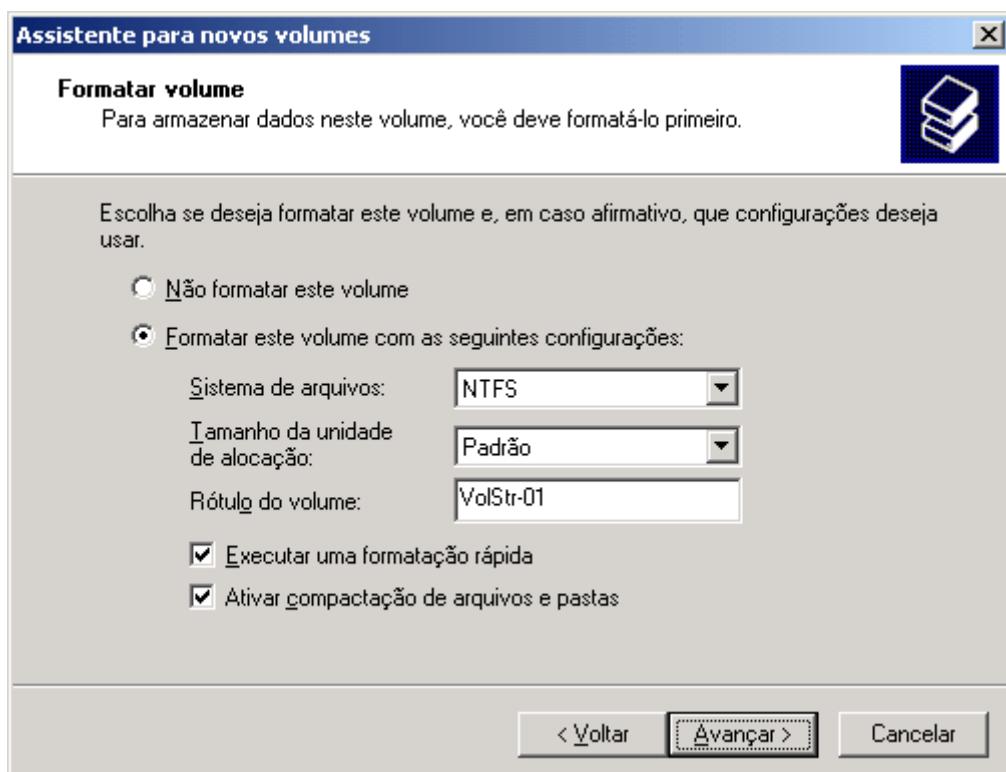


Figura 5.28 Criando um Striped Volume de 600 MB – 300 MB do disco 2 + 300 MB do disco 3.

9. Nesta tela são exibidos os discos com Armazenamento dinâmico que possuem espaço não alocado, os quais podem ser utilizados para criar o Striped Volume (Volume distribuído). Você pode utilizar todo o espaço não alocado de cada disco, bem como somente parte dele. Esta tela é dividida em duas colunas. Na coluna da direita estão os discos a partir dos quais você utilizará espaço não alocado. Observe que o disco no qual você clicou com o botão direito do mouse antes de iniciar o assistente, já aparece na coluna Selecionados. Observe também, que existem mais dois discos com espaço não alocado, os quais podem ser utilizados para criação do Volume distribuído. Para adicionar espaço de outros discos basta clicar no disco, na coluna Disponíveis e depois clicar em Adicionar, para incluir o disco na lista Selecionados (você também pode dar um clique duplo no disco, na coluna Disponíveis, para incluí-lo na coluna Selecionados). Em seguida clique no disco na lista Selecionados para selecioná-lo e defina o espaço que será utilizado deste disco. O espaço é informado no campo Selecione o espaço em MB. Você deve repetir esta operação para definir o espaço a ser utilizado em cada um dos discos que farão parte do Striped Volume, lembrando que deve ser utilizada a mesma quantidade de espaço de cada disco.. No exemplo da Figura 5-28 vou criar um Striped Volume de 600 MB, no qual utilizei 300 MB do disco 2 e 300 MB do disco 3 (espaços iguais de cada disco).
10. Defina as configurações para o volume e dê um clique no botão Avançar, para ir para a próxima etapa do Assistente.
11. Nesta etapa você define uma letra de Unidade associada com o Volume estendido. Selecione uma das letras disponíveis e dê um clique no botão Avançar, para ir para a próxima etapa do assistente.
12. Nesta etapa você define uma série de detalhes a respeito do volume que está sendo criado. Você define se irá formatá-la agora ou depois, qual o sistema de arquivos a ser utilizado (FAT ou NTFS). Se vai ou não utilizar compressão de arquivos. Pode ser definido um nome para o volume. Na Figura 5.29 mostro um exemplo onde o volume será formatado com o sistema de arquivos NTFS, foi mantido o tamanho padrão de unidade de alocação, o nome da unidade foi definido como VolStr-01, foi escolhida uma formatação rápida e foi habilitada a compactação de arquivos.



**Figura 5.29 Definindo as opções de formatação para o volume.**

13. Defina as opções de formatação e clique no botão Avançar, para seguir para a etapa final do assistente.
14. Na etapa final é apresentado um resumo das opções selecionadas. Caso alguma opção esteja incorreta, utilize o botão Voltar.
15. Dê um clique em Concluir para criar o Striped volume.
16. Em poucos instantes o Windows Server 2003 criará e formatará o Striped volume, conforme indicado na Figura 5.30:

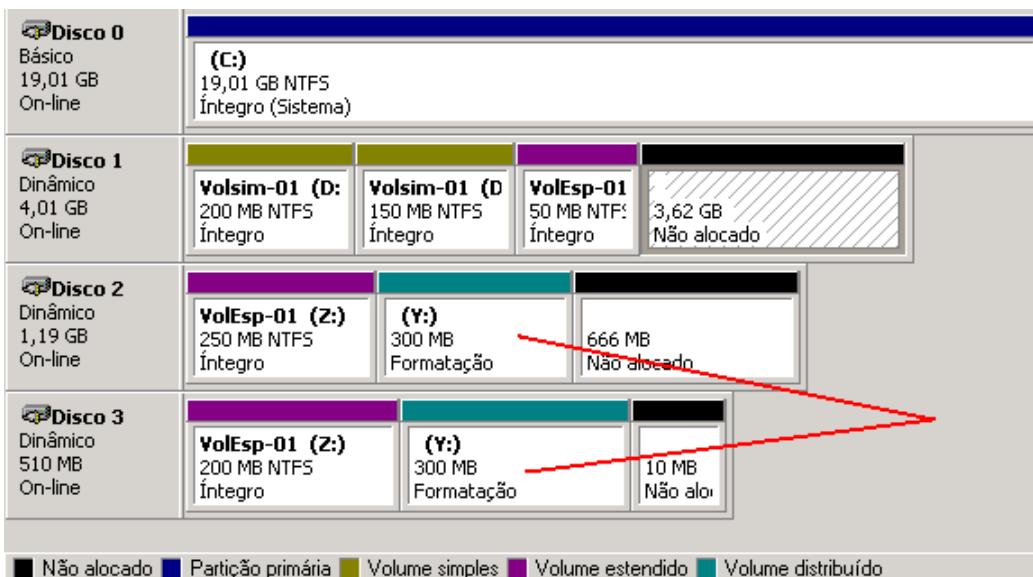


Figura 5.30 Striped Volume (Y:), ocupando espaços iguais em dois discos diferentes.

## Criando um volume RAID-5

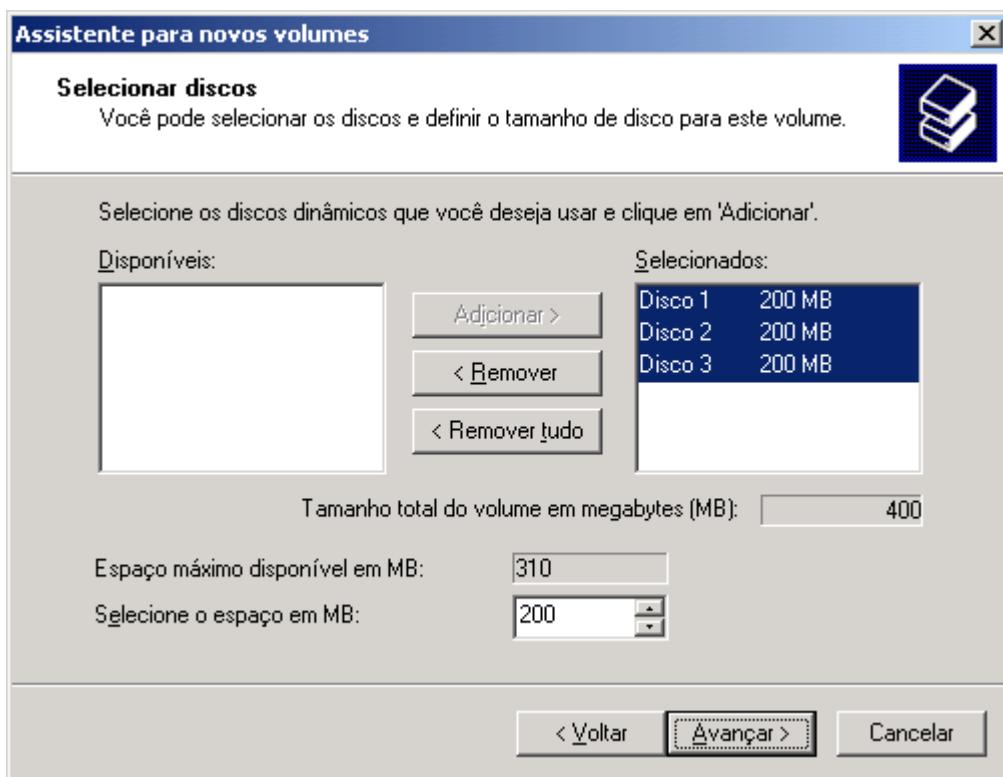
Um Volume RAID-5, em discos de Armazenamento dinâmico, é similar a um Striped set com paridade, nos discos de Armazenamento básico. Consiste de no mínimo três e no máximo 32 áreas de espaço não alocado, em discos diferentes. Todas as áreas devem ser do mesmo tamanho. Por exemplo se você tiver 200 MB em um disco e 150 MB em outro disco, e finalmente 100 MB em um terceiro disco o Volume RAID-5 somente poderá utilizar 100 MB de cada disco (menor espaço disponível entre os discos participantes). Utilizando 100 MB de cada um dos dois discos, o total ficará em 200, pois um terço do espaço (no caso de três discos), 100 MB, será utilizado para as informações de paridade, o que garante a tolerância a falhas, no caso de um dos discos apresentar problemas.

Você pode criar Volumes RAID-5 através do console Gerenciamento do computador, na opção Armazenamento – Gerenciamento de disco ou pode utilizar o console personalizado Gerenciamento de disco, criado no início deste tópico. Para que a opção Volume RAID-5 esteja habilitada, deve haver espaço livre em, pelo menos, três discos de Armazenamento dinâmico.

Exemplo: Para criar um Volume RAID-5 siga os seguintes passos:

1. Faça o logon como Administrador ou com uma conta com permissões de administrador.
2. Abra o console personalizado para Gerenciamento de disco, criado anteriormente.
3. Clique na opção Gerenciamento de disco.
4. Em poucos instantes o Windows Server 2003 exibe as informações sobre os discos instalados no seu computador.
5. Certifique-se de que você possui espaço não alocado em pelo menos três discos de Armazenamento dinâmico.
6. Clique com o botão direito do mouse em um dos espaços não alocados, e na opção que surge dê um clique em Novo Volume...

7. O Windows Server 2003 exibe o Assistente para criação de volumes. A primeira tela é somente informativa. Dê um clique no botão Avançar para ir para a segunda tela do Assistente.
8. Na tela que surge, marque a opção RAID-5, depois dê um clique no botão Avançar, para ir para a próxima etapa do Assistente.
9. Nesta tela são exibidos os discos com Armazenamento dinâmico que possuem espaço não alocado, os quais podem ser utilizados para criar o volume do tipo RAID-5. Você pode utilizar todo o espaço não alocado de cada disco (desde que o espaço não alocado seja o mesmo em cada disco), bem como somente parte dele. Esta tela é dividida em duas colunas. Na coluna da direita estão os discos a partir dos quais você utilizará espaço não alocado. Observe que o disco no qual você clicou com o botão direito do mouse, antes de iniciar o assistente, já aparece na coluna Selecionados. Observe também, que existem mais dois discos com espaço não alocado, os quais podem ser utilizados para criação do Volume estendido. Para adicionar espaço de outros discos basta clicar no disco, na coluna Disponíveis e depois clicar em Adicionar, para incluir o disco na lista Selecionados. Em seguida clique no disco na lista Selecionados para selecioná-lo e defina o espaço que será utilizado deste disco. O espaço é informado no campo Selecione o espaço em MB. Ao definir o espaço utilizado em um dos discos, o mesmo espaço será definido nos demais discos da coluna Selecionados. No exemplo da Figura 10-31 vou criar um RAID-5 de 600 MB, no qual utilize 200 MB de cada um dos discos: Disco 1, Disco 2 e Disco 3 (espaços iguais). Na prática, o espaço disponível será de 400 MB, pois 200 MB serão utilizados para gravar as informações de paridade, que é o que propicia a tolerância à falhas no caso da perda de um dos discos.



**Figura 5.31 Criando um Striped Volume de 600 MB – 200 MB de cada disco.**

10. Defina as configurações para o volume e dê um clique no botão Avançar, para ir para a próxima etapa do Assistente.
11. Nesta etapa você define uma letra de Unidade associada com o Volume estendido. Selecione uma das letras disponíveis e dê um clique no botão Avançar, para ir para a próxima etapa do assistente.
12. Nesta etapa você define uma série de detalhes a respeito do volume que está sendo criado. Você define se irá formatá-la agora ou depois, qual o sistema de arquivos a ser utilizado (FAT ou NTFS). Se vai ou não utilizar compressão de

arquivos. Pode ser definido um nome para o volume. Na Figura 5.32 mostro um exemplo onde o volume será formatado com o sistema de arquivos NTFS, foi mantido o tamanho padrão de unidade de alocação, o nome da unidade foi definido como VolRaid-05, foi escolhida uma formatação rápida e não foi habilitada a compactação de arquivos.

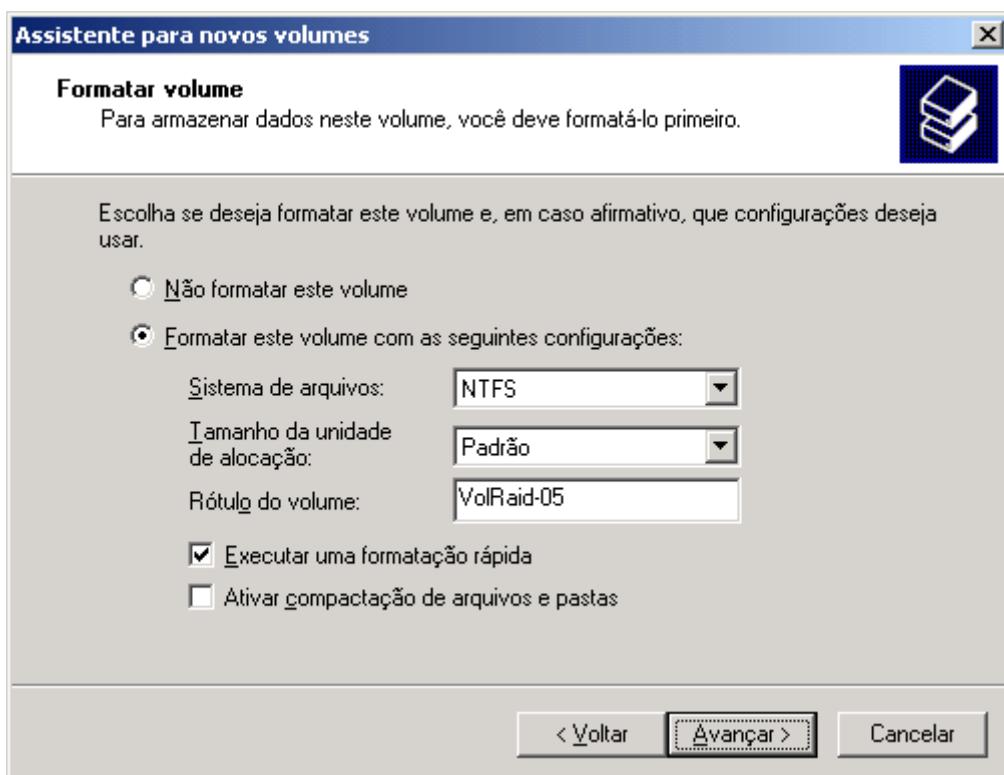


Figura 5.32 Definindo as opções de formatação para o volume.

13. Defina as opções de formatação e clique no botão Avançar, para seguir para a etapa final do assistente.
14. Na etapa final é apresentado um resumo das opções selecionadas. Caso alguma opção esteja incorreta, utilize o botão Voltar.
15. Dê um clique em Concluir para criar o volume RAID-5.
16. Em poucos instantes o Windows Server 2003 criará e formatará o volume RAID-5, conforme indicado na Figura 5.33:

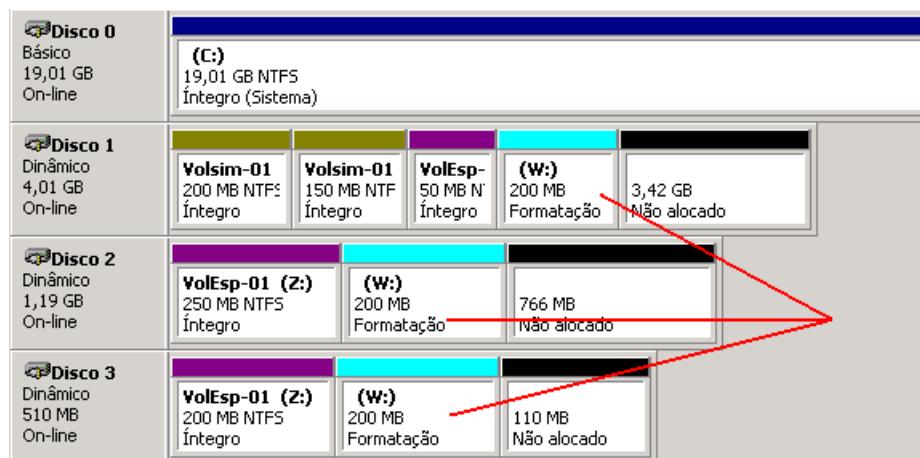


Figura 5.33 Volume RAID-5 (S:), ocupando espaços iguais em três discos diferentes.

## Criando um volume espelhado

Um Volume espelhado, em discos de Armazenamento dinâmico, é similar a um Disk mirror, nos discos de Armazenamento básico. Consiste de dois volumes do mesmo tamanho, em discos diferentes, sendo que um é a cópia fiel (espelho) do outro. Por exemplo se você tiver um Volume simples de 300 MB que deseja espelhar, preciso de um espaço não alocado de, no mínimo, 300 MB em um outro disco.

Você pode criar Volumes espelhados através do console Gerenciamento do computador, na opção Armazenamento – Gerenciamento de disco. Para que a opção Volume espelhado esteja habilitada, deve haver espaço livre, em pelo menos um disco de Armazenamento dinâmico.

Exemplo: Para criar um Volume espelhado siga os seguintes passos:

1. Faça o logon como Administrador ou com uma conta com permissões de administrador.
2. Abra o console personalizado para Gerenciamento de disco, criado anteriormente.
3. Clique na opção Gerenciamento de disco.
4. Em poucos instantes o Windows Server 2003 exibe as informações sobre os discos instalados no seu computador.
5. Certifique-se de que você possui espaço não alocado em pelo menos um disco diferente do disco onde está o volume que você deseja espelhar.
6. Clique com o botão direito do mouse no Volume a ser espelhado e no menu que surge dê um clique na opção Adicionar espelho...
7. O Windows Server 2003 exibe uma janela, onde são exibidos os discos com espaço não alocado suficiente para fazer o espelhamento, conforme indicado na Figura 5.34:

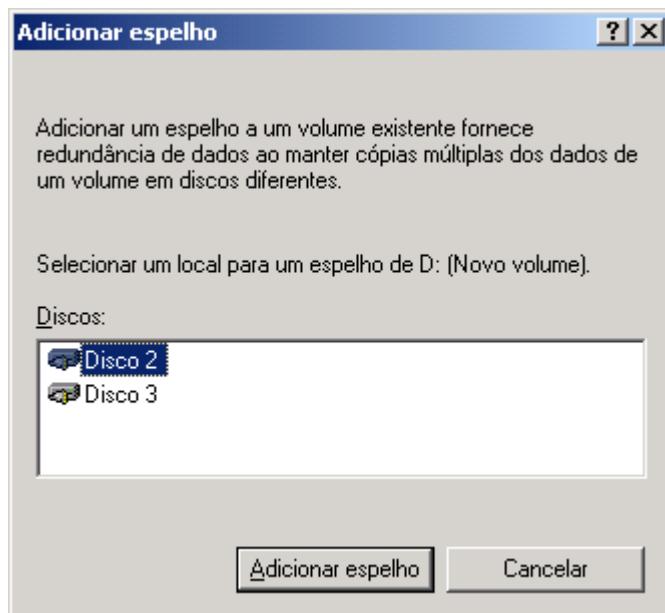


Figura 5.34 Selecionando o disco onde será feito o espelhamento.

8. Clique no disco onde será feito o espelhamento e clique em Adicionar espelho.
9. Dependendo do tamanho e da quantidade de dados do Volume que está sendo espelhado, a operação pode demorar alguns minutos. Depois disso o Volume espelhado passa a ser exibido no console de Gerenciamento de disco, conforme indicado na Figura 5.35:



**Figura 5.35 Volume espelhado recém criado.**

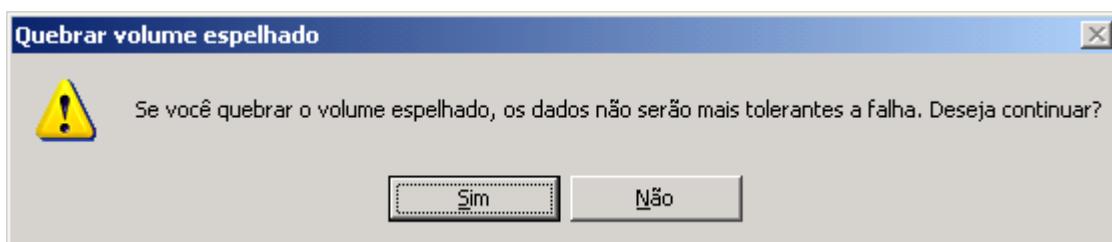
Pronto, o volume foi espelhado e os dados duplicados no segundo disco. O Windows Server 2003 mantém o espelho sempre atualizado, ou seja, quando são feitas alterações no volume original, estas são também efetuadas no volume espelhado.

## Restabelecendo um volume do tipo mirror (espelhado)

Pode acontecer de um dos discos onde está o espelhamento apresentar falhas. Por exemplo, uma falha física que compromete todo o disco. Neste caso existem alguns passos que devem ser efetuados para que o Mirror (Espelhamento) possa ser restabelecido, conforme descrito a seguir.

Passos para restabelecer um espelhamento:

1. Quebrar o espelhamento. Para isso basta acessar o console de Gerenciamento de discos, clicar com o botão direito do mouse em uma das partes do espelhamento (de preferência na parte que está no disco bom, sem problemas). No menu que é exibido clique em Quebrar o Volume espelhado...
2. Surge uma mensagem avisando que se o espelhamento for quebrado não haverá mais tolerância a falhas, conforme indicado na Figura 5.36:



**Figura 5.36 Confirmando a quebra do espelhamento.**

3. Clique em Sim para confirmar a quebra do espelhamento.
4. Desligue o servidor e substitua o disco com defeito.
5. Reinicie o servidor e faça o espelhamento novamente, usando espaço não alocado no novo disco. Pronto, o espelhamento será restabelecido e novamente haverá tolerância à falhas, no caso de falha de um dos discos.

## Restabelecendo um volume do tipo RAID-5

Pode acontecer de um dos discos onde compõem um volume RAID-5, falhar. Por exemplo, uma falha física que compromete todo o disco. Neste caso existem alguns passos que devem ser efetuados para que o RAID-5 possa ser restabelecido, conforme descrito a seguir.

Passos para restabelecer um volume do tipo RAID-5:

1. Desligue o servidor e substitua o disco com defeito.
2. Reinicialize o servidor, acesse o console de Gerenciamento de disco. Clique com o botão direito do mouse no volume RAID-5 e no menu de opções que é exibido clique em Reativar Volume. Surge uma mensagem de aviso informando que é recomendado o uso do comando chkdsk no volume que está sendo reativado. O comando chkdsk é utilizado para detectar erros em um volume e será explicado mais adiante.
3. Clique em OK para fechar esta mensagem.
4. O volume será reativado e o status mudará de failed redundancy (Falha na redundância) para Resynching (resincronizando) e depois para Healthy (algo parecido com saudável, com saúde, disponível).
5. Pronto, o RAID-5 foi restabelecido e com tolerância a falhas. É importante salientar que mesmo durante a falha de um dos discos, o volume RAID-5 continua disponível para ser utilizado, porém sem fornecer tolerância a falha, uma vez que se mais um disco falhar (enquanto o primeiro ainda não foi substituído), os dados serão perdidos, aí só restaurando a partir do Backup. Quando um volume RAID-5 apresenta falha em um dos discos e continua sendo utilizado, o desempenho cai muito, a velocidade de acesso fica muito prejudicada.

## Configurações e personalizações do snap-in gerenciamento de discos

Você pode personalizar diversas configurações do console Disk Management (Gerenciamento de discos). É possível definir a cor associada com cada tipo de partição/volume, a escala de exibição e outros aspectos da interface do console Gerenciamento de discos.

Para definir a cor associada com cada tipo de partição/volume e também a escala de exibição, siga os seguintes passos:

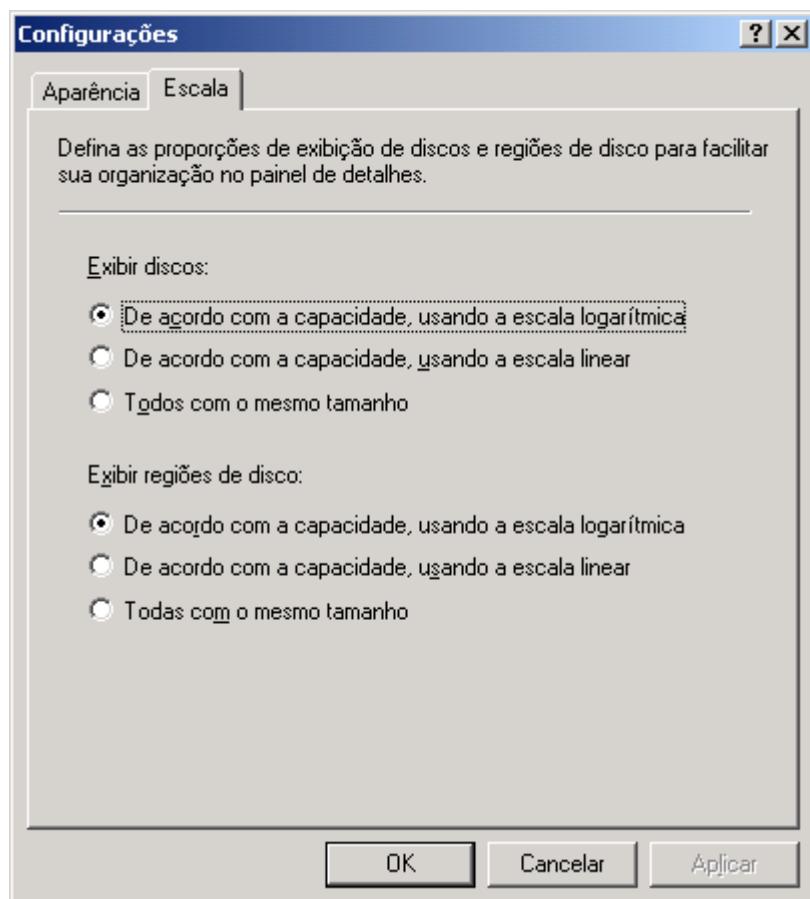
1. Abra o console personalizado Gerenciamento de discos, criado anteriormente.
2. Selecione o comando Exibir -> Configurações...
3. Será exibida a janela. Esta janela tem duas guias:
  - ◆ **A guia Aparência:** Nesta guia você define a cor associada com cada tipo de partição/volume. Para definir a cor, dê um clique no tipo de volume/partição e depois selecione a cor desejada. Você também pode definir um padrão de preenchimento tal como sólido, linhas cruzadas, linhas inclinadas, etc.
  - ◆ **A guia Escala:** Nesta guia, indicada na Figura 5.37, estão disponíveis as seguintes opções:

No grupo Exibir discos estão disponíveis as opções que definem a exibição do tamanho do disco com um todo, independente dos volumes/partições definidos no disco. Neste grupo temos as seguintes opções:

- ◆ **De acordo com a capacidade, usando a escala logarítmica:** Exibe discos usando uma escala logarítmica de acordo com a capacidade de cada disco. Use Logarítmica se você gerenciar discos de tamanhos variados e muito diferentes como por exemplo um disco de 2 GB e um de 40 GB.
- ◆ **De acordo com a capacidade, usando a escala linear:** Exibe cada disco com base em seu tamanho em relação ao maior disco. Use Linear se você gerenciar discos de tamanhos semelhantes. Por exemplo, se você tem um disco de 500 MB e um disco de 40 GB e selecionar Linear, o disco de 500 MB quase não será visível. Se você selecionar Logarítmica, os discos serão exibidos proporcionalmente.
- ◆ **Todos com o mesmo tamanho:** Exibe cada tamanho de disco igualmente, independentemente da capacidade do disco.

No grupo Exibir regiões de disco, estão disponíveis opções que definem a exibição do tamanho de cada volume/partição em relação ao tamanho total do respectivo disco. Neste grupo estão disponíveis as seguintes opções:

- ◆ **De acordo com a capacidade, usando a escala logarítmica:** Exibe volumes usando a escala logarítmica de acordo com a capacidade de cada volume. Use Logarítmica se você gerenciar volumes de tamanhos variados e muito diferentes como por exemplo um volume de 500 MB e um de 10 GB.



**Figura 5.37 A guia Escala.**

- ◆ **De acordo com a capacidade, usando a escala linear:** Exibe cada volume com base em seu tamanho em relação ao maior volume. Use Linear se você gerenciar volumes de tamanhos semelhantes. Por exemplo, se você tem um volume de 500 MB e um volume de 40 GB e selecionar Linear, o volume de 500 MB quase não será visível. Se você selecionar Logarítmica, os volumes serão exibidos proporcionalmente. De acordo com a capacidade, usando a escala linear:
- ◆ **Todos com o mesmo tamanho:** Exibe cada tamanho de volume igualmente, independentemente da capacidade do volume

Selecione as opções desejadas e dê um clique no botão OK para aplicá-las.

O comando Exibir -> Personalizar... abre a janela Personalizar Exibição, conforme indicado na Figura 5.38. Nesta janela você pode definir quais elementos do console Gerenciamento de discos serão exibidos e quais ficarão ocultos. Selecione as opções desejadas e clique em OK.

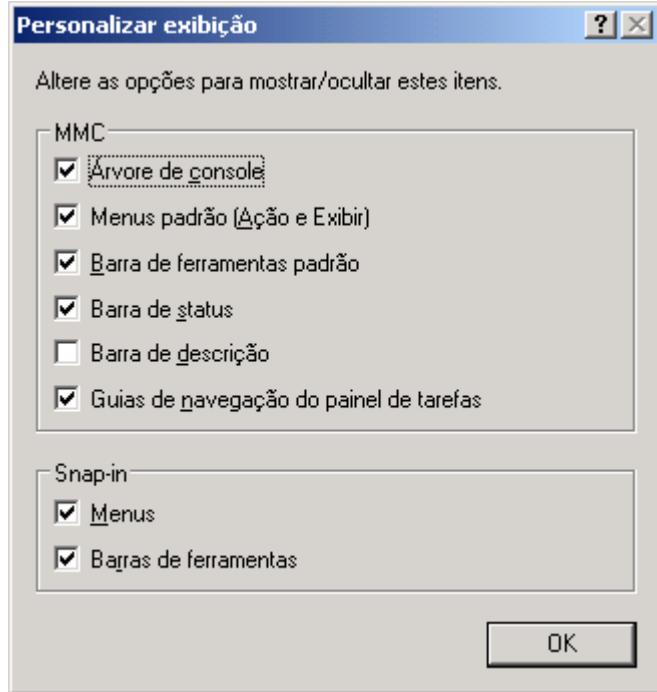


Figura 5.38 A janela Customize Personalizar Exibição.

## Ferramentas Para Manutenção de Discos e Volumes

Neste tópico apresentarei uma série de ferramentas e comandos para a manutenção, verificação de erros e otimização de discos e volumes.

### O conceito de fragmentação

A medida que arquivos vão sendo gravados, eliminados e alterados em um volume ou partição, pode ocorrer um processo conhecido como fragmentação. O Windows Server 2003 grava as informações de um arquivo em “pedaços/incrementos” chamados cluster. O cluster é a menor unidade de informação que pode ser gravada ou lida de um disco rígido. Por exemplo, imagine que um determinado volume ou partição possuí um cluster de 8 KB. Ao gravar um arquivo de 1 KB, este arquivo irá comprometer todo um cluster, mesmo que não utilize todo o espaço do cluster. Isso acaba acarretando desperdício do espaço de armazenamento do disco rígido.

Para entender o que vem a ser a fragmentação, considere o seguinte. Suponha que existe uma arquivo de 20 KB gravado no disco rígido. Para 20 KB, serão necessários alocar 3 cluster (supondo um cluster de 8 KB). Ao excluir este arquivo de 20 KB, os 3 cluster por ele alocados, serão liberados. Agora vamos supor que você vá gravar um arquivo de 160 KB. Serão necessários 20 cluster (ainda supondo um cluster de 8 KB). O Windows Server 2003 utilizará os três cluster livres, depois procura por mais espaço livre no restante do disco. Com isso você pode notar que os clusters que formam o arquivo de 160 KB, não estão necessariamente gravados em regiões contínuas do disco, podendo, dependendo do tamanho do arquivo, estar espalhados por diversas regiões do disco. Este processo, em que diferentes clusters de um arquivo estão em regiões separadas do disco, é conhecido como Fragmentação. A medida que o Windows Server 2003 vai gravando, eliminando e alterando arquivos, a Fragmentação vai aumentando, podendo chegar a níveis que comprometem o desempenho das operações de leitura e escrita no disco. Para solucionar este problema existe um utilitário de “Desfragmentação”, o qual deve ser utilizado para minimizar, se não eliminar, a fragmentação em volumes.

e partições. O Processo de desfragmentação, simplesmente procura “juntar” as diversas partes de cada arquivo, de tal forma que o desempenho no acesso ao disco seja otimizado.

Na documentação do Windows Server 2003, encontramos a seguinte definição de cluster: “É a menor quantidade de espaço em disco que pode ser alocada para manter um arquivo. Todos os sistemas de arquivos usados pelo Windows organizam discos rígidos com base em clusters, que consistem em um ou mais setores contíguos. Quanto menor o tamanho de cluster utilizado, mais eficiente será o armazenamento de informações no disco. Se nenhum tamanho de cluster for especificado durante a formatação, o Windows assumirá os padrões com base no tamanho do volume. Esses padrões são selecionados para reduzir a quantidade de espaço perdido e a quantidade de fragmentação no volume. Um cluster também é chamado de unidade de alocação.”

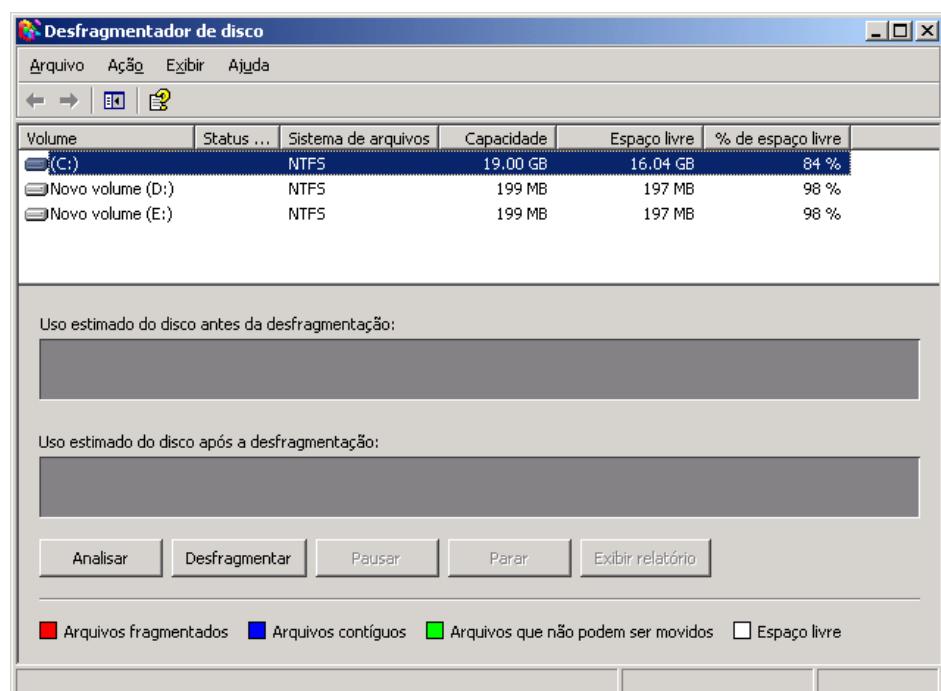
## O utilitário de desfragmentação

O utilitário de Desfragmentação do Windows Server 2003, permite que seja feita uma análise no volume ou partição. Com base na análise, o utilitário recomenda ou não que o processo de desfragmentação seja executado. Como regra geral, somente devemos desfragmentar um volume ou partição, quando isto for indicado pelo utilitário de desfragmentação. O utilitário de desfragmentação do Windows Server 2003 está bem melhor do que nas versões anteriores.

Agora vamos aprender a utilizar este utilitário.

Exemplo: Para analisar e desfragmentar um volume ou partição, faça o seguinte:

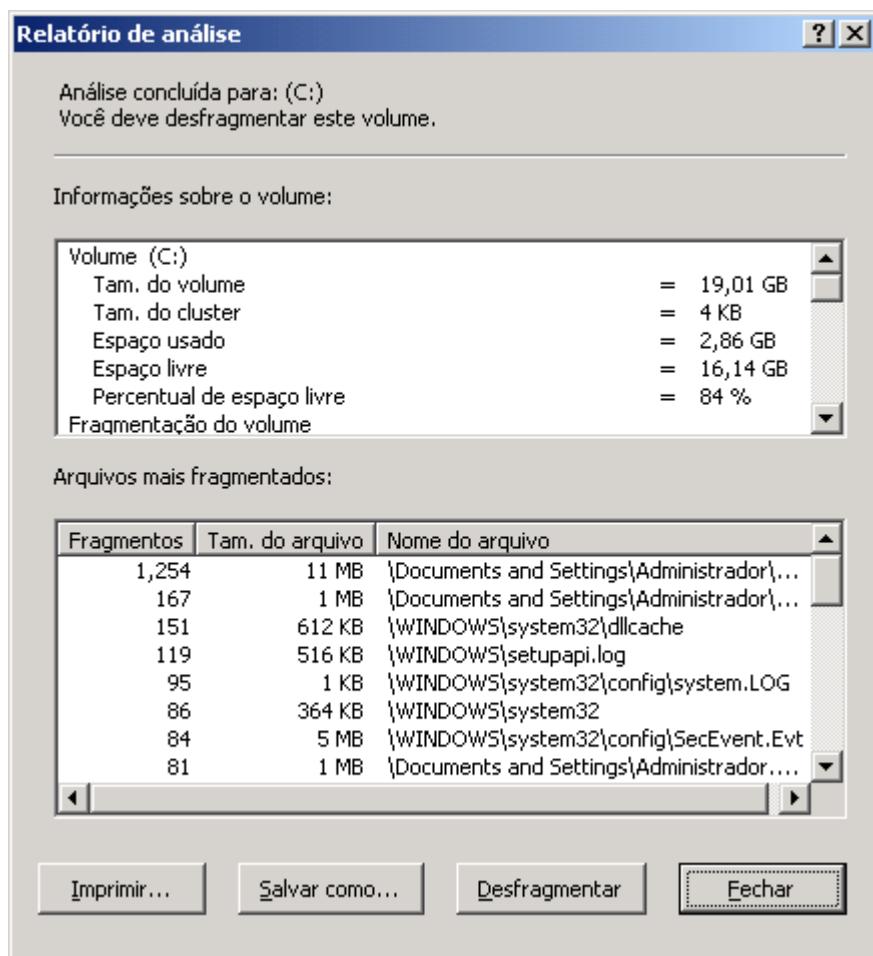
1. Faça o logon como administrador ou com uma conta do tipo Administrador do computador.
2. Selecione o comando Iniciar -> Todos os programas -> Acessórios -> Ferramentas do sistema -> Desfragmentador de disco.
3. Será aberto o utilitário para a desfragmentação de unidades, conforme indicado pela Figura 5.39:



**NOTA:** Você também pode acessar o Desfragmentador de disco utilizando o Meu computador ou o Windows Explorer. Localize o drive (C:, D:, etc.) a ser desfragmentado, clique com o botão direito do mouse no referido drive e no menu que surge dê um clique na opção Propriedades. Será exibida a janela de propriedades do drive, com a guia Geral selecionada. Dê um clique na guia Ferramentas e nesta guia, dê um clique no botão Desfragmentar agora... Você também pode abrir as propriedades de um drive, utilizando o console Gerenciamento de discos. Neste console, clique com o botão direito do mouse no volume correspondente ao drive a ser desfragmentado. No menu de opções que surge, dê um clique na opção Propriedades. Será aberta a mesma janela de propriedades descrita no início deste parágrafo.

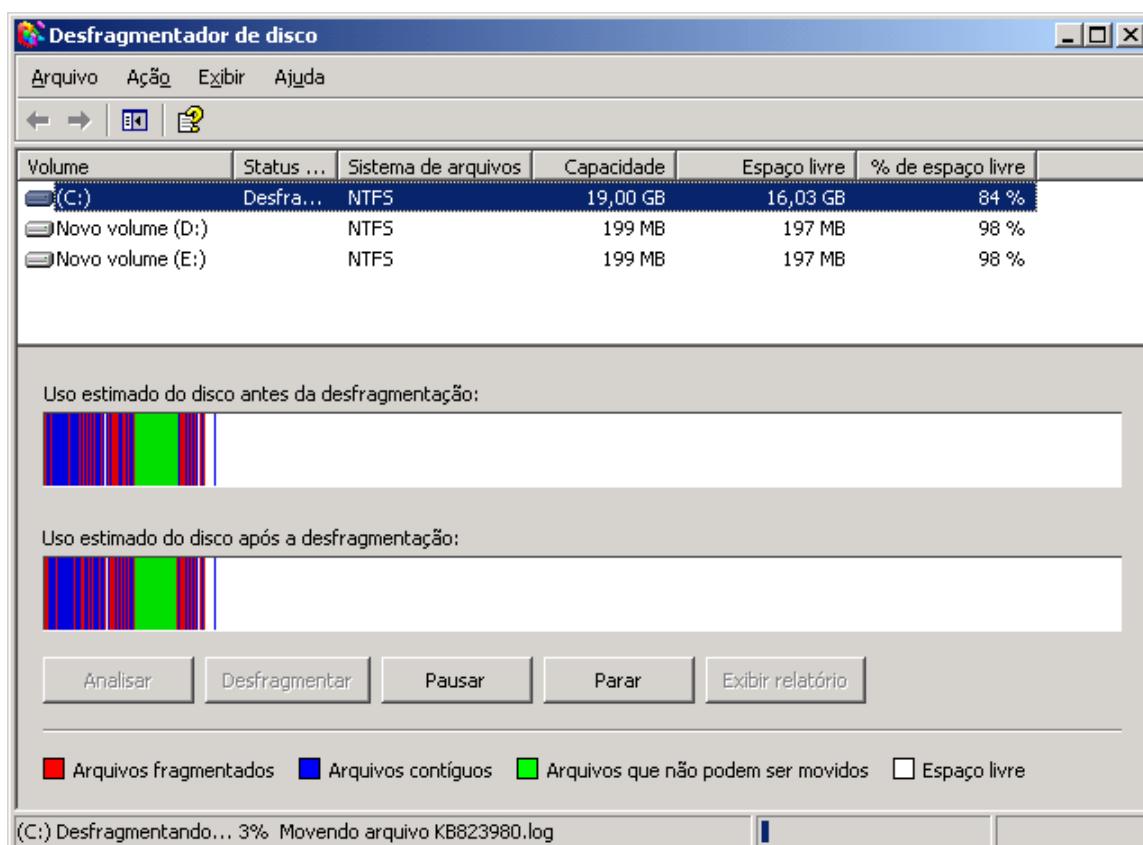
Figura 5.39 O utilitário para desfragmentação de volumes e partições.

- Na parte de cima da janela, é exibida uma listagem com as unidades (volumes) disponíveis. Na parte de baixo é exibida a legenda, bem como os botões para ações tais como: Analisar, Desfragmentar, Pausar, Parar e Exibir relatório. Na parte do meio, é exibido um indicativo do andamento dos processos de Análise e Desfragmentação, quando um destes processos estiverem em andamento.
- Para analisar o drive C:, dê um clique para marcá-lo e depois dê um clique no botão Analisar. O Windows Server 2003 inicia o processo de análise.
- Após terminar a análise, o Windows 2000 Server exibe uma janela informando se a desfragmentação é ou não recomendada. Nesta janela, está disponível um botão Exibir relatório. O relatório fornece uma série de detalhes sobre a unidade analisada, conforme exemplo indicado pela Figura 5.40:



**Figura 5.40 Relatório informando se o volume deve ou não ser desfragmentado.**

- Dê um clique no botão Desfragmentar, para iniciar o processo de desfragmentação.
- O Windows Server 2003 mostra o andamento da desfragmentação, conforme indicado na Figura 5.41.
- O processo de desfragmentação pode demorar bastante tempo, dependendo do tamanho da unidade e da porcentagem de fragmentação. Além disso a unidade sendo desfragmentada não deve ter atividades de leitura e gravação, pois isso pode atrasar ainda mais o processo. O ideal é que a desfragmentação seja feita fora do horário normal de serviço, ou até mesmo agendada para rodar em horários específicos, utilizando o Agendamento de tarefas do Windows Server 2003 (que será descrito no Capítulo 8).



**Figura 5.41 Andamento do processo de desfragmentação.**

10. Você pode Pausar e até mesmo Interromper o processo de desfragmentação, utilizando os botões Parar e Pausar. Caso você interrompa o trabalho de desfragmentação, o trabalho já realizado, não será perdido. Se você Pausar o processo, o Windows Server 2003 inicia do ponto onde você parou, ou seja, não será necessário iniciar todo o processo novamente.
11. Aguarde o final do processo, quando o Windows Server 2003 exibe uma mensagem. Na janela da mensagem está disponível o botão Exibir relatório, o qual mostra um relatório detalhado sobre a desfragmentação do drive. Clique no botão Fechar. Você estará de volta a janela do Desfragmentador de disco. Agora observe a diferença na indicação dos Arquivos contíguos (indicados pela área azul), depois que o processo finaliza. A área em branco indica o espaço livre na unidade.
12. Feche o Desfragmentador de disco.

**NOTA:** É recomendado que você verifique a necessidade de desfragmentação, pelo menos, uma vez por mês. O sistema de arquivos NTFS evoluiu muito, desde a sua versão original. Devido a diminuição do tamanho utilizado para o cluster, a fragmentação foi bastante reduzida. Se você utiliza volumes formatados com FAT32, você estará mais sujeito a fragmentação. Nestes casos sugiro que você verifique a necessidade de desfragmentação pelo menos duas vezes a cada quinze dias.

## Algumas recomendações sobre o processo de desfragmentação

Na documentação oficial do Windows Server 2003, você encontra as seguintes recomendações relacionadas ao processo de desfragmentação de unidades:

- ◆ **Analizar antes de desfragmentar:** Analise os volumes antes de desfragmentá-los. Depois de analisar um volume, uma caixa de diálogo informa a porcentagem de pastas e arquivos fragmentados no volume e recomenda o procedimento a ser adotado. Analise os volumes regularmente e

desfragmente-os apenas quando o Desfragmentador de disco recomendar. Uma boa diretriz é analisar os volumes pelo menos uma vez por semana. Se você raramente precisar desfragmentar os volumes, analise-os mensalmente em vez de semanalmente.

- ◆ **Analizar depois que vários arquivos forem adicionados:** Os volumes podem se tornar excessivamente fragmentados quando os usuários adicionam um grande número de arquivos ou pastas; portanto, certifique-se de analisar os volumes depois que isso acontecer. Normalmente, os volumes em servidores de arquivos devem ser desfragmentados com mais freqüência do que aqueles em estações de trabalho de um único usuário. Isto acontece porque em pastas compartilhadas, em servidores de arquivos, existem vários usuários gravando e excluindo arquivos pela rede. Este tipo de utilização faz com que o volume onde encontra-se a pasta compartilhada, fique bastante fragmentado. Tal fato acaba por comprometer o desempenho do compartilhamento, tornando as operações com arquivos bem mais lentas do que o normal.
- ◆ **Certifique-se de que o disco tenha pelo menos 15% de espaço livre:** Um volume deve ter pelo menos 15% de espaço livre para que o Desfragmentador de disco desfragmente-o completa e adequadamente. O Desfragmentador de disco utiliza esse espaço como uma área de classificação para fragmentos de arquivo. Se um volume tiver menos de 15% de espaço livre, o Desfragmentador de disco o desfragmentará apenas parcialmente. Para aumentar o espaço livre em um volume, exclua os arquivos desnecessários, ou mova-os para outro disco.
- ◆ **Desfragmentar durante períodos de pouco uso:** Desfragmente volumes de servidor de arquivos durante os períodos de pouco uso para minimizar os efeitos do processo de desfragmentação no desempenho do servidor de arquivos. O tempo que o Desfragmentador de disco leva para desfragmentar um volume depende de diversos fatores, inclusive do tamanho do volume, do número de arquivos que ele contém, do número de arquivos fragmentados e dos recursos de sistema disponíveis.
- ◆ **Desfragmentar depois de instalar um software ou o Windows:** Desfragmente volumes depois de instalar algum software ou depois de fazer uma atualização ou instalação completa do Windows. Freqüentemente, os volumes ficam fragmentados depois de instalar softwares que gravam um grande número de arquivos no disco rígido; por isso, executar o Desfragmentador de disco ajuda a garantir o melhor desempenho do sistema de arquivos.

## O comando defrag

Além do Desfragmentador de discos, você também pode utilizar o comando defrag, para efetuar a desfragmentação de partições/volumes. O comando defrag localiza e consolida arquivos de inicialização fragmentados, arquivos de dados e pastas em volumes locais.

A sintaxe para o comando defrag é a seguinte:

**defrag volume [/opções]**

Onde temos as seguintes opções de linha de comando:

- ◆ **/a:** Analisa o volume e exibe um resumo do relatório de análise.
- ◆ **/v:** Exibe a análise completa e os relatórios de desfragmentação.

Quando usado juntamente com /a, exibe somente o relatório de análise. Quando usado sozinho, exibe a análise e os relatórios de desfragmentação.

- ◆ **/f:** Força a desfragmentação do volume, independentemente da necessidade de desfragmentação.
- ◆ **/?:** Exibe ajuda no prompt de comando.

**NOTA:** Os comandos são executados no Prompt de Comando: Iniciar -> Todos os Programas -> Acessórios -> Prompt de Comando. No Prompt de Comando você digita o comando e pressiona Enter para executá-lo. O Prompt de Comando é muito semelhante a uma janela do bom e velho MS-DOS.

Algumas observações importantes:

Você não pode desfragmentar volumes que o sistema tenha marcado como o status Dirty (sujos), o que indica que podem estar corrompidos. É necessário executar o comando chkdsk em um volume com o status Dirty (sujo) antes de desfragmentá-lo. Para determinar se um volume é sujo, use o seguinte comando:

```
fsutil dirty query letra_da_unidade
```

A seguir mostro o resultado da execução do comando fsutil dirty query C:

```
C:\>fsutil dirty query C:  
Volume - C: is NOT Dirty  
C:\>
```

Enquanto o comando defrag estiver analisando e desfragmentando um volume, ele exibirá um cursor piscando. Quando o comando defrag terminar de analisar e desfragmentar o volume, será exibido um relatório de análise, o relatório de desfragmentação ou ambos e o prompt de comando será fechado. Por padrão, o comando defrag exibe um resumo dos relatórios de análise e desfragmentação se você não especificar os parâmetros /a ou /v.

É possível enviar relatórios para um arquivo de texto digitando > nome\_do\_arquivo.txt, após o comando defrag e as opções, onde nome\_do\_arquivo.txt é o nome de arquivo que você especificar. Por exemplo:

```
defrag C: /v >resultado_da_desfragmentação.txt
```

Para interromper o processo de desfragmentação, na linha de comando, pressione CTRL+C.

A utilização do comando defrag é indicada para a criação de scripts administrativos e para o agendamento do processo de desfragmentação, para que ocorra em horários e datas específicas, como por exemplo uma vez por semana, aos sábados de madrugada.

## Verificando e reparando erros no sistema de arquivos e no disco rígido

O Windows Server 2003 disponibiliza a ferramenta Verificação de erros, para efetuar a verificação de erros em volumes (discos dinâmicos) e partições (discos básicos). Você pode utilizar a ferramenta Verificação de erros para verificar se há erros no sistema de arquivos e se existem setores defeituosos no seu disco rígido. É recomendado que você utilize esta ferramenta, antes de utilizar o desfragmentador, para garantir que o volume a ser desfragmentado, esteja livre de erros.

Exemplo: Para utilizar a ferramenta Verificação de erros, faça o seguinte:

1. Faça o logon como Administrador ou com uma conta do tipo Administrador do computador.
2. Abra o Meu computador.
3. Localize a unidade na qual você quer fazer a verificação e correção de erros, clique com o botão direito do mouse na referida unidade e, no menu que é exibido, dê um clique na opção Propriedades.
4. Será aberta a janela de propriedades da unidade, com a guia Geral selecionada. Dê um clique na guia Ferramentas.
5. Na guia Ferramentas dê um clique no botão Verificar agora...

Será exibida a janela Verificar disco Disco local (C:), conforme indicado na Figura 5.42.

Nesta janela estão disponíveis as seguintes opções marcar as seguintes opções:

- ◆ Corrigir erros do sistema de arquivos automaticamente: Especifica se o Windows Server 2003 deve automaticamente reparar erros de sistema de arquivos encontrados durante a verificação de disco. Todos os

arquivos devem estar fechados para que o programa seja executado. Se a unidade estiver em uso no momento, uma mensagem perguntará se você deseja reagendar a verificação de disco para a próxima vez que reiniciar o computador. A unidade não ficará disponível para executar outras tarefas enquanto o disco estiver sendo verificado.



Figura 5.42 A janela Verificar disco.

- ◆ **Procurar setores defeituosos e tentar recuperá-los:** Especifica se o Windows Server 2003 repara erros de sistema de arquivos encontrados durante a verificação de disco, localiza setores defeituosos e recupera informações legíveis. Todos os arquivos devem estar fechados para que o programa seja executado. Se a unidade estiver em uso no momento, uma mensagem perguntará se você deseja reagendar a verificação de disco para a próxima vez que reiniciar o computador. A unidade não ficará disponível para executar outras tarefas enquanto o disco estiver sendo verificado. Se você selecionar esta opção, não precisará marcar Corrigir erros do sistema de arquivos automaticamente. O Windows corrige os erros no disco.
6. Marque as opções desejadas e dê um clique no botão Iniciar. Se algum programa estiver utilizando o disco, uma mensagem perguntará se você deseja agendar a verificação de disco para a próxima vez que o sistema for inicializado.
  7. Clique em Sim para agendar a verificação para a próxima reinicialização.
  8. Você estará de volta à janela de Propriedades. Dê um clique no botão OK para fechar-a.
  9. Feche todos os programas que estiverem abertos e reinicialize o computador. Observe que durante a reinicialização é disparado o processo de verificação e correção de erros. Enquanto este processo não for concluído, a inicialização do Windows Server 2003 não é completada para que você possa fazer o logon.

**NOTA:** Em determinadas situações, como por exemplo uma queda de energia, o Windows Server 2003 pode iniciar automaticamente o processo de verificação e correção de erros, durante a inicialização do sistema.

## Comandos para a verificação e correção de erros

Além da ferramenta Verificação de erros, o Windows Server 2003 disponibiliza os comandos chkdsk e chkntfs. A seguir mostrarei como utilizar estes dois comandos.

### O comando chkdsk

Este comando é utilizado para analisar um volume e criar um relatório de status (da situação) para um disco. O relatório descreve com está o sistema de arquivos e relatas os problemas encontrados. O comando Chkdsk também lista e corrige erros no disco. Quando utilizado sem parâmetros, chkdsk exibe o status do disco na unidade atual.

Sintaxe para o comando chkdsk:

```
chkdsk [volume:][[caminho] nome_de_arquivo] [/f] [/v] [/r] [/x] [/i] [/c] [/l[:tamanho]]
```

A seguir apresento a descrição de cada um dos parâmetros do comando chkdsk:

- ◆ **volume:** Especifica a letra da unidade (seguida de dois-pontos), o ponto de montagem ou o nome do volume. Por exemplo: C:, D:, etc.
- ◆ **[caminho] nome\_de\_arquivo:** Especifica o local e o nome de um arquivo ou conjunto de arquivos que chkdsk deve verificar para determinar se há fragmentação. Você pode utilizar caracteres curingas (isto é, \* e ?) para especificar vários arquivos. Por exemplo: C:\Documentos\\*.doc, especifica todos os arquivos .DOC da pasta C:\Documentos.
- ◆ **/f:** Corrige erros no disco. O disco deve ser bloqueado. Se chkdsk não puder bloquear a unidade, será exibida uma mensagem perguntando se você deseja verificar a unidade na próxima vez que o computador for reiniciado. Se você responder que sim, uma verificação será agendada para a próxima inicialização do sistema. Corresponde a opção “Corrigir erros do sistema de arquivos automaticamente”, da ferramenta Verificação de erros, descrita no tópico anterior.
- ◆ **/v:** Exibe o nome de todos os arquivos contidos em cada pasta à medida que o disco é verificado.
- ◆ **/r:** Localiza setores defeituosos e recupera informações legíveis. O disco deve ser bloqueado. Se chkdsk não puder bloquear a unidade, será exibida uma mensagem perguntando se você deseja verificar a unidade na próxima vez que o computador for reiniciado. Se você responder que sim, uma verificação será agendada para a próxima inicialização do sistema. Corresponde a opção “Procurar setores defeituosos e tentar recuperá-los”, da ferramenta Verificar erros, descrita no tópico anterior.
- ◆ **/x:** Use esta opção somente com partições/volumes formatados com o sistema NTFS. Ela força primeiro a desmontagem do volume, se necessário. Todos os identificadores abertos para a unidade serão invalidados. A opção /x também inclui a funcionalidade da opção /f.
- ◆ **/i:** Use esta opção somente com partições/volumes formatados com o sistema NTFS. Efetua uma verificação menos rígida das entradas de índice, reduzindo o tempo necessário para a execução de chkdsk.
- ◆ **/c:** Use esta opção somente com partições/volumes formatados com o sistema NTFS. Ela ignora a verificação de ciclos dentro da estrutura de pastas, reduzindo o tempo necessário para a execução de chkdsk.
- ◆ **/l[:tamanho]:** Use esta opção somente com partições/volumes formatados com o sistema NTFS. Ela utilizará o tamanho digitado por você em vez do tamanho do arquivo de log. Se você omitir o parâmetro de tamanho, /l exibirá o tamanho atual.
- ◆ **/?:** Exibe informações de ajuda no prompt de comando.

Para executar o comando chkdsk em um disco fixo, é preciso permissão de Administrador.

O comando chkdsk examina o espaço em disco e a utilização do disco pelos sistemas de arquivos, verifica a tabela de alocação de arquivos (FAT) e NTFS. Chkdsk fornece informações específicas de cada sistema de arquivos em um relatório de status. O relatório de status exibe os erros encontrados no sistema de arquivos. Se chkdsk for executado sem a opção de linha de comando /f em uma partição ativa, ele poderá reportar erros indesejáveis, pois não conseguirá bloquear a unidade. Você deve utilizar o comando chkdsk em cada disco periodicamente para verificar se há erros. Você pode utilizar o comando chkdsk para agendar uma tarefa que faça a verificação periódica das unidades e salve o relatório com os resultados da verificação em um arquivo de texto para verificação posterior.

O comando chkdsk só corrigirá erros de disco se você especificar a opção de linha de comando /f. É necessário que Chkdsk possa bloquear a unidade para corrigir os erros. Como a reparação geralmente altera a tabela de

alocação de arquivos de um disco e, às vezes, causa perda de dados, chkdsk enviará uma mensagem de confirmação semelhante a esta:

**10 unidades de alocação perdidas encontradas em 3 cadeias.**

**Deseja converter cadeias perdidas em arquivos?**

Se você pressionar S, o Windows salvará cada cadeia perdida na pasta raiz como um arquivo com um nome no formato de arquivo nnnn.chk. Quando chkdsk for concluído, você poderá verificar esses arquivos para descobrir se contêm quaisquer dados necessários. Se você pressionar N, o Windows corrigirá o disco, mas não salvará o conteúdo das unidades de alocação perdidas.

Se você não usar a opção de linha de comando /f, chkdsk enviará uma mensagem se for necessário corrigir algum arquivo, mas não corrigirá nenhum erro.

Se você utilizar chkdsk /f em um disco muito grande (por exemplo, 70 GB) ou em um disco com um número muito grande de arquivos (por exemplo, milhões de arquivos), chkdsk poderá levar muito tempo (talvez vários dias) para ser concluído. O computador não ficará disponível durante esse período, porque chkdsk só liberará o controle depois de ser concluído.

Windows exibe relatórios de status de chkdsk referentes a um disco FAT no seguinte formato:

**O número de série do volume é B1AF-AFBF**

**72.214.528 bytes de espaço total em disco**

**73.728 bytes em 3 arquivos ocultos**

**30.720 bytes em 12 pastas**

**11.493.376 bytes em 386 arquivos do usuário**

**61.440 bytes em setores defeituosos**

**60.555.264 bytes disponíveis no disco**

**2.048 bytes em cada unidade de alocação**

**35.261 unidades de alocação totais no disco**

**29.568 unidades de alocação disponíveis no disco**

O Windows exibe relatórios de status de chkdsk referentes a um disco NTFS no seguinte formato:

**O tipo do sistema de arquivos é NTFS.**

**CHKDSK está verificando os arquivos...**

**Verificação de arquivos concluída.**

**CHKDSK está verificando índices...**

**Verificação dos índices concluída.**

**CHKDSK está verificando os descritores de segurança...**

**Verificação de descritores de segurança concluída.**

**12.372 quilobytes de espaço total em disco.**

**3 KB em 1 arquivo do usuário.**

**2 KB em 1 índice.**

**4.217 KB em uso pelo sistema.**

```
8.150 KB disponíveis em disco.  
512 bytes em cada unidade de alocação.  
24.745 unidades de alocação totais no disco.  
16.301 unidades de alocação disponíveis em disco.
```

## Usando chkdsk com arquivos abertos

Se você especificar a opção de linha de comando /f, chkdsk enviará uma mensagem de erro se forem encontrados arquivos abertos no disco. Se você não especificar a opção de linha de comando /f e existirem arquivos abertos, chkdsk poderá reportar a existência de unidades de alocação perdidas no disco. Isso poderá acontecer se os arquivos abertos ainda não tiverem sido gravados na tabela de alocação de arquivos. Se chkdsk reportar a perda de uma grande quantidade de unidades de alocação, é aconselhável reparar o disco.

A seguir temos a lista com os códigos de saída reportados por chkdsk após sua conclusão.

- ◆ 0: Não foram encontrados erros.
- ◆ 1: Foram encontrados erros e corrigidos.
- ◆ 2: A limpeza de disco, como a coleta de lixo, foi efetuada, ou a limpeza não foi efetuada porque /f não foi especificado.
- ◆ 3: Não foi possível verificar o disco, não foi possível corrigir os erros ou os erros não foram corrigidos porque a opção /f não foi especificada.

Para verificar o disco na unidade C e fazer com que o Windows corrija os erros, digite:

```
chkdsk C: /f
```

Chkdsk fará uma pausa e exibirá mensagens, se encontrar erros. Chkdsk será concluído exibindo um relatório que lista o status do disco. Você só poderá abrir qualquer arquivo na unidade especificada depois que chkdsk for concluído.

## O comando chkntfs

Este comando é utilizado para exibir ou especificar se a verificação automática do sistema está agendada para ser executada em um volume FAT, FAT32 ou NTFS quando o computador for iniciado.

Sintaxe para o comando chkntfs:

```
chkntfs volume: [/opções]
```

A seguir descrevo os parâmetros/opções do comando chkntfs:

- ◆ **volume:** [...]: É obrigatório. Especifica a letra da unidade (seguida de dois-pontos), o ponto de montagem ou o nome do volume. Exibe uma mensagem que identifica o sistema de arquivos do volume especificado. Se a verificação automática de arquivos estiver agendada para ser executada, este parâmetro exibirá uma mensagem indicando se o volume foi ou não corrompido, o que exigirá que o comando chkdsk seja executado. O comando chkdsk foi descrito no item anterior.
- ◆ **/d:** Restaura todas as configurações padrão de chkntfs, com exceção do tempo de contagem regressiva para a verificação automática de arquivos. O comportamento padrão é verificar todos os volumes quando o computador é iniciado.
- ◆ **/t[:tempo]:** Altera o tempo de contagem regressiva inicial de Autochk.exe para o tempo especificado em segundos. Se você não especificar :tempo, /t exibirá o tempo de contagem regressiva atual.

- ◆ **/x volume:** [...]: Exclui o volume especificado da verificação quando o computador é iniciado, mesmo se o volume estiver marcado de modo a exigir que chkdsk seja executado.
- ◆ **/c volume:** [...]: Agenda a verificação do volume especificado para quando o computador for iniciado.
- ◆ **/?**: Exibe informações de ajuda no prompt de comando.

Para executar chkntfs, é necessário que você tenha permissão de Administrador.

Embora você possa definir o tempo de contagem regressiva inicial de Autochk.exe como zero, não será possível cancelar uma verificação automática de arquivos que levará provavelmente muito tempo se você defini-lo como zero.

Por exemplo, para agendar uma verificação automática para o drive D:, quando o sistema é inicializado, utilize o seguinte comando:

```
chkntfs /c D:
```

## Outros comandos importantes para trabalhar com discos e volumes

Neste item apresento mais alguns comandos que são úteis para o trabalho com discos e volumes.

### O comando convert

Este comando é utilizado para converter volumes FAT (file allocation table) e FAT32 para o sistema de arquivos NTFS, deixando intactos os arquivos e pastas existentes. Os volumes convertidos ao sistema de arquivos NTFS não poderão ser convertidos de volta em FAT ou FAT32.

Sintaxe:

```
convert [Volume] /fs:ntfs [/v] [/cvtarea:NomeDoArquivo] [/nosecurity] [/x]
```

O comando convert tem os seguintes parâmetros:

- ◆ **Volume:** Especifica a letra da unidade (seguida de dois-pontos), o ponto de montagem ou o nome do volume a ser convertido em NTFS.
- ◆ **/fs:ntfs:** Necessário. Converte o volume em NTFS.
- ◆ **/v:** Especifica o modo de detalhe, isto é, todas as mensagens serão exibidas durante a conversão.
- ◆ **/cvtarea:nome\_de\_arquivo:** Apenas para usuários avançados. Especifica que a tabela de arquivos mestre (MFT) e outros arquivos de metadados NTFS serão gravados em um arquivo existente de espaço reservado contíguo. O arquivo deve estar localizado na pasta raiz do sistema de arquivos a ser convertido. O uso do parâmetro /CVTAREA poderá resultar em um sistema de arquivos menos fragmentado após a conversão. Para obter melhores resultados, o tamanho do arquivo deve ser 1 KB multiplicado pelo número de arquivos e pastas contidos no sistema de arquivos, no entanto, o utilitário de conversão aceita arquivos de qualquer tamanho.
- ◆ **/nosecurity:** Especifica que as configurações de segurança das pastas e arquivos convertidos poderão ser acessadas por qualquer pessoa.
- ◆ **/x:** Desmonta o volume, se necessário, antes de ser convertido. Os identificadores abertos para o volume não serão mais válidos.

---

**IMPORTANTE:** Não esqueça que é possível usar o comando convert, para converter um volume de FAT ou FAT32 para NTFS, sem perda de dados. Por outro lado, não é possível converter um volume NTFS de volta para FAT ou FAT32. Neste caso, é preciso fazer um backup completo dos dados, excluir o volume, recriá-lo novamente como FAT ou FAT32 e depois baixar os arquivos do backup.

---

Se o comando convert não puder bloquear a unidade (por exemplo, o volume do sistema ou a unidade atual), ele sugerirá que o volume seja convertido na próxima vez que o computador for reiniciado. Se você não puder reiniciar o computador imediatamente para concluir a conversão, planeje o momento de reiniciar o computador e reserve um tempo adicional para o processo de conversão.

No caso de volumes convertidos de FAT ou FAT32 em NTFS, devido à utilização de disco já existente, a MFT é criada em um local diferente, em comparação a um volume originalmente formatado com NTFS. Devido a isso, o desempenho do volume pode não ser tão bom quanto em volumes originalmente formatados com NTFS. Para obter o desempenho ideal, considere a possibilidade de recriar esses volumes e formatá-los com o sistema de arquivos NTFS.

Os volumes convertidos de FAT em NTFS deixam os arquivos intactos, porém, poderão não dispor de alguns benefícios de desempenho se comparados a volumes inicialmente formatados com NTFS. Em volumes convertidos, por exemplo, a MFT pode ficar fragmentada. Além disso, em volumes de inicialização convertidos, o convert aplica a mesma segurança padrão que é aplicada durante a instalação do Windows.

Exemplo: Para converter o volume na unidade E em NTFS e exibir todas as mensagens, digite:

```
convert e: /fs:ntfs /v
```

## O utilitário DiskPart

O utilitário DiskPart.exe é um interpretador de comandos em texto que permite gerenciar objetos (discos, partições ou volumes) por scripts ou entrada direta em um prompt de comando. Antes de usar os comandos de DiskPart.exe, exiba primeiro o objeto e, em seguida, selecione-o. Com o objeto selecionado, qualquer comando de DiskPart.exe digitado agirá sobre esse objeto.

Você pode listar os objetos disponíveis e determinar o número ou a letra de unidade de um objeto por meio dos comandos list disk, list volume e list partition. Os comandos list disk e list volume exibem todos os discos e volumes do computador. Entretanto, o comando list partition somente exibe partições do disco que está em foco. Quando você usar os comandos list, um asterisco (\*) é exibido ao lado do objeto em foco. Um objeto é selecionado por seu número ou letra de unidade, como disco 0, partição 1, volume 3 ou volume C.

Quando você seleciona um objeto, o foco permanece nele até que seja selecionado um objeto diferente. Por exemplo, se o foco estiver no disco 0 e você selecionar o volume 8 no disco 2, o foco mudará do disco 0 para o disco 2, volume 8. Alguns comandos mudam automaticamente o foco. Por exemplo, quando você cria uma nova partição, o foco muda automaticamente para a nova partição.

Só é possível colocar em foco uma partição do disco selecionado. Quando ela está em foco, o volume relacionado (se houver), também fica em foco. Quando um volume tem foco, o disco e a partição relacionados também ficam em foco se o volume mapear para uma única partição específica. Se não for esse o caso, o foco no disco e na partição se perde.

O utilitário Diskpart.exe oferece, sem exagero, milhares de comandos e opções diferentes. Seria possível, sem ser muito prolixo, escrever um capítulo inteiro sobre o utilitário Diskpart. Você encontra informações completas e exemplos detalhados sobre o Diskpart, diretamente na ajuda do Windows Server 2003. Para acessar a página de ajuda do utilitário Diskpart, abra a Ajuda do Windows Server 2003 e pesquise pela palavra Diskpart. A seguir alguns exemplos simples de utilização de comandos, dentro do utilitário Diskpart. Para executar estes comandos, primeiro você deve abrir um

**IMPORTANTE:** É necessário criar o arquivo de espaço reservado usando o comando fsutil file createnew antes de executar o comando convert. Convert não cria esse arquivo. Ele substitui esse arquivo com os metadados NTFS. Depois da conversão, qualquer espaço não utilizado nesse arquivo será liberado. Para obter mais informações sobre o comando fsutil file, consulte Tópicos relacionados.

Prompt de comando e digitar Diskpart e pressionar enter. Será aberto o prompt do utilitário Diskpart. Pronto, agora você pode executar os comandos específicos do Diskpart, conforme exemplos a seguir:

Exemplo 01: Listar informações sobre os discos do sistema:

```
list disk
```

na Figura 5.43, você encontra um exemplo de execução do comando list disk:

| Disco   | ### | Status  | Tamanho | Livre   | Din | Gpt |
|---------|-----|---------|---------|---------|-----|-----|
| Disco 0 |     | On-line | 19 GB   | 8033 KB |     | *   |
| Disco 1 |     | On-line | 4103 MB | 3903 MB | *   | *   |
| Disco 2 |     | On-line | 1216 MB | 1016 MB | *   | *   |
| Disco 3 |     | On-line | 510 MB  | 510 MB  | *   | *   |

Figura 5.43 Listando informações sobre os discos do sistema.

Exemplo 02: Listar informações sobre as partições em discos básicos:

```
list partition
```

Exemplo 03: Listar informações sobre os volumes em discos dinâmicos:

```
list volume
```

Exemplo 04: Seleciona o disco 04 e depois converte-o para dinâmico:

```
select disk 4
```

```
convert dynamic
```

Com o utilitário Diskpart você pode executar qualquer operação com discos e volumes, tais como converter discos de básico para dinâmico, criar volumes de qualquer tipo, excluir volumes e assim por diante.

## O comando Fsutil: file

Este comando, normalmente, é utilizado por profissionais de suporte. Localiza um arquivo por nome de usuário (caso as cotas de disco estejam habilitadas), consulta intervalos alocados para um arquivo, define o nome curto de um arquivo, define o comprimento de dados válido para um arquivo, define uma quantidade de dados nula para um arquivo ou cria um novo arquivo

Sintaxe:

```
fsutil file [createnew] NomeDoArquivo Comprimento  
fsutil file [findbysid] NomeDoUsuário Diretório
```

```

fsutil file [queryallocranges] offset=Deslocamento length=Comprimento NomeDoArquivo
fsutil file [setshortname] NomeDoArquivo NomeCurto
fsutil file [setvaliddata] NomeDoArquivo ComprimentoDosDados
fsutil file [setzerodata] offset=Deslocamento length=Comprimento NomeDoArquivo

```

Parâmetros:

- ◆ **createnew**: Cria um arquivo com o nome e o tamanho especificados, cujo conteúdo consiste em zeros.
- ◆ **NomeDoArquivo**: Especifica o caminho completo até o arquivo, incluindo o nome e a extensão do arquivo. Por exemplo, C:\documentos\nomedearquivo.txt.
- ◆ **Comprimento**: Especifica o tamanho válido dos dados do arquivo.
- ◆ **findbysid**: Em volumes NTFS em que as cotas de disco estão habilitadas, localiza arquivos que pertencem a um usuário específico. O usuário é identificado pelo nome de usuário. Findbysid é bastante eficiente, pois examina a tabela de arquivos mestre (MFT) NTFS, o que é muito mais eficiente do que uma pesquisa recursiva através da estrutura do diretório.
- ◆ **NomeDoUsuário**: Especifica o nome de usuário ou nome de logon do usuário.
- ◆ **Diretório**: Especifica o caminho completo até o diretório, por exemplo, C:\usuários.
- ◆ **queryallocranges**: Pesquisa os intervalos alocados para um arquivo em um volume NTFS. É útil para determinar se um arquivo possui regiões esparsas.
- ◆ **offset=Deslocamento**: Especifica o início do intervalo a ser zerado.
- ◆ **length=Tamanho**: Especifica o tamanho do intervalo, em bytes.
- ◆ **setshortname**: Define o nome curto (nome de arquivo com 8.3 caracteres de comprimento) para um arquivo em um volume NTFS.
- ◆ **NomeCurto**: Especifica o nome curto do arquivo.
- ◆ **setvaliddata**: Define o tamanho válido para os dados de um arquivo em um volume NTFS.
- ◆ **ComprimentoDosDados**: Especifica o tamanho do arquivo, em bytes.
- ◆ **setzerodata**: Define um intervalo (especificado por Deslocamento e Comprimento) do arquivo como zeros, o que esvazia o arquivo. Caso se trate de um arquivo esparsa, as unidades de alocação subjacentes serão descomprometidas.

---

**IMPORTANTE:** Em NTFS, existem dois importantes conceitos de tamanho de arquivo: o marcador de fim de arquivo (EOF) e o comprimento válido dos dados (VDL). O EOF indica o tamanho real do arquivo. O VDL identifica o tamanho dos dados válidos no disco. Qualquer leitura entre VDL e EOF retorna automaticamente 0 a fim de preservar o requisito de reutilização do objeto C2.

---

O parâmetro setvaliddata só está disponível para administradores porque requer o privilégio para realizar tarefas de manutenção no volume (SeManageVolumePrivilege). Este recurso só é necessário em situações de multimídia avançada e de rede de área do sistema. O parâmetro setvaliddata deve ser um valor positivo superior ao VDL atual, mas inferior ao tamanho do arquivo atual.

Exemplos de uso do comando fsutil:

Para localizar arquivos que pertençam ao usuário jsilva na unidade C, digite:

```
fsutil file findbysid jsilva C:\usuarios
```

Para pesquisar os intervalos alocados para um arquivo em um volume NTFS, digite:

```
fsutil file queryallocranges offset=1024 length=64 C:\dados\relat.doc
```

Para definir o nome curto do arquivo nomearquivolongo.txt na unidade C como arqlongo.txt, digite:

```
fsutil file setshortname C:\nomearquivolongo.txt arqlongo.txt
```

Para definir o tamanho válido para os dados de um arquivo em um volume NTFS, digite:

```
fsutil file setvaliddata C:\argteste.txt 4096
```

Para definir um intervalo de um arquivo em um volume NTFS a ser zerado para esvaziá-lo, digite:

```
fsutil file setzerodata offset=100 length=150 C:\Temp\exemplo.txt
```

## Criptografia de Arquivos em Partições NTFS

### Criptografia – definições e conceitos

O Windows Server 2003 fornece suporte a criptografia de pastas e arquivos através do EFS – Encrypted File System (Sistema de arquivos com Criptografia). O suporte ao EFS foi introduzido no Windows 2000 Server e também está disponível no Windows 2000 Professional e Windows XP Professional. Com o uso de criptografia o usuário tem um nível de segurança maior do que somente com o uso de permissões NTFS (assunto do Capítulo 6). Somente é possível criptografar arquivos e pastas em volumes formatados com o sistema de arquivos NTFS. Com a criptografia o Windows Server 2003 garante que somente o usuário que criptografou um determinado arquivo tenha acesso ao arquivo.

Criptografia é o processo de converter dados em um formato que não possa ser lido por um outro usuário, a não ser o usuário que criptografou o arquivo. Depois que um usuário criptografar um arquivo, esse arquivo permanecerá automaticamente criptografado quando for armazenado em disco.

Descriptografia é o processo de converter dados do formato criptografado no seu formato original. Depois que um usuário descriptografar um arquivo, esse arquivo permanecerá descriptografado quando for armazenado em disco.

Com as permissões NTFS (veja Capítulo 6) temos alguns problemas quanto a segurança dos dados:

- ◆ O Administrador da máquina pode usar o recurso de Take Ownership (Tornar-se dono), tornando-se desta forma dono dos arquivos/pastas desejados, mesmo sem ter permissão de acesso a estes arquivos/pastas. Após ter “dado um Take Ownership”, o Administrador pode atribuir permissões de acesso para si mesmo e, com isso, acessar qualquer arquivo ou pasta.
- ◆ Um usuário pode utilizar um disquete de boot ou instalar um outro sistema operacional no computador e utilizar alguns programas comerciais existentes, para ter acesso a pastas e arquivos protegidas por permissões NTFS.

A grande questão é a seguinte: “Com o uso da criptografia, mesmo que o seu computador seja roubado ou que outro usuário tenha acesso ao computador, não será possível acessar os arquivos e pastas que você criptografou. A única maneira de ter acesso é fazendo o logon com a sua conta e senha”. Em resumo: Com a criptografia, os dados estão protegidos, mesmo que outras pessoas tenham acesso ao seu computador, a única maneira de acessar os arquivos criptografados é fazendo o logon com a conta do usuário que criptografou os arquivos ou com a conta configurada como Agente de Recuperação, conforme descreverei mais adiante. Já com as permissões NTFS, conforme descrito anteriormente, este nível de proteção não existe, no caso do computador ser roubado ou de um usuário mal intencionado ter acesso ao computador.

Claro que existem situações adversas que podem surgir com o uso da criptografia. Por exemplo, vamos supor que um funcionário criptografou arquivos importantes para a empresa. Neste meio tempo o funcionário foi demitido. Como é que a empresa poderá ter acesso aos arquivos criptografados se o funcionário demitido se negar a fazer o logon com a sua conta e descriptografar os arquivos ou se a sua conta tiver sido excluída?? Por isso que o EFS permite que uma ou mais contas sejam configuradas como Agente de Recuperação, a qual pode ser utilizada em situações como a descrita neste parágrafo. Mais adiante tratarei, em detalhes, sobre o agente de recuperação.

O uso de criptografia é especialmente recomendado para usuários de notebooks e outros dispositivos semelhantes. Não é raro a ocorrência de roubos de notebooks, sendo que estes podem conter dados importantes da empresa, tais como planos estratégicos e relatórios de pesquisa e desenvolvimento de novos produtos. O uso da criptografia é a forma mais indicada para proteger estes dados, mesmo em situações de roubo de um notebook.

A criptografia é transparente para o usuário que criptografou o arquivo. Isso significa que o usuário não precisa descriptografar manualmente o arquivo criptografado para poder usá-lo. Ele pode abrir e alterar o arquivo da maneira habitual. Por exemplo, vamos supor que você criptografou um documento do Word. Ao dar um clique duplo no documento, o Windows Server 2003 descriptografa, automaticamente, o arquivo, abre o Word e carrega o arquivo para você. Observe que para o usuário toda a operação é transparente, ou seja, é como se o arquivo não estivesse criptografado. Se outro usuário, que não o que criptografou o arquivo, tentar utilizá-lo, receberá uma mensagem de acesso negado.

O uso do EFS é semelhante ao uso de permissões para arquivos e pastas. Ambos os métodos podem ser usados para restringir o acesso aos dados. No entanto, um intruso que obtenha acesso físico não-autorizado aos seus arquivos ou pastas criptografados não conseguirá acessá-los. Se o intruso tentar abrir ou copiar sua pasta ou arquivo criptografado, verá uma mensagem de acesso negado. As permissões definidas para arquivos e pastas não os protege contra ataques físicos não-autorizados, conforme já descrito anteriormente.

Você criptografa ou descriptografa uma pasta ou arquivo definindo a propriedade de criptografia para pastas e arquivos da mesma forma como define qualquer outro atributo, como somente leitura, compactado ou oculto. Se você criptografar uma pasta, todos os arquivos e subpastas criados na pasta criptografada serão automaticamente criptografados. É recomendável que você use a criptografia para pastas e não para arquivos individualmente, pois isso facilita a administração dos arquivos criptografados.

---

**NOTA:** Você também pode criptografar ou descriptografar um arquivo ou pasta usando o comando cipher. Tratarei deste comando mais adiante.

---

Antes de aprender a criptografar arquivos e pastas, vou apresentar algumas observações importantes sobre a criptografia no Windows Server 2003:

- ◆ Somente arquivos e pastas em volumes NTFS podem ser criptografados.
- ◆ As pastas e os arquivos compactados não podem ser criptografados. Se o usuário marcar um arquivo ou pasta para criptografia, ele será descompactado. Falarei sobre a compactação de pastas e arquivos em volumes NTFS, no Capítulo 6.
- ◆ Se você mover arquivos descriptografados para uma pasta criptografada, esses arquivos serão automaticamente criptografados na nova pasta. No entanto, a operação inversa não descriptografa automaticamente os arquivos. Nesse caso, é necessário descriptografar manualmente os arquivos.
- ◆ Os arquivos marcados com o atributo Sistema não podem ser criptografados, bem como os arquivos da pasta raiz do sistema, isto é C:\ ou D:\ e assim por diante.
- ◆ Criptografar um arquivo ou uma pasta não protege contra exclusão ou listagem de arquivos ou pastas. Qualquer pessoa com permissões NTFS adequadas pode excluir ou listar pastas ou arquivos criptografados. A proteção da criptografia é contra o acesso aos arquivos, ou seja, somente o usuário que criptografou o arquivo terá acesso. Para proteção contra listagem e exclusão recomenda-se o uso do EFS em combinação com permissões NTFS (descritas no Capítulo 6), utilizando as permissões NTFS para impedir que outros usuários possam excluir e até mesmo listar os arquivos que estão em um pasta criptografada.
- ◆ Você pode criptografar ou descriptografar pastas e arquivos localizados em um computador remoto ativado para criptografia remota. No entanto, se você abrir o arquivo criptografado na rede, os dados transmitidos na rede através desse processo não serão criptografados. Outros protocolos, como a camada de soquetes de segurança/

segurança da camada de transporte (SSL/TLS) ou IP Seguro (IPSec), devem ser usados para criptografar dados durante a transmissão.

Agora que já temos um bom entendimento sobre os aspectos teóricos relacionados com o EFS, é hora de aprender sobre as tarefas práticas, relacionadas com a criptografia de arquivos e pastas no Windows Server 2003.

Em primeiro lugar vou falar sobre algumas medidas preventivas que devem ser tomadas, para garantir que você sempre possa ter acesso aos arquivos e pastas criptografados.

## Garantindo a recuperação dos dados

A criptografia utilizada pelo Windows Server 2003 é baseada na utilização de um par de chaves de criptografia. Uma chave é utilizada para criptografar os dados e a outra chave do par é utilizada para descriptografar os dados. A única maneira de descriptografar os dados e ter acesso às informações é tendo acesso as chaves de criptografia. Estas chaves são armazenadas em um Certificado digital, certificado este que é gerado, automaticamente, pelo Windows Server 2003, a primeira vez que o usuário criptografa um arquivo ou pasta. Neste Certificado digital estão todas as informações necessárias para criptografar e descriptografar arquivos.

Cada usuário que criptografa/descriptografa arquivos, possui o seu próprio Certificado digital, gerado automaticamente pelo Windows Server 2003. Um certificado adicional também é gerado para a conta configurada como Agente de recuperação. Desta maneira se o usuário que criptografou arquivos ou pastas deixar a empresa, será possível descriptografar os seus dados, utilizando a conta configurada como Agente de recuperação, uma vez que esta conta possui cópia do Certificado digital necessário a tal operação.

O Certificado digital nada mais é do que um arquivo que contém as informações necessárias para trabalhar com criptografia no Windows Server 2003. Como todo arquivo, fica gravado no disco rígido do computador. Acontece que se houver um problema com o disco rígido, a cópia do certificado do usuário e do certificado do agente de recuperação serão perdidas (caso não haja uma cópia de segurança) e, sem um destes certificados, ficará impossível descriptografar os arquivos/pastas criptografados pelo usuário. Na prática, significa que o acesso aos dados criptografados será perdido. Para evitar que isto aconteça, deve ser feita uma cópia de segurança, preferencialmente em disquete ou em um drive de rede, do Certificado digital gerado para o usuário. É importante lembrar que este certificado, somente será gerado na primeira vez que o usuário criptografar alguma pasta ou arquivo.

A seguir mostrarei como fazer o backup do certificado digital do usuário, do certificado do agente de recuperação e como restaurar o certificado digital do usuário. Por padrão, a conta Administrator (Administrador) é configurada como agente de recuperação.

Para um member server, o agente de recuperação padrão é a conta Administrator (Administrador) local. Para um domínio baseado no Active Directory, a conta configurada com agente de recuperação é a conta Administrator (Administrador) do domínio. No exemplo a seguir mostrarei como fazer uma cópia de segurança, em disquete, do certificado digital da conta Administrator do domínio.

Exemplo 1: Para fazer o backup do certificado do Agente de recuperação para o domínio, siga os seguintes passos:

1. Faça o logon com uma conta com permissões de Administrador.
2. Abra o console Diretiva de segurança de domínio: Iniciar -> Ferramentas Administrativas -> Diretiva de segurança de domínio. Clique no sinal de + ao lado da opção Configurações de segurança.
3. Nas opções que são exibidas, dê um clique no sinal de + ao lado da opção Diretivas de chave pública.

4. Nas opções que são exibidas dê um clique na opção Sistemas de arquivos criptografados. No painel da direita será exibido o Certificado do Agente de recuperação, que por padrão é a conta Administrator (Administrador), conforme indicado na Figura 5.44:

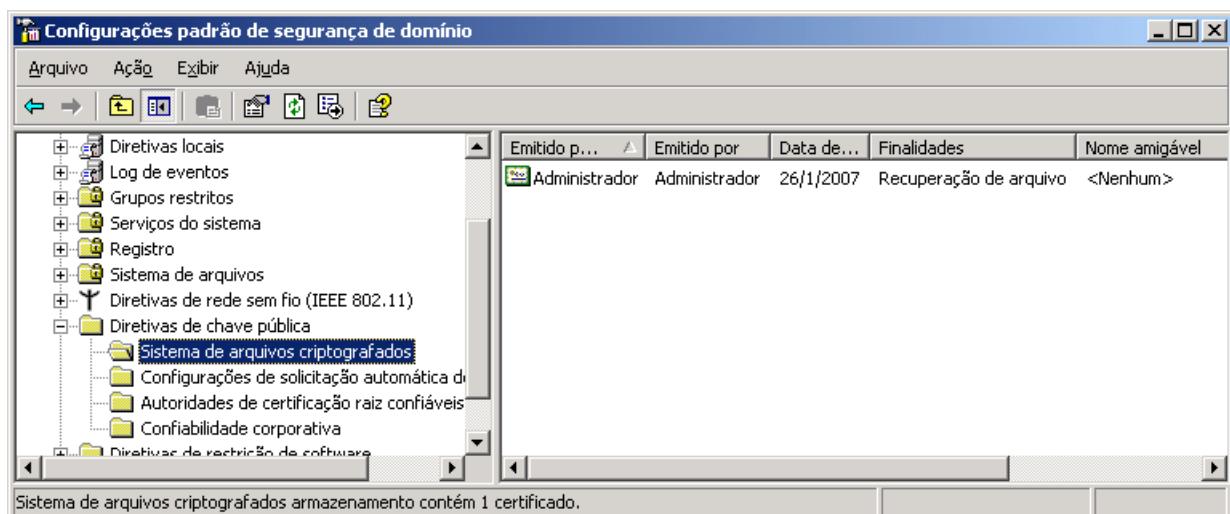


Figura 5.44 Conta Administrator – por padrão é o agente de recuperação.

5. No painel da direita, clique com o botão direito do mouse na conta Administrator. No menu que é exibido selecione o comando Todas as tarefas -> Exportar... Será aberto o Assistente para exportação de certificados.  
 6. A primeira tela é apenas informativa. Dê um clique no botão Avançar, para ir para a próxima etapa do assistente.  
 7. Nesta etapa você deve optar por exportar ou não a Chave particular do certificado. A Chave particular é um meio de proteger o acesso ao Certificado digital, através de uma senha. Se você não tiver uma senha definida, apenas estará habilitada a opção Não, não exportar a chave particular. Marque a opção Não, não exportar a chave particular, conforme indicado na Figura 5.45:

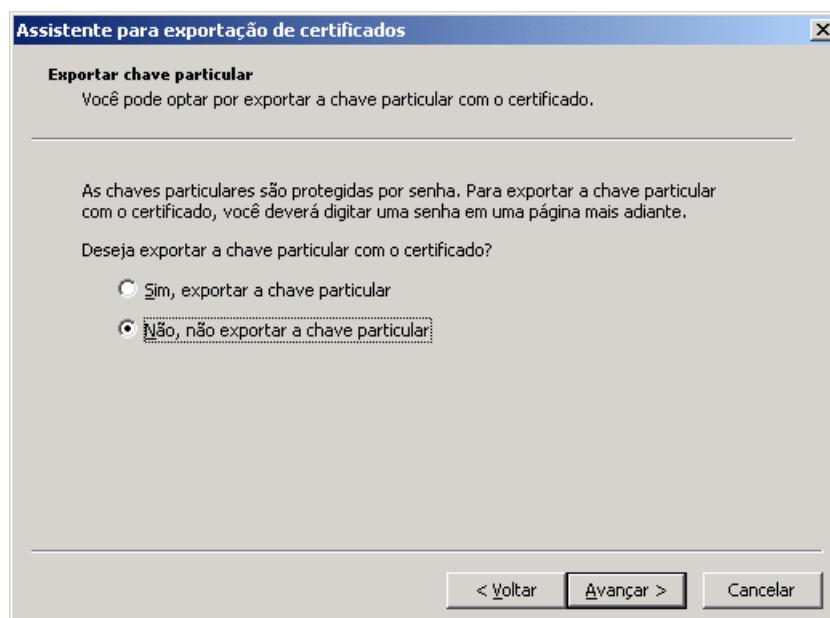


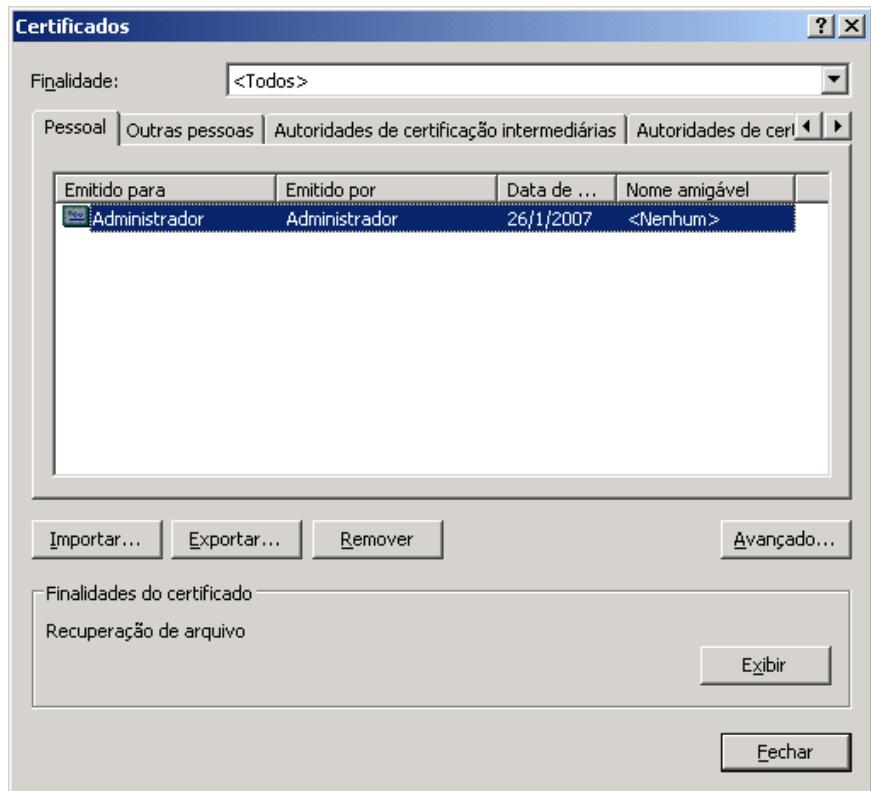
Figura 5.45 Definindo opções de exportação do certificado do agente de recuperação.

8. Certifique-se de que a opção Não, não exportar a chave particular esteja marcada e dê um clique no botão Avançar, para ir para a próxima etapa do assistente.
9. Surge uma tela perguntando o formato para exportação do certificado. Certifique-se de que a opção X.509 binário codificado por DER (\*.cer) esteja selecionada e dê um clique no botão Avançar, para ir para a próxima etapa do assistente.
10. Surge uma tela solicitando o nome do arquivo para o qual será exportado o certificado. É recomendado que você exporte para um disquete ou para um drive de rede. Certifique-se de que você colocou um disquete no drive e, no campo Nome do arquivo, digite: A:\cert\_ag\_recup.
11. Dê um clique no botão Avançar, para ir para a próxima etapa do assistente. O Windows Server 2003 exporta o certificado, para o arquivo especificado no drive de disquete.
12. Será exibida a tela final do assistente, com um resumo das opções selecionadas. Se você quiser fazer alguma alteração, pode utilizar o botão Voltar. Dê um clique no botão Concluir, para fechar o Assistente para exportação de certificados.
13. Surge uma mensagem informando que a exportação foi concluída com êxito. Dê um clique no botão OK para fechar esta mensagem.
14. Você estará de volta ao console Configurações locais de segurança e uma cópia do Certificado digital do Agente de recuperação, foi gravada no disquete. No evento de uma falha do disco rígido, esta cópia pode ser utilizada para descriptografar os arquivos e pastas criptografados. Feche o console Configurações locais de segurança.

Muito bem, o backup do certificado do agente de recuperação foi efetuado. Em caso de falha no HD você pode importar este certificado para descriptografar arquivos que tenham sido criptografados anteriormente a falha. Claro que deve existir backup destes arquivos, caso contrário com a falha no HD você perderá os arquivos e aí não haverá utilização para a cópia do certificado do agente de recuperação que você fez no passo 1.

Exemplo 2: Para fazer o backup do Certificado digital do usuário, gerado automaticamente pelo Windows Server 2003, quando o usuário criptografa um arquivo ou pasta pela primeira vez, faça o seguinte:

1. Faça o logon com um a conta do usuário, para o qual você deseja fazer uma cópia de segurança do Certificado digital.
2. Abra o Internet Explorer.
3. Selecione o comando Ferramentas -> Opções da Internet...
4. Na janela Opções da Internet que é aberta dê um clique na guia Conteúdo.
5. Na guia Conteúdo dê um clique no botão Certificados... Será aberta a janela Certificados.
6. Na guia Pessoal, dê um clique no certificado que corresponde ao nome do usuário logado, conforme indicado na Figura 5.46, onde foi marcado o certificado para o usuário Administrador.
7. Clique no botão Exportar..., será aberto o Assistente para exportação de certificados, com o qual você já trabalhou no exemplo 1.
8. A primeira tela do assistente é apenas informativa, dê um clique no botão Avançar, para ir para a próxima etapa do assistente.
9. Nesta etapa você deve optar por exportar ou não a Chave particular do certificado.
10. Certifique-se de que a opção Sim, exportar a chave particular esteja marcada e dê um clique no botão Avançar, para ir para a próxima etapa do assistente.
11. Surge uma tela perguntando o formato para exportação do certificado. Aceite as configurações sugeridas pelo assistente e dê um clique no botão Avançar, para ir para a próxima etapa do assistente.



**Figura 5.46 A guia Pessoal da janela Certificados.**

12. Nesta etapa é solicitada uma senha de proteção para abertura do arquivo no qual será gravado o certificado. Digite a senha duas vezes para confirmação e dê um clique no botão Avançar, para ir para a próxima etapa do assistente. Esta senha não precisa ser igual a senha de logon da conta do usuário.
13. Surge uma tela solicitando o nome do arquivo para o qual será exportado o certificado. É recomendado que você exporte para um disquete ou para um drive de rede. Certifique-se de que você colocou um disquete no drive e, no campo Nome do arquivo, digite: A:\Admin.
14. Dê um clique no botão Avançar, para ir para a próxima etapa do assistente. O Windows Server 2003 exporta o certificado, para o arquivo especificado no drive de disquete.
15. Será exibida a tela final do assistente, com um resumo das opções selecionadas. Se você quiser fazer alguma alteração, pode utilizar o botão Voltar. Dê um clique no botão Concluir, para fechar o Assistente para exportação de certificados.
16. Surge uma mensagem informando que a exportação foi concluída com êxito. Dê um clique no botão OK para fechar esta mensagem.
17. Você estará de volta a guia Pessoal da janela Certificados e uma cópia do Certificado digital do usuário logado, foi gravada no disquete. No evento de uma falha do disco rígido, esta cópia pode ser utilizada para descriptografar os arquivos e pastas criptografados pelo usuário.
18. Clique no botão Fechar para fechar a janela Certificados.
19. Você estará de volta à janela Opções da Internet. Dê um clique no botão OK para fechá-la.
20. Você estará de volta ao Internet Explorer. Feche-o.

Com estes dois exemplos, você aprendeu a exportar o certificado do agente de recuperação e também o certificado de um usuário. Estes certificados podem ser importados a partir do disquete, no evento de falha do respectivo certificado original. É sempre recomendado que você proteja os certificados com a definição de uma senha e mantenha o disquete

em local seguro, pois caso contrário qualquer usuário que tiver acesso ao disquete poderá importar o certificado (conforme mostrarei logo a seguir) e utilizá-lo para ter acesso aos seus arquivos e pastas criptografados. Por isso a importância da definição de uma senha para exportação do certificado, pois esta senha será solicitada quando da importação do certificado. O certificado somente será importado com sucesso, se a senha correta for informada.

Na Figura 5.47 mostro os dois arquivos, com os certificados que foram exportados nos exemplos 1. e 2. Observe que o Windows Server 2003 usa ícones diferentes para o certificado do Agente de recuperação e para o certificado de usuário.

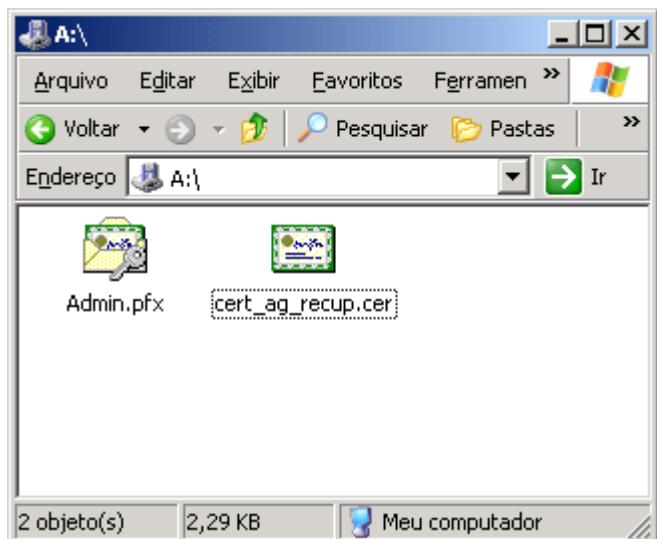


Figura 5.47 Cópia de segurança dos certificados.

Agora vou mostrar como importar um certificado a partir de um arquivo.

Exemplo 3: Para importar um certificado siga os passos indicados a seguir:

1. Abra a pasta onde está o certificado. No nosso exemplo, use o Meu computador ou o Windows Explorer para acessar o disquete (A:\), onde está o arquivo com o certificado a ser importado.
2. Clique com o botão direito do mouse no arquivo com o certificado a ser importado. Se você estiver importando o certificado do agente de recuperação, no menu que surge, dê um clique na opção Instalar certificado. Se você estiver importando o certificado de um usuário, no menu de opções que é exibido, dê um clique na opção Instalar PFX.
3. No nosso exemplo você irá importar o certificado de usuário, exportado no Exemplo 2. Clique com o botão direito do mouse no arquivo correspondente ao certificado a ser importado (Admin.pfx) e no menu de opções que surge, dê um clique na opção Instalar PFX.
4. Será aberto o Assistente para importação de certificados.
5. A primeira tela é apenas informativa. Dê um clique no botão Avançar, para seguir para a próxima etapa do assistente.
6. O campo Nome do arquivo já vem preenchido com o caminho e o nome do arquivo no qual clicamos com o botão direito do mouse. Dê um clique no botão Avançar, para seguir para a próxima etapa do assistente.
7. Se houver uma senha definida para o certificado, surgirá uma tela solicitando que seja digitada a senha. Digite a senha e dê um clique no botão Avançar, para seguir para a próxima etapa do assistente.
8. Nesta etapa você deve indicar o local para onde será importado o certificado. Aceita a opção sugerida pelo assistente, que por padrão é Selecionar automaticamente o armazenamento de certificados conforme o tipo de certificado, conforme indicado na Figura 5.48:

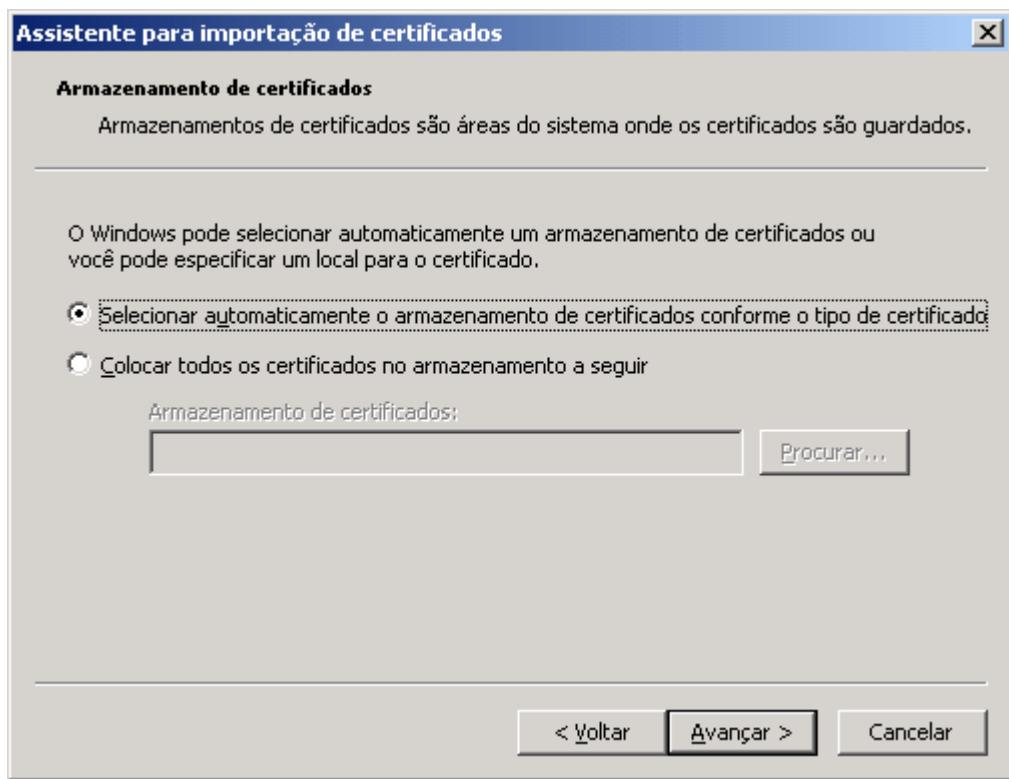


Figura 5.48 Definindo o local de armazenamento dos certificados.

9. Dê um clique no botão Avançar, para ir para a próxima etapa do assistente.
10. Será exibida a tela final do assistente, com um resumo das opções selecionadas. Se você quiser fazer alguma alteração, pode utilizar o botão Voltar. Dê um clique no botão Concluir, para fechar o Assistente para importação de certificados.
11. Surge uma mensagem informando que a importação foi concluída com êxito. Dê um clique no botão OK para fechar esta mensagem.

Agora sim, você já sabe exportar e importar certificados, para garantir o acesso aos dados criptografados. Agora é hora de começar a trabalhar com a criptografia no Windows Server 2003.

## Criptografando arquivos e pastas

É possível criptografar arquivos individualmente, porém é recomendado que você utilize a criptografia sempre em pastas. Ao criptografar uma pasta, todos os novos arquivos que forem criados dentro da pasta já serão automaticamente criptografados. Com isso você garante que todo o conteúdo da pasta está protegido.

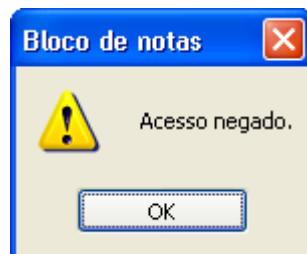


Figura 5.49 Mensagem de acesso negado.

Ao criptografar uma pasta e o seu conteúdo, somente o usuário que criptografou a pasta, terá acesso aos seus arquivos. Outros usuários poderão entrar na pasta e até mesmo verão uma listagem dos arquivos, porém ao tentar abrir um arquivo, receberão a mensagem indicada na Figura 5.49.

Exemplo 1: Para criptografar uma pasta e todo o seu conteúdo, siga os passos indicados a seguir:

1. Faça o logon com a sua conta de usuário. Somente você terá acesso aos arquivos da pasta que forem criptografados enquanto você estava logado com a sua conta de usuário.
2. Usando o Meu computador ou o Windows Explorer, localize a pasta a ser criptografada.
3. Clique com o botão direito do mouse na pasta a ser criptografada e, no menu de opções que é exibido, dê um clique na opção Propriedades. Será aberta a janela de propriedades da pasta, com a guia Geral selecionada.
4. Dê um clique no botão Avançado... Será aberta a janela Atributos avançados.
5. Para criptografar a pasta marque a opção Criptografar o conteúdo para proteger os dados, conforme indicado no exemplo da Figura 5.50:

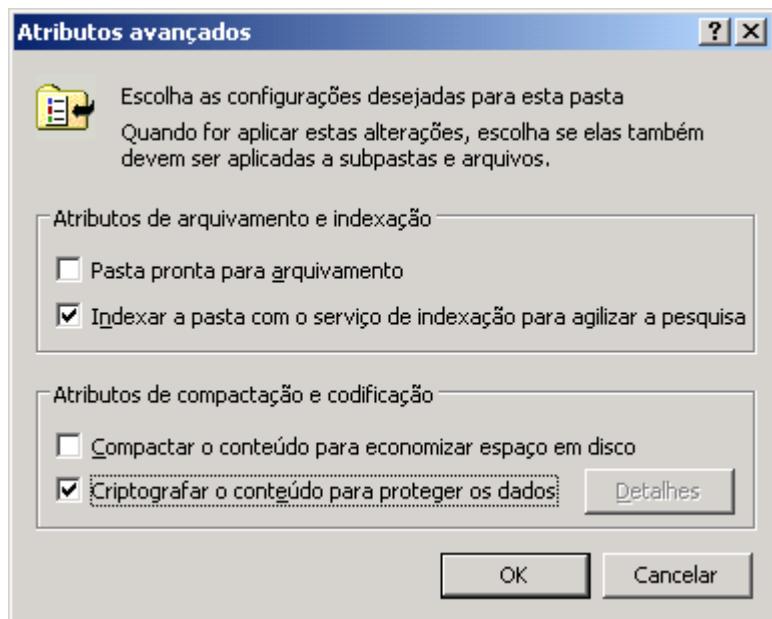


Figura 5.50 A opção Criptografar o conteúdo para proteger os dados.

6. Dê um clique no botão OK. Você estará de volta à janela de propriedades da pasta.
7. Dê um clique no botão OK. Surge uma janela perguntando se você deseja criptografar somente a pasta em questão ou todas as suas subpastas e arquivos. Selecione a opção Aplicar as alterações a esta pasta , subpastas e arquivos e dê um clique no botão OK.
8. O Windows Server 2003 inicia o processo de criptografia da pasta e de todo o seu conteúdo. Dependendo da quantidade de arquivos e subpastas, o processo de criptografia pode demorar alguns minutos. Durante este processo é exibida uma janela com o progresso da criptografia.

Pronto. A pasta está criptografada e somente o usuário que a criptografou terá acesso a pasta.

**IMPORTANTE:** Para impedir que outros usuários possam entrar em uma pasta que você criptografou e visualizar a listagem de arquivos, configure as permissões NTFS de tal maneira que somente você possa listar os arquivos desta pasta. Para maiores detalhes sobre a configuração de permissões NTFS, consulte o Capítulo 6.

Algumas observações muito importantes e que não devem ser esquecidas para o exame:

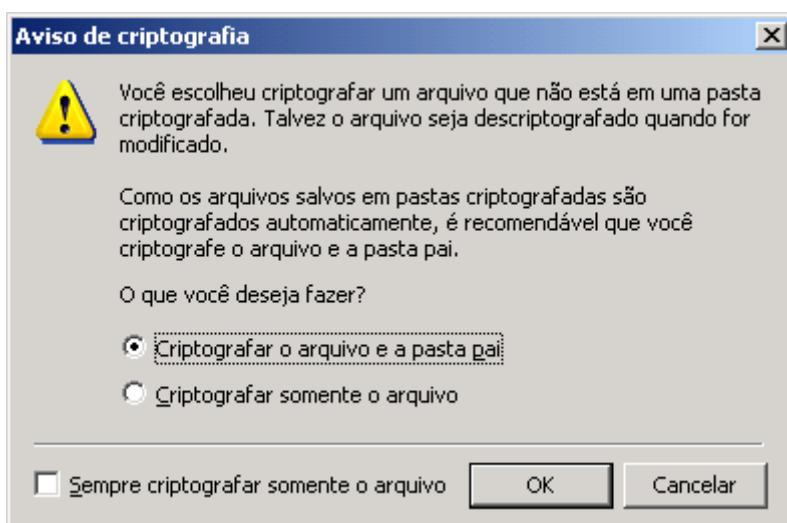
FIG5-4.tif

- ◆ As pastas e os arquivos compactados não podem ser, ao mesmo tempo, criptografados. Se você criptografar uma pasta ou um arquivo compactado, essa pasta ou esse arquivo será descompactado.
- ◆ Os arquivos marcados com o atributo Sistema não podem ser criptografados, bem como os arquivos que se encontram na estrutura de diretórios raiz dos volumes (C:\, D:\ e assim por diante).
- ◆ Ao criptografar um único arquivo, você poderá optar se deseja criptografar a pasta que contém o arquivo. Se você escolher essa opção, todos os arquivos e subpastas que forem adicionados posteriormente à pasta serão criptografados quando forem adicionados.
- ◆ Ao criptografar uma pasta, você poderá optar se deseja que todos os arquivos e subpastas dentro da pasta também sejam criptografados. Se você escolher essa opção, todos os arquivos e subpastas atualmente na pasta serão criptografados, bem como quaisquer arquivos e subpastas que forem adicionados à pasta mais tarde. Se você optar por criptografar somente a pasta, todos os arquivos e subpastas que se encontram atualmente na pasta não serão criptografados. No entanto, quaisquer arquivos e subpastas que forem adicionados à pasta mais tarde serão criptografados quando forem adicionados. É aconselhável que você sempre opte por criptografar todo o conteúdo da pasta, conforme descrito no passo 7 do Exemplo anterior. Com isso você não terá que manter um controle sobre quais pastas e/ou arquivos estão criptografados e quais não estão.

Para criptografar um único arquivo, o processo é semelhante a criptografar uma pasta, conforme descrito nos passos a seguir:

1. Utilizando o Windows Explorer ou o Meu computador, localize o arquivo a ser criptografado.
2. Clique com o botão direito do mouse no arquivo a ser criptografado. No menu de opções que surge, dê um clique na opção Propriedades. Será aberta a janela de propriedades do arquivo, com a guia Geral selecionada por padrão.
3. Dê um clique no botão Avançado... Será exibida a janela Atributos avançados.
4. Marque a opção Criptografar o conteúdo para proteger os dados e dê um clique no botão OK.
5. Será aberta a janela Aviso de criptografia, perguntando se você deseja criptografar o arquivo e a pasta pai (pasta onde está o arquivo) ou somente o arquivo, conforme indicado na Figura 5.51:

**NOTA:** Se você não quiser mais receber este aviso e fazer com que o Windows Server 2003 faça sempre a criptografia somente do arquivo, marque a opção Sempre criptografar somente o arquivo.



**IMPORTANTE:** Você também pode criptografar arquivos e pastas que estão em pastas compartilhadas, em outros computadores da rede. Basta mapear uma unidade para a pasta compartilhada (pastas compartilhadas e mapeamento de unidades será assunto do Capítulo 6), onde estão os arquivos e pastas a ser criptografados e utilizar os procedimentos descritos neste tópico, para criptografa-los.

Figura 5.51 A janela Aviso de criptografia.

6. Na janela Aviso de criptografia selecione a opção desejada e dê um clique no botão OK.
7. Você estará de volta à janela de propriedades do arquivo.
8. Dê um clique no botão OK. O Windows criptografa o arquivo e, dependendo das opções que você selecionou, também a pasta onde está o arquivo.

## Operações com Arquivos Criptografados (para o exame, não esqueça destes detalhes)

Ao copiar ou mover arquivos criptografados, diferentes situações podem ocorrer dependendo de a pasta de destino ser ou não criptografada e de estar ou não em um volume formatado com NTFS. A seguir descrevo algumas situações envolvendo ações de copiar e mover com arquivos criptografados.

- ◆ Ao copiar um arquivo não criptografado, para uma pasta criptografada, a cópia do arquivo será criptografada na pasta de destino. Por exemplo, você copia o arquivo não criptografado memo.doc, da pasta Meus documentos para a pasta Documentos pessoais, a qual está criptografada. O arquivo memo.doc copiado para a pasta Documentos pessoais será criptografado.
- ◆ Ao copiar um arquivo criptografado, para um volume NTFS em outro computador com o Windows 2000, Windows XP Professional ou Windows Server 2003, o arquivo manterá a criptografia. Se o computador de destino estiver rodando o Windows NT ou o volume for formatado com FAT, a cópia do arquivo não será criptografada.
- ◆ Se você mover um arquivo criptografado para outra pasta, no mesmo volume, o arquivo mantém a criptografia. Se você mover um arquivo criptografado para outro volume, o Windows Server 2003 considerará esta operação como sendo uma cópia, onde o arquivo é excluído na pasta de origem e copiado para a pasta de destino. Neste caso, o arquivo segue as regras explicadas no primeiro item.
- ◆ Se você renomear um arquivo criptografado, o arquivo continuará criptografado.
- ◆ Ao excluir um arquivo, a cópia do arquivo que fica na Lixeira, continuará criptografada.
- ◆ Se você fizer uma cópia de segurança de arquivos criptografados para uma fita de Backup ou para um outro volume NTFS, a cópia de segurança permanecerá criptografada.
- ◆ Se você quiser utilizar arquivos criptografados em outro computador, terá que importar o seu Certificado digital no computador de destino, conforme descrito anteriormente.
- ◆ Descriptografando arquivos e pastas.

**IMPORTANTE:** Se você tentar mover um arquivo criptografado por outro usuário, para um volume formatado com FAT, na tentativa de obter uma cópia não criptografada do arquivo, você receberá uma mensagem de Acesso negado, pois para descriptografar o arquivo (o que é necessário para move-lo para um volume FAT), você teria que ter acesso ao Certificado digital do usuário que criptografou o arquivo, conforme descrito anteriormente.

Enquanto um determinado arquivo estiver criptografado, o uso deste arquivo não muda para o usuário, ou seja, quando o usuário abre um arquivo criptografado, o Windows Server 2003 utiliza as informações do Certificado digital do usuário para descriptografar o arquivo e fornecer os dados para o usuário. Este processo é completamente transparente para o usuário, conforme já descrito anteriormente.

O usuário pode descriptografar um arquivo e/ou pasta a qualquer momento que desejar. O usuário pode utilizar este mecanismo em diversas situações, como por exemplo, para fornecer acesso ao arquivo para outros usuários. Para descriptografar um arquivo ou pasta é extremamente simples, basta seguir os seguintes passos:

1. Localize o arquivo ou pasta a ser descriptografado e dê um clique com o botão direito do mouse nele.

2. No menu de opções que surge dê um clique em Propriedades. Será exibida a janela de propriedades do arquivo/pasta.
3. Na guia Geral, da janela de Propriedades, dê um clique no botão Avançado...
4. Na janela Atributos avançados, desmarque a opção Criptografar o conteúdo para proteger os dados.
5. Dê um clique no botão OK.
6. Você estará de volta à janela Propriedades. Dê um clique no botão OK.
7. Se você estiver descriptografando uma pasta, surge a mensagem indicada perguntando se você deseja descriptografar apenas a pasta ou todo o seu conteúdo. Selecione a opção desejada e dê um clique no botão OK.
8. A pasta será descriptografada e também o seu conteúdo, dependendo das opções selecionadas. Se você optar por descriptografar somente a pasta, novos arquivos criados na pasta não serão criptografados, porém os arquivos já existentes, manterão a criptografia.

## Permitindo que outros usuários tenham acesso a arquivos e pastas que você criptografou

Você pode permitir que outros usuários acessem arquivos ou pastas que você criptografou. Pode ser que além de você, outros usuários também devam ter acesso ao arquivo criptografado. Nesta situação você continua utilizando a criptografia, para garantir a segurança dos dados e pode autorizar um ou mais usuários a acessar o arquivo.

Exemplo: Para permitir o acesso de outros usuários a um arquivo criptografado, faça o seguinte:

1. Faça o logon com a sua conta de usuário.
2. Usando o Meu computador ou o Windows Explorer, localize e o arquivo que você criptografou e para o qual você quer configurar acesso para outros usuários.
3. Clique com o botão direito do mouse no arquivo e no menu que é exibido dê um clique na opção Propriedades. A janela Propriedades do arquivo será aberta, com a guia Geral selecionada.
4. Dê um clique no botão Avançados... Será exibida a janela Atributos avançados.
5. Dê um clique no botão Detalhes, ao lado da opção Criptografar o conteúdo para proteger os dados. Será exibida a janela Detalhes de criptografia. Nesta janela é exibida a lista de usuários com acesso ao arquivo criptografado. Por padrão, consta na lista, apenas o nome do usuário que criptografou o arquivo. Para adicionar permissão de acesso a outros usuários, dê um clique no botão Adicionar...

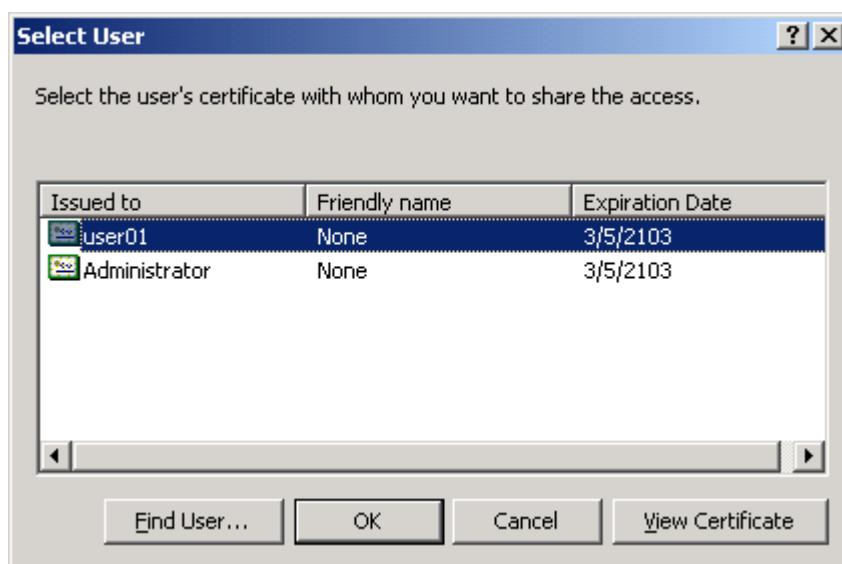
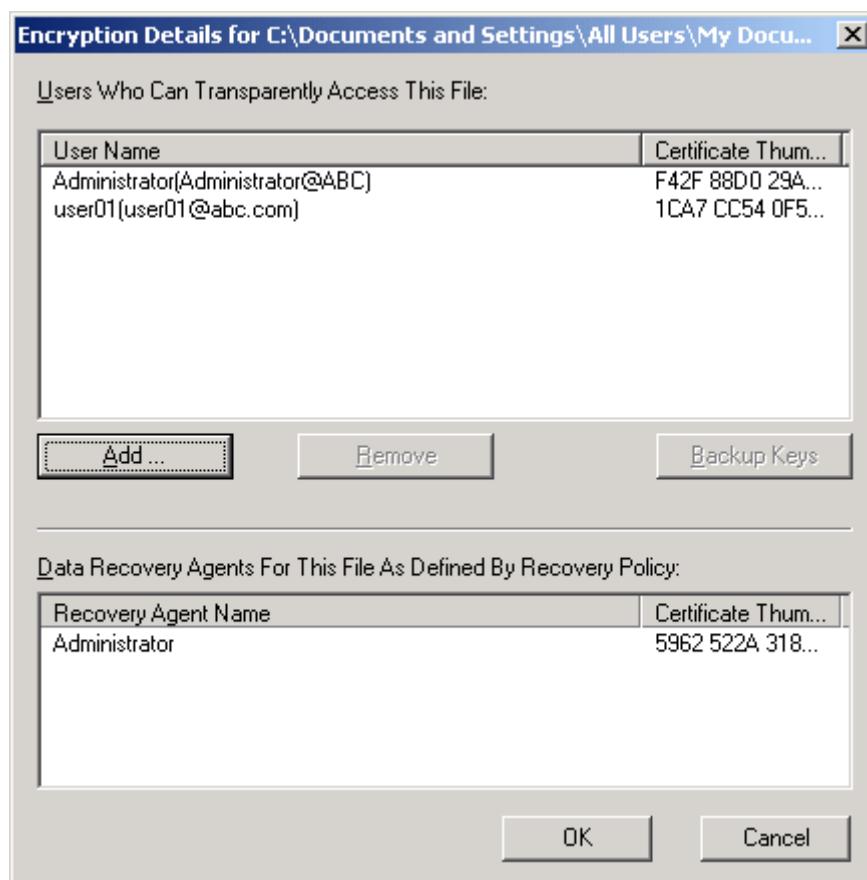


Figura 5.52 Permitindo acesso para outros usuários.

6. Será exibida a janela Seleione o usuário. Nesta janela é exibida a listagem de todos os usuários que possuem um Certificado digital, ou seja, de todos os usuários que já criptografaram pelo menos um arquivo ou pasta no computador que você está utilizando. Selecione o usuário para o qual você deseja permitir acesso, conforme exemplo da Figura 5.52 (baseada em um servidor com o Windows Server 2003 em Inglês) e dê um clique no botão OK.
7. Você estará de volta à janela Detalhes de criptografia e o usuário selecionado na janela da Figura 5.52 já aparece na lista, conforme indicado na Figura 5.53:



**Figura 5.53 A janela Detalhes de criptografia.**

8. Repita os passos 5, 6 e 7 para adicionar mais usuários a lista de usuários com permissão de acesso ao arquivo criptografado.
9. Dê um clique no botão OK. Você estará de volta à janela Atributos avançados.
10. Dê um clique no botão OK para fechar a janela Atributos avançados. Você estará de volta à janela de propriedades do arquivo.
11. Dê um clique no botão OK para fechar a janela de Propriedades do arquivo.

**IMPORTANTE:** Não é possível adicionar grupos para acessar a criptografia de arquivos, a permissão tem que ser definida usuário por usuário.

## Alterando a diretiva de recuperação do Computador local

É possível alterar as configurações do Agente de recuperação do seu computador ou no caso de trabalhar em um domínio, do domínio como um todo. Você pode adicionar novas contas, além da conta padrão Administrador, pode inclusive excluir todos os usuários da lista de Agentes de recuperação, o que implicará na desabilitação do sistema de criptografia, conforme será detalhado mais adiante.

Exemplo: Para alterar a diretiva de recuperação do domínio, faça o seguinte:

1. Faça o logon com uma conta com permissões de Administrador.
2. Abra o console Diretiva de segurança de domínio: Iniciar -> Ferramentas Administrativas -> Diretiva de segurança de domínio. Clique no sinal de + ao lado da opção Configurações de segurança.
3. Nas opções que são exibidas dê um clique no sinal de + ao lado da opção Diretivas de chave pública.
4. Nas opções que são exibidas dê um clique na opção Sistemas de arquivos criptografados. No painel da direita será exibido o Certificado do Agente de recuperação, que por padrão é a conta Administrator (Administrador).
5. Clique com o botão direito do mouse na opção Sistema de arquivos criptografados e siga uma dos seguintes caminhos:
  - 5.1. Para designar um usuário como agente de recuperação adicional através do Assistente para adicionar agente de recuperação, clique na opção Adicionar agente de recuperação de dados... e siga os passos do assistente.
  - 5.2. Para solicitar um novo certificado de recuperação de arquivo através do Assistente para solicitação de certificados, clique em Novo -> Agente de recuperação de dados.... Será aberto o Assistente para adicionar agente de recuperação. Siga os passos do assistente.
  - 5.3. Para excluir essa diretiva de EFS e todos os agentes de recuperação, clique em Todas as Tarefas -> Excluir diretiva. Se você selecionar essa opção, os usuários não poderão mais usar criptografia nos computadores do domínio. O Windows Server 2003 não permite que você faça a criptografia de arquivos se não houver um Agente de recuperação configurado. Para voltar a habilitar a criptografia de arquivos, você deve seguir os passos descritos neste exemplo e adicionar um Agente de recuperação.
6. Após ter configurado as opções desejadas, feche o MMC. Surge uma janela perguntando se você deseja salvar o console. Clique em Não.

Algumas observações importantes:

- ◆ Antes de qualquer alteração na diretiva de recuperação, você deve fazer um backup das chaves de recuperação em um disquete, conforme descrito nos exemplos anteriores. Este procedimento garante que os arquivos poderão ser descriptografados caso haja algum problema com as configurações do Agente de recuperação.
- ◆ É necessário fazer logon como administrador ou com uma conta com permissões de administrador para executar estas ações.
- ◆ Se a sua conta for configurada como Agente de recuperação, você poderá descriptografar arquivos criptografados por outros usuários, simplesmente acessando as propriedades do arquivo, clicando no botão Avançado... e desmarcando a opção Criptografar o conteúdo para proteger os dados. Para realizar tal operação, o Certificado digital correspondente a conta do Agente de recuperação deve estar instalado no computador onde a operação será realizada. Para maiores detalhes sobre a Importação e Exportação de certificados, consulte a parte inicial deste tópico.

## Recomendações sobre a criptografia de pastas e arquivos

Neste item coloco algumas recomendações sobre a criptografia de pastas e arquivos. Estas recomendações são baseadas na documentação oficial da Microsoft:

- ◆ Para obter o máximo de segurança, criptografe as pastas antes de criar arquivos importantes nelas. Isso faz com que os arquivos criados sejam automaticamente criptografados e seus dados nunca sejam gravados em disco como texto sem formatação.
- ◆ Se você salvar a maior parte dos seus documentos na pasta Meus documentos, criptografe-a. Isso assegura que seus documentos pessoais sejam criptografados por padrão. No caso de perfis de usuários móveis, deve-se fazer isso apenas se a pasta Meus documentos for redirecionada para um local de rede.

- ◆ Criptografe pastas em vez de arquivos individuais para que, caso um programa crie arquivos temporários durante a edição, eles também sejam criptografados.
- ◆ O agente de recuperação designado deverá exportar o certificado de recuperação de dados e a chave particular para um disco, guardá-los em um local seguro e excluir do sistema a chave particular de recuperação de dados. Dessa forma, a única pessoa que poderá recuperar dados do sistema será aquela que possui acesso físico à chave particular de recuperação de dados. Estes procedimentos foram descritos no início deste tópico.
- ◆ Deve-se manter o menor número possível de agentes de recuperação designados. Desse modo, menos chaves ficarão expostas ao ataque criptográfico e haverá mais garantias de que os dados criptografados não sejam descriptografados inadequadamente.

## O comando cipher

O comando cipher é utilizado para exibir ou alterar a criptografia de pastas e arquivos em volumes NTFS. Quando utilizado sem parâmetros, cipher exibe o estado de criptografia da pasta atual e de quaisquer arquivos que ela contenha.

Sintaxe para o comando cipher, conforme documentação oficial da Microsoft:

```
cipher [{/e}|/d] [/s:dir] [/a] [/i] [/f] [/q] [/h] [/k] [/u[/n]] [nome_de_caminho [...]] | [/r:nome_de_caminho_sem_extensão] | [/w:nome_de_caminho]
```

Na tabela 5.2, apresento a descrição dos parâmetros do comando cipher.

**Tabela 5.2 Parâmetros do comando cipher**

| Parâmetro | Descrição   |
|-----------|---|
| /e        | Criptografa as pastas especificadas. As pastas serão marcadas para que os arquivos adicionados a elas posteriormente também sejam criptografados.   |
| /d        | Descriptografa as pastas especificadas.   |
| /s:dir    | Efetua a operação selecionada na pasta especificada e em todas as subpastas.  |
| /a        | Efetua a operação nos arquivos e pastas.  |
| /i        | Continua a efetuar a operação especificada mesmo após a ocorrência de erros. Por padrão, cipher é interrompido quando um erro é encontrado.   |
| /f        | Força a criptografia ou descriptografia de todos os objetos especificados. Por padrão, os arquivos que já tenham sido criptografados ou descriptografados serão ignorados por cipher.   |
| /q        | Reporta somente as informações mais essenciais.   |
| /h        | Exibe arquivos com atributos de sistema ou ocultos. Por padrão, esses arquivos não são criptografados ou descriptografados.   |
| /k        | Cria uma nova chave de criptografia de arquivo para o usuário que estiver executando o comando cipher. Se você usar esta opção, cipher ignorará todas as outras opções.   |
| /u        | Atualiza a chave de criptografia de arquivo do usuário ou a chave do agente de recuperação, utilizando as mais atuais em todos os arquivos criptografados nas unidades locais (isto é, se as chaves tiverem sido alteradas). Esta opção só funciona com /n. |

| Parâmetro     | Descrição   |
|---------------|---|
| /n            | Evita que as chaves sejam atualizadas. Use esta opção para localizar todos os arquivos criptografados nas unidades locais. Esta opção só funciona com /u.   |
| nomedecaminho | Especifica um padrão, arquivo ou pasta.   |
| /r :nome de   | Gera uma nova chave particular e um novo certificado de caminho sem agente de recuperação e grava-os nos arquivos com extensão o nome de arquivo especificado em nome_de_caminho_sem_extensão. Se você usar esta opção, cipher ignorará todas as outras opções. |
| /w:nome de    | Remove os dados que se encontram em partes não utilizadas caminho de um volume. nome_de_caminho pode indicar qualquer pasta no volume desejado. Se você usar esta opção, cipher ignorará todas as outras opções.  |
| /?            | Exibe informações de ajuda no prompt de comando.  |

O comando cipher não criptografa arquivos que estejam marcados como somente leitura.

Eis alguns exemplos do comando cipher:

1. Para usar o comando cipher para criptografar uma subpasta denominada Memorandos em uma pasta denominada Documentos, utilize o seguinte comando:  
**cipher /e Documentos\Memorandos**
2. Para criptografar a pasta Documentos, e todas as suas subpastas, digite o seguinte comando:  
**cipher /e /s:Documentos**
3. Para criptografar apenas o arquivo finanças.xls na subpasta Planilhas, da pasta Documentos, utilize o seguinte comando:  
**cipher /e /a Documentos\Planilhas\finanças.xls**
4. Para criptografar todos os arquivos .xls da subpasta Planilhas, da pasta Documentos, digite o seguinte comando:  
**cipher /e /a Documentos\Planilhas\\*.xls**
5. Para determinar se a pasta Documentos está criptografada, utilize o seguinte comando:  
**cipher Documentos**

Para determinar os arquivos na pasta Documentos que estão criptografados, utilize o seguinte comando:

```
cipher Documentos\*
```

## Conclusão

Neste capítulo apresentei os conceitos de armazenamento básico e armazenamento dinâmico, bem como a diferença entre ambos. Em seguida mostrei como realizar um série de tarefas administrativas relacionadas com discos, partições (em discos básicos) e volumes (em discos dinâmicos). Você aprendeu sobre os diferentes tipos de partições que podem ser criadas em discos básicos e os diferentes tipos de volumes que podem ser criados em discos dinâmicos. Também aprendeu a converter um disco básico para disco dinâmico.

O próximo passo foi falar sobre as ferramentas para manutenção preventiva de volumes e partições. Você aprendeu sobre o conceito de fragmentação de discos e aprendeu a utilizar o utilitário de desfragmentação de volumes (e partições), o qual está bem mais eficiente no Windows Server 2003 em relação ao utilitário de desfragmentação do Windows 2000 Server. Você também aprendeu sobre os utilitários de linha de comando disponíveis para o gerenciamento de discos e volumes.

Na seqüência apresentei diversos detalhes sobre uma das características que é exclusiva do sistema de arquivos NTFS: Criptografia de Arquivos.

A tecnologia de criptografia do Windows Server 2003 é baseada no EFS – Encrypted File System (Sistema de arquivos criptografados). O EFS fornece todo o suporte necessário para trabalhar com arquivos criptografados. Somente arquivos e pastas em volumes NTFS podem ser criptografados. Esta, aliás, é uma das tantas vantagens do sistema de arquivos NTFS em relação ao sistema FAT/FAT32. Estas diferenças serão discutidas em detalhes no Capítulo 6.

Você aprendeu a trabalhar com os certificados que gerenciam a criptografia de arquivos, aprendeu a criptografar e a descriptografar arquivos e pastas, aprendeu o que acontece quando arquivos e pastas criptografadas são copiados e/ou movidos para diferentes destinos e também aprendeu a utilizar o comando cipher, para gerenciar a criptografia de arquivos e pastas. O uso do comando cipher é especialmente útil quando você cria scripts para administração da criptografia de pastas e arquivos.

No próximo capítulo você estudará o sistema NTFS em detalhes, aprenderá a compartilhar pastas e arquivos, aprenderá sobre permissões de compartilhamento, permissões NTFS, interação entre estes dois tipos de permissão e uma série de outros assuntos relacionados com o sistema de arquivos NTFS.

# Introdução

Conforme descrito no Capítulo 2, o Windows Server 2003 desempenha o papel de servidor de rede. O principal recurso, o recurso mais utilizado é o compartilhamento de arquivos através da rede. Os arquivos ficam em uma pasta compartilhada no servidor e são acessados a partir das estações de trabalho da rede. O acesso pode ser feito via drive mapeado o diretamente usando o caminho UNC – Universal Naming Convention, também descrito no Capítulo 2.

Neste capítulo você aprenderá a criar e a administrar Pastas compartilhadas. Ao compartilhar uma pasta, esta passa a estar acessível para outros computadores da rede. O uso de pastas compartilhadas é a maneira de possibilitar a todos os usuários da rede, o acesso a uma ou mais pastas, na qual são gravados arquivos de interesse comum, utilizados por um grupo de pessoas. Por exemplo, pode ser o caso de uma equipe de projeto que utiliza uma pasta compartilhada em um servidor, para gravar os arquivos com os manuais e a documentação do projeto. Desta maneira todos tem acesso aos referidos arquivos. O mais importante é que ao utilizar um único local de armazenamento – a pasta compartilhada – todos estão tendo acesso a mesma versão de cada documento. Isto evita a situação em que os documentos estão espalhados em pastas de vários computadores e um documento é alterado. Neste caso, para que os demais participantes do grupo possam ter acesso a versão atualizada do documento, é necessário copiar o arquivo com a versão atualizada para cada um dos computadores. Vejam que este seria um método bem mais trabalhoso. Com a pasta compartilhada não, alterou um documento, todos acessam a versão atualizada.

Ao criar uma pasta compartilhada o administrador pode definir quais usuários tem acesso à pasta e qual o nível de acesso de cada usuário ou grupo. Por exemplo, o administrador pode dar permissão de leitura e escrita para um determinado grupo e somente de leitura para outro grupo e, ainda, negar o acesso para um terceiro grupo. Para definir as permissões, conforme comentado no Capítulo 2, é recomendada a utilização de grupos, ao invés de definir as permissões individualmente para cada usuário. Não que não seja possível definir as permissões para cada usuário individualmente. Possível é, apenas é recomendado que se utilize grupos, para facilitar a definição e a administração das permissões de acesso.

Uma pasta compartilhada pode ser acessada de diversas maneiras, conforme mostrarei neste capítulo. Pode-se usar diretamente o caminho para a pasta ou pode-se montar um drive. Montar um drive significa que será exibido um novo drive no sistema, como por exemplo: X: ou Y: ou S:. Na prática, este drive é um atalho para a pasta compartilhada, ou seja, ao acessar o referido drive, o usuário está, na verdade, acessando a pasta compartilhada. O uso de drives montados facilita o acesso as pastas compartilhadas, pois o usuário não precisa lembrar o nome do servidor e o nome do compartilhamento, tudo o que o usuário precisa é acessar o drive que serve como atalho para a pasta compartilhada.

Em seguida falarei um pouco sobre sistemas de arquivos e mais especificamente sobre o sistema de arquivos NTFS. Mostrarei que com o sistema de arquivos NTFS é possível definir permissões de acesso para pastas e arquivos, é possível

# CAPÍTULO

# 6

## Criando e Administrando Pastas Compartilhadas e Permissões de acesso

compactar pastas e arquivos, criptografar (assunto visto no Capítulo 5) e configurar auditoria de acesso a pastas e arquivos. Você aprenderá sobre os tipos de permissões NTFS existentes e como configurá-las. Farei diversos exemplos prático para que você possa entender como funcionam as permissões NTFS e como são combinadas as permissões de pastas com as permissões de arquivos e com as permissões de compartilhamento.

Você aprenderá a definir permissões para usuários e grupos e verá que as permissões são cumulativas. Também falarei sobre a precedência de negar sobre permitir. Por fim mostrarei como são combinadas as permissões NTFS com as permissões de compartilhamento. Pode existir situações em que existe um conjunto de permissões de compartilhamento e um conjunto diferente de permissões NTFS. Nestes casos você tem que saber avaliar qual a permissão efetiva resultante. Também falarei sobre o conceito de “Tornar-se dono de um arquivo ou pasta – Take Ownership”. Mostrarei como realizar esta operação e em que situações é necessário o uso de Take Ownership para recuperar o acesso a arquivos e pastas.

Para finalizar o capítulo falarei sobre o DFS – Distributed File System. O DFS é um serviço que permite a consolidação de diversos compartilhamentos com a criação de uma Árvore de Compartilhamentos. O usuário tem acesso aos vários compartilhamentos através de um único drive, o qual aponta para a raiz da árvore e cada compartilhamento individual aparece como uma pasta do drive mapeado. O DFS apresenta importantes melhorias no Windows Server 2003, em relação ao Windows 2000 Server. A principal melhoria é a possibilidade de criar mais de uma árvore DFS (chamdo DFS root) por servidor.

## Pastas compartilhadas, Permissões de Compartilhamento e Permissões NTFS.

Vou iniciar o capítulo apresentando os conceitos teóricos relacionados com o compartilhamento de pastas, permissões de compartilhamento, permissões NTFS e a interação entre permissões de compartilhamento e permissões NTFS.

Quando o administrador compartilha uma pasta, ele está permitindo que o conteúdo da pasta seja acessado por outros computadores da rede. Quando uma pasta é compartilhada, os usuários podem acessá-la através da rede, bem como o conteúdo (subpastas e arquivos) da pasta que foi compartilhada. Por exemplo, você pode criar uma pasta compartilhada onde são colocados documentos, orientações e manuais, de tal forma que os estes possam ser acessados a partir de qualquer estação de trabalho conectada à rede.

Ao compartilhar uma pasta todo o conteúdo da pasta passa a estar disponível para acesso através da rede. Isso significa que se houverem outras subpastas, dentro da pasta compartilhada, estas também estarão disponíveis para acesso pela rede.

Considere o exemplo da Figura 6.1. Se a pasta C:\Documentos for compartilhada, todo o seu conteúdo e também o conteúdo das subpastas C:\Documentos\Ofícios e C:\Documentos\Memorandos estarão disponíveis para acesso através da rede.

Quando uma pasta é compartilhada em um computador, é criado um caminho para acessar esta pasta a partir dos demais computadores da rede. Este caminho segue o padrão UNC – Universal Naming Convention (Convenção Universal de Nomes). Todo caminho que segue o padrão UNC inicia com duas barras invertidas, seguida pelo nome do computador onde está o recurso compartilhado (que pode ser uma pasta compartilhada, um impressora compartilhada, etc), mais uma barra invertida e o nome do compartilhamento. Imagine que você está compartilhando recursos em um servidor da rede cujo nome é: SRVRS001. Neste servidor são criadas três pastas compartilhadas com os seguintes nomes de compartilhamento: documentos, manuais e memorandos. No servidor SRVRS001 você também compartilha uma impressora com o nome de compartilhamento lasera1. Qual seria o caminho para acessar estes recursos, segundo o padrão UNC?

- ◆ \\SRVRS001\documentos
- ◆ \\SRVRS001\manuais
- ◆ \\SRVRS001\memorandos
- ◆ \\SRVRS001\lasera1

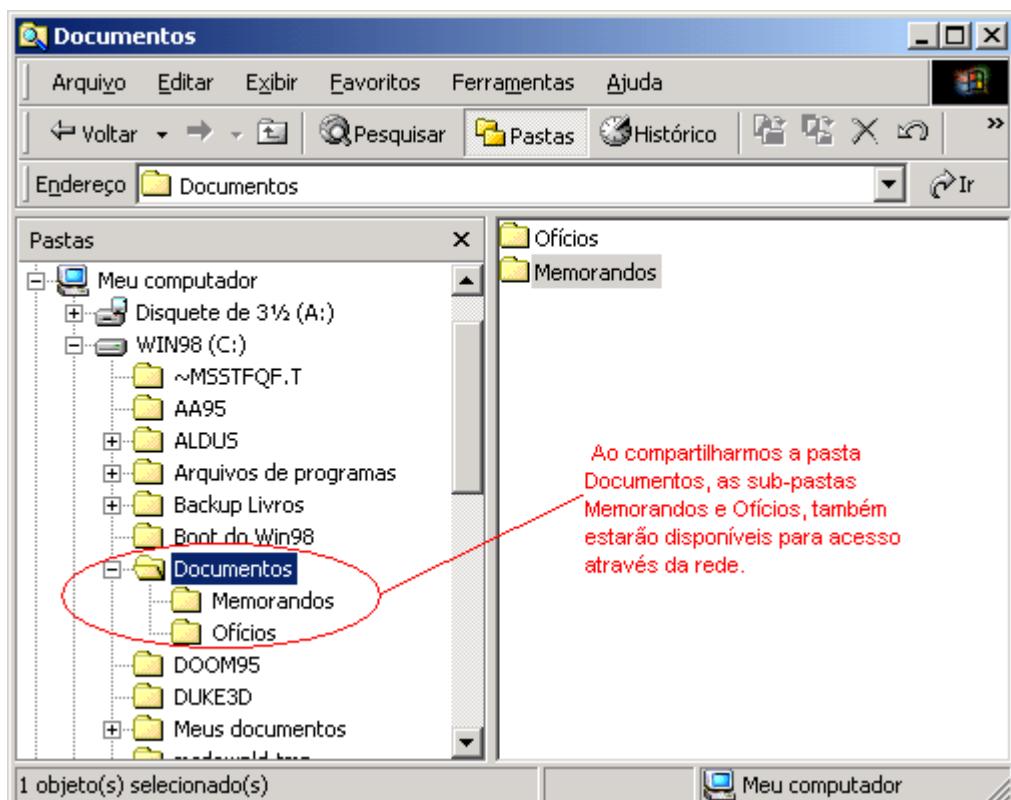


Figura 6.1 Ao compartilhar uma pasta, todo o seu conteúdo estará disponível.

## Restringindo o acesso às pastas compartilhadas.

Porém quando uma pasta é compartilhada, não significa que o seu conteúdo deva ser acessado por todos os usuários da rede. É possível restringir quais usuários terão acesso à pasta compartilhada, e qual o número máximo de usuários que podem acessar a pasta simultaneamente. Esta restrição é feita através de Permissões de compartilhamento.

Com o uso de permissões de compartilhamento é possível definir quais os usuários que poderão acessar o conteúdo da pasta compartilhada. Para isso, é criada uma lista com o nome dos usuários e grupos que possuem permissão de acesso. Esta lista é tecnicamente conhecida como ACL – Access Control List (Lista de Controle de Acesso).

Também é possível limitar o que os usuários com permissão de acesso podem fazer. Pode haver situações em que alguns usuários devem ter permissão apenas para ler o conteúdo da pasta compartilhada, podem haver outras situações em que alguns usuários devem ter permissão de leitura e escrita, enquanto outros devem ter permissões totais, tais como leitura, escrita e até exclusão de arquivos e assim por diante.

**NOTA:** Conforme mostrarei na parte prática, o nome do compartilhamento não precisa ser igual ao da pasta que está sendo compartilhada. É recomendado que o nome do compartilhamento sirva como indicação para o conteúdo da pasta compartilhada, para facilitar a localização dos recursos disponíveis na rede e a pesquisa no Active Directory.

Na Figura 6.2, mostro um exemplo, em que o grupo Gerentes possui permissões de Controle total, enquanto o grupo Usuários possui permissões apenas para leitura.

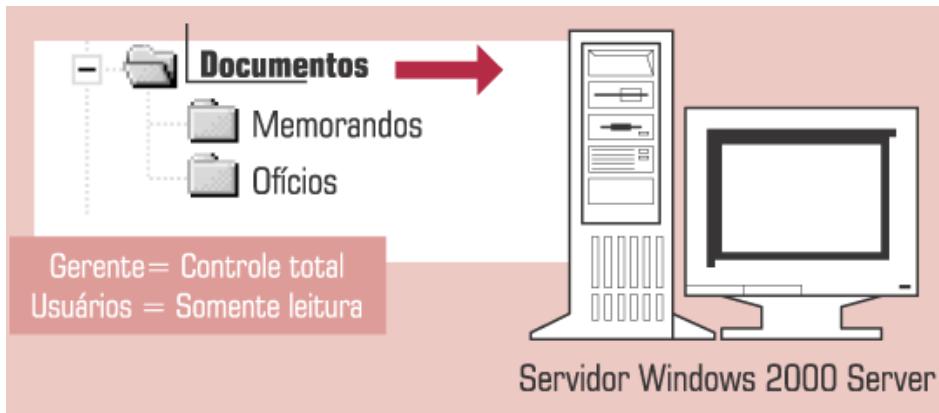


Figura 6.2 Grupos diferentes com permissões diferentes.

Ao criar um compartilhamento em uma pasta, por padrão o Windows Server 2003 atribui como permissão de compartilhamento Read (Somente Leitura) para o grupo Everyone (Todos), que conforme o nome sugere, significa qualquer usuário com acesso ao computador, seja localmente, seja pela rede. Ou seja, ao criar um compartilhamento, automaticamente será permitida a leitura em todo o conteúdo do compartilhamento para todos os usuários da rede. Esta situação já é um pouco melhor do que ocorria com o Windows 2000 Server, onde era definida, por padrão, permissão Full Control (Controle Total) para o grupo Everyone (Todos). Por isso ao criar um compartilhamento, o administrador já deve configurar as permissões necessárias, a menos que esteja sendo compartilhada uma pasta de domínio público, onde todos os usuários devam ter acesso de leitura em todos os arquivos e subpastas da pasta que está sendo compartilhada.

## Entendendo as permissões de compartilhamento.

Existem três níveis de permissões de compartilhamento, conforme descrito a seguir:

Leitura: A permissão de Leitura permite ao usuário:

- ◆ Listar os nomes de arquivos e de subpastas, dentro da pasta compartilhada.
- ◆ Acessar as subpastas dentro da pasta compartilhada.
- ◆ Abrir os arquivos para leitura.
- ◆ Execução de arquivos de programa (.exe, .com, etc).

Alteração: Permite ao usuário os mesmos direitos da permissão leitura, mais os seguintes direitos:

- ◆ Criação de arquivos e subpastas.
- ◆ Alteração de dados nos arquivos
- ◆ Exclusão de subpastas e arquivos

**IMPORTANTE:** As permissões definem o que o usuário pode fazer com o conteúdo de uma pasta compartilhada, desde somente leitura, até um controle total sobre o conteúdo da pasta compartilhada. Porém as permissões de compartilhamento somente tem efeito se o acesso for feito pela rede. Se o usuário fizer o logon no computador onde está a pasta compartilhada e acessa-la localmente, através do drive C: (ou outro drive qualquer onde está a pasta compartilhada), as permissões de compartilhamento não serão verificadas e, portanto, não terão nenhum efeito. Para limitar o acesso, mesmo localmente, usa-se as permissões NTFS, as quais serão descritas mais adiante.

**Não esqueça:** Permissões de compartilhamento, não impedem o acesso ao conteúdo da pasta localmente, isto é, se um usuário fizer o logon no computador onde está a pasta compartilhada, o usuário terá acesso a todo o conteúdo da pasta, a menos que as Permissões NTFS estejam configurados de acordo. Permissões NTFS é assunto para daqui a pouco.

**IMPORTANTE:** Pastas e arquivos possuem atributos, que o Windows Server 2003 utiliza para gerenciar

- ◆ **Controle total:** Esta é a permissão padrão que se aplica a todos os novos compartilhamentos. Essa permissão era atribuída ao grupo Everyone (Todos) ao compartilhar um recurso no Windows 2000 Server. Já no Windows Server 2003 é atribuída a permissão Read (Somente Leitura) ao grupo Everyone (Todos) por padrão, quando um novo compartilhamento é criado. Controle total possibilita as mesmas operações que Leitura e Alteração, mais as seguintes:
  - ◆ Alteração de permissões (apenas para arquivos e pastas do NTFS)
  - ◆ Apropriação (Take Ownership), apenas para arquivos e pastas em um volume formatado com NTFS.

As permissões de compartilhamento: Leitura, Alteração e Controle total, podem ser Permitidas ou Negadas. Ou seja podemos permitir o acesso com um determinado nível (leitura, alteração ou Controle total) ou negar explicitamente o acesso para um usuário ou grupo para quaisquer uma destas permissões. Considere um exemplo prático. Suponha que todos os usuários do grupo Gerentes devem ter acesso de Leitura a uma pasta compartilhada, com exceção de um gerente cuja conta de usuário é jsilva, o qual deve ter negado o direito de leitura na referida pasta. Para simplificar a atribuição de permissões o administrador faz o seguinte:

- ◆ Permissão de Leitura para o grupo Gerentes – Permitir.
- ◆ Permissão de Leitura para o usuário jsilva – Negar.

Com isso todos os usuários do grupo Gerentes terão permissão de leitura, com exceção do usuário “jsilva”, o qual teve a permissão de leitura negada. Outra recomendação é que sempre devemos atribuir permissões para grupos de usuários, ao invés de atribuir para usuários individuais, pois isso facilita a administração, conforme descrito no Capítulo 4.

## Quando um usuário pertence a mais de um grupo, como é que fica a permissão efetiva do usuário??

Quando um usuário pertence, por exemplo, a dois grupos e os dois grupos recebem permissão para acessar um compartilhamento, sendo que os dois grupos possuem permissões diferentes, por exemplo, um tem permissão de Leitura e o outro de Alteração. Como é que ficam as permissões do usuário que pertence aos dois grupos ?

Para responder a esta questão, considere as seguintes observações:

- ◆ Quando um usuário pertence a mais de um grupo, cada qual com diferentes níveis de permissões para uma pasta compartilhada, o nível de permissão para o usuário que pertence a mais de um grupo, é a combinação das permissões atribuídas aos diferentes grupos.

No exemplo a seguir, o usuário pertence a dois grupos, um com permissão de somente leitura e outro com permissão de alterações. A nível de permissão do usuário é de alterações, pois é a soma das permissões dos dois grupos, conforme indicado na Figura 6.3:

os arquivos. Por exemplo, existe um atributo Somente leitura, que uma vez marcado torna o arquivo somente leitura, isto é, não podem ser feitas alterações no arquivo. Para ver os atributos de um arquivo ou pasta, basta dar um clique com o botão direito do mouse no arquivo ou pasta, e no menu que surge dê um clique na opção Propriedades. O Windows Server 2003 exibe uma janela onde é possível verificar e modificar os atributos do arquivo ou pasta, desde que o usuário tenha as devidas permissões.

**IMPORTANTE:** No Windows Server 2003, objetos como pastas e arquivos possuem um “dono”, o qual por padrão é o usuário que estava logado e que criou a pasta ou arquivo. Conforme mostrarei no final deste capítulo é possível, ao Administrador, tornar-se dono de uma pasta ou arquivo, utilizando uma ação de Take Ownership (Tornar-se dono).

**IMPORTANTE:** Negar sempre tem precedência sobre permitir. Por exemplo, se o usuário pertencer a cinco grupos, sendo que quatro dos quais tem permissão de acesso e o outro grupo tem negada a permissão de acesso, o usuário terá negada a permissão de acesso. A permissão negar acesso, herdada de um dos grupos, terá precedência sobre todas as demais permissões herdadas dos demais grupos.

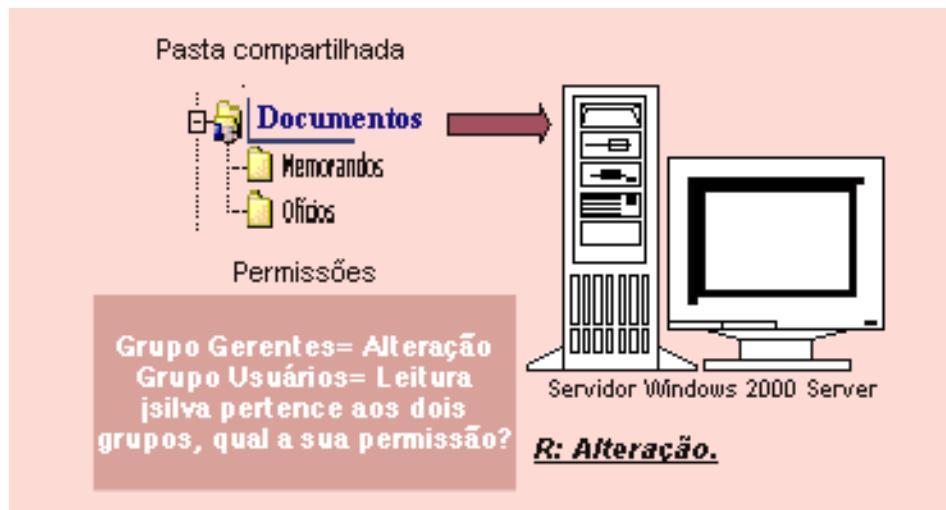


Figura 6.3 Usuário que pertence a mais de um grupo.

Negar têm precedência sobre quaisquer outras permissões:

Vamos considerar o exemplo do usuário que pertence a três grupos. Se em um dos grupos ele tiver permissão de leitura e em outro grupo permissão de alteração. Mas se para o terceiro grupo, for negada a permissão de leitura, o usuário terá o acesso negado, uma vez que Negar tem precedência sobre quaisquer outras permissões, conforme indicado pela Figura 6.4.

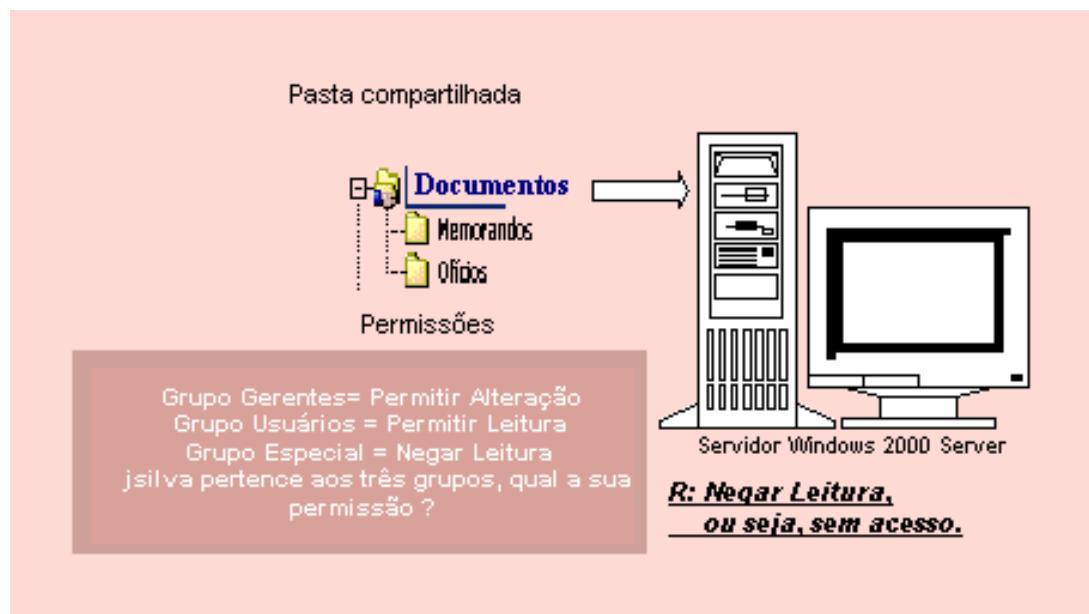


Figura 6.4 Negar tem precedência sobre permitir.

---

**IMPORTANTE:** Quando uma pasta compartilhada é copiada, a pasta original permanece compartilhada, porém a cópia não é compartilhada. Quando o administrador move uma pasta compartilhada , a pasta deixa de ser compartilhada.

## Orientações para a criação de pastas compartilhadas:

Todo compartilhamento deve ter um nome, para que o compartilhamento possa ser acessado pela rede, conforme descrito anteriormente e será demonstrado na parte prática mais adiante. O nome do compartilhamento pode ser diferente do nome da pasta. Uma recomendação importante é para que seja escolhido um nome descritivo do conteúdo da pasta, de tal maneira que o compartilhamento seja mais facilmente localizada na rede. Você não colocaria um nome de compartilhamento “Projetos” em uma pasta compartilhada com documentos contábeis ?

- ◆ Organize os recursos, de tal maneira que todos os pastas que devam ser acessadas pelo mesmo grupo de usuários, com o mesmo nível de permissão, estejam dentro da mesma pasta compartilhada. Por exemplo, se você possui sete pastas com documentos e programas, os quais devem ser acessados pelos grupos Contabilidade e Marketing. Coloque estas pastas dentro de uma pasta principal e compartilhe a pasta principal, ao invés de criar sete compartilhamentos individuais. Em seguida atribua permissões de acesso somente para os grupos Contabilidade e Marketing.
- ◆ Configure o nível de permissão mínimo necessário para que os usuários realizem o seu trabalho. Por exemplo se os usuários precisam apenas ler os documentos em uma pasta compartilhada, atribua permissão de Leitura e não de Alteração ou Controle total.
- ◆ Sempre que possível, atribua permissões para grupos de usuários e não para usuários individuais, pois isso facilita a administração, conforme já salientado diversas vezes neste capítulo e no Capítulo 4.
- ◆ Determine quais grupos necessitam acesso a quais pastas compartilhadas e com quais níveis de permissão. Documente bem todo esse processo, para que você possa ter um bom controle sobre os recursos compartilhados e as permissões atribuídas.

**NOTA:** Se você ainda tem clientes baseados no Windows 3.x ou no MS-DOS, você deve utilizar nomes de compartilhamento com o máximo de 8 caracteres para o nome. Nomes de compartilhamento maiores do que 8 caracteres não estarão visíveis para clientes baseados no Windows 3.x e no MS-DOS. Estes clientes verão os nomes de pastas e artigos no formato truncado, adaptado para o formato 8.3 (oito caracteres para o nome e três caracteres para a extensão), que é o formato suportado pelo Windows 3.x e pelo MS-DOS.

## Sistemas de arquivos e permissões NTFS – conceito.

Agora mostrarei alguns detalhes sobre os sistemas de arquivos que o Windows Server 2003 reconhece e também sobre permissões NTFS.

Um sistema de arquivos determina a maneira como o Windows Server 2003 organiza e recupera as informações no Disco rígido ou em outros tipos de mídia. O Windows Server 2003 reconhece os seguintes sistemas de arquivos:

- ◆ FAT
- ◆ FAT32
- ◆ NTFS
- ◆ NTFS 5

O sistema FAT vem desde a época do MS-DOS e tem sido mantido por questões de compatibilidade. Além disso se você tiver instalado mais de um Sistema Operacional no seu computador, alguns sistemas mais antigos (DOS, Windows 3.x e as primeiras versões do Windows 95) somente reconhecem o sistema FAT. Com o sistema de arquivos FAT, a única maneira de restringir o acesso ao conteúdo de uma pasta compartilhada, é através das permissões de compartilhamento, as quais, conforme descrito anteriormente, não terão nenhum efeito se o usuário estiver logado localmente, na máquina onde a pasta foi compartilhada. Com a utilização do sistema FAT, alguns recursos avançados, tais como compressão, criptografia e auditoria, não estão disponíveis.

O sistema FAT32 apresenta algumas melhorias em relação ao sistema FAT. Existe um melhor aproveitamento do espaço no disco, o que consequentemente gera menor desperdício do espaço em disco (este melhor uso do espaço em disco tem a ver com a questão da Fragmentação de Volumes, discutida no Capítulo 5). Um grande inconveniente do sistema FAT32 é que ele não é reconhecido pelo Windows NT Server 4.0. Com o sistema de arquivos FAT32, a única maneira de restringir o acesso ao conteúdo de uma pasta compartilhada, é através das permissões de compartilhamento, as quais, conforme descrito anteriormente, não terão nenhum efeito se o usuário estiver logado localmente, na máquina onde a pasta foi compartilhada. Com a utilização do sistema FAT32, alguns recursos avançados, tais como compressão e criptografia e auditoria , não estão disponíveis.

O sistema de arquivos NTFS é utilizado no Windows NT Server 4.0 e foi mantido no Windows 2000 Server por questões de compatibilidade. É um sistema bem mais eficiente do que FAT e FAT32, além de permitir uma série de recursos avançados, tais como:

- ◆ Permissões de controle de acesso a arquivos e pastas – permissões NTFS.
- ◆ Compressão de arquivos e pastas.
- ◆ Auditoria de acesso.
- ◆ Partições bem maiores do que as permitidas com FAT e FAT32.
- ◆ Desempenho bem superior do que com FAT e FAT32.
- ◆ Menor índice de fragmentação de partições e volumes.

Uma das principais vantagens do NTFS é que ele permite que sejam definidas permissões de acesso para arquivos e pastas, isto é, posso ter arquivos em uma mesma pasta, com permissões diferentes para usuários e grupos diferentes. Além disso, as permissões NTFS têm efeito localmente, isto é, mesmo que o usuário faça o logon no computador onde um determinado arquivo existe, se o usuário não tiver as permissões NTFS necessárias, ele não poderá acessar o arquivo. Isso confere um alto grau de segurança, desde que as permissões NTFS sejam configuradas corretamente.

No Windows 2000 Server foi introduzido NTFS 5, a nova versão do NTFS, que é a versão utilizada pelo Windows Server 2003. O NTFS 5 apresenta diversas melhorias em relação a versão mais antiga do NTFS, tais como:

- ◆ Criptografia de arquivos e pastas (a criptografia é uma maneira de “embaralhar” a informação de tal forma que mesmo que um arquivo seja copiado, o arquivo se torna ilegível, a não ser para a pessoa que possui a chave para descriptografar o arquivo). Para detalhes sobre Criptografia de arquivos e pastas consulte o Capítulo 5.
- ◆ Quotas de usuário, fazendo com que seja possível limitar o espaço em disco que cada usuário pode utilizar.
- ◆ Gerenciamento e otimização melhorados.

Conforme descrito anteriormente, o administrador pode definir permissões de acesso para pastas ou arquivos, mas somente em unidades formatadas com o sistema de arquivos NTFS (seja na versão do NT Server 4.0 ou o NTFS 5 do Windows 2000 Server/Windows Server 2003 ). Por isso que é aconselhável instalar o Windows Server 2003 sempre em unidades formatadas com NTFS, pois isso permite uma maior segurança e proteção dos dados. As partições NTFS apresentam um desempenho um pouco inferior do que as partições FAT32, em termos de velocidade. Porém em termos de segurança não existe comparação, por isso recomendo a utilização do sistema NTFS. Se você estiver em dúvida, no momento da instalação do Windows Server 2003, pode optar por formatar o disco rígido utilizando FAT 32. Depois é possível converter para NTFS, sem perda de dados. Porém cuidado, uma vez convertido o disco rígido para NTFS não é possível reverter para FAT32. A única maneira é fazer um backup do disco rígido, formatando-o novamente com FAT32 e restaurar o backup.

Com relação as permissões NTFS, existe um conjunto diferente de permissões quando tratamos de pastas ou arquivos. Na Figura 6.5 apresento um resumo das permissões de pasta e de arquivos, com as ações associadas com cada permissão.

| Permissões especiais           | Controle total | Modificar | Ler e executar | Listar conteúdo de pastas (somente para pastas) | Ler | Gravar |
|--------------------------------|----------------|-----------|----------------|---|-----|--------|
| Desviar pasta/executar arquivo | x              | x         | x              | x   |     |        |
| Listar pasta/Ler dados         | x              | x         | x              | x   | x   |        |
| Ler atributos                  | x              | x         | x              | x   | x   |        |
| Ler atributos estendidos       | x              | x         | x              | x   | x   |        |
| Criar arquivos/Gravar dados    | x              | x         |                |   |     | x      |
| Criar pastas/Acrecentar dados  | x              | x         |                |   |     | x      |
| Gravar atributos               | x              | x         |                |   |     | x      |
| Gravar atributos estendidos    | x              | x         |                |   |     | x      |
| Excluir subpastas e arquivos   | x              |           |                |   |     |        |
| Excluir                        | x              | x         |                |   |     |        |
| Ler permissões                 | x              | x         | x              | x   | x   | x      |
| Alterar permissões             | x              |           |                |   |     |        |
| Apropriar-se                   | x              |           |                |   |     |        |
| Sincronizar                    | x              | x         | x              | x   | x   | x      |

Figura 6.5 Ações associadas com as permissões de pasta e arquivos.

A seguir apresento a descrição, com maiores detalhes, para cada uma das permissões listadas na Figura 6.5:

- ◆ **Traverse Folder/Execute File (Permissão Desviar pasta/Executar arquivo):** Estas permissões são aplicadas a pastas e arquivos. Para as pastas, Desviar pasta permite ou nega o movimento através de pastas para acessar outros arquivos ou pastas, mesmo que o usuário não tenha permissões referentes às pastas desviadas (aplica-se somente a pastas). Por exemplo vamos supor que o usuário tem permissão na pasta C:\Documentos, não tem permissão na pasta C:\Documentos\Ofícios e tem na pasta C:\Documentos\Ofícios\2001. Neste caso, o usuário para chegar até a pasta 2001, terá que passar pela pasta Ofícios, para a qual ele não tem permissão. Para que o usuário possa passar pela pasta Ofício, o administrador deve atribuir-lhe a permissão Desviar pasta. Desviar pasta tem efeito apenas quando o grupo ou usuário não tem o direito de usuário Ignorar verificação com desvio no snap-in de diretivas de grupo. (Por padrão, o grupo Todos tem o direito de usuário Ignorar verificação com desvio.)
- ◆ **Para os arquivos:** Execute File (Executar arquivo) permite ou nega a execução de arquivos de programa (aplica-se somente a arquivos). Ao definir a permissão Traverse Folder (Desviar Pasta) em uma pasta, você não está automaticamente definindo a permissão Executar arquivo em todos os arquivos dessa pasta.

- ◆ **Permissão List Folder/Read Data (Listar Pasta/Ler Dados):** List Folder (Listar Pasta) permite ou nega a exibição de nomes de arquivos e subpastas dentro da pasta. Essa permissão afeta apenas o conteúdo da pasta em questão, não afetando o fato de a pasta na qual a permissão está sendo definida ser listada ou não. Aplica-se somente a pastas. Read Data (Ler Dados) permite ou nega a exibição de dados em arquivos (aplica-se somente a arquivos). Por exemplo, se o usuário tem permissão de Ler dados em um arquivo do Word, este usuário poderá abrir o arquivo, porém não poderá alterá-lo ou excluí-lo.
- ◆ **Permissão Read Attributes (Ler Atributos):** Permite ou nega a exibição de atributos de um arquivo ou pasta, como os atributos somente leitura ou oculto. Os atributos são definidos pelo NTFS. Para acessar os atributos de uma pasta ou arquivo, clique com o botão direito do mouse na pasta/arquivo e, no menu que surge, dê um clique na opção Properties (Propriedades).
- ◆ **Permissão Read Extended Attributes (Ler Atributos Estendidos):** Permite ou nega a exibição de atributos estendidos de um arquivo ou pasta. Os atributos estendidos são definidos por programas e podem variar de acordo com o programa.
- ◆ **Permissão Create Files/Write Data (Criar Arquivos/Gravar Dados):** Criar arquivos permite ou nega a criação de arquivos dentro da pasta (aplica-se somente a pastas). Gravar dados permite ou nega as alterações no arquivo e a substituição de um conteúdo existente (aplica-se somente a arquivos). Esta permissão é mais conhecida por permissão de Escrita (ou Alteração).
- ◆ **Create Folders/Append Data (Permissão Criar Pastas/Acrecentar Dados):** Criar pastas permite ou nega a criação de pastas dentro da pasta na qual a permissão foi definida (aplica-se somente a pastas). Acrecentar dados permite ou nega as alterações no final do arquivo, mas não a alteração, exclusão ou substituição de dados existentes (aplica-se somente a arquivos).
- ◆ **Permissão Write Attributes (Gravar Atributos):** Permite ou nega a alteração de atributos de um arquivo ou pasta, como somente leitura ou oculto. Os atributos são definidos pelo NTFS. A permissão Gravar atributos não implica na criação ou exclusão de arquivos ou pastas, apenas inclui a permissão para efetuar alterações nos atributos de um arquivo ou de uma pasta.
- ◆ **Permissão Write Extended Attributes (Gravar Atributos Estendidos):** Permite ou nega a alteração de atributos estendidos de um arquivo ou pasta. Os atributos estendidos são definidos por programas e podem variar de acordo com o programa. A permissão Gravar atributos estendidos não implica na criação ou exclusão de arquivos ou pastas, apenas inclui a permissão para efetuar alterações nos atributos de um arquivo ou de uma pasta
- ◆ **Permissão Delete Subfolders and Files (Excluir Subpastas e Arquivos):** Permite ou nega a exclusão de subpastas e arquivos, mesmo que a permissão Excluir não tenha sido concedida na subpasta ou arquivo. (aplica-se a pastas). Por exemplo, se você não tem permissão de Excluir na pasta Documentos, mas tem permissão de Excluir em um arquivo memo.doc, que está na pasta Documentos, você conseguirá Excluir o documento memo.doc, pois as permissões de arquivo tem precedência sobre as permissões de pastas, quando conflitantes.
- ◆ **Permissão Delete (Excluir):** Permite ou nega a exclusão da pasta e/ou arquivo. Se o usuário não tiver permissão de excluir em um arquivo ou pasta, ele ainda poderá excluir o arquivo ou pasta, se ele tiver permissão Delete Subfolders and Files (Excluir Subpastas e Arquivos) na pasta pai. Por exemplo, suponha uma pasta Documentos, na qual o usuário tem permissão Delete Subfolders and Files. Dentro da pasta Documentos tem a pasta Ofícios, na qual o usuário não tem permissão Delete. Mesmo assim ele poderá excluir a pasta Ofícios, pois ele tem permissão Delete Subfolders and Files na pasta Pai de Ofícios que é a pasta Documentos.
- ◆ **Permissão Read Permissions (Ler Permissões):** Permite ou nega a leitura de permissões do arquivo ou pasta, como Controle total, Ler e Gravar. Se o usuário não tiver esta permissão, ele não poderá exibir a lista com as permissões definidas para um arquivo e/ou pasta.

- ◆ **Permissão Change Permissions (Alterar Permissões):** Permite ou nega a alteração de permissões do arquivo ou pasta, como Controle total, Ler e Gravar. Esta é uma permissão “poderosa” e que deve ser utilizada com cuidado. Uma vez que o usuário tem permissão para Alterar permissões, ele pode perfeitamente atribuir Controle total para ele mesmo, ou seja, para a sua conta de usuário.
- ◆ **Permissão Take Ownership (Apropriar-se) :** Permite ou nega a apropriação (tornar-se dono) do arquivo ou pasta. O proprietário de um arquivo ou pasta sempre pode alterar permissões, independentemente de qualquer permissão existente que proteja o arquivo ou pasta. O dono de um arquivo ou pasta, por padrão, é o usuário que cria o arquivo /pasta.

Todo arquivo ou pasta em uma unidade formatada com NTFS, possui uma “Lista de controle de acesso (Access Control List ) – ACL. Nesta ACL fica uma lista de todas as contas de usuários e grupos para os quais foi garantido acesso para o recurso, bem como o nível de acesso de cada um deles.

- ◆ Permissões NTFS são cumulativas, isto é , se um usuário pertence a mais de um grupo, os quais tem diferentes níveis de permissão para um recurso, a permissão efetiva do usuário é a soma das permissões atribuídas aos grupos aos quais o usuário pertence.
- ◆ Permissões NTFS para um arquivo têm prioridade sobre permissões NTFS para pastas. Por exemplo se um usuário têm permissão NTFS de escrita em uma pasta, mas somente permissão NTFS de leitura para um arquivo dentro desta pasta, a sua permissão efetiva será somente a de leitura, pois a permissão para o arquivo tem prioridade sobre a permissão para a pasta.
- ◆ Negar uma permissão NTFS tem prioridade sobre permitir. Por exemplo, se um usuário pertence a dois grupos diferentes. Para um dos grupos foi dado permissão de leitura para um arquivo e para o outro grupo foi Negada a permissão de leitura, o usuário não terá o direito de leitura, pois Negar tem prioridade sobre Permitir.

**IMPORTANTE:** Existem alguns detalhes que devem ser reforçados/revisados sobre as permissões NTFS:

Agora que você já viu a teoria necessária, é hora de praticar um pouco. Nas próximas lições você irá aprender a compartilhar pastas, atribuir permissões de compartilhamento. Irá aprender a acessar pastas compartilhadas através da rede. Depois irá trabalhar um pouco com as permissões NTFS. Mostrarei como atribuir permissões NTFS e testar uma série de situações práticas.

```
Usuário: user1    senha: senha;123
Usuário: user2    senha: senha;123
Usuário: user3    senha: senha;123
Usuário: user4    senha: senha;123
Usuário: user5    senha: senha;123
```

Grupos locais do domínio aos quais pertence cada usuário:

|                         |                                |
|-------------------------|--------------------------------|
| <b>Grupo: Diretoria</b> | <b>Usuários:</b> Administrador |
|                         | user2                          |
|                         | user4                          |
| <b>Grupo: Vendas</b>    | <b>Usuários:</b> user3         |
|                         | user4                          |
|                         | user5                          |
| <b>Grupo: Empresa</b>   | <b>Usuários:</b> user1         |
|                         | user2                          |
|                         | user3                          |
|                         | user4                          |
|                         | user5                          |

**IMPORTANTE:** Para os exemplos práticos a seguir, vamos utilizar as contas de usuários e contas de grupos: user1, user2, user3, user4 e user5, bem como os respectivos grupos: vendas, diretoria e empresa. Com isso vou utilizar a seguinte configuração de usuários/grupos:

# Compartilhando pastas, definindo permissões de compartilhamento e NTFS

Neste tópico apresentarei uma série de exemplos para verificação de como funciona o mecanismo de pastas compartilhadas e permissões.

Vou iniciar com um exemplo prático, onde vou criar uma estrutura de pastas, depois vou compartilhar algumas pastas, definir permissões de acesso e, finalmente, acessar as pastas compartilhadas, a partir de outro computador ligado em rede. Para este exemplo prático, estou utilizando dois computadores ligados em rede, um com o nome de microxp01 e outro com o nome de microxp02, conforme ilustrado no diagrama da Figura 6.6:

**NOTA:** Utilizarei estes grupos e usuários para definir as permissões de compartilhamento e também as permissões NTFS, nos exemplos práticos. Você pode utilizar outros grupos e usuários, o uso destes grupos tem por objetivo facilitar o acompanhamento dos exemplos práticos, mesmo que você não esteja fazendo o acompanhamento diretamente em um servidor, apenas fazendo a leitura dos exemplos.

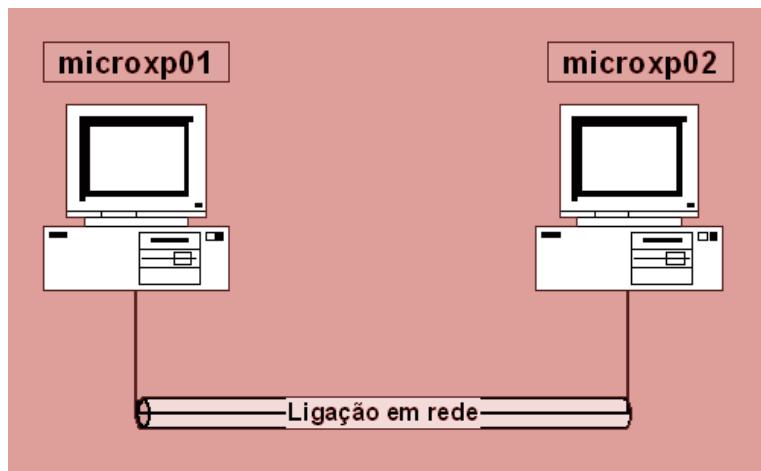


Figura 6.6 Computadores ligados em rede, para o exemplo proposto.

Passo 1 – executado no computador microxp01: Criar a estrutura de pastas e subpastas indicadas na Figura 6.7, no disco rígido C:

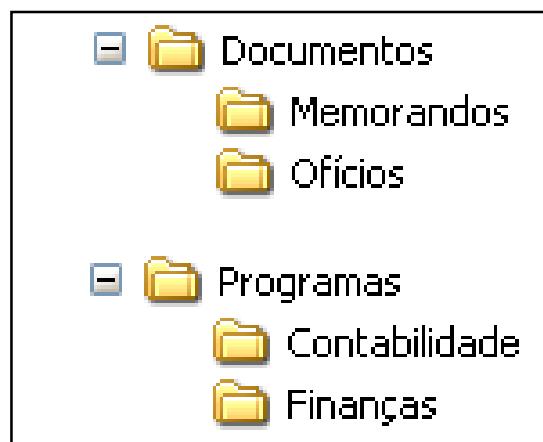


Figura 6.7 Estrutura de pastas para o exemplo proposto.

Passo 2 – executado no computador microxp01: Compartilhar a pasta Documentos com as seguintes permissões de compartilhamento:

|               |                   |                   |                          |
|---------------|-------------------|-------------------|--------------------------|
| <b>Grupo:</b> | <b>Diretoria:</b> | <b>Permissão:</b> | <b>Leitura e escrita</b> |
| <b>Grupo:</b> | <b>Vendas:</b>    | <b>Permissão:</b> | <b>Leitura e escrita</b> |
| <b>Grupo:</b> | <b>Empresa:</b>   | <b>Permissão:</b> | <b>Leitura</b>           |

1. Faça o logon com uma conta com permissão de Administrador e abra o Windows Explorer.
2. Localize a pasta Documentos.
3. Clique com o botão direito do mouse na pasta Documentos e no menu de opções que é exibido, dê um clique na opção Compartilhamento e segurança...
4. Será aberta a janela de propriedades da pasta, com a guia Compartilhamento selecionada. Dê um clique na opção Compartilhar esta pasta.
5. No campo Nome do compartilhamento digite: Documentos.
6. No campo Comentário) digite: Documentos no computador microxp01.
7. Limite o número máximo de usuários conectados (Permitir este número de usuários) a 5, conforme indicado na Figura 6.8:

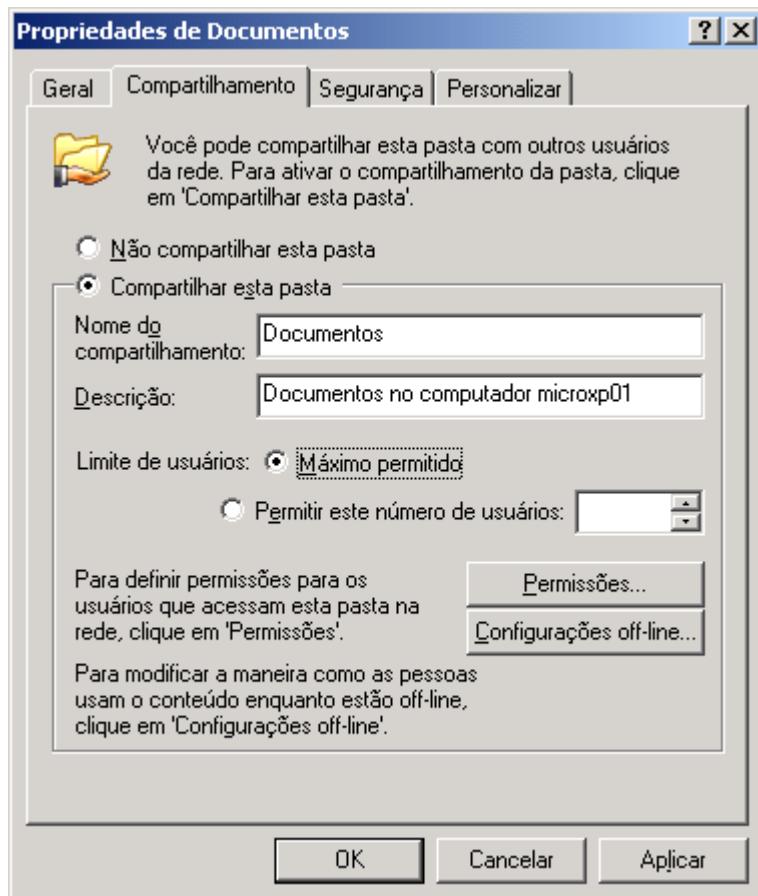
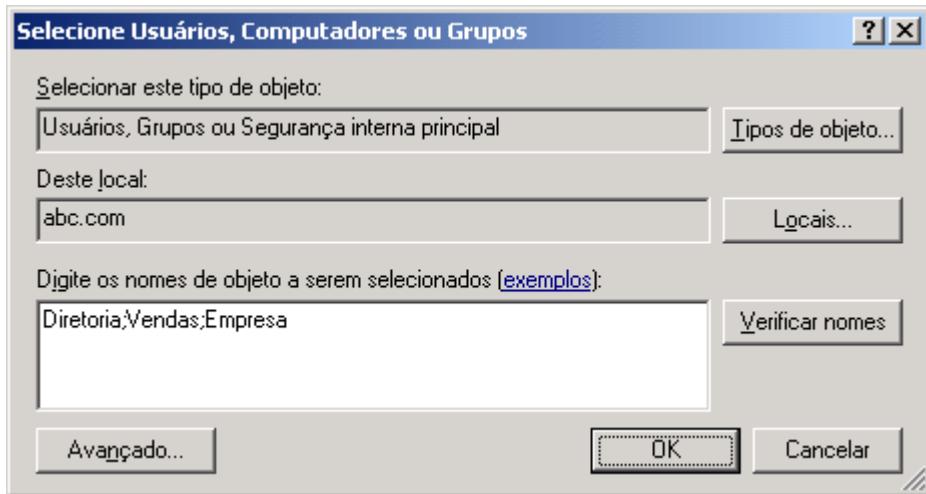


Figura 6.8 Janela para configuração do compartilhamento.

8. Dê um clique no botão Permissões. Observe que por padrão é definida a permissão de compartilhamento Leitura, para o grupo Todos, conforme já descrito anteriormente.

9. Dê um clique no botão Adicionar. Será exibida a janela Seleciona Usuários, Computadores ou Grupos. Você definirá permissões para os grupos Diretoria, Vendas e Empresa. Digite o nome dos grupos separados por ponto e vírgula, conforme indicado na Figura 6.9.



**Figura 6.9 Adicionando os grupos que receberão permissões no compartilhamento.**

10. Dê um clique no botão OK. Você estará de volta à janela Permissões para Documentos. Observe que os grupos Diretoria, Vendas e Empresa já estão na lista de grupos. Agora é hora de remover o grupo Todos e depois configurar permissões solicitadas para os demais grupos.
11. Dê um clique no grupo Todos para selecioná-lo e depois clique no botão Remover. O grupo é retirado da lista.
12. Dê um clique no grupo Diretoria e marque as permissões Alteração e Leitura.
13. Dê um clique no grupo Vendas e marque as permissões Alteração e Leitura.
14. Dê um clique no grupo Empresa e marque somente a opção Leitura. Aliás esta é a opção que vem marcada por padrão, quando um novo grupo ou usuário é inserido na lista de permissão.
15. Dê um clique no botão OK. Você estará de volta a janela de definição do compartilhamento.
16. Dê um clique no botão OK e pronto, a pasta será compartilhada e as permissões de compartilhamento definidas. Observe que após ter compartilhada a pasta, a figura de uma pequena mão, segurando a pasta é exibida.

Uma questão importante: Com base nas permissões atribuídas aos grupos, quais as permissões de compartilhamento efetivas dos usuários: user1, user2, user3, user4 e user5?? Vou analisar caso a caso:

- ◆ **user1:** Pertence somente ao grupo Empresa, portanto somente herda a permissão de leitura que foi atribuída ao grupo Empresa. Este usuário ao acessar a pasta compartilhada Documentos, pela rede, terá permissão somente de leitura.
- ◆ **user2:** Pertence aos grupos Diretoria e Empresa. Herdará as permissões dos dois grupos, que na soma resulta em Leitura e Escrita.
- ◆ **user3:** Pertence aos grupos Vendas e Empresa. Herdará as permissões dos dois grupos, que na soma resulta em Leitura e Escrita, ou seja, o usuário vai acumulando as permissões de todos os grupos aos quais ele pertence.

---

**NOTA:** Você também pode usar o botão Avançado, descrito no Capítulo 4, para exibir a lista de usuários do Active Directory e selecionar os grupos que receberão permissões de acesso a partir desta lista.

---

- ◆ **user4:** Pertence aos três grupos. Herdará as permissões dos três grupos, o que na soma dá Leitura e Escrita.
- ◆ **user5:** Pertence aos grupos Vendas e Empresa. Herdará as permissões dos dois grupos, que na soma resulta em Leitura e Escrita.

Vamos fazer algumas perguntas para entender bem como funciona esta combinação de permissões?

*1) O que aconteceria se negássemos permissão de leitura para o grupo Empresa??*

R: Como todos os usuários pertencem ao grupo Empresa e, negar tem precedência sobre permitir, ao negar Leitura para o grupo Empresa, você está negando Leitura para todos os usuários: user1, user2, user3, user4 e user5. Com esta configuração, ao tentar acessar a pasta compartilhada pela rede, os usuários iriam receber uma mensagem de acesso negado.

*2) Se o usuário user2 fizer o logon no computador onde está a pasta compartilhada Documentos, qual a permissão efetiva de compartilhamento??*

R: Nenhuma, isto é, terá todas as permissões NTFS definidas para ele. Lembre que as permissões de compartilhamento não tem efeito localmente, somente através da rede. Localmente somente tem efeito as permissões NTFS. Se o usuário user2 ou um grupo ao qual ele pertence, tiver as permissões NTFS necessárias, ele poderá acessar a pasta Programas com o nível de acesso definido pelas permissões NTFS.

*3) Criei um compartilhamento chamado Documentos, no computador microxp01. Muito bem, qual o caminho que eu uso em outro computador da rede, para acessar este compartilhamento?*

R: \\microxp01\documentos

Passo 3 – executado no computador microxp01: Compartilhar a pasta Porgramas, com o nome de compartilhamento Programas, com um número máximo de 10 usuários simultâneos e com as seguintes permissões de compartilhamento:

|               |                   |                   |                          |
|---------------|-------------------|-------------------|--------------------------|
| <b>Grupo:</b> | <b>Diretoria:</b> | <b>Permissão:</b> | <b>Negado Leitura</b>    |
| <b>Grupo:</b> | <b>Vendas:</b>    | <b>Permissão:</b> | <b>Leitura e escrita</b> |
| <b>Grupo:</b> | <b>Empresa:</b>   | <b>Permissão:</b> | <b>Controle total</b>    |

1. Com base no que foi explicado no Passo 2, crie e configure o compartilhamento Programas, no computador microxp01.

Vamos fazer algumas perguntas para entender bem como funciona esta combinação de permissões?

*1) Qual a permissão para o usuário user2, com base nas permissões atribuídas aos grupos Diretoria, Vendas e Empresa?*

R: Sempre começamos a análise verificando se existe a permissão Negado para algum grupo. No nosso caso existe: Negado Leitura para o grupo Diretoria. Como o usuário user2 pertence ao grupo Diretoria e negado tem precedência sobre qualquer outra permissão, o usuário user2 terá acesso negado ao compartilhamento documentos. O mesmo é válido para o usuário user4, o qual também pertence ao grupo Diretoria.

*2) Se o usuário user2 fizer o logon no computador onde está a pasta compartilhada Programas, ele terá acesso Negado a pasta Programas??*

R: Não, pois ao acessar localmente as permissões de compartilhaemnto não tem efeito. Localmente somente tem efeito as permissões NTFS. Se o usuário user2 ou um grupo ao qual ele pertence, tiver as permissões NTFS necessárias, ele poderá acessar a pasta Programas.

*3) Criei um compartilhamento chamado Programas, no computador microxp01. Muito bem, qual o caminho que eu uso em outro computador da rede, para acessar este compartilhamento?*

R: \\microxp01\Programas

Bem, os compartilhamentos foram criados e foram definidas as permissões de compartilhamento. Agora você irá no computador microxp02, e tentará acessar os compartilhamentos criados no computador microxp01.

Passo 4 – Executado no computador microxp02: Fazer o logon como user1, no computador microxp02 e montar um drive M:, o qual acessa o compartilhamento Documentos que está no computador microxp01: \\microxp01\Documentos. Lembrando o que foi comentado anteriormente, que montar um drive M:, significa associar uma letra de unidade com um compartilhamento. Neste exemplo, após o drive M: ter sido montado, sempre que o usuário acessar o drive M:, ele estará, na verdade, acessando o compartilhamento: \\microxp01\Documentos

1. Faça o logon como user2 no computador microxp02.
2. Selecione o comando Iniciar -> Executar.
3. No campo Abrir digite \\microxp01 e dê um clique no botão OK.
4. Observe que as pastas compartilhadas Documentos e Programas já são exibidas na janela que é aberta.
5. Para associar um drive (no nosso exemplo M:), com uma pasta compartilhada, clique com o botão direito do mouse na pasta desejada. No nosso exemplo, clique com o botão direito do mouse na pasta Documentos.
6. No menu que é exibido, dê um clique na opção Mapear unidade de rede... Será exibida uma janela para que você selecione a unidade que será associada com a pasta compartilhada e se você deseja refazer o mapeamento toda vez que o usuário atual (no nosso exemplo o usuário logado é o usuário user1) fizer o logon, conforme indicado na Figura 6.10.

---

**NOTA:** Ao executar o comando \\microxp01, Windows Server 2003 exibe uma janela com todos os recursos compartilhados no computador microxp01. Quer sejam pastas compartilhadas, quer sejam impressoras compartilhadas.

---

**IMPORTANTE:** Se você quiser ocultar um compartilhamento, de tal maneira que ele não seja exibido na lista de recursos compartilhados quando for usado o comando \\nome\_do\_computador, basta finalizar o nome do compartilhamento com o caractere \$. Por exemplo, se você criar um compartilhamento chamado Docs\$, este será um compartilhamento oculto, o qual somente poderá ser acessado se for utilizado o caminho comando: \\nome\_do\_computador\Docs\$. Por padrão, o Windows Server 2003 cria alguns compartilhamentos ocultos para funções específicas do próprio Sistema Operacional. Estes compartilhamentos também tem permissões específicas. Por exemplo, é criado um compartilhamento C\$, o qual dá acesso a pasta raiz do disco rígido, porém somente usuários com conta de Administrador tem acesso a este compartilhamento.

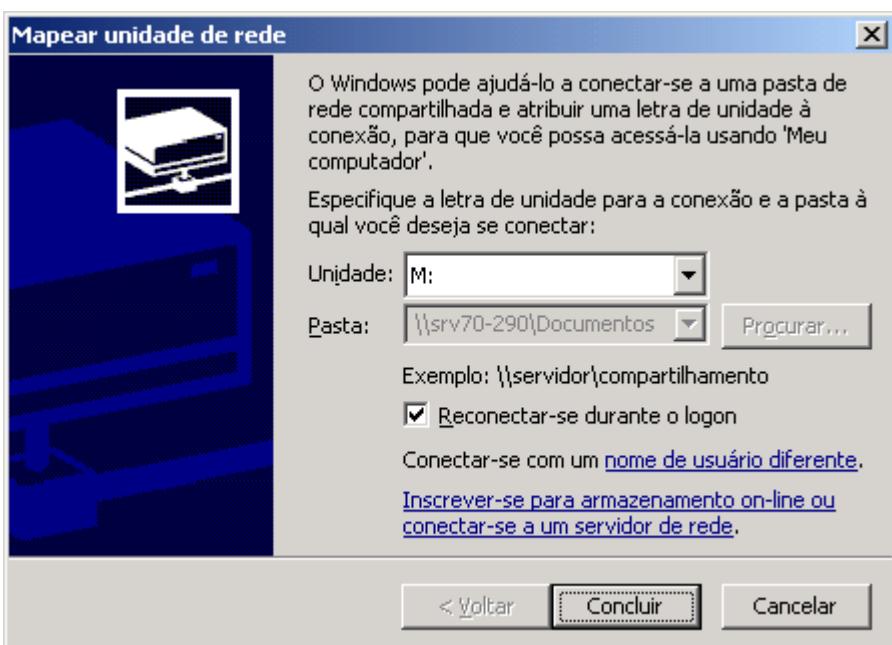
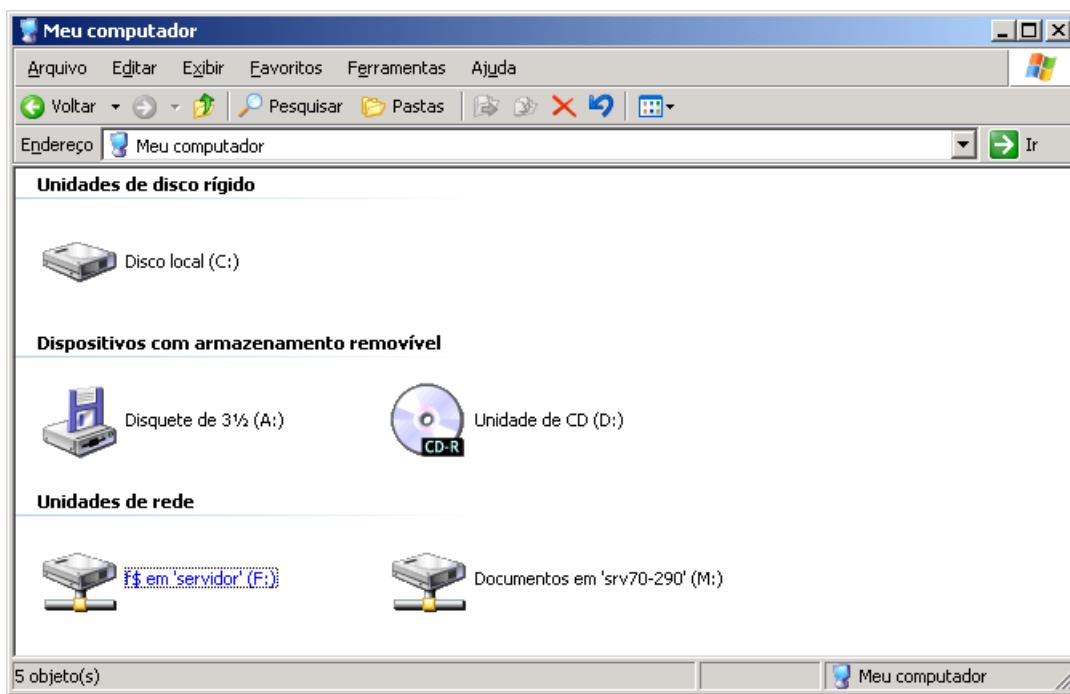


Figura 6.10 Mapeando uma unidade de rede.

7. Dê um clique no botão Concluir. O Windows Server 2003 abre uma janela onde são exibidas as subpastas de Documentos. Feche esta janela.

8. Abra o Meu computador e observe, já deve ser exibido um drive de rede M:, conforme indicado na Figura 6.11.



-Figura 6.11 O drive de rede M:

A partir deste momento, toda vez que o usuário acessar o drive M:, estará acessando, na prática, a pasta compartilhada Documentos, no computador \\microxp01. Observe que a utilização de drives mapeados (drives de rede), facilita bastante o acesso às pastas compartilhadas, pois serve como um atalho para estas pastas. Um procedimento muito comum é incluir o mapeamento de drivers de rede no script de logon utilizado pelas contas de usuários do domínio.

9. Dê um clique duplo no drive M:, para acessá-lo. Abra a pasta Memorandos.
10. Agora faça o logoff do usuário user02 e faça o logon como usuário user01. Abra o Meu computador e observe que o drive M não é exibido para o usuário user01. Isso porque o mapeamento de drives faz parte da profile de cada usuário, ou seja, das configurações pessoais de cada usuário. Com base no que foi explicado nos passos anteriores, monte o drive M:, estando logado como usuário user01.
11. Agora o usuário user01 (usuário atualmente logado) tentará criar um novo arquivo de texto, no drive M:. Abra o Meu computador e dê um clique duplo no drive M: para abri-lo. Clique com o botão direito do mouse na área em branco, na pasta Documentos. No menu que surge selecione o comando Novo -> Documento de texto. Você deve receber uma mensagem de acesso negado, conforme indicado na Figura 6.12:

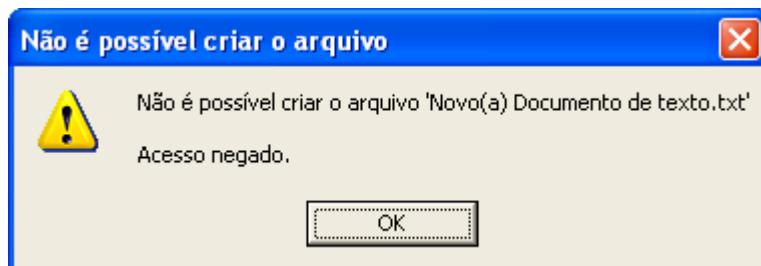


Figura 6.12 Acesso negado para o usuário user01 criar um novo arquivo.

Por que você recebeu esta mensagem de acesso negado?? Porque, conforme descrito anteriormente, o usuário user01 tem permissão de compartilhamento somente de Leitura. Com esta permissão ele não poderá criar e salvar novos arquivos na pasta Documentos e nas suas subpastas.

Muito bem, com isso encerro o nosso estudo sobre Compartilhamentos, drives de rede e permissões de compartilhamento. Agora você aprenderá a usar o console Gerenciamento do computador, para gerenciar/administrar as pastas compartilhadas locais em um servidor e em um servidor remoto.

## O console para monitoração de compartilhamentos.

O administrador pode utilizar a opção Ferramentas do Sistema -> Pastas compartilhadas, do console Gerenciamento do computador, para monitorar o acesso às pastas compartilhados em um servidor. Com esta ferramenta o administrador tem informações sobre todos as pastas que estão compartilhadas, o número de conexões com cada pasta, o número de sessões através da rede, e quais os arquivos que estão sendo acessados e quais usuários estão acessando cada arquivo.

Exemplo: Gerenciando pastas compartilhadas com o console Gerenciamento do Computador:

1. Faça o logon como Administrador ou com uma conta com permissão de Administrador.
2. Abra o console Gerenciamento do Computador: Iniciar -> Ferramentas administrativas -> Gerenciamento do computador.
3. Se a opção Ferramentas do sistema) não estiver aberta, dê um clique no sinal de + ao lado dela para abri-la.
4. Dê um clique no sinal de + ao lado da opção Pastas compartilhadas.
5. Dê um clique na opção Compartilhamentos. Observe que no painel da direita são exibidos todos os compartilhamentos do computador, inclusive os compartilhamentos ocultos (cujo nome termina com \$). Também é exibido o número de conexões por compartilhamento.
6. Dê um clique na opção Sessões. Serão listados todos os usuários e o número de seções por usuário. Cada arquivo ou pasta que um usuário abre é contabilizado como uma seção.
7. Dê um clique na opção Arquivos abertos. Será exibida uma lista com os arquivos que estão sendo utilizados pelos usuários (arquivos que estão abertos) e o nome de logon do usuário que está acessando cada arquivo, conforme exemplo da Figura 6.13.

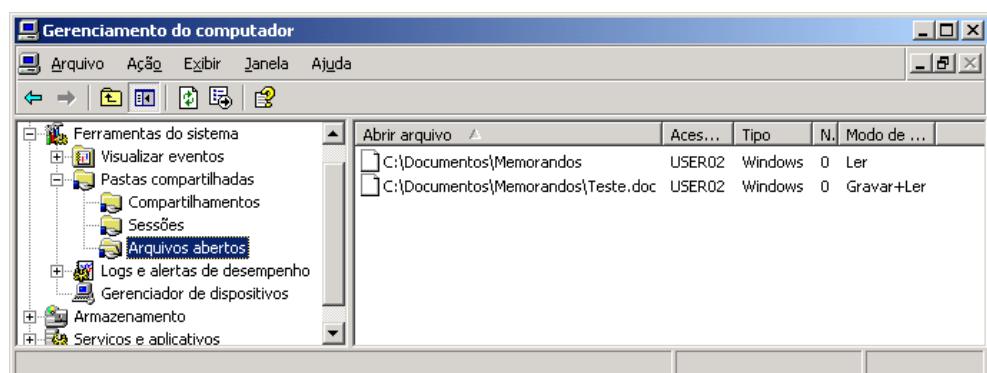


Figura 6.13 A lista de arquivos abertos e o respectivo usuário.

Quando você tem que desligar ou reiniciar um servidor, onde existem pastas compartilhadas que estão sendo acessadas por outros usuários, é importante que você avise os usuários antes de reiniciar o computador, pois caso contrário, o usuário perde a conexão com o drive de rede e não conseguirá salvar as alterações que fez no arquivo no qual estava trabalhando. Em determinadas situações o usuário poderá perder as suas alterações. Por isso é recomendado que você envie um aviso, para que o usuário possa salvar seu trabalho, antes que a conexão com o drive de rede seja perdida.

Para enviar um aviso aos usuários faça o seguinte:

1. Clique com o botão direito do mouse na opção Pastas Compartilhadas.
2. Selecione o comando: Todas as tarefas...-> Enviar mensagem do console...
3. Será aberta uma janela onde você pode digitar a mensagem e selecionar os destinatários. Por padrão, na lista de destinatários somente são exibidos os destinatários que estão conectados a alguma pasta compartilhada do computador, conforme indicado na Figura 6.14. Para adicionar outros usuários, dê um clique no botão Adiconar...

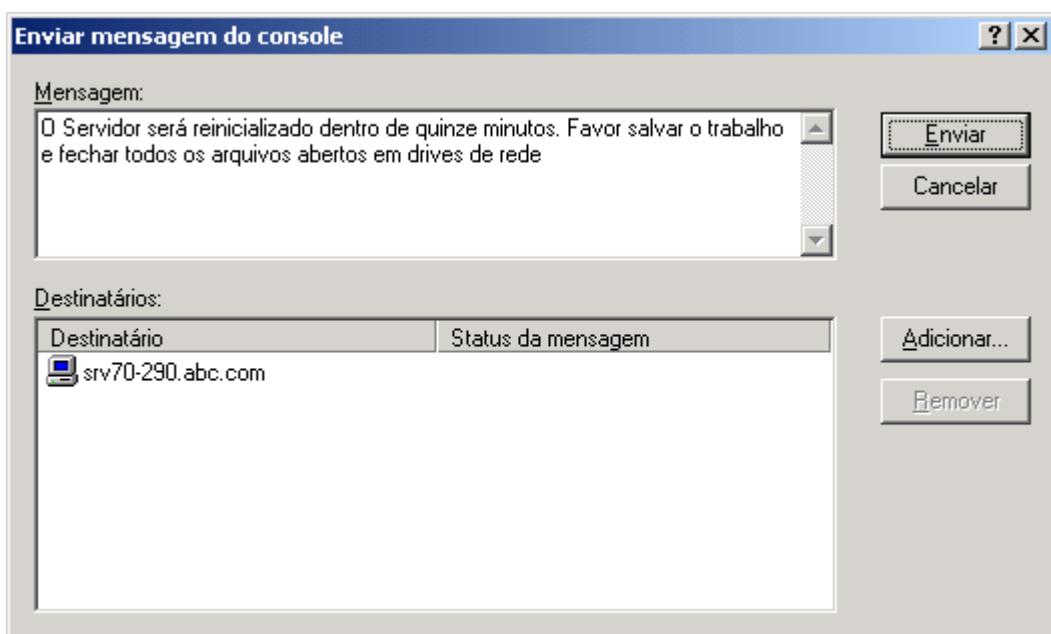


Figura 6.14 Enviando um aviso aos usuários conectados.

4. Digite a mensagem e dê um clique no botão Enviar.

Os destinatários receberão uma janela com a mensagem especificada na janela da Figura 6.14.

Ao receber esta mensagem o usuário terá tempo para salvar o seu trabalho, sem que haja perda de dados.

5. Feche o console Gerenciamento do computador.

## Criando e gerenciando compartilhamentos local e remotamente

O administrador pode utilizar a opção Compartilhamentos, do console Gerenciamento do computador, para criar novos compartilhamentos e para gerenciar os compartilhamentos já existentes no servidor onde ele está logado ou remotamente, de qualquer servidor da rede. Ou seja, a partir da sua estação de trabalho e do console Gerenciamento do computador, o administrador pode gerenciar todas as pastas compartilhadas em seu domínio ou até mesmo em outros domínios, desde que tenha as devidas permissões. Neste tópico mostrarei como usar a opção Compartilhamentos, para gerenciar compartilhamentos locais e remotamente, em outros servidores da rede.

Exemplo: Administrando os compartilhamentos existente e criando novos compartilhamentos no servidor local, usando a opção Compartilhamentos.

1. Faça o logon como Administrador ou com uma conta com permissão de Administrador.
2. Abra o console Gerenciamento do Computador: Iniciar -> Ferramentas administrativas -> Gerenciamento do computador.
3. Se a opção Ferramentas do Sistema não estiver aberta, dê um clique no sinal de + ao lado dela para abri-la.
4. Clique no sinal de + ao lado da opção Pastas compartilhadas para abri-la.
5. Clique com o botão direito do mouse na opção Compartilhamentos.
6. No menu de opções que é exibido clique em Novo compartilhamento...
7. Será aberto o assistente para criação de um novo compartilhamento. A tela inicial do assistente é apenas informativa. Clique em Avançar para ir para a próxima etapa do assistente.
8. Nesta etapa você deve informar o caminho para a pasta a ser compartilhada. Você pode digitar o nome de uma pasta que ainda não existe. Se você fizer isso, quando o assistente for para a próxima etapa, será exibindo uma mensagem informando que a pasta não existe e perguntando se você deseja criá-la. No exemplo da Figura 6.15 informei o caminho de uma pasta que ainda não existe (C:\NovosDocumentos).

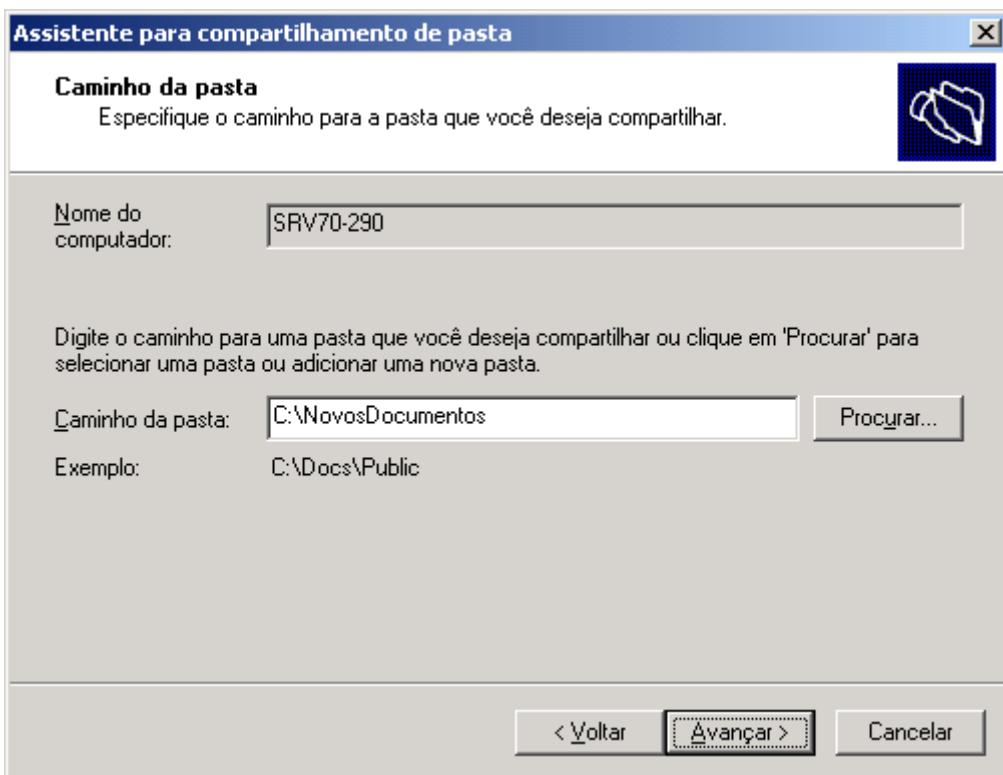


Figura 6.15 Informando o caminho da pasta a ser compartilhada.

9. Clique em Avançar para seguir para a próxima etapa do assistente.
10. Será exibida uma mensagem informando que a pasta C:\NovosDocumentos ainda não existe e perguntando se você deseja criá-la. Clique em Sim para fechar a mensagem e para criar a pasta C:\NovosDocumentos.
11. A próxima etapa do assistente será exibida. Neste etapa você define o nome do compartilhamento e uma descrição. Você também pode definir as configurações para acesso Off-line da pasta. Mais adiante você aprenderá sobre pastas Off-line. Defina o nome de compartilhamento e uma descrição conforme exemplo da Figura 6.16:

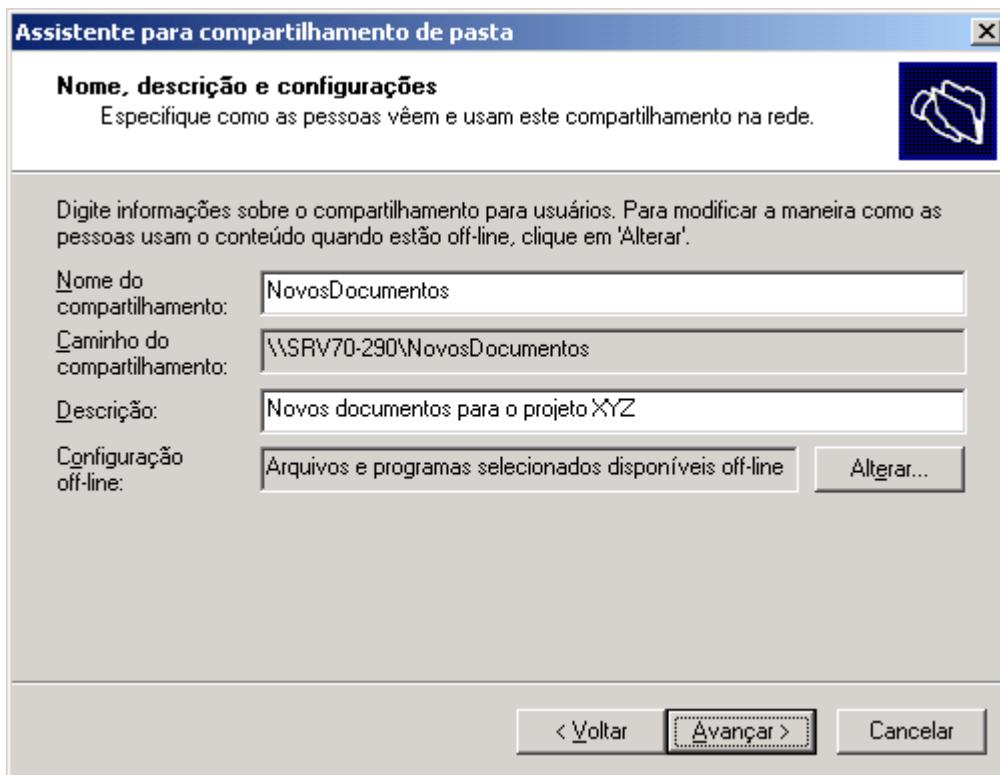


Figura 6.16 Definindo o nome de compartilhamento e a descrição.

12. Clique em Avançar para seguir para a próxima etapa do assistente.

Nesta etapa do assistente você pode definir as permissões de compartilhamento, para o novo compartilhamento que está sendo criado. O assistente oferece algumas opções prontas, tais como:

- ◆ **Todos os usuários possuem acesso somente leitura:** A própria opção é auto-descritiva. Com esta opção será definida permissão Leitura para o grupo Todos. Observe que esta é a permissão definida por padrão, sempre que um novo compartilhamento é criado, a não ser que o administrador configure um conjunto de permissões diferente.
- ◆ **Administradores possuem acesso total; outros usuários possuem acesso somente leitura:** Esta opção também é auto-descritiva, ou seja Controle Total para o grupo Administradores e Leitura para o grupo Todos.
- ◆ **Administradores possuem acesso total; outros usuários possuem acesso de leitura e gravação:** Também auto-descritiva, ou seja Controle Total para o grupo Administradores e Leitura e Escrita para o grupo Todos.
- ◆ **Usar permissões personalizadas de compartilhamento e pasta:** Se você marcar esta opção o botão Personalizar... será habilitado. O Administrador pode utilizar este botão para definir configurações personalizadas para usuários e grupos do domínio.

13. Defina as permissões a serem utilizadas e clique em Concluir para criar o Compartilhamento.

14. A etapa final do assistente será exibida com um resumo das opções escolhidas. Você pode marcar a opção Quando eu clicar em 'Fechar', execute o assistente novamente para que eu possa compartilhar outra pasta, para que após a criação do compartilhamento o assistente seja executado novamente para que você possa criar outro compartilhamento. Esta opção é útil quando o administrador precisa criar uma série de compartilhamentos. Neste caso ele pode executar o assistente, seguidamente, quantas vezes forem necessárias.

15. Clique em Fechar para encerrar o assistente.

16. O novo compartilhamento (NovosDocumentos no nosso exemplo), já deve aparecer na listagem de compartilhamentos da pasta Compartilhamentos, conforme indicado na Figura 6.17. Caso ele ainda não seja exibido na listagem, pressione a tecla F5 para atualizar a listagem.

| Nome de compartilhamento | Caminho da pasta   | Tipo    | Nº de conexões |
|--------------------------|--------------------|---------|----------------|
| ADMIN\$                  | C:\WINDOWS         | Windows | 0              |
| C\$                      | C:\                | Windows | 0              |
| Documentos               | C:\Documentos      | Windows | 1              |
| IPC\$                    |                    | Windows | 0              |
| NETLOGON                 | C:\WINDOWS\SYSV... | Windows | 0              |
| NovosDocumentos          | C:\NovosDocumentos | Windows | 0              |
| Programas                | C:\Programas       | Windows | 0              |
| SYSVOL                   | C:\WINDOWS\SYSV... | Windows | 0              |

Figura 6.17 O compartilhamento NovosDocumentos, recém criado.

Exemplo: Conectando o console Gerenciamento do computador com um servidor remoto:

1. Faça o logon como Administrador ou com uma conta com permissão de Administrador.
2. Abra o console Gerenciamento do Computador: Iniciar -> Ferramentas administrativas -> Gerenciamento do computador.
3. Clique na opção Gerenciamento do computador (Local) para selecioná-la.
4. Selecione o comando Ação -> Conectar-se a outro computador...
5. A janela Selecionar computador será exibida. Digite o nome ou o número IP do computador, conforme exemplo da Figura 6.18:

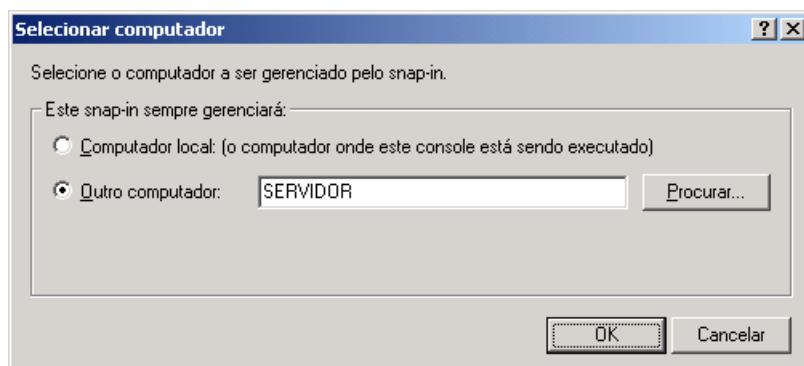


Figura 6.18 Conectando com um servidor remoto.

Dica: Você também pode usar o console Gerenciamento do computador para criar compartilhamentos remotamente, em outros servidores da rede. Os passos são exatamente os descritos anteriormente, a única diferença é que primeiro você deve se conectar com o computador de destino. Ou seja, primeiro você deve conectar o console Gerenciamento do computador com o servidor de destino, no qual você deseja gerenciar os compartilhamentos. Uma vez conectado é com se você estivesse na frente do computador de destino. Tudo o que você fizer no console Gerenciamento do computador, será executado no computador de destino, computador com o qual o console está conectado. A seguir descrevo os passos para você conectar o console Gerenciamento do computador com um servidor remoto, através da rede.

- Clique em OK. Pronto, o console Gerenciamento do computador será conectado com o servidor informado no passo 5. Agora todas as ações que você executar estão sendo feitas neste servidor remoto. É como se você estivesse na frente deste servidor, gerenciando-o diretamente. Assim você pode se conectar com qualquer servidor da rede (desde que você tenha as devidas permissões) para gerenciá-lo remotamente.

No próximo item vou fazer alguns exemplos práticos sobre permissões NTFS e logo em seguida, analisarei a combinação entre permissões de compartilhamento e permissões NTFS.

**Dica:** Não é só o console Gerenciamento do computador que permite a conexão com outros servidores da rede para o gerenciamento remoto. A maioria das ferramentas administrativas (para não dizer a sua totalidade) está habilitada para o gerenciamento remoto. Observe que isso facilita, e muito, a vida do administrador. A partir da sua estação de trabalho o administrador pode trabalhar em dezenas, até mesmo centenas, de servidores da rede, tudo remotamente.

## Permissões NTFS.

Neste tópico você aprenderá a atribuir permissões NTFS e a testar o efeito prático destas permissões, tanto localmente quanto através da rede. Para que você possa acompanhar todos os exemplos propostos nesta lição, é necessário que você tenha acesso a mais um computador em rede, além do computador onde foi criada a pasta compartilhada Documentos, no exemplo sobre pastas compartilhadas. Para os exemplos propostos, continuarei, a título de exemplo, a considerar dois computadores ligados em rede microxp01 e microxp02, conforme ilustrado na Figura 6.6, anteriormente.

Nos exemplos, utilizarei o computador microxp01 como sendo o computador onde se encontra a pasta compartilhada Documentos e microxp02 o outro computador em rede. Caso os nomes dos computadores e do domínio que você está utilizando para acompanhar esta lição, sejam diferentes, utilize-os no lugar dos nomes aqui descritos.

Exemplo: Atribuindo permissões NTFS.

Passo 1 – no computador microxp01: Atribuindo permissões NTFS para a pasta C:\Documentos:

- Efetue o logon como Administrador ou com permissões de administrador no microxp01.
- Abra o Windows Explorer.
- Localize a unidade onde você criou a pasta Documentos, abra a unidade e localize a pasta Documentos. No nosso exemplo é C:\Documentos.
- Dê um clique com o botão direito do mouse na pasta Documentos, e no menu de opções que surge dê um clique em Propriedades.
- Surge a janela Propriedades de Documentos, com a guia Geral selecionado por padrão.
- Dê um clique na guia Segurança, que é a guia utilizada para configurar as permissões NTFS para uma pasta ou arquivo. Surge a janela indicada na Figura 6.19.

Na lista de usuários com permissão, dê um clique no grupo Usuários (ABC\Usuários). Este grupo representa todos os usuários do domínio. Observe que as permissões Ler & Executar, Listar conteúdo da pasta e Leitura estão habilitadas para o grupo Usuários. Porém se você tentar alterá-las, clicando com o mouse, nada acontece, é como se estas opções estivessem bloqueadas para alteração. Isso acontece, porque quando uma você criou a pasta Documentos, ela “herdou” as permissões do objeto pai, que no caso é a pasta raiz da unidade onde a pasta Documentos foi criada (C:\). Esse é o comportamento padrão do Windows Server 2003, baseado no que já acontecia no Windows 2000 e também no Windows XP Professional.

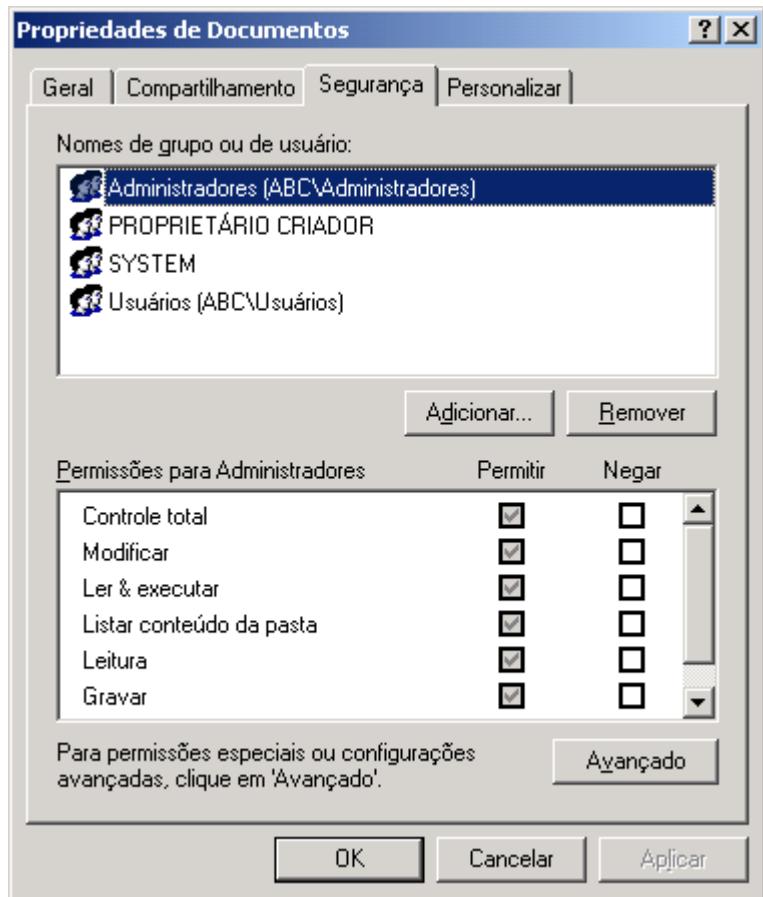


Figura 6.19 A guia Segurança.

Outro detalhe importante, é que as permissões NTFS herdadas não podem ser alteradas, a menos que o mecanismo de herança seja desativado. Ou seja, enquanto o mecanismo de herança não for desativado (você aprenderá a fazer isso logo em seguida), não poderão ser alteradas ou excluídas as permissões herdadas do objeto Pai, somente poderão ser definidas novas permissões para outros usuários e/ou grupos.

7. Para verificar se o mecanismo de herança está habilitado, dê um clique no botão Avançado. Será exibida a janela Configurações de segurança avançadas para Documentos. Nesta janela, se a opção “Permitir que as permissões herdáveis do pai sejam propagadas a este objeto e a todos os objetos filho. Incluí-las nas entradas explicitamente definidas aqui”, estiver marcada, o mecanismo de herança está habilitado, conforme destacado na Figura 6.20:

---

**NOTA:** Se a guia Segurança não estiver disponível é porque a pasta está em uma partição formatada com o sistema de arquivos FAT, o qual não tem suporte ao mecanismo de permissões de segurança.

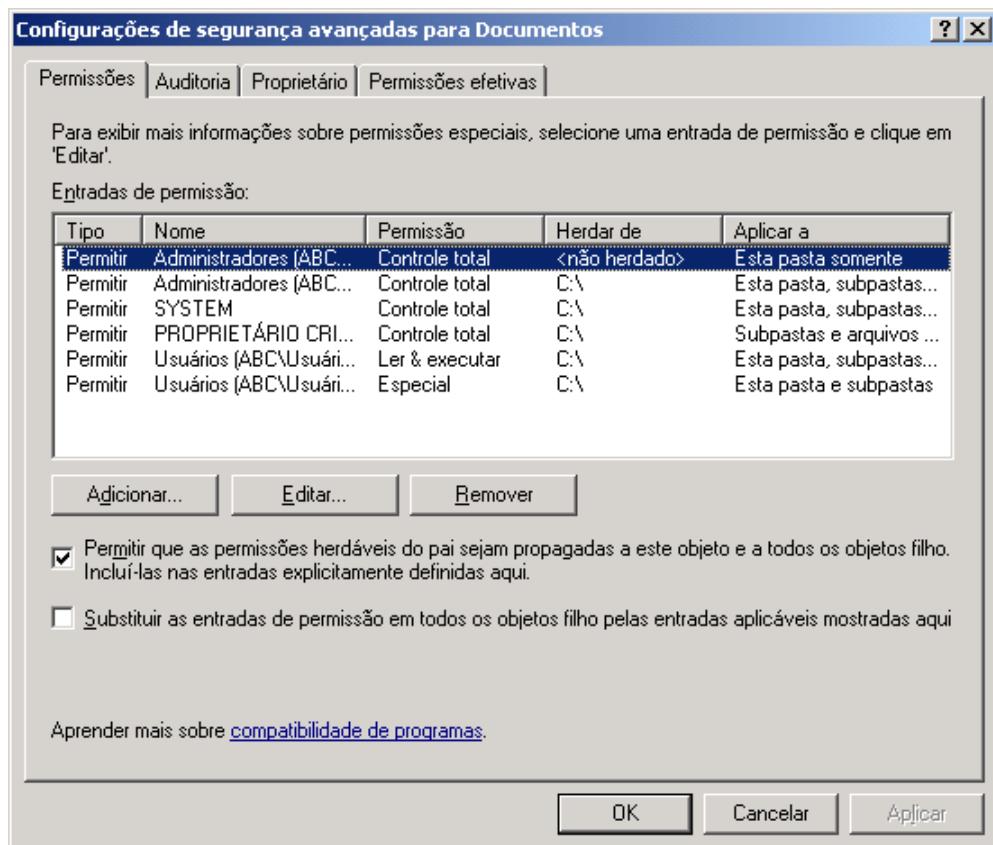


Figura 6.20 O mecanismo de Herança de permissões.

Além das permissões herdadas, você pode adicionar permissões NTFS para usuários ou grupos. Permissões adicionadas desta maneira são conhecidas como “Permissões explícitas”, as quais podem ser alteradas a qualquer momento pelo Administrador do sistema, conforme a necessidade. Já as permissões herdadas não podem ser alteradas pelo Administrador, enquanto o mecanismo de herança não for desabilitado.

- O Mecanismo de herança pode ser desativado. Para isso basta desmarcar a “Permitir que as permissões herdáveis do pai sejam propagadas a este objeto e a todos os objetos filho. Incluí-las nas entradas explicitamente definidas aqui”. Clique nesta opção para desmarca-la. Ao fazer isso o Windows Server 2003 abre uma janela perguntando se você deseja Copiar as permissões herdados – caso em que o Windows Server 2003 as transforma como se tivessem sido explicitamente definidas e com isso será possível alterá-las – ou se você deseja removê-las, caso em que todas as permissões herdadas serão removidas, com exceção da permissão para o grupo Local do domínio Administrators, a qual é mantida. Isso acontece porque o grupo Administrators é o dono da pasta Documentos. Esta janela está indicada na Figura 6.21:

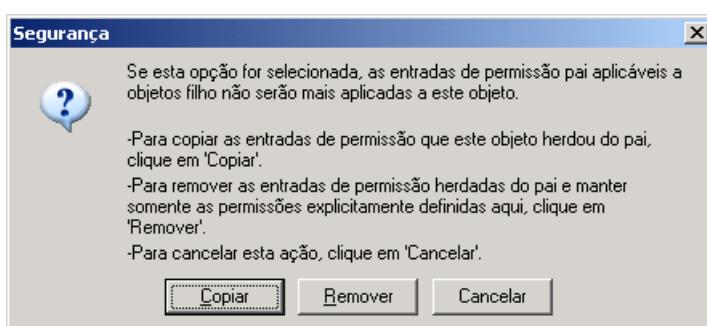


Figura 6.21 Desabilitando o mecanismo de herança para a pasta selecionada.

9. Dê um clique no botão Remover, para revomer todas as permissões NTFS herdadas do objeto pai.
10. Você estará de volta a janela de Configurações de segurança avançadas. Dê um clique no botão OK para fecha-la.
11. Agora é hora de definir configurações personalizadas. Você irá adicionar permissão Alteração para os usuários user1 e user2. Clique no botão Adicionar. Surge a janela Seleciona Usuários, Computadores ou Grupos.
12. Digite o nome dos usuários, separando os nomes por ponto e vírgula. No nosso exemplo, digite: user01;user02. Sua janela deve ficar conforme a indicada na Figura 6.22, onde foram adicionados os usuários user01 e user02.

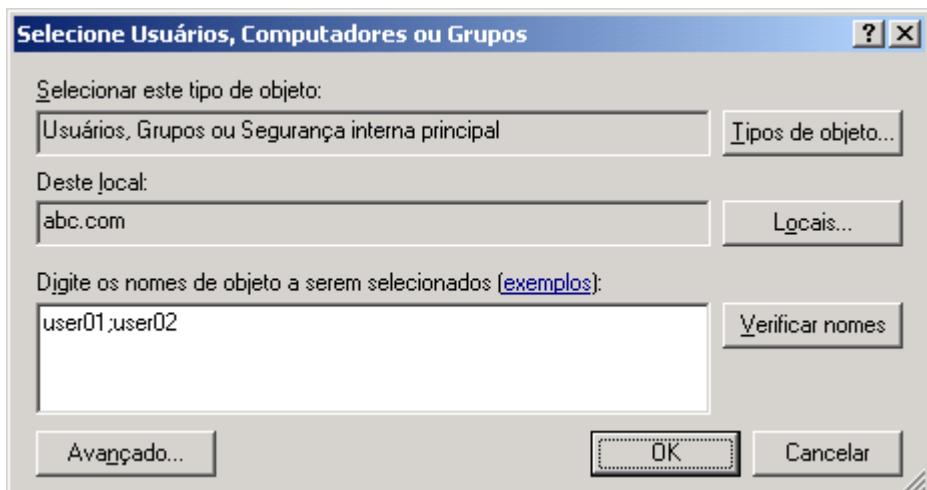


Figura 6.22 Adicionando os usuários user01 e user02.

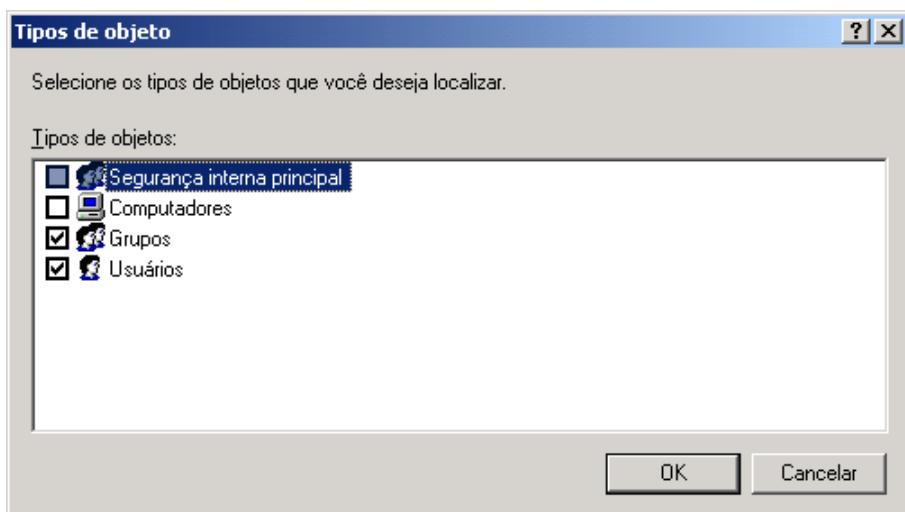


Figura 6.23 A janela Tipos de objeto.

**NOTA:** Quando o número de usuários é grande, fica difícil de lembrar o nome de cada usuário. Nestas situações você pode fazer com que o Windows Server 2003 exiba uma listagem de usuários e/ou grupos do domínio (ou do servidor local se for um member server ou um standalone server), para que você possa selecionar um ou mais usuários e/ou grupos nesta listagem. Em primeiro lugar deve ser definido que tipo de objetos deve ser exibido na listagem: Computadores, grupos ou usuários. Para definir os tipos de objetos que devem aparecer na listagem, dê um clique no botão Tipos de objeto..), da janela indicada na Figura 6.22. Será aberta a janela Tipos de objeto, onde você pode marcar os tipos de objetos que serão exibidos. Deixe marcada apenas as opções Grupos e a opção Usuários, conforme indicado na Figura 6.23. Dê um clique no botão OK.

Você estará de volta a janela Seleciona Usuário ou grupo. Dê um clique no botão Avançado. Será exibida a janela Seleciona Usuários, Computadores ou Grupos. Observe que no campo Selecionar este tipo de objeto, já vem preenchido o valor: Usuários ou Grupos. Para listar todos os usuários e grupos cadastrados no domínio, dê um clique no botão Localizar agora. Na parte de baixo da janela será exibida uma listagem com todos os usuários e grupos cadastrados no

domínio. Dê um clique no usuário ou grupo para o qual você deseja atribuir permissões NTFS e dê um clique no botão OK. Você estará de volta à janela Selecionar Usuário ou grupo. Se for necessário você pode utilizar as teclas Ctrl e Shift para selecionar vários usuários ou grupos de um só vez. Você também pode utilizar o botão Localizações... para selecionar um outro domínio a partir do qual você deseja selecionar usuários ou grupos. Lembre do que foi discutido no Capítulo 2, onde mostrei que devido ao mecanismo de relações de confiança é possível definir permissões de acesso para usuários de outros domínios e não apenas para os usuários do domínio onde está o recurso.

13. Você estará de volta a janela Propriedades de Documentos e os usuários user01 e user02 já aparecem e os usuários selecionados já aparecem na lista. Por padrão são atribuídas as permissões Ler & Executar, Listar conteúdo da pasta e Leitura. Estas permissões são atribuídas, por padrão, para todo novo usuário e/ou grupo que for adicionado à lista de usuários/grupos com permissões de acesso.

Além de adicionar os dois usuários, você deve configurar o nível de acesso das permissões NTFS de cada usuário. Vou atribuir uma permissão NTFS de alteração (Modificar) para ambos.

14. Dê um clique em user01 para marcá-lo. Na parte do meio da janela, onde tem Permissões, dê um clique na opção Modificar , na coluna Permitir. Observe que todas as outras opções abaixo de Modificar, são automaticamente selecionadas, inclusive Gravar. Isso acontece porque modificar engloba todas as demais opções que foram marcadas.
15. Repita a operação para o usuário user02 com as mesmas permissões do usuário user01. Adicione o usuário user03 e negue todas as permissões para este usuário, isto é, para o usuário user03, marque todas as opções da coluna Negado.
16. Use o botão Adicionar para incluir o usuário Administrador. Porém para o usuário Administrador, na coluna Permitir marque a permissão Controle total. Sua janela deve estar conforme indicado pela Figura 6.24:

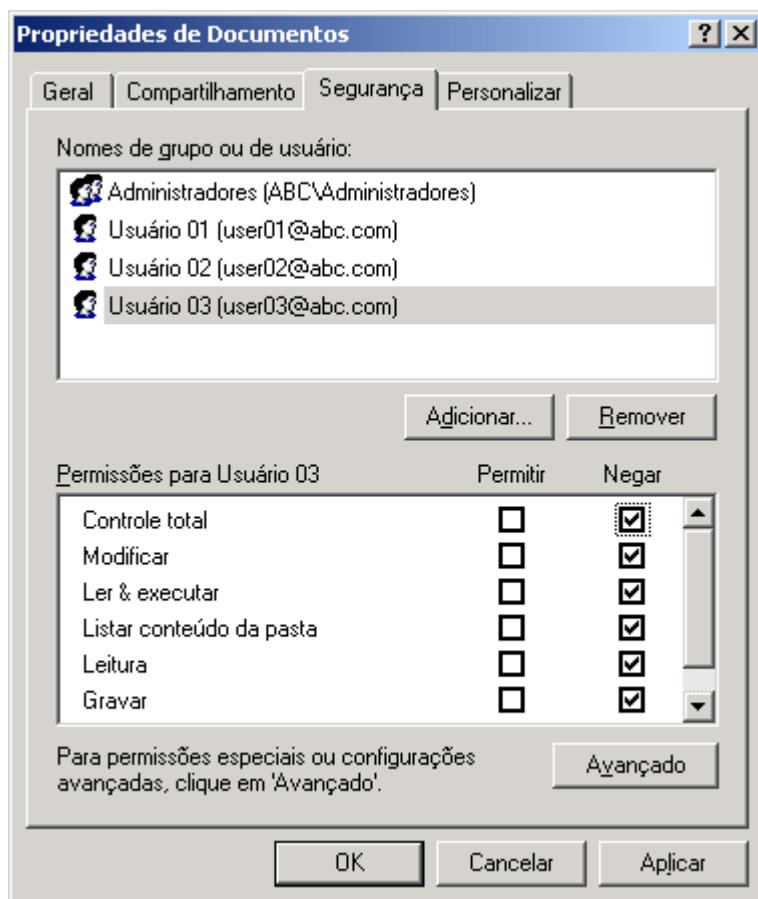


Figura 6.24 Permissões NTFS na pasta C:\Documentos.

17. Dê um clique no botão OK, para fechar a janela Propriedades de Documentos. Será exibida uma mensagem informando que você está negando permissões para um ou mais usuários, conforme indicado na Figura 6.25. Clique em Sim para confirmar as permissões Negar atribuídas ao usuário user03.

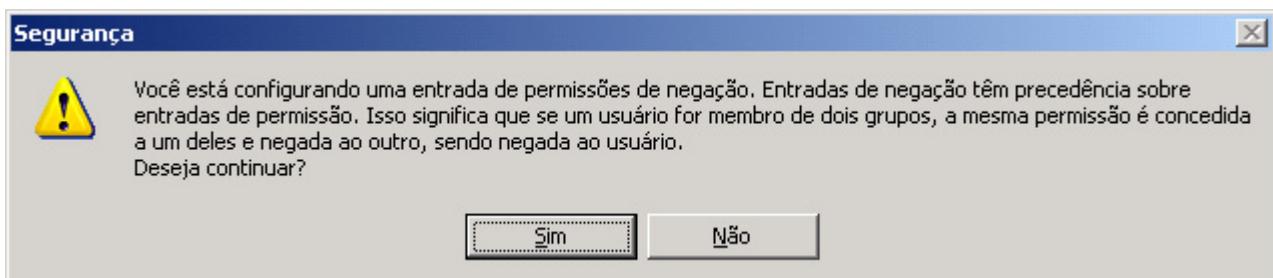


Figura 6.25 Mensagem de advertência devido a definição de negar permissão.

18. Agora a pasta Documentos possui permissões NTFS Modificar para os usuários user01 e user02, todas as permissões negadas para o usuário user03 e permissão Controle total para o usuário Administrator (Administrador). É hora de testar estas permissões, tanto através da rede, quanto localmente.

Passo 2 – no computador microxp02: Testando o funcionamento das permissões NTFS através da rede:

1. Faça o logon no computador microxp02 com a conta de usuário user02.
2. Selecione o comando Iniciar -> Executar.
3. No campo Abrir, digite \\microxp01\documentos e dê um clique no botão OK. Serão exibidos os compartilhamentos do computador microxp01.
4. Clique com o botão direito do mouse no compartilhamento Documentos e selecione a opção Mapear unidade de rede...
5. Na janela que é exibida selecione a letra Y para o drive e dê um clique no botão OK.
6. Você conseguiu? O drive é mapeado com sucesso? É claro que sim, uma vez que o usuário user02 tem permissão para acessar esse compartilhamento e também tem as permissões NTFS necessárias.
7. Abra o Meu computador.
8. Dê um clique duplo no drive de rede Y:
9. Abra a pasta Memorandos. Crie um arquivo de texto, digite algum texto e salve-o com o nome de teste de permissões.txt. Você conseguiu salvar o arquivo? É claro que sim, pois além de ter permissão de compartilhamento de Leitura e escrita (definida nos exemplos sobre compartilhamentos de pastas), o usuário user02 também tem as permissões NTFS Leitura e Gravação na pasta Documentos.

Permissões atribuídas ao usuário user02:

- ◆ **Permissões de compartilhamento:** O usuário user02 pertence ao grupo Diretoria, o qual tem permissões de compartilhamento Leitura e escrita. O usuário user02 também pertence ao grupo Empresa, o qual tem permissão de compartilhamento somente de leitura. O primeiro passo é definir qual a permissão de compartilhamento efetiva, do usuário user02. Para simplificar a questão, considere o esquema a seguir:

**IMPORTANTE:** Observe que neste caso temos dois conjuntos de permissões a ser considerados: Permissões de compartilhamento e permissões NTFS. Vou analisar o caso do usuário user02, para entender como funciona a combinação destes dois conjuntos de permissões. Mais adiante apresentarei mais alguns exemplos para que você possa fixar bem como funciona a combinação entre as permissões de compartilhamento e as permissões NTFS.

| Grupo     | Permissão de compartilhamento | Permissão de compartilhamento resultante |
|-----------|-------------------------------|--|
| Diretoria | Leitura e Alteração           | Leitura e Alteração                      |
| Empresa   | Leitura                       |  |

Então já sabemos que a permissão de compartilhamento efetiva para o usuário user02 é: Leitura e Alteração.

- ◆ Permissões NTFS: O usuário user02 tem as seguintes permissões NTFS: Modificar, Ler & Executar, Listar conteúdo da pasta, Leitura e Gravar.

Observe que tanto nas permissões de compartilhamento, quanto nas permissões NTFS, o usuário tem permissão para criar arquivos (Alteração no compartilhamento e Gravar no NTFS). Por isso que o usuário user02. pode criar e gravar um novo arquivo de texto

Passo 3 – no computador microxp01: Testando o funcionamento das permissões NTFS localmente.

Para testar o funcionamento das permissões NTFS localmente, faça o seguinte:

1. Faça o logon no computador microxp01 com a conta de usuário user03.
2. Abra o Meu computador, acesse o drive C:. Dentro do drive C: dê um clique duplo para acessar a pasta Documentos.
3. Você conseguiu ?
4. Não. Mas como é possível se você está acessando a pasta Documentos localmente, isto é, no computador onde ela foi criada ?
5. Feche a mensagem de acesso negado e efetue o logoff do usuário user03.

Agora você irá criar um arquivo de texto chamado teste.txt dentro da pasta Documentos e atribuir permissões NTFS para este arquivo.

Passo 4 – no computador microxp01: Criando um arquivo teste.txt e atribuindo permissões NTFS para este arquivo.

1. Efetue o logon como Administrador, no computador microxp01.
2. Abra o Windows Explorer.
3. Acesse a pasta Documentos criada anteriormente.
3. No painel da esquerda, dê um clique na pasta Documentos para abri-la.
4. No painel da direita, em qualquer espaço em branco, dê um clique com o botão direito do mouse, e no menu que surge aponte para Novo e nas opções do menu Novo dê um clique sobre a opção Documento de texto.
5. Surge uma caixa onde está escrito Novo documento de texto.txt.
6. Não clique em lugar nenhum nem tecle Enter, simplesmente digite o nome do arquivo que está sendo criada, no nosso exemplo digite teste.txt e tecle Enter. O Windows Server 2003 cria um documento de texto em branco, com o nome de teste.txt.
7. Dê um clique com o botão direito em teste.txt e no menu que surge dê um clique em Propriedades.
8. Surge a janela Propriedades de teste.txt, com a guia Geral selecionada por padrão. Dê um clique na guia Segurança, que é a guia utilizada para configurar as permissões NTFS

---

**IMPORTANTE:** Lembre-se de que você fez o logon no computador microxp01, onde a pasta Documentos foi criada, mas utilizando a conta de usuário user03, a qual possui as permissões NTFS "negadas" para acessar a pasta Documentos. Não esqueça que as permissões NTFS tem efeito tanto localmente quanto através da rede, diferente das permissões de compartilhamento, as quais não tem nenhum efeito localmente. Porém existe uma situação onde as permissões de compartilhamento são a única alternativa, que é no caso de unidades formatadas com FAT./FAT32 Para estas unidades não existem permissões NTFS.

---

Outro detalhe importante, é que as permissões NTFS herdadas não podem ser alteradas, a menos que seja desativado o mecanismo de herança, para o arquivo teste.txt, conforme já descrito anteriormente.

Além das permissões herdadas, você pode adicionar permissões NTFS para usuários ou grupos. Permissões adicionadas desta maneira são conhecidas como “Permissões explícitas”, as quais podem ser alteradas a qualquer momento pelo Administrador do sistema, conforme a necessidade.

8. Ao invés de excluir (como em um dos exemplos anteriores), você irá Copiar as permissões herdadas. Dê um clique no botão Avançado. Na janela que surge, desmarque a opção “Permitir que as permissões herdáveis do pai sejam propagadas a este objeto e a todos os objetos filho. Incluí-las nas entradas explicitamente definidas aqui”. Será exibida janela solicitando confirmação, dê um clique no botão Copiar. Com isso o mecanismo de herança foi desabilitado e as permissões herdadas, transformando-as em permissões explícitas, as quais podem ser alteradas. Dê um clique no botão OK para fechar a janela de configurações avançadas e voltar para a guia Segurança.
9. Dê um clique em user01 para marcá-lo. Na parte do meio da janela, na coluna Permitir, deixe apenas o opção Leitura marcada.
10. Repita a operação para o usuário user02.
11. Dê um clique no botão OK, para fechar a janela “Propriedades de teste.txt”.
12. Agora a pasta Documentos possui permissões NTFS Modificar para os usuários user01 e user02 e Controle total para o usuário Administrador. Já o arquivo teste.txt, dentro da pasta documentos, tem permissão Leitura para os usuários user01 e user02, e Controle total para o usuário Administrador.

Agora você tem permissões NTFS para a pasta Documentos e permissões NTFS diferentes para o arquivo teste.txt que está dentro da pasta Documentos. É hora de testar estas permissões, tanto através da rede, quanto localmente. Antes de iniciar os testes lembre que, no caso de conflito entra as permissões de pasta e as permissões do arquivo, prevalece as permissões do arquivo.

Passo 5 – no computador microxp02: Testando o funcionamento das permissões NTFS através da rede.

1. Faça o logon no computador microxp02 com a conta de usuário user02.
2. Tente acessar o compartilhamento Documentos, no computador microxp01. Você conseguiu ?

É claro que sim, uma vez que o usuário user02 tem permissão para acessar esse compartilhamento e também tem as permissões NTFS necessárias.

3. Dentro da pasta Documentos deve estar o arquivo teste.txt. Dê um clique para marcá-lo e pressione a tecla Delete para excluí-lo. Você conseguiu eliminar o arquivo teste.txt ?

Não. Isso porque o usuário user02 possui permissões NTFS modificar na pasta Documentos, mas no arquivo teste.txt, as permissões do usuário user02 são apenas Leitura. Como as permissões de arquivo tem prioridade sobre as permissões de pasta, a permissão efetiva do usuário user02 no arquivo teste.txt é Leitura, a que não permite que o arquivo seja excluído pelo usuário user02.

4. Você deve ter recebido uma mensagem de Acesso negado. Dê um clique em OK para fechá-la.
5. Faça o logoff do usuário user02.

**IMPORTANTE:** Observe que algumas opções na coluna Permitir estão marcadas para os usuários Administrador, user01, user02 e user03, porém não podem ser alteradas clicando com o mouse, pois estão desabilitadas para alteração. Isso acontece, porque quando criamos o arquivo teste.txt ele “herdou” as permissões do objeto pai, que no caso é a pasta Documentos. Esse é o comportamento padrão do Windows Server 2003.

Passo 6 – no computador microxp01: Testando o funcionamento das permissões NTFS localmente.

1. Faça o logon no computador microxp01 com a conta de usuário user02.
2. Abra o Windows Explorer e acesse a pasta C:\Documentos. Você conseguiu?
3. É claro que sim, uma vez que o usuário user02 tem as permissões NTFS necessárias para acessar a pastas Documentos.
4. Dentro da pasta Documentos deve estar o arquivo teste.txt. Dê um clique para marcá-lo e pressione a tecla Delete para eliminá-lo. Você conseguiu eliminar o arquivo teste.txt ?
5. Não. Isso porque o usuário user02 possui permissões NTFS modificar na pasta Documentos, mas no arquivo teste.txt, as permissões do usuário user02 são apenas Leitura. Como as permissões de arquivo tem prioridade sobre as permissões de pasta, a permissão efetiva do usuário user02 sobre o arquivo teste.txt é Leitura, a qual não permite que o arquivo seja excluído por este usuário.  
Além disso nunca é demais lembrar que as permissões NTFS são válidas tanto para acessos através da rede, quanto para acessos locais.
6. Você deve ter recebido uma mensagem de Acesso negado. Dê um clique em OK para fechá-la.
7. Faça o logoff do usuário user02.

Exercício: Crie uma pasta chamada Ofícios em uma unidade formatada com NTFS. Desative opção para herdar as permissões do objeto pai. Atribui permissões de leitura para o grupo de usuários Empresa e permissão de Controle total para o usuário user03. Poderá o usuário user03 criar um novo arquivo dentro da pasta Ofícios ?

Sim, pois a permissão efetiva do usuário user03 é a soma das permissões atribuídas aos grupos aos quais ele pertence, no caso ao grupo Empresa mais as permissões atribuídas ao próprio usuário, conforme explicado anteriormente.

## Combinando permissões de compartilhamento e permissões NTFS – estudo de casos.

Você pode estar se perguntando como é que o Windows Server 2003 trata quando existem diferenças entre as permissões de compartilhamento e as permissões NTFS. Por exemplo se nas permissões de compartilhamento o usuário maria tem direito de Controle total e nas permissões NTFS o usuário maria tem direito apenas de Leitura. Qual a permissão efetiva do usuário maria?

Eu já fiz alguns comentários sobre a combinação entre as permissões de compartilhamento e as permissões NTFS. Neste tópico vou detalhar este assunto através do uso de mais alguns exemplos.

É hora de analisar algumas situações práticas para fixar bem a combinação entre permissões de compartilhamento e NTFS.

Exemplo 01: Considere a situação indicada na Figura 6.26. Qual a permissão efetiva do usuário jsilva2, na pasta compartilhada Documentos ?

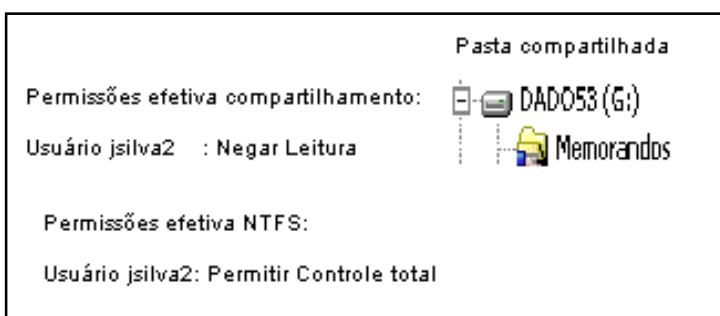


Figura 6.26 A permissão efetiva é a mais restritiva.

**IMPORTANTE:** Quando existem diferenças entre as permissões de compartilhamento e as permissões NTFS, a permissão efetiva é a MAIS RESTRITIVA, isto é, aquele que restringe mais as ações que podem ser tomadas. No exemplo do primeiro parágrafo, a permissão efetiva para o usuário maria seria Leitura, a qual é mais restritiva do que Controle total.

Para entender a situação da Figura 6.26, você deve ter em mente que no caso de diferenças entre as permissões de compartilhamento e as permissões NTFS, a permissão efetiva é a mais restritiva.

No exemplo da figura a permissão efetiva do usuário jsilva2 é Leitura a qual é a mais restritiva entre Controle total (a permissão NTFS do usuário jsilva2) e Leitura (permissão de compartilhamento do usuário jsilva2). A mesma análise é válida em relação ao usuário maria.

Agora considere uma situação um pouco mais complexa, onde tem que ser considerada a combinação das permissões dos diferentes grupos aos quais pertence um usuário, além da combinação entre permissões de compartilhamento e permissões NTFS.

Admita que o usuário jsilva2 pertença aos grupos Contabilidade e Marketing. Com base na Figura 6.27, qual seria a permissão efetiva para o usuário paulo na pasta compartilhada Documentos?

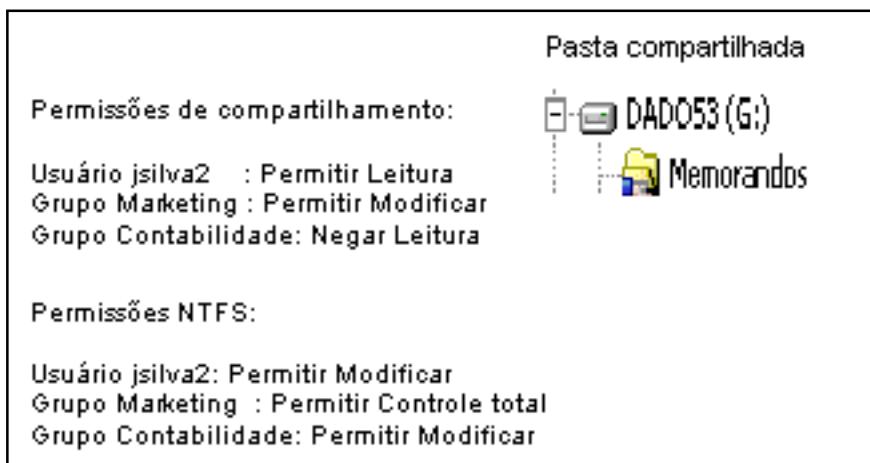


Figura 6.27 Usuário jsilva2 pertence aos grupos Marketing e Contabilidade.

Para definir a permissão efetiva para o usuário jsilva2, devem ser levadas em considerações diversas regras, já apresentadas ao longo deste capítulo:

- ◆ Quando um usuário pertence a vários grupos, os quais recebem diferentes permissões (quer sejam permissões de compartilhamento ou NTFS), a permissão efetiva é a soma das permissões. Além disso você deve lembrar que Negar tem prioridade sobre permitir. No caso das permissões de compartilhamento, um dos grupos ao qual o usuário jsilva2 pertence – grupo Contabilidade – tem a permissão de leitura negada. Logo a permissão efetiva de compartilhamento para jsilva2 é Negar leitura, independente das demais permissões atribuídas aos grupos aos quais pertence o usuário jsilva2.

A permissão efetiva NTFS para o usuário jsilva2 é a soma das permissões do usuário com as permissões dos grupos Marketing e Contabilidade. Com isso a permissão NTFS efetiva é Permitir Controle total.

Com isso é possível reduzir a situação proposta inicialmente, na Figura 6.27, a uma situação mais simplificada, conforme indicado na Figura 6.28.

- ◆ Agora é hora que lembrar que quando existe diferença entre as permissões de compartilhamento e NTFS vale a mais restritiva.

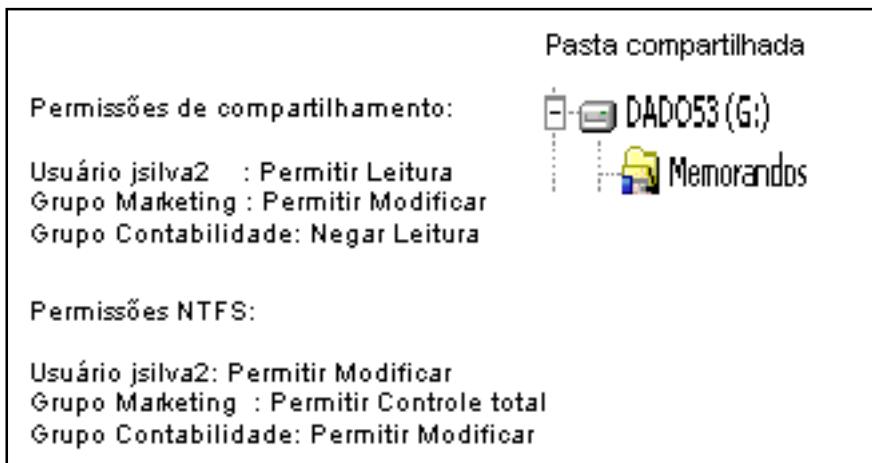


Figura 6.28 Simplificando a situação.

Com isso é possível determinar que a permissão efetiva do usuário jsilva2 no compartilhamento Documentos é “Negar Leitura”, isto é, o usuário não conseguirá nem listar o conteúdo da pasta.

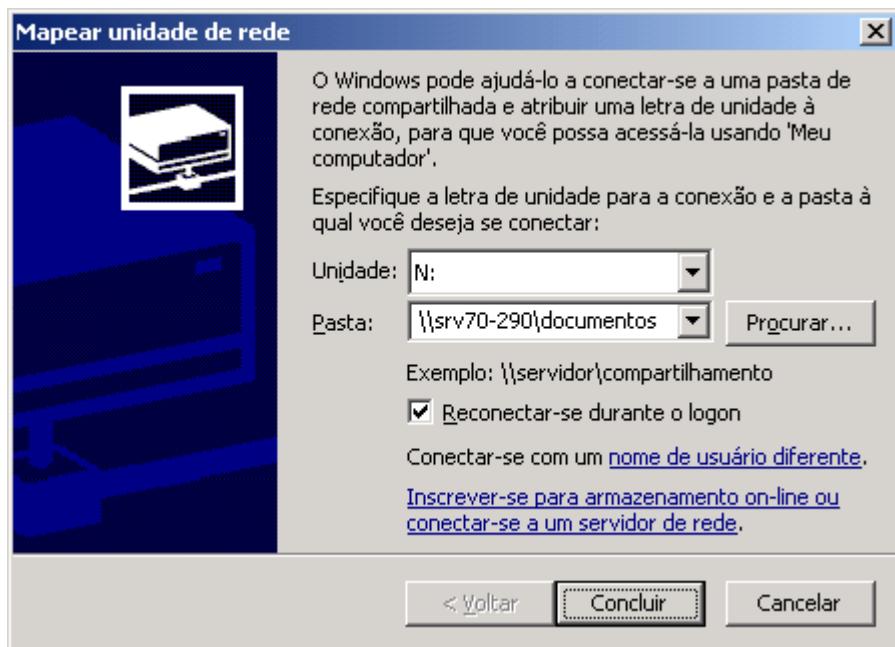
## Mapeando de unidades de rede.

Já falei sobre o mapeamento de unidades de rede, nos exemplos anteriores. Agora vou detalhar um pouco mais este conceito. Até agora você acessava uma pasta compartilhada, utilizando o comando Iniciar -> Executar. Quando é necessário acessar um determinado compartilhamento seguidamente, é mais prático “Mapear uma unidade de rede”, o que torna o acesso a pasta compartilhada, muito mais fácil. No caso prático de uma rede com servidores baseados no Windows Server 2003, as pastas compartilhadas ficarão em um ou mais servidores e nas estações de trabalho dos usuários serão mapeadas unidades, tais como M:, N:, X: e assim por diante. Ao acessar um destes drives de rede o usuário na verdade está acessando uma pasta compartilhada em um servidor. Normalmente os drives de rede são mapeados automaticamente, através de comandos no script de logon do usuário. No capítulo sobre Group Policies falarei um pouco mais sobre o script de logon.

Mapear uma unidade significa que você irá associar uma determinada letra com o compartilhamento da rede. Por exemplo, você poderia associar a unidade M:\ como o compartilhamento Documentos do computador microxp01. Com isso ao acessar a unidade M:\, na verdade o usuário está acessando o conteúdo da pasta compartilhada \\microxp01\Documentos. Além disso é possível fazer com que o Windows Server 2003 restabeleça este mapeamento toda vez que for feito o logon. Com isso a unidade estará sempre disponível. Em capítulos anteriores, me referi a estas unidades como Drives de rede. Os termos são sinônimos.

Exemplo: Mapeando o drive M: para a pasta compartilhada Documentos no computador microxp01.

1. Faça o logon como Administrador no computador microxp02.
2. Abra o Meu computador ou o Windows Explorer.
3. Selecione o comando Ferramentas -> Mapear unidade de rede... Será exibida a janela Mapear unidade de rede, indicada na Figura 6.29:



**Figura 6.29 Janela Mapear unidade de rede.**

4. Na lista de unidades (Drive) selecione M:
5. No campo Pasta: digite \\microxp01\Documentos. Este é o nome UNC do compartilhamento Documentos no computador microxp01.

Certifique-se que a opção Reconectar-se durante o logon esteja marcada. Esta opção faz com que o drive M: seja mapeado cada vez que o usuário Administrador fizer o logon. Observe que o drive somente será automaticamente montado para o usuário Administrador. É possível fazer com que um ou mais drives sejam montados automaticamente, para todos os usuários. Para isso utilizamos scripts de Inicialização.

6. Dê um clique no botão OK para concluir o mapeamento.
7. O Windows Server 2003 abre uma janela mostrando o conteúdo do drive mapeado. Feche essa janela.
8. Você estará de volta na janela Meu computador (ou ao Windows Explorer).
9. Procure por um drive M:. Se este ainda não aparece, dê um toque na tecla F5 para atualizar a listagem.
10. O drive M: deve aparecer na listagem de drives de rede.

Existem alguns compartilhamentos ocultos especiais, para os quais somente Administradores tem acesso e cujas permissões de acesso não podem ser modificadas. Por padrão o Windows Server 2003 cria compartilhamentos administrativos para todas as unidades de disco rígido do computador. Por exemplo, se você tem duas unidades de disco rígido C: e D:, o Windows Server 2003 irá criar dois compartilhamentos administrativos C\$ e D\$, para os quais somente o grupo Administradores tem acesso, podendo inclusive mapear uma unidade para um compartilhamento administrativo.

Quando não precisar mais de um drive mapeado você pode, facilmente, desconectá-lo.

Para desconectar um drive mapeado, faça o seguinte:

**NOTA:** Você pode utilizar a opção Conectar-se com um nome de usuário diferente, para acessar a pasta compartilhada como sendo um usuário diferente do usuário atualmente logado. Neste caso, valerão as permissões do usuário informado e não as permissões do usuário que está logado.

**NOTA:** Você pode acrescentar o símbolo do cifrão (\$) no final do nome de um compartilhamento. O efeito de acrescentar o cifrão é que você torna o compartilhamento oculto, isto é, este não pode ser

1. Abra o Meu computador.
2. Localize o drive a ser desconectado e dê um clique com o botão direito sobre o respectivo drive.
3. No menu que surge dê um clique na opção Desconectar-se e pronto. Caso o drive ainda esteja aparecendo tecle F5 para atualizar a listagem.

localizado através da opção Meus locais de rede. Por exemplo, se você criar um compartilhamento no computador microxp01, cujo nome de compartilhamento é Dados\$, a única maneira de acessá-lo é através do nome UNC: \\microxp01\Dados\$. Compartilhamentos deste tipo, são chamados de compartilhamentos ocultos. É possível mapear uma unidade de rede para um compartilhamento oculto, desde que você saiba o caminho para o compartilhamento.

---

## Distributed File System - DFS

### Entendendo o que é o Distributed File System - DFS.

Neste tópico apresentarei o serviço DFS – Distributed File System. Mostrarei quais as vantagens em utilizar este serviço, para facilitar a administração de pastas compartilhadas em uma rede de baseada no Windows Server 2003. Além dos conceitos teóricos, mostrarei um exemplo prático de utilização do DFS.

O principal motivo para a implementação de redes locais (LAN) e de longa distância (WAN) é o compartilhamento de recursos. A possibilidade de ter as informações centralizadas em um ou mais servidores, acessando estas informações a partir de qualquer estação de trabalho da rede é um grande benefício em termos de gerenciamento e produtividade para os usuários. Dentre os vários recursos compartilhados através de uma rede, sem sombra de dúvidas, o compartilhamento de arquivos é o mais utilizado, através do uso de pastas compartilhadas, conforme mostrei nos tópicos iniciais deste capítulo.

Em redes baseadas em tecnologias da Microsoft, com servidores rodando o Windows NT Server, Windows 2000 Server ou Windows Server 2003 e clientes rodando uma das versões do Windows – 9x, Me, NT Workstation, Windows 2000 Professional ou Windows XP Professional, o compartilhamento de arquivos é feito utilizando Pastas compartilhadas (Shared Folders).

Por exemplo, suponha que os arquivos da pasta C:\Manuais, do servidor SRV01, devam estar disponíveis para acesso através da rede. Basta compartilhar esta pasta no servidor SRV01, definir as permissões de compartilhamento e as permissões NTFS adequadas (veja os tópicos anteriores deste capítulo). Depois o acesso a pasta Manuais pode ser feito em cada estação de trabalho da rede. Normalmente este acesso é feito via a “montagem” de um drive de rede (veja tópico anterior). Montar um drive de rede, significa que o administrador irá associar uma unidade (F:, G: X:, etc) à pasta compartilhada. Para o usuário, a pasta compartilhada aparece como mais uma unidade no Meu computador ou no Windows Explorer. Por exemplo, se for montado um drive X:, associado com a pasta compartilhada Manuais, toda vez que o usuário acessar o drive X: estará, na prática, acessando o conteúdo da pasta Manuais, compartilhada no servidor SRV01.

---

**NOTA:** Normalmente a montagem de drives de rede é feita através do comando net use, no Script de logon da conta do usuário. Com isso, um ou mais drives de rede podem ser montados, automaticamente, quando o usuário faz o logon na rede.

---

Na Figura 6.30, mostro o exemplo de uma rede Cliente Servidor, onde os usuários acessam, através de um drive X:, uma pasta compartilhada no servidor SRV01:

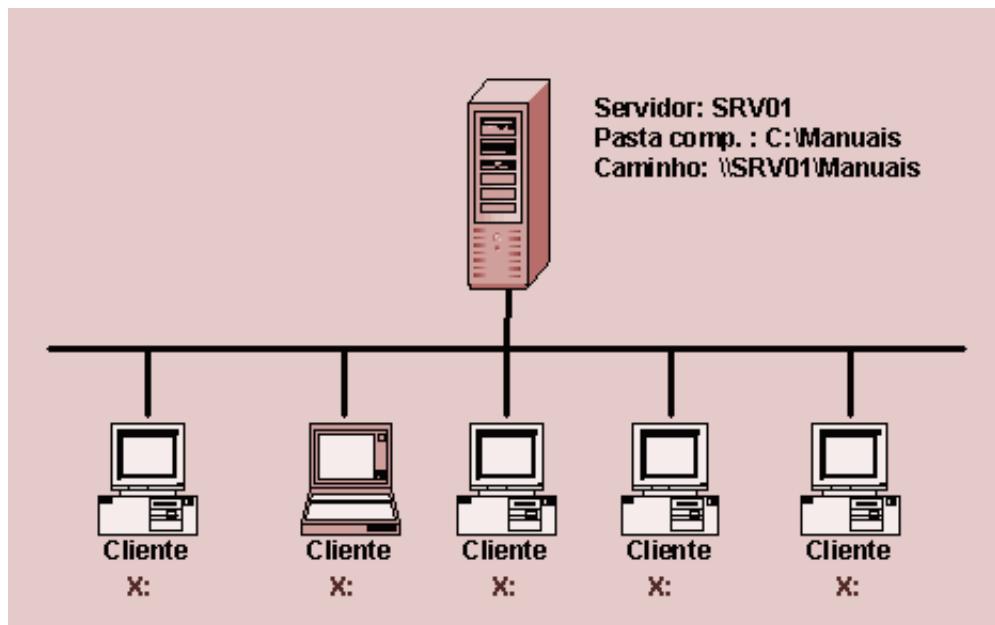


Figura 6.30 Compartilhamento de arquivos em uma rede local.

## DFS – Conceito e utilizações

O modelo proposto de pastas compartilhadas, funciona bem para pequenas redes, onde existe um número reduzido de pastas compartilhadas – digamos até cinco pastas compartilhadas em um ou mais servidores. Porém, para grandes redes, onde o número de pastas compartilhadas é grande, o uso de um drive de rede para acessar cada pasta compartilhada, pode tornar-se de difícil implementação, ou até mesmo impossível – quando existirem mais pastas compartilhadas do que o número de letras disponíveis no nosso alfabeto.

Mesmo em uma rede pequena, onde temos entre cinco e dez pastas compartilhadas, usar um drive para cada pasta não é a melhor solução. Este modelo é difícil de administrar, do ponto de vista do Administrador da rede, e difícil de utilizar, do ponto de vista do usuário.

Considere o diagrama da Figura 6.31, onde existem oito pastas compartilhadas, em três servidores diferentes:

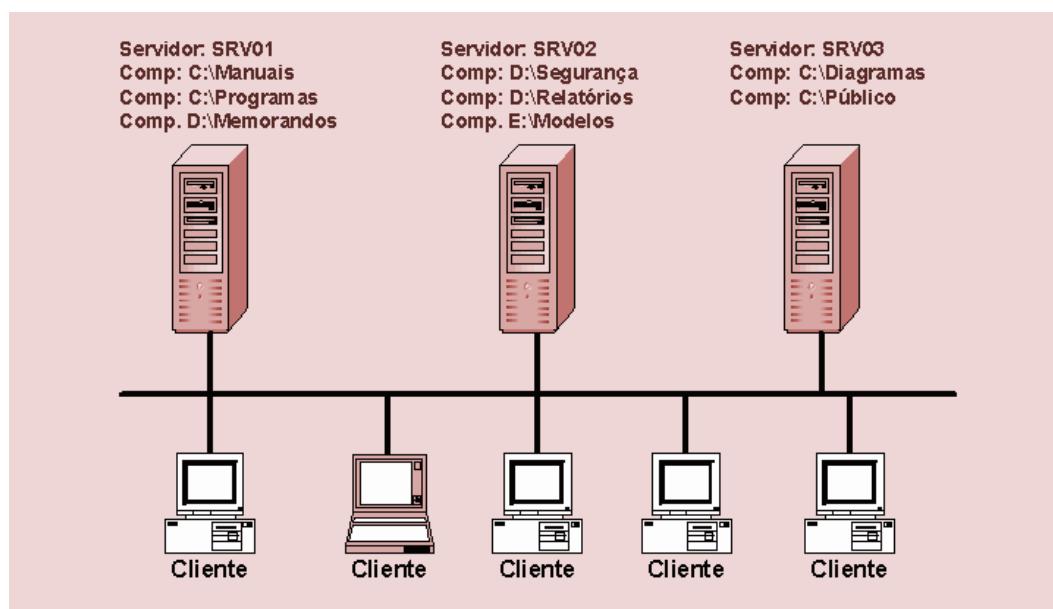


Figura 6.31 - Uma rede com oito pastas compartilhadas em diferentes servidores.

Na Tabela 6.1, apresento uma visão geral dos oito compartilhamentos da Figura 6.31, uma breve descrição de cada um, o caminho de rede para acessar o compartilhamento e uma sugestão de drive a ser utilizado, na estação cliente, para acesso ao compartilhamento:

**Tabela 6.1 – Informações detalhadas sobre os compartilhamentos da rede.**

| Compartilhamento | Nome de Comp. | Servidor | Caminho           | Drive |
|------------------|---------------|----------|-------------------|-------|
| C:\Manuais       | Manuais       | SRV01    | \SRV01\Manuais    | F:    |
| C:\Programas     | Programas     | SRV01    | \SRV01\Programas  | G:    |
| D:\Memorandos    | Memorandos    | SRV01    | \SRV01\Memorandos | H:    |
| D:\Segurança     | Segurança     | SRV02    | \SRV02\Segurança  | I:    |
| D:\Relatórios    | Relatórios    | SRV02    | \SRV02\Relatórios | J:    |
| E:\Modelos       | Modelos       | SRV02    | \SRV02\Modelos    | K:    |
| C:\Diagramas     | Diagramas     | SRV03    | \SRV03\Diagramas  | L:    |
| C:\Público       | Público       | SRV03    | \SRV03\Público    | M:    |

Os drives de F a M, necessários para acessar as pastas compartilhadas, poderiam ser montados, automaticamente, incluindo os seguintes comandos no script de logon dos usuários:

```
net use F: \\SRV01\Manuais /yes
net use G: \\SRV01\Programas /yes
net use H: \\SRV01\Memorandos /yes
net use I: \\SRV02\Segurança /yes
net use J: \\SRV02\Relatórios /yes
net use K: \\SRV02\Modelos /yes
net use L: \\SRV03\Diagramas /yes
net use M: \\SRV03\Público /yes
```

Este modelo apresenta diversos inconvenientes, dentre os quais gostaria de destacar os seguintes:

- ◆ O usuário tem acesso às informações através de diversos drives de rede (oito no nosso exemplo). Com isso o usuário não tem uma visão consolidada das informações disponíveis na rede.
- ◆ Além de ter de criar e configurar os compartilhamentos, o Administrador da rede precisa garantir que os drives necessários sejam corretamente configurados em todas as estações de trabalho da rede, onde houver necessidade de acesso aos drives.
- ◆ Não existe redundância e nem tolerância a falhas. Se um dos servidores estiver com problemas, os usuários não terão acesso às pastas compartilhadas deste servidor.

A seguir apresentarei qual o modelo proposto com o uso do DFS e quais os benefícios deste modelo.

## DFS: Modelo proposto e benefícios

Com o uso do DFS é possível resolver os problemas descritos anteriormente, onde foi utilizado um drive de rede para acessar cada uma das pastas compartilhadas. O DFS – Distributed File System (Sistema de Arquivos Distribuídos) é

um serviço que roda em servidores NT Server 4.0, Windows 2000 Server ou no Windows Server 2003. No Windows NT Server 4.0 e no Windows 2000 Server o DFS tem que ser instalado. No Windows Server 2003 o DFS é instalado automaticamente com o sistema operacional e não pode ser desinstalado. Para entender o modelo proposto pelo DFS, vou utilizar o exemplo do item anterior e mostrar como, com o uso do DFS, é possível dar acesso a todas as pastas compartilhadas, usando um único drive de rede, ao invés de usar oito drives.

Para entender o modelo proposto pelo DFS, considere o diagrama da Figura 6.32:

| Compartilhamento | Nome de comp. | Servidor | Caminho           | Drive |
|------------------|---------------|----------|-------------------|-------|
| C:\Manuais       | Manuais       | SRV01    | \SRV01\Manuais    | F:    |
| C:\Programas     | Programas     | SRV01    | \SRV01\Programas  | G:    |
| D:\Memorandos    | Memorandos    | SRV01    | \SRV01\Memorandos | H:    |
| D:\Segurança     | Segurança     | SRV02    | \SRV02\Segurança  | I:    |
| D:\Relatórios    | Relatórios    | SRV02    | \SRV02\Relatórios | J:    |
| E:\Modelos       | Modelos       | SRV02    | \SRV02\Modelos    | K:    |

Figura 6.32 – O modelo de compartilhamento do DFS.

É hora de entender os detalhes do modelo proposto na Figura 11.34:

- ◆ Conforme descrito anteriormente, o DFS é um serviço que faz parte do Windows Server 2003. Você pode verificar se o serviço DFS está configurado para inicializar automaticamente, usando o console Serviços, disponível no menu Ferramentas Administrativas.
- ◆ No servidor DFS, que no exemplo da Figura 6.32 é o servidor SRVDFS, é criado um Root DFS. Um Root DFS é associado com uma pasta local no servidor DFS. Mostrarei exemplos práticos mais adiante, neste tópico.
- ◆ Uma vez criado o Root DFS, o administrador passa a criar Links DFS. Cada link “aponta” para uma pasta compartilhada na rede, podendo esta pasta estar no próprio servidor DFS ou em qualquer outro servidor da rede. No exemplo da Figura 6.32, o Administrador poderia criar um link chamado Manuais, o qual aponta para \\SRV01\Manuais, um link chamado Programas, o qual aponta para \\SRV01\Programas, um link chamado Memorandos, o qual aponta para \\SRV01\Memorandos e assim por diante. Ao criar os links o administrador está montando uma árvore DFS.
- ◆ Após ter criados todos os links desejados, o administrador pode dar acesso aos clientes. No modelo do DFS, somente o Root DFS é compartilhado. Por exemplo, suponha que o Root DFS, no servidor SRVDFS tivesse sido compartilhado com o nome de ArqRede. Os usuários acessam o Root DFS, montando um drive de rede associado com o compartilhamento \\SRVDFS\ArqRede. Vamos supor que o usuário monta um drive X:, associado com o Root do DFS. Neste caso, cada um dos links da árvore DFS, aparece como uma pasta do drive X:. Observe que através de um único drive de rede (X:), o qual aponta para o Root DFS, o usuário terá acesso a várias pastas compartilhadas, sendo que cada pasta aparece como uma pasta do drive X:, ao invés de ser necessário um drive diferente para cada pasta compartilhada. Esta é a idéia, o modelo proposto pelo DFS.

No exemplo, o drive X: do usuário teria uma estrutura conforme indicado na Figura 6.33:

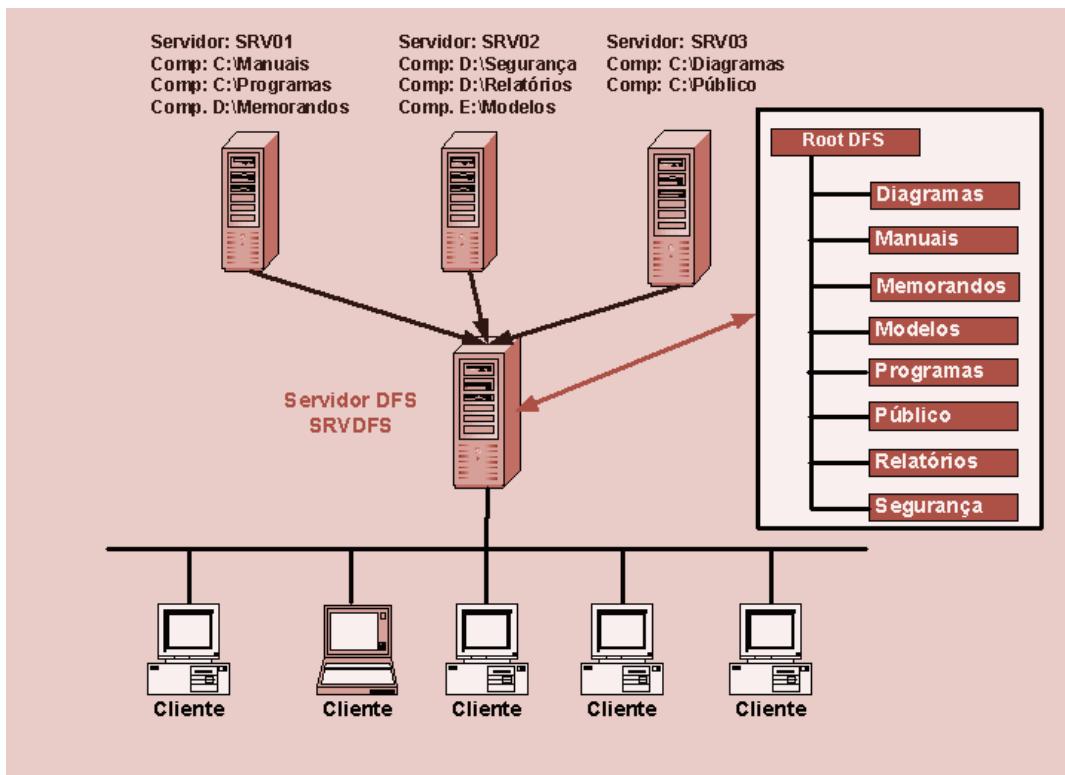


Figura 6.33 – Um único drive para acessar oito compartilhamentos diferentes.

Observe que com um único drive (X:), que aponta para o Root do DFS (\\\SRVDFS\ArqRede), o usuário tem acesso a oito pastas compartilhadas, sendo que cada Pasta compartilhada aparece como uma pasta do drive X:

Com o modelo proposto pelo DFS existem muitos benefícios, dentre os quais podem ser destacados os seguintes:

- ◆ O usuário tem uma visão geral das informações disponíveis da rede e, através de um único drive, tem acesso a todas as informações disponíveis.
- ◆ O Administrador tem um ponto central de Administração, o que facilita e simplifica o seu trabalho.
- ◆ As tarefas de Backup são simplificadas. Ao invés de programar o Backup de inúmeras pastas, em diferentes servidores, o Administrador programa o backup do Root do DFS.
- ◆ Com o uso de Roots DFS de Domínio (conforme mostrarei mais adiante), é possível criar redundância, através da disponibilização da mesma pasta compartilhada em dois ou mais servidores. Com isso mesmo que um servidor tenha problemas, o usuário continuará tendo acesso aos arquivos a partir de outros servidores, onde existem réplicas da pasta compartilhada. O uso desta funcionalidade, em conjunto com as configurações de Arquivos Off-line (as quais falarei mais adiante, neste capítulo), aumenta muito a disponibilidade dos arquivos da rede para o usuário final.
- ◆ Balanceamento de carga entre servidores, quando utilizamos Roots DFS de Domínio, com a duplicação de pastas compartilhadas em diferentes servidores.

## Limitações no Cliente e no Servidor

O serviço DFS é instalado automaticamente quando instalamos o Windows Server 2003. Este serviço também é configurado para iniciar automaticamente. Para conferir se o serviço DFS está configurado corretamente, você pode utilizar o console Serviços, o qual está é acessado através da opção: Iniciar -> -> Ferramentas administrativas -> Serviços.

O serviço DFS tem algumas limitações, as quais descrevo a seguir:

- ◆ O número máximo de caracteres para o caminho UNC (\servidor\compartilhamento) de uma pasta compartilhada é 260.
- ◆ O número máximo de réplicas de uma pasta compartilhada, em um Root DFS de Domínio é 256.
- ◆ No Windows 2000 Server cada servidor DFS pode ter um único Root DFS. Esta limitação não existe no Windows Server 2003, onde pode ser criado mais de um DFS Root por servidor DFS.
- ◆ O número máximo de links, por Root DFS, é de 1000.

O DFS é baseado em um modelo Cliente/Servidor. O Servidor é representado por um servidor com o Windows Server 2003 instalado, onde o serviço DFS está rodando. Podem existir diferentes clientes DFS. O Windows 2000 Professional e o Windows XP Professional podem atuar como clientes DFS, sem que seja necessária a instalação de software adicional. Para versões anteriores do Windows, considere os detalhes a seguir:

- ◆ **Windows 95:** O Cliente DFS para o Windows 95 está disponível para Download no site da Microsoft, no seguinte endereço: [http://download.microsoft.com/download/win95/dfs/1.0/W95/EN-US/dfs\\_v41\\_win95client.exe](http://download.microsoft.com/download/win95/dfs/1.0/W95/EN-US/dfs_v41_win95client.exe)
- ◆ **Windows 98:** O Cliente DFS faz parte do Windows 98, não é preciso instalar nenhum software adicional.
- ◆ **Windows NT 4.0:** O Cliente DFS está disponível para Download, no seguinte endereço: [http://download.microsoft.com/download/winntsrv40/dfs/1.0/NT4/EN-US/dfs\\_v41\\_i386.exe](http://download.microsoft.com/download/winntsrv40/dfs/1.0/NT4/EN-US/dfs_v41_i386.exe).
- ◆ **Windows 2000 e XP:** O cliente DFS faz parte do Sistema Operacional.

Agora que você já entendeu o modelo proposto pelo DFS e conhece as limitações do DFS, é hora de aprender, através de um exemplo prático, a criar e configurar uma árvore DFS.

## Implementando o DFS – um exemplo prático

Neste item vou apresentar um exemplo prático. Vou criar uma árvore DFS. Será criado um Root DFS de domínio e, em seguida, adicionados links para cinco pastas compartilhadas em dois servidores da rede. Também criarei uma réplica de uma das pastas, para testar a redundância. Na parte final do exemplo, acessarei o root DFS e farei alguns testes. Então mãos à obra.

## O ambiente em uso nos exemplos

Para o exemplo proposto utilizarei uma rede com dois servidores (na verdade a rede local de testes que uso em casa. Utilizo esta rede para fazer pesquisas, para escrever meus artigos, cursos e livros). Na rede de exemplo, existem dois servidores, conforme descrito na Tabela 6.2:

**Tabela 6.2 – Os servidores utilizados no exemplo prático.**

| Nome do Servidor | Sistema Operacional                             |
|------------------|---|
| servidor         | Windows 2000 Server em Português                |
| servidor2        | .NET Server, Beta 3, Compilação 3268, em Inglês |

Os servidores que estou utilizando fazem parte de um domínio baseado no Active Directory. O nome do domínio é groza.com.

Serão criados os compartilhamentos indicados na Tabela 6.3:

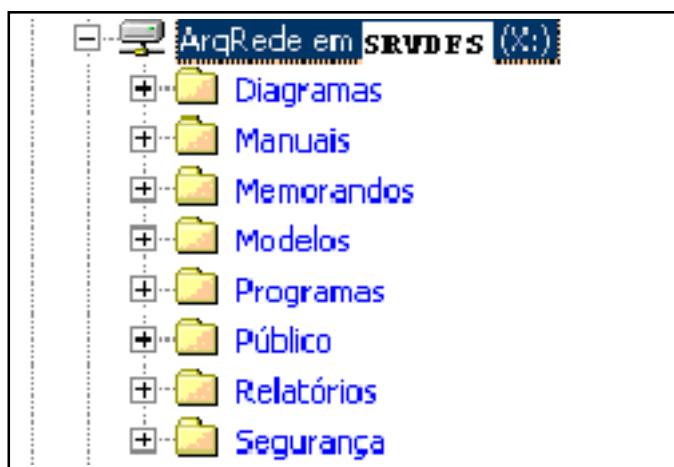
**Tabela 6.3 – Compartilhamentos que serão utilizados no exemplo prático.**

| Compartilhamento | Nome de Comp. | Servidor  | Caminho             |
|------------------|---------------|-----------|---------------------|
| E:\Manuais       | Manuais       | servidor  | \servidor\Manuais   |
| E:\Programas     | Programas     | servidor  | \servidor\Programas |
| C:\Público       | Público       | servidor2 | \servidor2\Público  |
| C:\Manuais       | Manuais       | servidor2 | \servidor2\Manuais  |

Observe que o compartilhamento Manuais está sendo criado nos dois servidores. Isto é necessário porque este será um compartilhamento redundante, ou seja, ao criar a árvore DFS vou criar o link para o compartilhamento Manuais no servidor “servidor” e um link para a réplica no servidor “servidor2”.

O root DFS será criado no servidor chamado “servidor” e será associado à pasta: E:\ArqDfs. Ao criar o root DFS, a pasta E:\ArqDfs será, automaticamente compartilhada. Na estação dos clientes, vamos montar um drive de rede S:, associado ao Root DFS. O caminho para o Root DFS será: \servidor\ArqDfs. Após a criação do Root DFS vou criar links DFS para as pastas compartilhadas indicadas na Tabela 6.3. Observe que para o compartilhamento Manuais vou criar o link (para o compartilhamento em servidor) e em seguida uma réplica (para o compartilhamento em servidor2).

Na diagrama da Figura 6.34 apresento uma visão geral do exemplo que será implementado.



**Figura 6.34 – O exemplo proposto.**

## O Console DFS

Para criar a administrar Árvores do DFS é utilizado o console Distributed File System (Sistema da arquivos distribuído), o qual pode ser acessado no seguinte caminho: Iniciar -> Ferramentas administrativas -> Sistema de arquivos distribuído. Utilizarei este console para realizar todas as tarefas para a criação e a manutenção de árvores DFS do exemplo proposto.

## Criando um root de domínio

O primeiro passo no exemplo proposto é criar um Root de domínio. Farei isso usando o console Sistema de arquivos, descrito no item anterior. É importante salientar que, antes de iniciar este exercício, os compartilhamentos indicados na Tabela 6.3, já devem ter sido criados. Para detalhes sobre o compartilhamento de pastas consulte a parte inicial deste capítulo.

Para criar um root DFS no computador chamado servidor, root este associado com a pasta E:\ArqDfs, siga os seguintes passos:

1. Faça o logon como administrador ou com uma conta com permissão de administrador.
2. Abra o console Sistema da arquivos distribuído, o qual pode ser acessado no seguinte caminho: Iniciar -> Ferramentas administrativas -> Sistema de arquivos distribuído.
3. Será exibida a janela Sistema de Arquivos Distribuídos, onde ainda não existe a árvore DFS, conforme indicado na Figura 6.35:

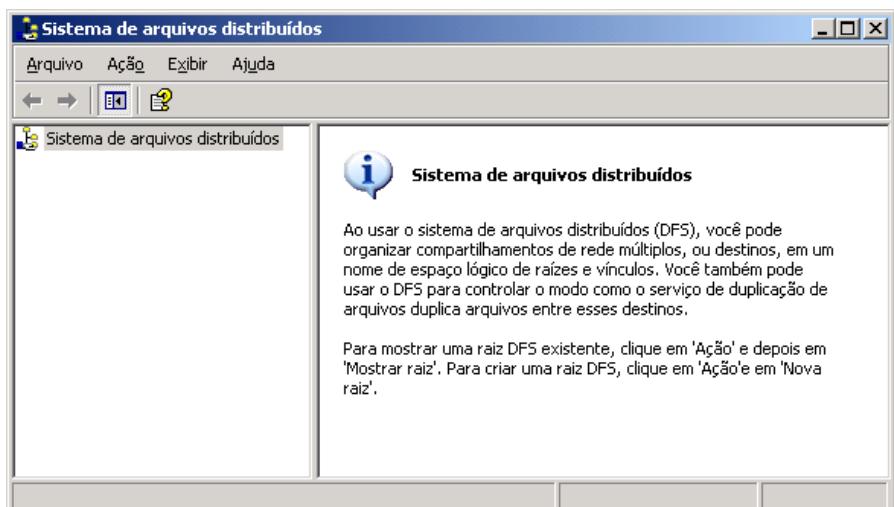


Figura 6.35 – O console Sistema de arquivos distribuídos.

4. Clique com o botão direito do mouse na opção Sistema de arquivos distribuídos). No menu que é exibido selecione o comando Nova Raiz...
5. Será aberto o Assistente para novas raízes DFS. A primeira tela é apenas informativa. Clique no botão Avançar para seguir para a próxima etapa do assistente.
6. Na segunda etapa você tem que definir se deseja criar um Root de Domínio ou um Root autônomo. Por padrão a opção Raiz de Domínio vem selecionada. Certifique-se de que esta opção esteja selecionada.
7. Clique no botão Avançar para seguir para a próxima etapa do assistente.
8. Surge uma tela perguntando o nome do domínio onde a raiz DFS será criada. No nosso exemplo será exibido o domínio groza.com, que é o domínio ao qual pertence o servidor no qual está sendo criada a raiz DFS, conforme indicado na Figura 6.36:

**IMPORTANTE:** Caso o console Sistema de arquivos distribuído não esteja disponível, no menu Ferramentas administrativas, é possível instalá-lo através da instalação de um pacote de ferramentas administrativas que vem com o Windows Server 2003. Na subpasta System32, da pasta onde está instalado o Windows Server 2003 (normalmente em uma pasta chamada C:\WINNT ou C:\WINDOWS), existe um arquivo chamado Adminpak.msi. Neste arquivo está contido um conjunto de consoles que são utilizados para administrar uma série de tarefas em uma rede com o Windows Server 2003. Uma das ferramentas disponíveis é o console Distributed File System (Sistema de Arquivos Distribuído). Para instalar o Adminpak.msi, basta abrir o Windows Explorer, localizar o arquivo Adminpak.msi e dar um clique duplo neste arquivo. Será aberto um assistente de instalação. Agora é só seguir os passos do assistente e pronto, uma série de consoles de administração serão instalados, dentre os quais o console para administração do DFS.

**IMPORTANTE:** Este conjunto de ferramentas também pode ser instalado em uma estação de trabalho com o Windows 2000 Professional ou Windows XP Professional. Neste caso o Administrador da rede, a partir da sua estação de trabalho com o Windows 2000 Pro-

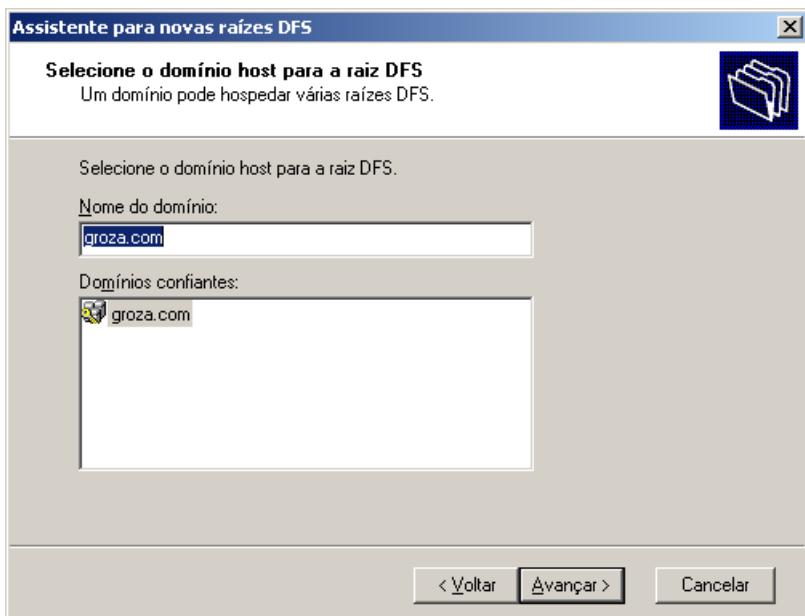


Figura 6.36 – Informando o domínio onde a raiz DFS será criada..

9. Clique no botão Avançar para seguir para a próxima etapa do assistente.
10. Surge uma tela perguntando o nome do servidor onde será criada a raiz DFS. No nosso exemplo, o nome do servidor é servidor.groza.com. Informe o nome do servidor.
11. Clique no botão Avançar para seguir para a próxima etapa do assistente.
12. Nesta etapa você deve informar o nome do root Dfs. A medida que você digita o nome, o campo Compartilhamento a ser utilizado vai sendo preenchido com o nome que você está digitando, conforme indicado na Figura.6.37:

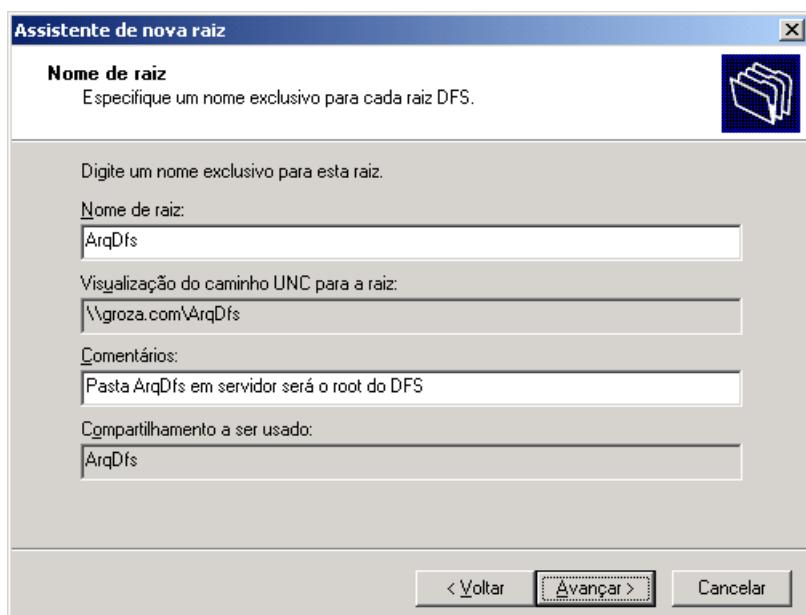
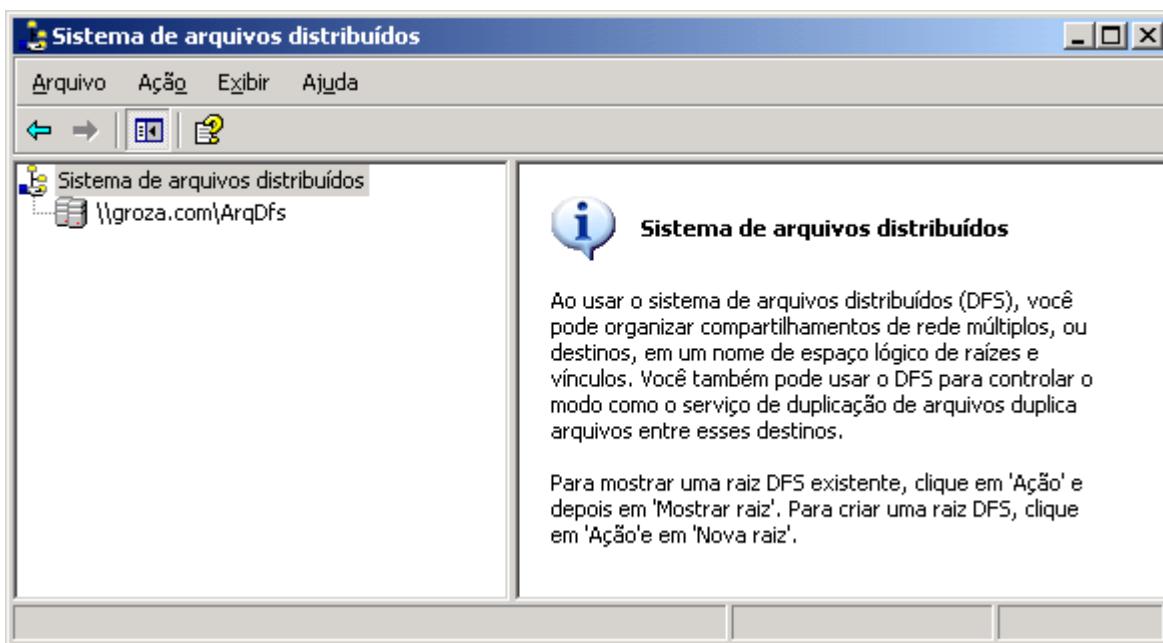


Figura 6.37 – Informando o nome do root DFS.

fessional ou Windows XP Professional, pode administrar os diversos serviços da rede, disponíveis em diversos servidores. Por exemplo, vamos supor que você está na estação de trabalho microadm01, na qual você deseja instalar o conjunto de consoles administrativos. Suponhamos que está disponível um servidor com o Windows Server 2003 instalado, chamado srv01. Neste caso, você pode acessar o compartilhamento administrativo C\$ do servidor srv01: \\srv01\C\$. Na janela que é aberta, acessa a pasta onde o Windows Server 2003 está instalado, normalmente a pasta WINNT. Dentro de WINNT acesse a pasta System32. Localize o arquivo AdminPak.msi e dê um clique duplo neste arquivo, para iniciar a instalação das ferramentas administrativas. Pronto, agora é só seguir os passos do assistente de instalação. Uma vez terminada a instalação das ferramentas administrativas, o Administrador terá na sua estação de trabalho, uma série de consoles administrativos, tais como o console do DNS, WINS, DHCP, Usuários e Computadores do Active Directory e assim por diante. Estes consoles são acessados através do menu Ferramentas administrativas.

13. Clique no botão Avançar para seguir para a próxima etapa do assistente.
14. Se o compartilhamento informado ainda não existir, o assistente exibe uma tela, pedindo que você informe qual pasta deve ser compartilhada com o nome de ArqDfs, que foi o nome que escolhemos no nosso exemplo. Informe o caminho para a pasta a ser compartilhada como Root do DFS e clique no botão Avançar para seguir para a próxima etapa do assistente.
15. Você estará na tela final do Assistente. Caso seja preciso alterar alguma opção, utilize o botão Voltar. Clique em Concluir e a raiz DFS será criada, conforme indicado na Figura 6.38:



**Figura 6.38 – A raiz DFS RootDfs, recém criada**

16. Mantenha o console Sistema de arquivos distribuídos aberto, pois você irá utilizá-lo nos próximos passos deste exemplo.

Agora você está apto a seguir para a próxima etapa do exercício, qual seja: Criar os links (ou usando uma metáfora: os ramos da árvore), sendo cada link associado com um compartilhamento.

### Criando links para as pastas compartilhadas na rede:

Agora é hora de “montar” a árvore DFS. Já temos a raiz (criada no passo anterior) e agora é hora de adicionar os ramos. Cada ramo é associado com um compartilhamento da rede. Você criará três ramos, conforme indicado na Tabela 6.4:

**Tabela 6.4 – Os “ramos” da árvore DFS.**

| Nome do Ramo | Associado com o compartilhamento |
|--------------|----------------------------------|
| Manuais      | \servidor2\Manuais               |
| Público      | \servidor2\Público               |
| Programas    | \servidor\Programas              |

Para criar os links propostos, siga os seguintes passos:

1. Você deve estar com o console Sistema de arquivos distribuídos) aberto.
2. Clique com o botão direito do mouse na raiz criada no tópico anterior.
3. No menu que é exibido selecione o comando Novo vínculo...
4. Será exibida a janela Novo vínculo, na qual você deve informar o nome do link que está sendo criado, o caminho para a pasta compartilhada associada ao link e um comentário.

**NOTA: O compartilhamento \\servidor\Manuais será utilizado para a criação de redundância do compartilhamento \\servidor2\Manuais, conforme exemplo prático mais adiante.**

Para adicionar o link Manuais, associado ao compartilhamento \\servidor2\Manuais, digite as informações indicadas na Figura 6.39:

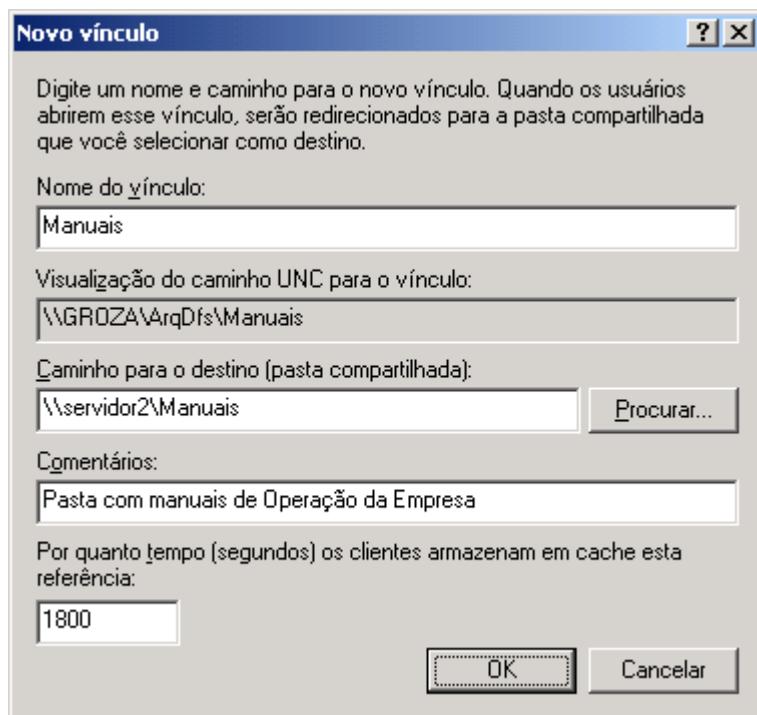
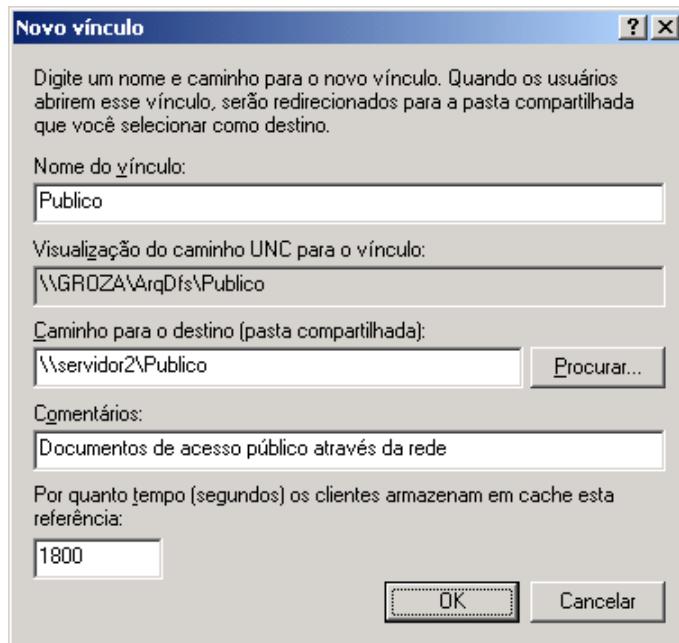


Figura 6.39 – Criando um link para a pasta Manuais.

5. Clique em OK e pronto, o novo link será criado.
6. Clique com o botão direito do mouse na raiz DFS.
7. No menu que é exibido selecione o comando Novo vínculo...
8. Será exibida a janela Novo vínculo, na qual você deve informar o nome do link que está sendo criado, o caminho para a pasta compartilhada associada ao link e um comentário.

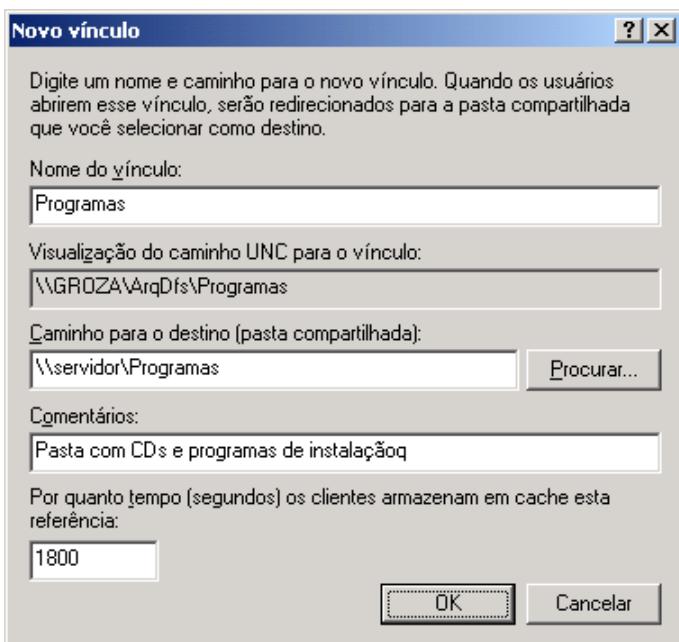
Para adicionar o link Público, associado ao compartilhamento \\servidor2\Público, digite as informações indicadas na Figura 6.40:



**Figura 6.40 – Criando um link para a pasta Público.**

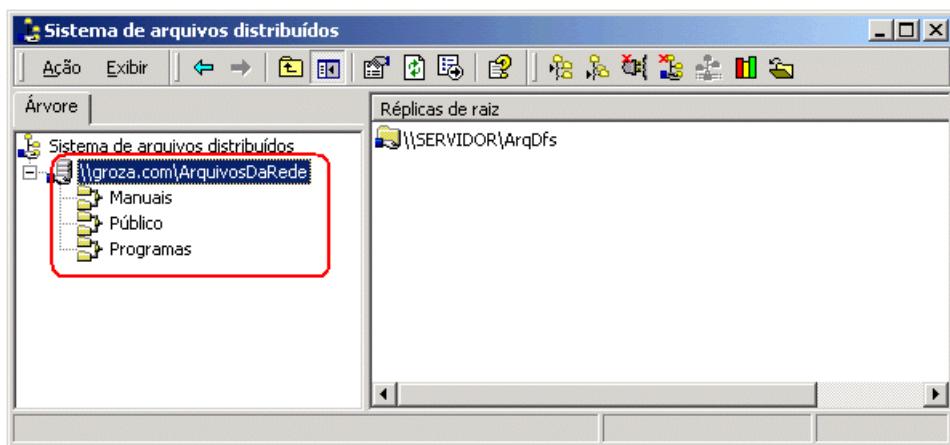
9. Clique em OK e pronto, o novo link será criado.
10. Clique com o botão direito do mouse na raiz DFS.
11. No menu que é exibido selecione o comando Novo vínculo
12. Será exibida a janela Novo vínculo, na qual você deve informar o nome do link que está sendo criado, o caminho para a pasta compartilhada associada ao link e um comentário.

Para adicionar o link Programas, associado ao compartilhamento \\servidor\Programas, digite as informações indicadas na Figura 6.41:



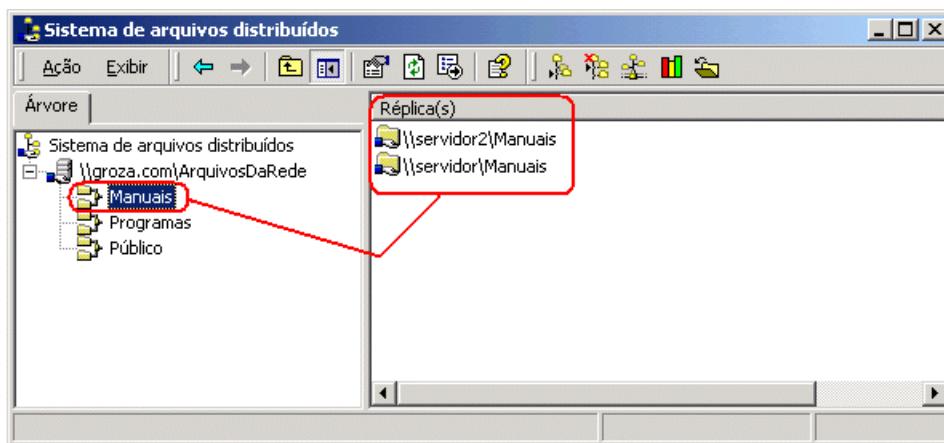
**Figura 6.41 – Criando um link para a pasta Programas.**

13. Clique em OK e pronto, o link Programas será criado.
14. A árvore DFS deve estar conforme indicado na Figura 6.42:



**Figura 6.42 – A árvore DFS com três links.**

15. Agora você adicionará redundância ao link Manuais. Lembrando que o link Manuais que foi adicionado anteriormente, está associado a pasta '\\servidor2\manuais'. Agora você adicionará um link redundante, associado com '\\servidor\Manuais'. Com isso, existirão duas cópias do conteúdo da pasta Manuais. Caso um dos servidores esteja fora da rede, os usuários poderão continuar acessando a cópia redundante. Observe que, com isso, estamos adicionando redundância a um dos links da árvore. Poderíamos adicionar mais de uma cópia redundante. O próprio DFS, juntamente com o serviço de replicação de arquivos do Windows Server 2003, se encarrega de manter o conteúdo da pasta Manuais sincronizado nos dois servidores.
16. Clique com o botão direito do mouse no link Manuais e, no menu que é exibido, dê um clique na opção Novo destino...
17. Será exibida a janela Novo destino. Nesta janela você deve informar o caminho para a réplica da pasta Manuais e se o conteúdo das réplicas deve ou não ser automaticamente sincronizado. No campo Caminho para destino (pasta compartilhada), digite: '\\Servidor\Manuais'.
18. Clique em OK.
19. A nova réplica está configurada, conforme pode ser visto, em destaque, na Figura 6.43:



**Figura 6.43 – Réplica criada para a pasta Manuais.**

20. Agora a árvore DFS está pronta. Vamos testá-la.

### Acessando a raiz DFS no cliente:

Agora vou montar um drive X: associado com a raiz da árvore DFS: \\servidor\ArqDfs. Lembrando do que foi dito na introdução teórica deste tutorial, cada link da árvore DFS irá aparecer como uma pasta do drive X:. Por exemplo, o link Manuais aparecerá como uma pasta Manuais, dentro do drive X:. Quando o usuário estiver acessando esta pasta estará, na prática, acessando uma das réplicas do link Manuais: \\servidor2\Manuais ou \\servidor\Manuais. Quando o usuário acessar a pasta Público estará, na prática, acessando a pasta \\servidor2\Público e assim por diante.

Para montar um drive X:, associado à raiz da árvore DFS, siga os seguintes passos:

1. Faça o logon em uma das estações da rede.
2. Abra um Prompt de comando: Na janela do Prompt de comando digite o seguinte comando:

```
net use x: \\servidor\ArqDfs /yes
```

3. Pressione Enter. O drive x: será montado.
4. Digite Exit e pressione Enter, para fechar o Prompt de comando.

5. Abra o Meu computador e acesso o drive X:. Você deverá obter o resultado indicado na Figura 6.44:

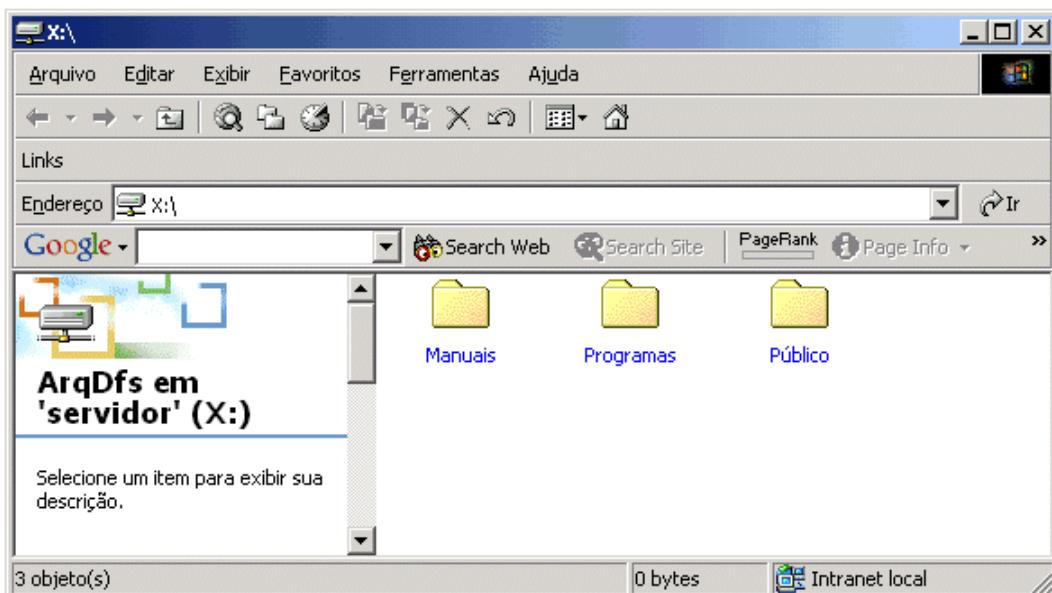


Figura 6.44 – O drive X: para acesso à Árvore DFS.

6. Isto comprova que a nossa árvore DFS e os respectivos links foram criados com sucesso e estão funcionando corretamente.

Muito bem, sobre DFS era isso. Agora faltam mais três importantes assuntos, relacionados com pastas compartilhadas, volumes e o sistema de arquivos NTFS: Definição de cotas de usuário, pastas off-line e compactação de arquivos.

# Definição de cotas em volumes e partições.

## Configurando cotas de disco no Windows Server 2003.

O mecanismo de cotas de disco é utilizado para limitar o espaço em disco que cada usuário pode utilizar. Somente é possível definir cotas de disco, em volumes formatados com o sistema de arquivos NTFS. As cotas são definidas em cada volume separadamente. Por exemplo, posso implementar o mecanismo de cotas no drive C:, porém não implementá-lo no drive D:. Se você tiver um disco rígido de 30 GB, o qual foi dividido em três volumes de 10 GB: C:, D: e E:. As cotas de disco são definidas, separadamente para cada um dos volumes. Por exemplo, possa definir uma cota de 100 MB para o usuário jsilva no drive C, uma cota de 120 MB para o usuário jsilva no drive D: e uma cota de 200 MB para o usuário jsilva no drive E:. Ou seja, as cotas são definidas por volume por usuário. As cotas são definidas individualmente, para cada usuário. Ou seja, podemos definir um cota de 500 MB para o usuário jsilva e uma cota de 200 MB para o usuário user1 em um determinado volume.

*Uma das novidades do .NET Server (agora Windows Server 2003), que será o sucessor do Windows 2000 Server, será justamente a possibilidade de definir cotas de disco para grupos de usuários.*

Porém esta informação não se confirmou e no Windows Server 2003 não é possível definir cotas para grupos de usuários, mas somente para usuários individualmente, exatamente como funciona o mecanismo de cotas no Windows 2000 Server.

O Windows Server 2003 calcula o espaço em disco utilizado por cada usuário, com base nos arquivos em que o usuário é o dono do arquivo. Normalmente o dono do arquivo é o usuário que criou ou copiou o arquivo para o disco. A cota utilizada pelo usuário é a soma do tamanho de todos os arquivos dos quais ele for o dono. Quando o mecanismo de cotas é habilitado em um volume, o Windows Server 2003 faz uma varredura de todo o volume, calculando quanto de espaço em disco cada usuário está utilizando. Este cálculo é feito com base no dono de cada arquivo.

O administrador pode utilizar as cotas de diferentes maneiras. Por exemplo, o administrador pode impedir o uso do espaço em disco e registrar um evento no log de Eventos do Windows Server 2003, quando um usuário ultrapassar o limite de espaço em disco especificado pela sua cota, isto é, o espaço em disco que ele tem permissão para utilizar.

Também é possível registrar um evento no log de eventos do Windows Server 2003, quando um usuário ultrapassar um nível de notificação de espaço em disco especificado, isto é, o ponto no qual um usuário estiver se aproximando de sua cota limite.

Ao ativar as cotas de disco, o Administrador irá definir dois valores: o limite de cota de disco e o nível de notificação de cota de disco. Por exemplo, é possível definir um limite de cota de disco de um usuário como 300 megabytes (MB) e o nível de notificação de cota de disco como 250 MB. Nesse caso, o usuário só poderá armazenar até 300 MB de arquivos no volume. Se ele armazenar mais de 250 MB de arquivos no volume, você poderá configurar o sistema de cota de disco para registrar um evento no log de eventos do sistema. É necessário que você seja membro do grupo Administradores para administrar cotas em um volume.

---

**IMPORTANTE:** Não é possível definir cotas para grupos de usuários, de tal maneira que todos os membros do grupo tenham a mesma cota de disco em um determinado volume. No meu livro "Windows XP Home & Professional Para Usuários e Administradores" eu escrevi o seguinte trecho:

---

Quando você ativa as cotas de disco para um volume, o uso do volume é rastreado automaticamente para todos os usuários, desse momento em diante. Você pode ativar cotas em volumes locais, volumes de rede e unidades removíveis desde que estejam formatados com o sistema de arquivos NTFS. Além disso, os volumes de rede devem ser compartilhados na pasta raiz do volume, o que já é feito, automaticamente, pelo Windows Server 2003. Conforme citado anteriormente, o Windows Server 2003 cria compartilhamentos especiais, ocultos, para a pasta raiz de cada volume (C\$, D\$, E\$ e assim por diante).

Você não pode utilizar a compactação de arquivos para impedir que os usuários ultrapassem seus limites de cota porque os arquivos compactados são controlados com base em seu tamanho antes da compactação. Por exemplo, se um arquivo tiver 250 MB, mas ficar com 140 MB após a compactação, o Windows considera o tamanho original do arquivo (250 MB) em relação ao limite de cota.

## Configurando cotas de disco em um volume NTFS.

Vou apresentar um exemplo prático sobre a configuração de cotas de disco em um volume NTFS.

Exemplo: Configurar cotas no drive C:

1. Faça o logon com uma conta com permissão de administrador e abra o Meu computador.
2. Clique com o botão direito do mouse no drive C: e, no menu de opções que é exibido, dê um clique na opção Propriedades.
3. Será aberta a janela de propriedades do drive C:
4. Dê um clique na guia Cota.
5. Para ativar o gerenciamento de cotas de disco, marque a opção Ativar gerenciamento de cota, conforme indicado na Figura 6.45:

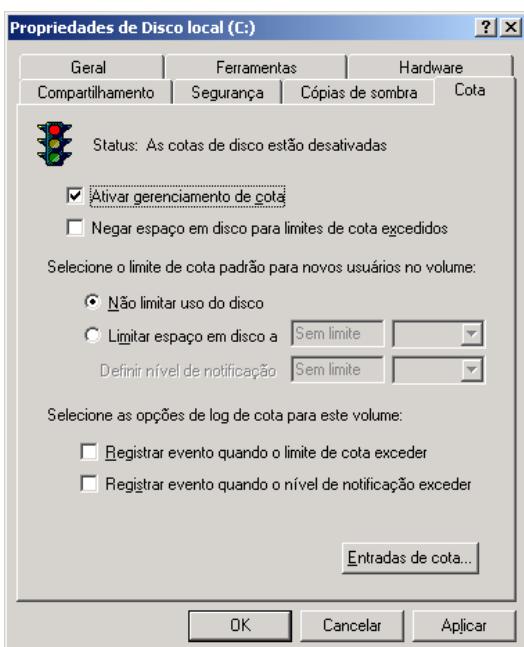


Figura 6.45 A opção Ativar gerenciamento de cota.

**NOTA:** No Capítulo 10 falarei mais sobre o log de eventos do sistema.

**IMPORTANTE:** É possível especificar que os usuários possam exceder seus limites de cota, sem que sejam impedidos de continuar gravando arquivos no volume. O procedimento de ativar as cotas e não limitar o uso do espaço em disco é útil quando você não deseja negar aos usuários o acesso a um volume em caso de exceder a cota, mas deseja controlar o uso do espaço em disco (saber quanto cada usuário está utilizando) para cada usuário. Também é possível especificar se um evento deverá ou não ser registrado quando os usuários excederem seus níveis de notificação de cota ou seus limites de cota.

Ao marcar esta opção, as demais opções da guia Quota (Cota) serão habilitadas. A seguir descrevemos estas opções:

- ◆ **Negar espaço em disco para limites do cota excedidos:** Ao marcar esta opção, o usuário não poderá mais gravar no disco a partir do momento em que a sua cota de disco tiver sido atingida. Para gravar novas informações no disco, o usuário terá que excluir arquivos ou movê-los para outros volumes.
  - ◆ **Não limitar uso do disco:** Se você marcar esta opção, o gerenciamento de cotas continua habilitado, porém não existe limite de espaço em disco para os usuários, a não ser o próprio tamanho do volume. Esta opção é utilizada quando o administrador apenas quer gerenciar o quanto de espaço em disco cada usuário está ocupando, sem definir uma cota de espaço para cada usuário.
  - ◆ **Limitar espaço em disco a:** Esta opção é utilizada para definir uma cota de disco padrão, ou seja, uma cota que será aplicada para todos os usuários, com exceção dos usuários para os quais o Administrador, explicitamente, definiu um outro valor para a cota em disco, conforme mostrarei logo a seguir. Ao selecionar esta opção, automaticamente é habilitada a opção Definir nível de notificação. Esta opção define um valor de espaço em disco que, quando atingido, faz com que um evento seja gravado no log de eventos do Windows Server 2003. O Administrador pode acompanhar estes eventos, para notificar usuários que estejam próximos de atingir o limite de espaço definido na sua cota de disco.
  - ◆ **Registrar evento quando o limite do cota excede:** Seleccione esta opção para gerar uma entrada no log de eventos do Windows Server 2003, quando o uso de espaço em disco do usuário ultrapassar o limite de cota de disco atribuído a ele.
  - ◆ **Registrar evento quando o nível de notificação excede:** Seleccione esta opção para gerar uma entrada no log de eventos do Windows Server 2003, quando o uso de espaço em disco do usuário ultrapassar o nível de notificação de cota atribuído a ele.
6. Configure as opções desejadas de acordo com as necessidades do servidor que você está administrando.
  7. Para definir cotas personalizadas para determinados usuários, dê um clique no botão Entradas de Cota...
  8. Será exibida a janela Entradas de cota de disco local (C:).
  9. Para adicionar uma cota personalizada para um novo usuário, utilize o comando Cota -> Nova entrada de cota...
  10. Será aberta a janela Selecionar usuários, já em diversos exemplos, no Capítulo 4, quando você aprendeu a adicionar novos usuários a um grupo. Você pode digitar o nome do usuário para o qual será definida uma cota ou clicar no botão Avançado..., para selecionar o usuário em uma lista de usuários. Você definirá uma nova cota de disco para o usuário user01, conforme indicado na Figura 6.46:

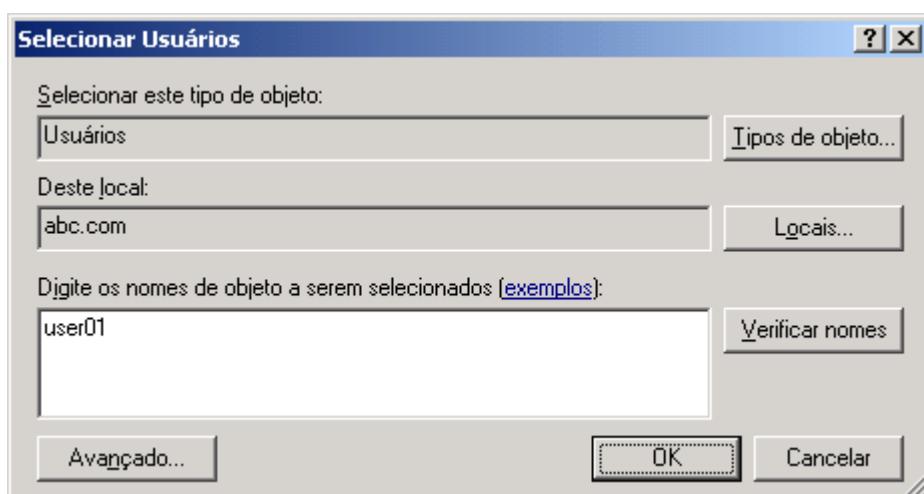


Figura 6.46 Definindo uma cota para o usuário user01.

11. Clique no botão OK. Será aberta a janela Adicionar nova entrada de cota. Nesta janela você podemos optar por limitar ou não o uso do espaço em disco, para o usuário user01. Se optar por limitar, você deverá definir o espaço que o usuário pode utilizar, bem como um limite de aviso. Defina os valores indicados na Figura 6.47 e dê um clique no botão OK.



Figura 6.47 Configurando a cota para o usuário user01.

12. Você estará de volta à janela Entradas de cota de Disco local (C:). Observe que a entrada de cota para o usuário user01 já aparece na listagem, bem como informações sobre a cota já utilizada pelo usuário, o limite de cota e o limite de aviso, conforme exemplo da Figura 6.48. Repita os passos de 7 à 11 para definir cotas para outros usuários.

| Entradas de cota de Disco local (C:) |                      |                |                  |                |                      |                  |
|--------------------------------------|----------------------|----------------|------------------|----------------|----------------------|------------------|
| Status                               | Nome                 | Nome de logon  | Quantidade usada | Limite de cota | Nível de notificação | Percentagem usad |
| OK                                   | Usu...               | user01@abc.com | 0 bytes          | 200 MB         | 185 MB               |                  |
| OK                                   | BUILTIN\Administr... |                | 0 bytes          | Sem limite     | Sem limite           | N/               |

Total de 2 item(ns), 1 selecionados.

Figura 6.48 Cota já definida para o usuário user01.

Na janela Entradas de cota de Disco local..., você pode realizar uma série de operações referentes a cotas, conforme descrito a seguir:

- ◆ Para adicionar uma nova cota utilize o comando Cota -> Nova entrada de cota...
- ◆ Para atualizar as informações da listagem de cotas pressione a tecla F5.
- ◆ Para excluir a definição de uma cota, clique na cota a ser excluída e pressione a tecla Delete.

- ◆ Se você tiver um grande número de entradas, você pode utilizar o comando Editar -> Localizar..., para encontrar definições de cota para um usuário específico. Na janela Pesquisar, o nome do usuário deve ser digitado no seguinte formato: NOME DO DOMÍNIO\NOME DE LOGON. Por exemplo: ABC\user1, GROZA\jsilva e assim por diante.
  - ◆ Você pode classificar a listagem de cotas de diferentes maneiras, utilizando o comando Exibir -> Organizar itens.
13. Feche a janela Entradas de cota de Disco local..., para isso utilize o comando Cota -> Fechar.
14. Você estará de volta a guia Cota, da janela de propriedades do drive C:
15. Dê um clique no botão Aplicar. Surge uma mensagem avisando que as informações sobre cotas serão atualizadas e que isso poderá demorar alguns minutos. Dê um clique no botão OK. As informações serão atualizadas e você estará de volta a janela de propriedades do drive C:. Dê um clique no botão OK para fechar a janela de propriedades.
16. Você estará de volta ao Meu computador. Feche-o.

As cotas de disco funcionam com todos os volumes NTFS nos sistemas Windows 2000 ou Windows Server 2003. No entanto, os arquivos em volumes que tiverem sido convertidos de FAT ou FAT32 em NTFS pertencerão automaticamente ao usuário administrador, isto é, terão como dono o usuário Administrador e, portanto, a cota nesses arquivos é creditada para conta do administrador. Isso raramente é um problema porque os administradores podem utilizar o volume de forma ilimitada. Isso só se aplica aos arquivos que existiam antes da conversão em NTFS; os arquivos criados após a conversão pertencem ao usuário apropriado, ou seja, o usuário logado quando o arquivo foi criado.

Para uma descrição detalhada das opções do comando convert, utilize o seguinte comando:

```
convert /?
```

A conversão será agendada para a próxima reinicialização do sistema.

Para desativar as cotas de disco, basta acessar a guia Cota, das propriedades do volume no qual as cotas serão desativadas e desmarcar a opção: Ativar gerenciamento de cota.

## Recomendações sobre o uso de cotas de disco:

A seguir coloco algumas recomendações contidas na documentação oficial do Windows Server 2003, sobre o uso de cotas de disco em volumes NTFS:

- ◆ **Aplique limites adequados de cota de disco:** Aplique limites de cota de disco de acordo com as necessidades reais de espaço em disco dos usuários. Comece classificando os usuários pela quantidade de espaço em disco que você supõe que eles necessitarão (por exemplo, os usuários que trabalham com fotografias digitalizadas ou artes gráficas poderão necessitar de uma quantidade maior de espaço em disco). Em seguida, estruture seus volumes de acordo com essas classes e use as cotas de disco para limitar a quantidade de espaço em disco permitida para os usuários em cada volume.

**IMPORTANTE:** Você pode exportar a listagem com as informações sobre as definições de cotas, para uma planilha do Excel. Com isso fica mais fácil classificar e analisar as informações. Para gerar uma planilha do Excel, com as informações de cotas faça o seguinte: Na janela Entradas de cota de Disco local..., selecione o comando Editar -> Selecionar tudo ou pressione Ctrl+A. Todas as entradas de cota serão selecionadas. Selecione o comando Editar -> Copiar. Abra o Excel e selecione o comando Editar -> Colar. Salve a planilha e utilize os comandos do Excel para fazer as análises desejadas.

**IMPORTANTE:** Você pode fazer alterações nas cotas a qualquer momento que for necessário, para isso basta acessar a janela de propriedades do drive onde as alterações devem ser feitas e utilizar os comandos adequados.

**NOTA:** Para converter um volume de FAT para NTFS, utilize o comando convert. Por exemplo, para converter o drive C: de FAT para NTFS, utilizamos o seguinte comando: convert C: /FS:NTFS

- ◆ **Defina limites padrão:** Defina limites padrão moderadamente restritivos para todas as contas de usuário e modifique os limites para conceder mais espaço em disco aos usuários que trabalham com arquivos maiores. Pode ser melhor aumentar os limites de cota de disco para algumas contas de usuário do que obrigar alguns usuários a trabalhar com limites de cota que não correspondam às suas necessidades.
- ◆ **Permita crescimento:** Defina os limites de cota em um nível que permita crescimento no uso do espaço em disco. Quando os aumentos de cotas forem garantidos, aumente-as em uma percentagem do valor atual.
- ◆ **Exclua entradas de cota dos usuários:** Quando um usuário não precisar mais usar um volume específico (por exemplo, quando ele sair da empresa), exclua sua entrada de cota para esse volume e exclua, move ou se aproprie (take ownership) de quaisquer arquivos pertencentes ao usuário. Isso o ajudará a eliminar o uso do espaço no volume por arquivos desnecessários. Para excluir uma entrada de cota, acesse as propriedades do volume, clique na guia Cota e dê um clique no botão Entradas de cota. Será aberta a janela Entradas de cota de Disco local... Na listagem que é exibida, localize a entrada a ser excluída, clique nela e pressione o botão Delete. Se o usuário ainda for o dono de arquivos gravados no volume, será aberta uma janela com a listagem de todos os arquivos dos quais o usuário é dono. Nesta janela você pode Excluir os arquivos, Apropriar-se (Take Ownership) ou Mover os arquivos para outro volume.
- ◆ **Limite a instalação aos administradores:** Se você ativar configurações de cota de disco no volume em que o Windows e outros programas estiverem instalados, limite a instalação dos programas e componentes do Windows a membros do grupo local Administradores. Como o grupo Administradores não possui limites de cota, isso impedirá que o espaço em disco usado para instalar componentes e programas faça com que um usuário ultrapasse seu limite de cota. Quando um programa é instalado, uma série de arquivos são copiados para o disco rígido. Estes arquivos são contabilizados na cota do usuário logado que está instalando o programa.

## O comando fsutil quota.

Além da interface gráfica, o administrador pode utilizar o comando fsutil quota, para efetuar configurações de cota de disco. Conforme já descrito em outros capítulos, o uso de comandos é especialmente útil quando o Administrador cria scripts de administração, para automatizar determinadas tarefas.

O comando “fsutil quota” gerencia cotas de disco em volumes NTFS para fornecer um controle mais preciso do armazenamento em rede. Temos a seguinte sintaxe para este comando:

```
fsutil quota [disable] nome_do_volume
fsutil quota [enforce] nome_do_volume
fsutil quota [modify] nome_do_volume limite_máximo limite [nome_do_usuário]
fsutil quota [query] nome_do_volume
fsutil quota [track] nome_do_volume
fsutil quota [violations]
```

A seguir apresento a descrição dos parâmetros utilizados por este comando:

- ◆ **disable:** Desativa o controle e a ativação de cotas no volume especificado.
- ◆ **enforce:** Ativa o uso de cotas no volume especificado.
- ◆ **modify:** Modifica uma cota de disco existente ou cria uma nova cota.
- ◆ **query:** Lista as cotas de disco existentes.
- ◆ **track:** Controla o uso do disco no volume especificado.
- ◆ **violations:** Pesquisa os logs do sistema e de aplicativos e exibe uma mensagem para indicar que foram detectadas violações de cotas, ou que um usuário atingiu seu limite ou limite máximo de cotas.
- ◆ **nome\_do\_volume:** Especifica a letra da unidade para o volume (seguida por dois-pontos).

- ◆ **limite\_máximo:** O limite em que são emitidos avisos.
- ◆ **limite:** O uso máximo de espaço em disco permitido, ou seja, a cota de disco do usuário no volume.
- ◆ **nome\_do\_usuário:** Especifica o domínio ou nome do usuário.

A seguir apresento um exemplo de utilização do comando fsutil quota, para obter informações sobre as configurações de cota do drive C:

```
C:\>fsutil quota query C:
FileSystemControlFlags = 0x00000032
    As cotas estão controladas e aplicadas neste volume
    Ativação de log para limites e limiares de cota
    Os valores de cota estão atualizados
Limiar de cota padrão      = 0x00000000000000400
Limite de cota padrão      = 0x00000000000000400
Nome SID      = BUILTIN\Administradores (alias)
Hora da alteração      = Tue Feb 26 11:46:22 2002
Cota utilizada      = 4890964992
Limiar de cota = 18446744073709551615
Limite de cota      = 18446744073709551615
Nome SID      = MICROXP01\user1 (usuário)
Hora da alteração      = Sun Apr 07 20:34:25 2002
Cota utilizada      = 1107968
Limiar de cota = 183500800
Limite de cota      = 209715200
Nome SID      = MICROXP01\groza (usuário)
Hora da alteração      = Sun Apr 07 21:16:28 2002
Cota utilizada      = 7419904
Limiar de cota = 1024
Limite de cota      = 1024
Nome do SID      = AUTORIDADE NT\LOCAL SERVICE (grupo_conhecido)
Hora da alteração      = Sun Apr 07 21:16:28 2002
Cota utilizada      = 1015808
Limiar de cota = 1024
Limite de cota      = 1024
Nome SID      = MICROXP01\Administrador (usuário)
Hora da alteração      = Sun Apr 07 21:16:28 2002
Cota utilizada      = 27444224
Limiar de cota = 1024
Limite de cota      = 1024
Erro: Não foi feito mapeamento entre os nomes de conta e as identificações de segurança.
Hora da alteração      = Sun Apr 07 21:16:28 2002
Cota utilizada      = 5709824
Limiar de cota = 1024
Limite de cota      = 1024
Nome do SID      = AUTORIDADE NT\NETWORK SERVICE (grupo_conhecido)
Hora da alteração      = Sun Apr 07 21:16:28 2002
Cota utilizada      = 869376
Limiar de cota = 1024
Limite de cota      = 1024
Erro: Não foi feito mapeamento entre os nomes de conta e as identificações de segurança.
Hora da alteração      = Sun Apr 07 21:16:28 2002
Cota utilizada      = 1582900224
Limiar de cota = 1024
Limite de cota      = 1024
Erro: Não foi feito mapeamento entre os nomes de conta e as identificações de segurança.
Hora da alteração      = Sun Apr 07 21:16:28 2002
Cota utilizada      = 3622912
Limiar de cota = 1024
Limite de cota      = 1024
Nome do SID      = AUTORIDADE NT\SYSTEM (grupo_conhecido)
```

```

Hora da alteração      = Sun Apr 07 21:16:28 2002
Cota utilizada        = 1532928
Limiar de cota = 1024
Limite de cota       = 1024
Erro: Não foi feito mapeamento entre os nomes de conta e as identificações de segurança.
Hora da alteração      = Sun Apr 07 21:16:28 2002
Cota utilizada        = 3027968
Limiar de cota = 1024
Limite de cota       = 1024
Erro: Não foi feito mapeamento entre os nomes de conta e as identificações de segurança.
Hora da alteração      = Sun Apr 07 21:16:29 2002
Cota utilizada        = 1924096
Limiar de cota = 1024
Limite de cota       = 1024
Nome SID              = MICROXP01\Pedro Pereira Xunaré (usuário)
Hora da alteração      = Sun Apr 07 21:16:29 2002
Cota utilizada        = 1250304
Limiar de cota = 1024
Limite de cota       = 1024
Nome SID              = MICROXP01\user2 (usuário)
Hora da alteração      = Sun Apr 07 21:16:29 2002
Cota utilizada        = 3034112
Limiar de cota = 1024
Limite de cota       = 1024
Nome SID              = MICROXP01\user3 (usuário)
Hora da alteração      = Sun Apr 07 21:16:29 2002
Cota utilizada        = 1047552
Limiar de cota = 1024
Limite de cota       = 1024

```

Observe que são exibidas informações detalhadas sobre as configurações de cotas para o drive C:, com detalhes de utilização por usuário.

## Entendendo e Utilizando Pastas off-line

### Pastas Off-line: conceito e utilizações.

Com o Windows Server 2003 (já era possível com o Windows 2000 e também no Windows XP Professional), você pode configurar uma pasta compartilhada, para que o usuário possa ter acesso aos arquivos do compartilhamento, mesmo quando não estiver conectado à rede. Em um primeiro momento pode parecer estranho: “Como ter acesso aos arquivos de uma pasta compartilhada, sem estar conectado à rede??” Na prática o que acontece é que, ao configurar um compartilhamento para acesso Off-line, o administrador está orientando os clientes que acessam o compartilhamento, a fazer uma cópia local dos arquivos do compartilhamento, com isso o usuário fica trabalhando na cópia local, em caso de perda da conexão com a rede. De tempos em tempos as alterações feitas na cópia local (também conhecido como Cache local de arquivos), são sincronizadas com a cópia original, na pasta compartilhada. Se por algum motivo, o computador perder o acesso à rede, o usuário continua trabalhando na cópia local, podendo inclusive desligar o computador. Na próxima vez que o computador for conectado à rede, os arquivos serão sincronizados. Você deve ter notado que o uso de pastas Off-line é ideal para usuários de Notebooks, que precisam trabalhar e alterar arquivos quando não estão conectados à rede da empresa, como por exemplo em casa, em aeroportos ou em uma sala de reunião na empresa de um cliente.

Quando estiver trabalhando com arquivos off-line, você poderá exibi-los na sua pasta Arquivos off-line e excluí-los dela. Também poderá especificar quando e como os arquivos serão sincronizados ou então criptografar os arquivos off-line.

Agora você aprenderá a configurar e a utilizar arquivos Off-line.

## Configurando o computador dos usuários para que ele esteja apto a usar o recurso de arquivos off-line.

O primeiro passo é configurar os computadores dos clientes para que estes possam trabalhar com arquivos off-line. Por exemplo, você deverá fazer as configurações indicadas a seguir no notebook de um usuário que precise utilizar os arquivos off-line.

Exemplo: Este exemplo deve ser executado em um dos computadores clientes da rede. Neste exemplo utilizarei um computador com o Windows XP Professional. O procedimento para um cliente com o Windows 2000 Professional é praticamente igual. Para configurar o computador do cliente, para trabalhar com arquivos off-line, siga os seguintes passos:

1. Faça o logon como Administrador ou com uma conta de usuário com permissão de administrador.
2. Abra o Meu computador.
3. Selecione o comando Ferramentas -> Opções de pasta...
4. Na janela Opções de pasta dê um clique na guia Arquivos off-line.
5. Certifique-se de que a opção Ativar arquivos off-line esteja marcada, conforme indicado na Figura 6.49, onde estou configurando o acesso a arquivos Off-line em um computador com o Windows XP Professional instalado.

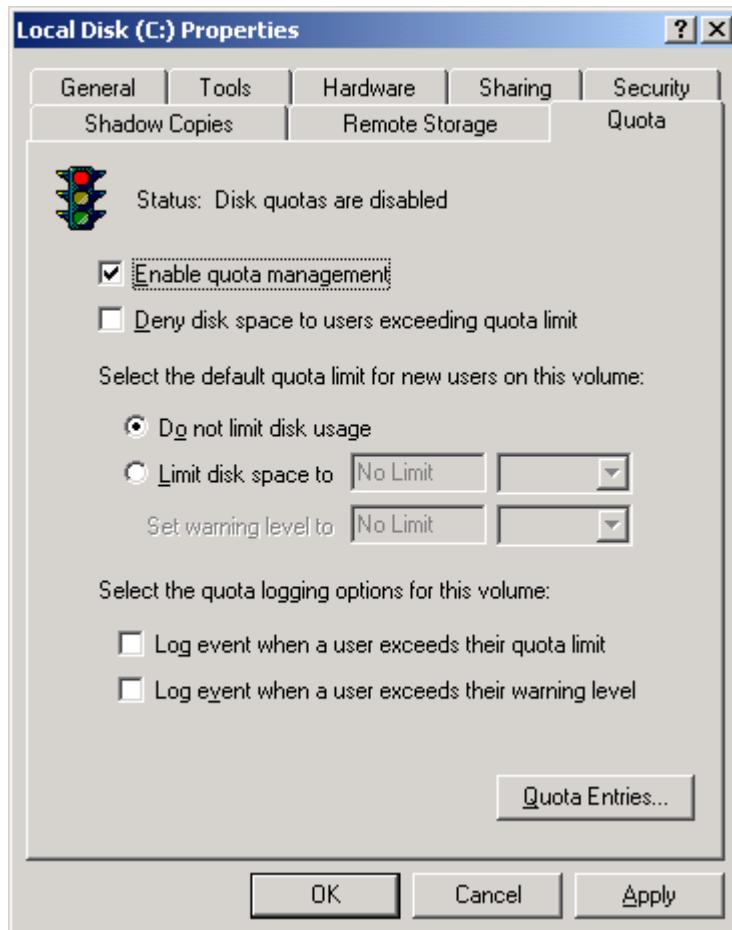


Figura 6.49 Habilitando o uso de Arquivos off-line.

7. Ao habilitar a opção Ativar arquivos off-line, outras opções de configuração são habilitadas, conforme descrito a seguir:
- ◆ **Sincronizar todos os arquivos off-line ao fazer o logon:** Especifica que todos os arquivos de rede configurados em compartilhamentos habilitados para o acesso off-line serão totalmente sincronizados quando você fizer logon. Isso garante que os arquivos de rede refletem as alterações mais recentes e que você tenha as versões mais atuais dos arquivos no seu computador. Se você não marcar essa caixa de seleção, será executada uma sincronização rápida quando fizer logon. Uma sincronização rápida fornece as versões completas dos arquivos off-line, mas não fornece as versões mais recentes dos arquivos off-line.
  - ◆ **Sincronizar todos os arquivos off-line antes de fazer o log off:** Especifica que todos os arquivos de rede disponíveis off-line serão totalmente sincronizados quando você fizer log off. Isso garante que os arquivos de rede refletem as alterações mais recentes e que você tenha as versões mais atuais dos arquivos no computador. Se você não marcar essa caixa de seleção, será feita uma sincronização rápida quando o usuário fizer log off. Uma sincronização rápida fornece as versões completas dos arquivos off-line, mas não fornece as versões mais recentes dos arquivos off-line.
  - ◆ **Exibir lembrete a cada ‘x’ minutos:** Especifica que os lembretes apareçam na área de notificação quando os computadores estiverem off-line.
  - ◆ **Criar um atalho para arquivos off-line na Área de trabalho:** Especifica que um atalho para a pasta Arquivos off-line seja colocado em sua área de trabalho.
  - ◆ **Criptografar os arquivos off-line para proteger dados:** Criptografa arquivos off-line. Quando um arquivo de rede fica disponível off-line, uma cópia é armazenada no computador local. Se você criptografar arquivos off-line, a cópia do arquivo de rede localizada no computador local será criptografada. Além disso, como alguns aplicativos criam cópias temporárias de arquivos em outras pastas, como a pasta Temp, pode ser que você queira criptografá-las também.
  - ◆ **O controle ‘Espaço em disco a ser usado para os arquivos off-line temporários:’**: Ajusta o valor máximo de espaço em disco usado no computador para arquivos de rede que você não optou por tornar disponíveis off-line. O espaço em disco está sempre reservado para os arquivos que você tornou disponíveis off-line, mas alguns deles tornam-se automaticamente disponíveis para você pelo administrador.
  - ◆ **Botão Excluir arquivos...:** Clique para excluir arquivos que você tornou disponíveis off-line. Isso pode aumentar o espaço disponível em disco no computador. Os arquivos que você selecionar serão excluídos somente do seu computador local. Eles não serão excluídos da pasta compartilhada na rede.
  - ◆ **Botão Exibir arquivos:** Clique para exibir uma lista de arquivos que estejam disponíveis off-line.
  - ◆ **Botão Avançado:** Clique neste botão para alterar o modo como os computadores são manipulados quando se tornam indisponíveis, isto é, quando o computador perde a conexão com a rede. Se você perder a conexão com um computador, poderá escolher continuar trabalhando com os arquivos desse computador ou parar. Ao clicar neste botão será exibida a janela Arquivos off-line configurações avançadas, indicada na Figura 6.50:

**IMPORTANTE:** Se a opção Usar a troca rápida de usuário estiver habilitada, as opções da guia Arquivos off-line estarão desabilitadas. Para informações sobre como desabilitar a opção “Usar a troca rápida de usuário”, consulte o Capítulo 6 do livro Windows XP Home & Professional Para Usuários e Administradores, Axel Books, 2002.

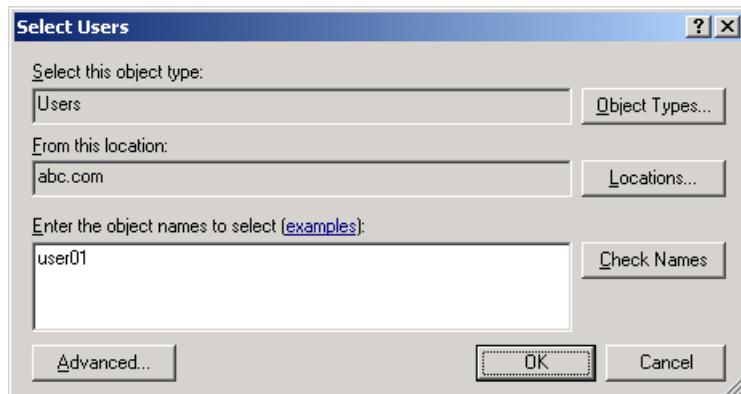


Figura 6.50 Janela de configurações avançadas.

- Configure as opções desejadas e dê um clique no botão OK para aplicar as alterações. Pronto, agora o seu computador está habilitado para trabalhar com arquivos off-line.

## Configurando um compartilhamento para que os seus arquivos possam ser acessados off-line.

O próximo passo é configurar os compartilhamentos que darão suporte ao uso de arquivos off-line. Estas configurações são feitas nas pastas compartilhadas nos servidores da rede.

Exemplo: Configurando um compartilhamento para dar suporte a arquivos off-line. Este exemplo será feito em uma pasta compartilhada em um servidor com o Windows Server 2003.

- Faça o logon como Administrador ou com uma conta com permissão de Administrador.
- Abra o Meu computador ou o Windows Explorer.
- Localize a pasta compartilhada a ser configurada, clique com o botão direito do mouse na pasta e, no menu de opções que é exibido, dê um clique na opção Compartilhamento e segurança...
- Será exibida a janela de propriedades da pasta, com a guia Compartilhamento selecionada. Dê um clique no botão Configurações Off-line. Será exibida a janela Configurações Off-line, indicada na Figura 6.51:

**NOTA:** Para maiores detalhes sobre a criação de compartilhamentos e a definição de permissões de acesso, consulte a parte inicial deste capítulo.

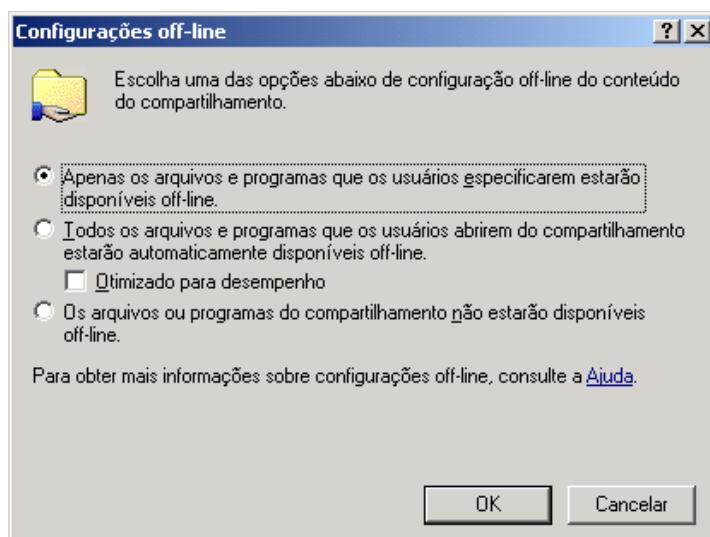


Figura 6.51 A janela Configurações Off-line.

Você pode utilizar uma das opções descritas a seguir:

- ◆ **Apenas os arquivos e programas que os usuários especificarem estarão disponíveis off-line:** Ao marcar esta opção (que é a padrão), somente serão armazenados no cache off-line, na estação de trabalho do cliente, aqueles arquivos e programas que o usuário especificamente definiu para estarem disponíveis off-line. Esta opção é a mais indicada para compartilhamentos acessados por muitos usuários, pois aí cada usuário marca para acesso off-line somente os arquivos que forem do seu interesse.
  - ◆ **Todos os arquivos e programas que os usuários abrirem do compartilhamento estarão automaticamente disponíveis off-line:** Com esta opção, sempre que o usuário abrir um arquivo da pasta compartilhada, este arquivo será marcado para estar disponível para acesso off-line. Esta opção é ideal para compartilhamentos que contém arquivos que não são alterados com freqüência e podem estar disponíveis para acesso off-line.
  - ◆ **Os arquivos ou programas do compartilhamento não estarão disponíveis off-line:** Ao marcar esta opção você desabilita o acesso off-line aos arquivos do compartilhamento.
5. Certifique-se que a opção Apenas os arquivos e programas que os usuários especificarem estarão disponíveis off-line esteja selecionada e dê um clique no botão OK para aplicar as alterações.
  6. Você estará de volta a guia Compartilhamento. Dê um clique no botão OK para fechar a janela de propriedades da pasta compartilhada.

## Definindo quais arquivos serão armazenados no cache, para acesso off-line.

Você já configurou o cliente para trabalhar com arquivos off-line e o compartilhamento no servidor para dar suporte a arquivos off-line. Agora, no computador cliente, onde você for acessar os arquivos da pasta compartilhada, você precisa definir quais arquivos deseja que sejam disponibilizados para acesso off-line. Neste tópico veremos como realizar esta operação em um cliente com o Windows XP Professional.

Exemplo: Definindo quais arquivos ou pastas deverão estar disponíveis para acesso off-line em um cliente com o Windows XP Professional.

1. Faça o logon no computador cliente, no qual você irá acessar a pasta compartilhada que foi configurada no tópico anterior.
2. Monte um drive que acessa a pasta compartilhada. Para maiores detalhes sobre a montagem de drives relacionados com pastas compartilhadas, verifico o item sobre mapeamento de drives, anteriormente, neste capítulo. Acesse o respectivo drive.
3. Dentro do drive associado com a pasta compartilhada, acesse a pasta ou arquivo que você deseja tornar disponível off-line.
4. Clique com o botão direito do mouse na pasta/arquivo a ser utilizada off-line e, no menu de opções que é exibido, dê um clique na opção Tornar disponível off-line. Pronto, a partir deste momento, a pasta/arquivo passará a estar disponível off-line, de acordo com as configurações que você definiu no item anterior.
  - ◆ Por padrão os arquivos off-line são sincronizados durante o logon e também durante o logoff, para garantir que você sempre tenha uma cópia atualizada dos arquivos.
  - ◆ Se você trabalhou desconectado da rede e alterou algum arquivo off-line e o arquivo não foi alterado na pasta compartilhada, o Windows atualiza a versão que está na pasta compartilhada a partir do arquivo atualizado no seu computador.
  - ◆ Se você trabalhou desconectado da rede e não alterou nenhum arquivo off-line porém arquivos foram alterados na pasta compartilhada no servidor, o Windows atualiza a sua cópia off-line, para ficar sincronizada com as alterações que houve na pasta compartilhada.

- ◆ Se as duas versões de um arquivo, no servidor e na sua cópia local, foram alteradas, o Windows Server 2003 exibe uma caixa de diálogo perguntando se você deseja manter ambas as versões ou salvar uma em detrimento da outra.
- ◆ Se uma das duas versões for excluída e a outra não foi alterada, durante a sincronização, a outra cópia também será excluída. Por exemplo, se enquanto você esteve off-line, um arquivo foi excluído na pasta compartilhada e você não alterou este arquivo, durante a sincronização, a sua cópia off-line do arquivo também será excluída. Se você alterou o arquivo enquanto esteve off-line, uma caixa de diálogo será exibida, perguntando se você deseja salvar a versão alterada off-line, para a pasta compartilhada no servidor.
- ◆ Se você excluir a versão local e a versão no servidor tiver sido alterada, uma caixa de diálogo será exibida, perguntando se você deseja excluir a versão no servidor ou copiar a versão alterada para o cache local.
- ◆ Se novos arquivos forem adicionados no servidor, estes arquivos serão copiados para o seu cache local, caso você tenha configurado a pasta onde os arquivos foram adicionados, para acesso off-line.

**IMPORTANTE:** Quando você marca uma pasta para estar disponível off-line, o Windows disponibilizará todo o conteúdo da pasta (subpastas e arquivos) para estar disponível off-line. Se a pasta tiver subpastas, será exibida uma janela perguntando se você deseja tornar as subpastas também disponíveis off-line. Ao fazer esta configuração, o Windows faz uma cópia dos arquivos selecionados para o cache local do computador e passa a fazer a sincronização entre a cópia local e os arquivos na pasta compartilhada, de acordo com as seguintes regras:

## O gerenciador de sincronização.

O Windows XP Professional (usado na estação de trabalho cliente) fornece um gerenciador de sincronização, o qual pode ser utilizado para configurar a maneira como o conteúdo off-line é sincronizado, bem como para forçar uma sincronização a qualquer momento, desde que você esteja conectado à rede.

Para abrir o gerenciador de sincronização faça o seguinte:

1. Clique em Iniciar -> Executar.
2. No campo Abrir digite: mobsync e dê um clique no botão OK.
3. Será aberto o Gerenciador de sincronização, conforme indicado na Figura 6.52:

The screenshot shows a Windows application window titled "Quota Entries for Local Disk (C:)". The menu bar includes "Quota", "Edit", "View", and "Help". Below the menu is a toolbar with icons for New, Delete, Edit, and Search. A status bar at the bottom indicates "2 total item(s), 0 selected." The main area is a table with columns: Status, Name, Logon Name, Amount Used, Quota Limit, Warning Level, and Percent Used. There are two entries:

| Status | Name    | Logon Name             | Amount Used | Quota Limit | Warning Level | Percent Used |
|--------|---------|------------------------|-------------|-------------|---------------|--------------|
| OK     | User... | user01@abc.com         | 0 bytes     | 200 MB      | 185 MB        | 0            |
| OK     |         | BUILTIN\Administrators | 0 bytes     | No Limit    | No Limit      | N/A          |

Figura 6.52 O Gerenciador de sincronização.

Para sincronizar um item, clique para marca-lo e dê um clique no botão Sincronizar. Para configurar as opções de sincronização marque o item e dê um clique no botão Configurar, será exibida a janela Configurações de sincronização, indicada na Figura 6.53, na qual você pode definir se a sincronização deve ser feita no logon, no logoff, dentre outras opções.

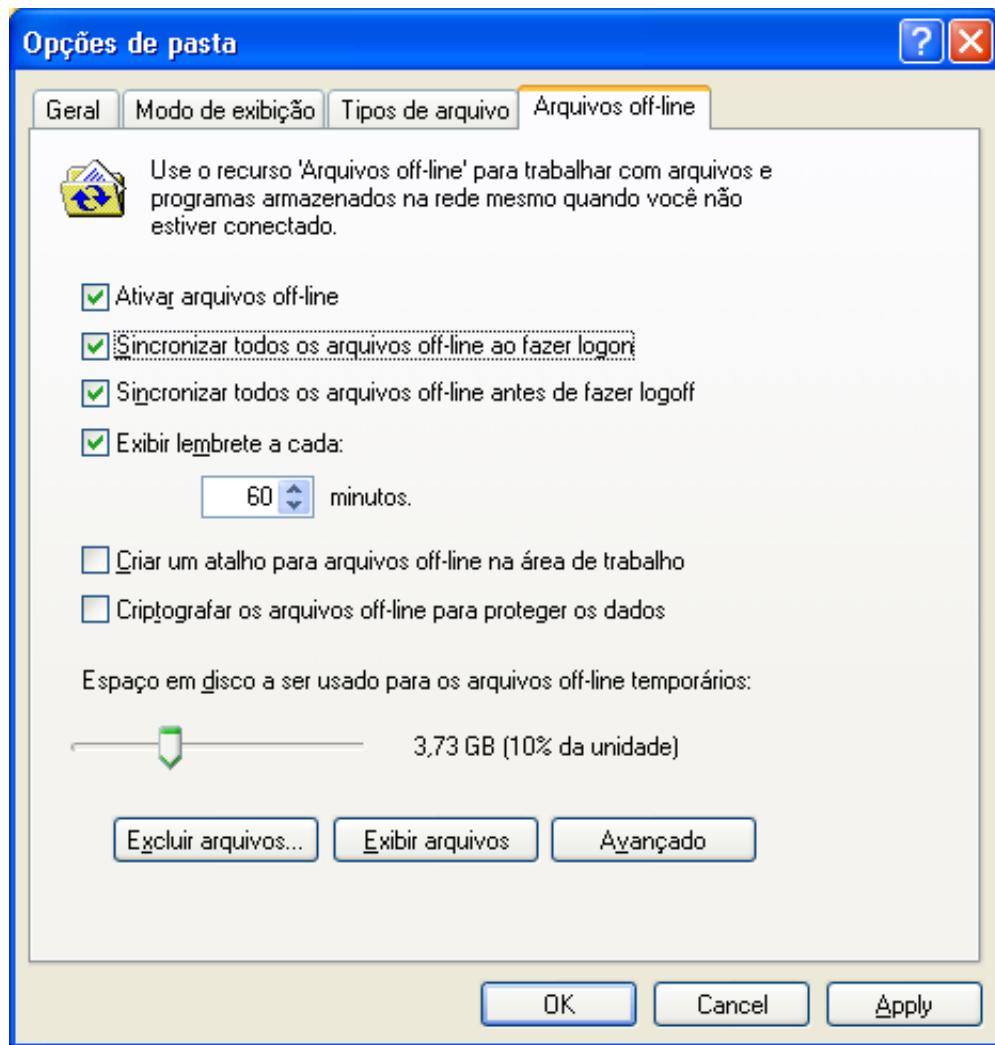


Figura 6.53 Configurações de sincronização.

## Compactação de pastas e arquivos.

### Compactação de arquivos e pastas.

Em volumes formatados com o sistema de arquivos NTFS é possível compactar pastas, arquivos individuais ou até mesmo todo o volume. A compactação NTFS não gera arquivos separados no padrão .zip, ao invés disso, os arquivos compactados permanecem com o nome original, apenas o seu conteúdo é gravado usando um algoritmo de compactação do Windows Server 2003. Quando o usuário acessa um arquivo compactado, o Windows Server 2003 descompacta o arquivo automaticamente e fornece os dados para o usuário. Ou seja, do ponto de vista do usuário, a exemplo do que acontece com a criptografia de arquivos, o processo de compactação/descompactação é transparente. Ao abrir um arquivo compactado, o Windows automaticamente o descompactará para você e ao fechá-lo, o Windows o compactará novamente. A compactação no Windows Server 2003 não afeta de maneira significativa o desempenho. Ao trabalhar com arquivos e pastas compactadas, pode haver uma pequena queda no desempenho, devido ao trabalho de compactação/descompactação realizado pelo Windows Server 2003. Na maioria dos casos esta queda no desempenho é praticamente desconsiderável.

## Compactando e descompactando pastas e arquivos em volumes NTFS.

Exemplo: Para compactar uma pasta e todo o seu conteúdo, faça o seguinte:

1. Faça o logon com uma conta que tem permissão de acesso à pasta a ser compactada.
2. Usando o Meu computador ou o Windows Explorer, localize a pasta ou o arquivo a ser compactado.
3. Clique com o botão direito do mouse na pasta/arquivo a ser compactado e, no menu de opções que é exibido, dê um clique na opção Propriedades. Será aberta a janela de propriedades da pasta/arquivo, com a guia Geral selecionada.
4. Dê um clique no botão Avançado... Será aberta a janela Atributos avançados.
5. Para compactar a pasta/arquivo, marque a opção Compactar o conteúdo para economizar espaço em disco, conforme indicado na Figura 6.54:

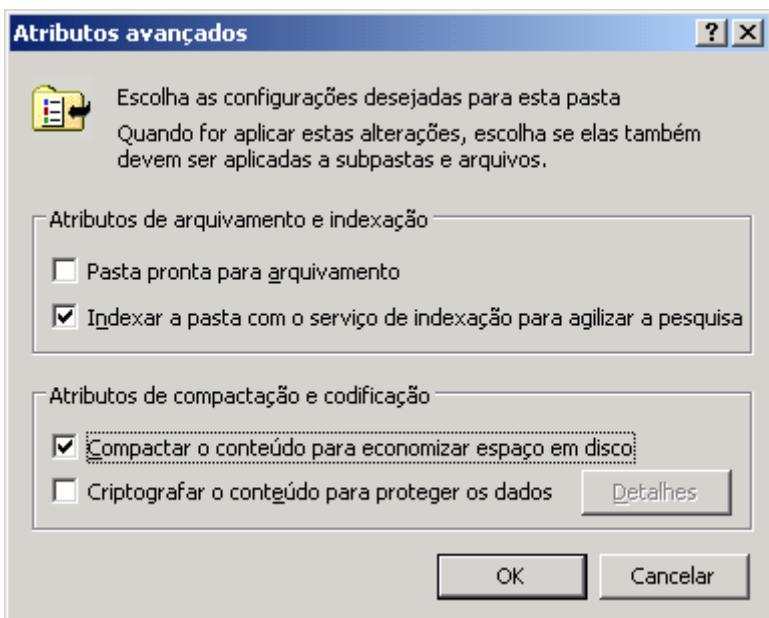


Figura 6.54 A opção Compactar o conteúdo para economizar espaço em disco.

6. Dê um clique no botão OK. Você estará de volta à janela de propriedades da pasta.
7. Dê um clique no botão OK. Surge uma janela perguntando se você deseja compactar somente a pasta em questão ou todas as suas subpastas e arquivos. Selecione a opção Aplicar as alterações a esta pasta , subpastas e arquivos e dê um clique no botão OK.
8. O Windows Server 2003 inicia o processo de compactação da pasta e de todo o seu conteúdo. Dependendo da quantidade de arquivos e subpastas, o processo de compactação pode demorar alguns minutos. Durante este processo é exibida uma janela com o progresso da compactação.

**IMPORTANTE:** As pastas e arquivos compactados em volumes com NTFS só permanecerão compactados enquanto estiverem armazenados em um volume NTFS, ou seja, ao copiar um arquivo compactado para um volume formatado com FAT, o arquivo será primeiro descompactado e depois copiado para o local de destino. Em volumes FAT a única opção de compactação é a criação de arquivos e pastas compactados no padrão .zip. No próximo item mostrarei como o Windows Server 2003 (a exemplo do Windows XP) consegue trabalhar diretamente com arquivos no padrão .zip, sem precisar de um programa externo como por exemplo o Winzip.

**IMPORTANTE:** Vale lembrar, conforme já citado anteriormente, que a compactação NTFS e a criptografia são recursos mutuamente excludentes, ou seja não é possível compactar uma pasta criptografada ou criptografar uma pasta compactada.

**NOTA:** O Percentual de compactação que você obtém varia muito com o tipo de arquivo. Por exemplo, arquivos de imagens no formato Bitmap - .bmp, obtém taxas de compactação elevadas, normalmente próximas a 90 %, já arquivos executáveis - .exe ou arquivos .dll obtém taxas de compactação muito pequenas, muitas vezes menores do que 1%.

Pronto. A pasta e todo o seu conteúdo foram compactados.

Para descompactar um arquivo/pasta, basta seguir os passos descritos no exemplo anterior e desmarcar a opção Compactar o conteúdo para economizar espaço em disco. Deve haver espaço suficiente no volume, para comportar os arquivos que estão sendo descompactados, uma vez que após descompactados, estes arquivos ocuparão mais espaço em disco do que quando estavam compactados.

Você deve ter um cuidado especial ao compactar arquivos que fazem parte do Windows Server 2003, como por exemplo a pasta onde está instalado o Windows Server 2003 e suas subpastas. É aconselhável que você substitua o disco rígido por um de maior capacidade do que compactar as pastas onde está instalado o Windows Server 2003, pois isso pode causar uma queda no desempenho do sistema como um todo. Esta situação é específica para os arquivos do Windows Server 2003 e não para arquivos de dados em geral, onde a compactação praticamente não afeta o desempenho, conforme descrito anteriormente.

**IMPORTANTE:** Se algum arquivo estiver em uso, surge uma mensagem avisando que o arquivo em uso não poderá ser compactado. Nesta janela de aviso você tem opção de Cancelar a compactação, Ignorar o arquivo em uso, neste caso ele não será compactado e a opção Ignorar todos, a qual informa ao Windows Server 2003 para ignorar qualquer arquivo que esteja em uso, ou seja, não compactar arquivos que estejam em uso.

## Arquivos compactados no padrão .ZIP.

### Trabalhando com pastas e arquivos compactados no padrão .ZIP.

Nas versões do Windows, até o Windows 2000, para trabalhar com arquivos compactados no padrão .zip (que é o padrão mais utilizado), era necessário um programa específico, como por exemplo o Winzip ou o Power Archive ou o Winrar. Estes programas eram utilizados para compactar e descompactar pastas e arquivos, utilizando o padrão .zip. Ou seja, para trabalhar com arquivos no padrão .zip, você tinha que adquirir um programa que desse suporte a este padrão.

Acontece que o padrão/algoritmo de compactação .zip é amplamente conhecido e pode ser facilmente implementado. Com base nisso, a Microsoft implementou, como uma funcionalidade do Windows Server 2003, a capacidade de trabalhar com arquivos no padrão .zip. Por isso, no Windows Server 2003 (e também no Windows XP), não é preciso de nenhum software adicional para criar arquivos compactados e para descompactar arquivos no padrão .zip. Conforme mostrarei nos exemplos práticos a seguir, é extremamente simples trabalhar com arquivos .zip

**NOTA:** Por padrão o Windows Server 2003 exibe pastas e arquivos compactados em cor azul e pastas ou arquivos criptografados em cor verde.

**IMPORTANTE:** Quando você copia arquivos compactados, de um volume NTFS para um disquete, para um volume formatado com FAT ou para um CD-ROM (caso você tenha um gravador de CD), os arquivos serão descompactados, antes de ser copiados para o destino. Isso acontece porque as referidas mídias não dão suporte ao sistema de arquivos NTFS e somente é possível utilizar a compactação em volumes formatados com o sistema NTFS.

### Gerando um arquivo compactado no padrão .zip.

Exemplo: Compactar um arquivo, gerando um arquivo .zip.

1. Abra o Windows Explorer ou o Meu computador.
2. Localize o arquivo a ser compactado. No nosso exemplo, vou compactar o arquivo Curso de Word Avançado.doc, indicado na Figura 6.55. Observe que o tamanho original do arquivo é de 6243 KB.

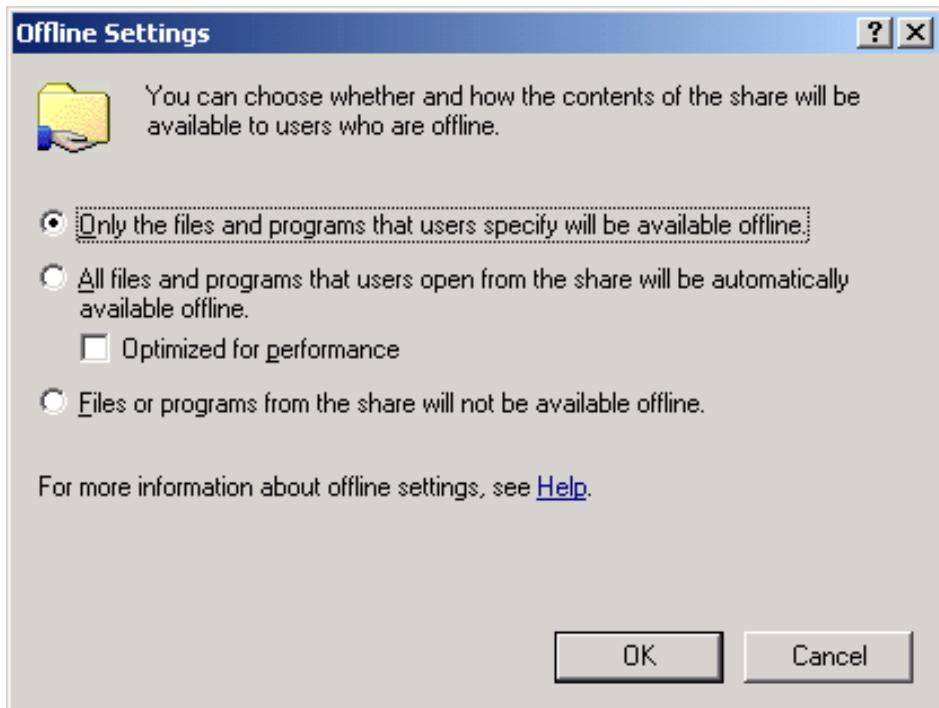


Figura 6.55 Compactando um arquivo com o Windows Server 2003.

**NOTA:** Alguns arquivos apresentam um percentual de compactação bastante elevado, isto é, o tamanho do arquivo, depois de compactado, é drasticamente reduzido. Existem casos em que o tamanho é reduzido em mais de 90%. Já outros tipos de arquivos, tais como executáveis (.exe) e arquivos do sistema, tais como DLLs (.dll) não sofrem grande redução ao serem compactados. Normalmente documentos do Word (.doc), planilhas do Excel (.xls) e arquivos gráficos (.bmp, .tif, .png, etc), sofrem um bom percentual de redução no tamanho, quando compactados.

3. Clique com o botão direito do mouse no arquivo a ser compactado. No menu de opções que surge dê um clique na opção Enviar para -> Pasta compactada (zipada).

O Windows Server 2003 gera um arquivo .zip, com o mesmo nome do documento e com a extensão .zip, ou seja, no nosso exemplo será gerado o arquivo Curso de Word Avançado.zip. O arquivo é gerado na mesma pasta do arquivo que está sendo compactado. Observe que o arquivo compactado ficou com o tamanho de 514 KB, ou seja, uma taxa de compactação de cerca de 92%.

Para abrir um arquivo .zip, no Windows Server 2003 é extremamente simples, basta dar um clique duplo no arquivo .zip que o Windows Server 2003 abre o arquivo e exibe o seu conteúdo. É possível compactar diversos arquivos em um único arquivo .zip. Neste caso se você der um clique duplo no arquivo .zip, serão exibidos todos os arquivos que fazem parte do arquivo compactado. Para descompactar um dos arquivos é só clicar com o botão direito do mouse e selecionar o comando Copiar. Depois navegue até a pasta de destino, clique com o botão direito do mouse e selecione Colar. Uma cópia descompactada do arquivo selecionado, será colado na pasta de destino.

O Windows Server 2003 trata os arquivos compactados como se fossem pastas. Você dá um clique duplo no arquivo .zip e o Windows Server 2003 exibe a listagem com todos os arquivos que fazem parte do arquivo .zip. Se você der um clique duplo em um dos arquivos, o Windows Server 2003 abre o arquivo no aplicativo relacionado. Por exemplo, se você der um clique duplo em um arquivo .doc, que está dentro de um arquivo .zip, o Windows Server 2003 descompacta o arquivo e abre-o no Word.

Exemplo: Para adicionar mais arquivos a um arquivo compactado (.zip) já existente:

1. Neste exemplo, vou adicionar mais três arquivos .doc, ao arquivo Curso de Word Avançado .zip, criado anteriormente.
2. Utilizando o Windows Explorer ou o Meu computador, localize e selecione os arquivos a serem adicionados. Uma vez selecionados os arquivos, utilize o comando Editar -> Copiar ou pressione Ctrl+C.

3. Localize o arquivo .zip no qual você quer adicionar novos arquivos. Dê um clique duplo para abrir o arquivo .zip.
4. Selecione o comando Editar -> Colar ou pressione Ctrl+V. Os arquivos selecionados anteriormente serão compactados e adicionados ao arquivo .zip. Ou seja, é uma simples operação de Copiar e Colar.

## Conclusão.

Neste Capítulo tratou sobre pastas compartilhadas, permissões de compartilhamento e permissões NTFS, uso do DFS, definição de cotas de disco, uso de pastas off-line, compactação de pastas e arquivos e uso de arquivos compactados no padrão .zip.

O uso de pastas compartilhadas é um dos recursos mais utilizados, se não “o mais utilizado”, em redes de computadores.

Mostrei que, ao criar um compartilhamento, é possível definir quais usuários e/ou grupos terão acesso a este compartilhamento. As permissões de compartilhamento somente tem efeito para acesso pela rede, ou seja, elas não tem efeito localmente. A permissão efetiva do usuário é a soma de todas as permissões que ele herda dos grupos aos quais ele pertence, mas as permissões atribuídas diretamente ao usuário. Além disso, negar sempre tem precedência sobre permitir.

O administrador também pode definir permissões NTFS para pastas e arquivos. Se houver conflito entre as permissões NTFS da pasta e do arquivo, vale as permissões do arquivo. Ao criar uma pasta ou arquivo, as permissões NTFS para o objeto que está sendo criado, são herdadas da pasta “pai” do objeto. É possível desabilitar este mecanismo de herança, conforme foi tratado neste capítulo.

Quando existem conflitos entre as permissões de compartilhamento e as permissões NTFS, vale a mais restritiva. Por exemplo, se um usuário tem permissão de compartilhamento Controle total e permissão NTFS somente leitura, a permissão efetiva deste usuário será Somente leitura.

Também apresentei os conceitos teóricos relacionados ao DFS e as suas vantagens. Mostrei que através do uso do DFS, o Administrador pode implementar um sistema centralizado de administração das pastas compartilhadas, em diferentes servidores da rede. Também é possível criar redundância, através da criação de réplicas de uma mesma pasta, em diferentes servidores.

Em seguida você aprendeu a criar e a utilizar uma árvore DFS, utilizando o console Sistema de arquivos distribuídos.

Para maiores informações sobre o DFS, consulte as seguintes referências:

- ◆ Windows 2000 Server Distributed System Guide”, Microsoft Press, Capítulo 17. Este livro faz parte do Resource Kit do Windows 2000 Server e está disponível, OnLine, no seguinte endereço: <http://www.microsoft.com/windows2000/techinfo/reskit/default.asp>.
- ◆ Microsoft Windows 2000 Server Administrator’s Companion”, Microsoft Press, Capítulo 16.
- ◆ Você encontra uma série de artigos, papers e tutoriais sobre DFS, no seguinte endereço: <http://www.labmice.net/windows2000/FileMgmt/DFS.htm>.

No próximo Capítulo falarei sobre instalação, configuração, compartilhamento e administração de impressoras.

---

**NOTA:** Observe que agora existem quatro arquivos que fazem parte do arquivo compactado **Curso de Word Avançado.zip**.

---

# Introdução

Este capítulo é todo dedicado ao trabalho de instalação, administração e resolução de problemas relacionados com impressoras no Windows Server 2003. É comum a utilização de impressoras de melhor qualidade e maior velocidade instaladas em servidores. Estas impressoras são compartilhadas no servidor e acessadas pelos usuários a partir de suas estações de trabalho. Existem várias vantagens em ter as impressoras administradas através dos servidores, tais como: Administração centralizada, controle de impressão através do uso de permissões de acesso, auditoria do volume de impressão por usuário e assim por diante.

Vou iniciar o capítulo apresentando aspectos teóricos, relacionados com o sistema de impressão do Windows Server 2003. Vou apresentar os termos utilizados pelo Windows Server 2003, para que não haja confusão entre, por exemplo, o termo que se refere a impressora, dispositivo físico (hardware) e o termo que faz referência ao driver da impressora, ou seja, a impressora como ela aparece na opção Impressoras no Windows Server 2003. Também falarei sobre o sistema de impressão do Windows Server 2003 e alguns detalhes sobre o planejamento para implementação de impressoras em rede.

Mostrarei as características que devem ser observadas na compra de uma impressora. Farei alguns cálculos para demonstrar que, dependendo do volume de impressão, é mais importante o “custo de propriedade” do que o “custo de aquisição”.

Em seguida partirei para a parte prática. Você aprenderá a instalar, configurar e a trabalhar com Impressoras. Mostrarei como instalar uma Impressora, quer seja para uso localmente, quer seja para uso através da rede. Você também aprenderá a atribuir permissões de acesso para o uso da Impressora (para usuários e grupos). Serão explicadas algumas propriedades importantes, bem como procedimentos para administração e resolução de problemas de impressão.

Em seguida vamos aprender a instalar e a configurar uma impressora local, isto é, uma impressora ligada diretamente no servidor. Tratarei sobre a importância do driver da impressora e como configurar opções da impressora que serão utilizadas por todos os programas que utilizam a impressora. Mostrarei que é possível ter mais de um driver de impressora instalado, neste caso temos que definir uma das impressoras como sendo a impressora padrão.

Na seqüência você aprenderá a compartilhar uma impressora, para que esta possa ser utilizada nos demais computadores da rede. Compartilhar uma impressora é muito semelhante a compartilhar uma pasta. A maneira como o usuário acessa uma impressora compartilhada também é praticamente igual a maneira como acessamos uma pasta compartilhada. Também mostrarei como publicar impressoras e pastas compartilhadas no Active Directory e depois como pesquisar no Active Directory para localizar estes objetos.

Você aprenderá a definir permissões de acesso à impressora. Mostrarei que estas permissões definem quais usuários podem utilizar a impressora e com que nível de permissão. Por exemplo, você pode definir que o grupo Empresa somente

# CAPÍTULO

## 7

### Instalação, Configuração e Administração de Impressoras

pode imprimir documentos, já o grupo Gerentes pode imprimir documentos e administrar a fila de impressão.

Você também aprenderá a configurar propriedades avançadas de uma impressora, tais como:

- ◆ Horários em que a impressora está disponível.
- ◆ Diferentes prioridades para diferentes grupos.

Mostrarei como administrar a fila de documentos da impressora. É possível excluir um documento da fila, alterar a posição do documento na fila, “pausar” um documento e reiniciar a sua impressão mais tarde e também é possível excluir todos os documentos da fila.

Mostrarei que é possível administrar impressoras utilizando o Internet Explorer. Para isso é necessário que, no servidor onde está a impressora, esteja instalado o IIS – Internet Information Services, que é o servidor Web da Microsoft, o qual será detalhado no Capítulo 13.

Para finalizar o capítulo apresentarei alguns comandos que são úteis para o gerenciamento e resolução de problemas em pastas e impressoras compartilhadas. Você verá também comandos úteis para a resolução de problemas de impressão.

Com os conhecimentos apresentados neste capítulo, o amigo leitor terá todas as condições para instalar, configurar Impressoras, quer seja locais ou da rede; além de estar apto a resolver os principais problemas que ocorrem no dia-a-dia, relacionados com Impressoras.

## O Sistema de Impressão do Windows Server 2003 – Conceitos Teóricos

No início da informatização das empresas, uma das “promessas” da informática era a criação de um “Escritório sem papel”, ou seja, toda a informação contida nos sistemas e consultada através do computador. Sabemos que esta é uma realidade que está longe de se concretizar. Não por causa da tecnologia, pois no estágio atual é perfeitamente possível ter toda a informação em sistemas informatizados e consultar a informação usando o computador.

Acontece que existe o “Mundo Real” e neste mundo, ainda se usa muito papel, talvez até mais do que antes da informatização chegar nas empresas. Quer seja por exigências legais e burocráticas (devido a processos de negócio mal projetados), quer seja pelas preferências pessoais dos usuários, o fato é que ainda se gasta muito papel, ainda se imprime muita informação na empresa.

Claro que em algumas situações a impressão é inevitável, como por exemplo em papéis que, por exigência legal, devam ser assinados e remetidos para outras empresas ou órgão públicos, ou plantas de projetos que devam ser enviados para homologação e assim por diante. Em outras situações é simplesmente uma preferência pessoal do usuário, o qual prefere ter as informações em papel a ler na tela.

O fato real é que os sistemas de impressão ainda são um dos serviços mais utilizados em uma rede de computadores. Sendo este um serviço bastante utilizado, cabe ao administrador entender como funciona o sistema de impressão do Windows Server 2003 e como executar as ações práticas para administração e implementação de um sistema de impressão eficiente e de baixo custo.

Embora o custo das impressoras tenha sido reduzido consideravelmente nos últimos anos, ainda é muito mais econômico ter um número reduzido de impressoras de maior qualidade e velocidade compartilhadas nos servidores, do que ter uma impressora na estação de trabalho de cada usuário. Não só pela questão do custo, como também pela questão da administração centralizada e do controle do volume de impressão por usuários.

## **Uma bela confusão de termos**

Talvez por excesso de criatividade, a equipe da Microsoft tem feito um belo trabalho para “confundir” o administrador do sistema de impressão, ao usar diferentes termos para fazer referência a impressora propriamente dita e ao driver da impressora (o software de controle da impressora instalado no servidor).

Para piorar um pouco mais, esta terminologia mudou novamente no Windows Server 2003, em relação a terminologia que era utilizada no Windows NT Server 4.0 e no Windows 2000 Server. Para ajudar o amigo leitor a se situar um pouco melhor neste “emaranhado” de termos, descrevo a terminologia oficial, utilizada nas diferentes versões do Windows, em relação à Impressoras.

No Windows NT Server 4.0 e no Windows 2000 Server são utilizados os seguintes termos:

- ◆ **print device (dispositivo de impressão):** Este termo refere-se a impressora propriamente dita, ao hardware. Ou seja, uma HP Deskjet 660 C, uma Rima Okidata 1100, uma Epson LX 300 e assim por diante.
- ◆ **printer (impressora):** faz referência ao driver da impressora, ao software instalado e que controla a impressora. É o elemento que aparece na pasta Printers (Impressoras).

No Windows Server 2003 são utilizados os seguintes termos:

- ◆ **printer (Impressora):** Este termo refere-se a impressora propriamente dita, ao hardware. Ou seja, uma HP Deskjet 660 C, uma Rima Okidata 1100, uma Epson LX 300 e assim por diante (que no Windows NT Server 4.0 e Windows 2000 Server era chamado de print device)
- ◆ **logical printer:** faz referência ao driver da impressora, ao software instalado e que controla a impressora. É o elemento que aparece na pasta Printers (Impressoras). Também aparece, em alguns pontos da documentação oficial, o termo printer driver (driver da impressora).

Neste capítulo utilizarei os termos adotados pelo Windows Server 2003, ou seja: printer faz referência ao hardware, a impressora propriamente dita e logical printer faz referência ao driver, ao software que controla a impressora.

Conforme mostrarei na parte prática, você pode instalar a mesma impressora (printer) várias vezes (mais de um logical printer) no mesmo servidor. Para cada instalação (cada logical driver) o administrador pode definir diferentes configurações. Por exemplo, imagine que você tem uma impressora laser, colorida, de alta velocidade. Esta impressora deve ser utilizada pelos estagiários e pelos gerentes, porém os trabalhos enviados pelos gerentes devem ter maior prioridade de impressão (serem impressos antes) do que os trabalhos enviados pelos estagiários. Para resolver esta questão você pode instalar a impressora duas vezes. Na primeira vez você compartilha com o nome de Estagiários e configura uma prioridade baixa. Neste compartilhamento você define permissão de acesso para os estagiários. Você instala novamente o driver da impressora, com um nome diferente do anterior e cria um compartilhamento Gerentes. Neste compartilhamento você define uma prioridade mais alta (do que a prioridade para a instalação dos Estagiários) e define permissão de acesso somente para o grupo Gerentes. Com isso somente os gerentes poderão utilizar esta impressora com a prioridade alta e os estagiários utilizarão com a prioridade mais baixa. Este é um exemplo onde existe uma impressora (printer) e o driver instalado duas vezes, com diferentes configurações (duas logical printer).

O contrário também pode ser feito, ou seja, instalar um único driver e associá-lo com diferentes impressoras. Este procedimento pode ser feito desde que todas as impressoras utilizem o mesmo driver. Este arranjo é conhecido como “printer pool” e é utilizado para distribuição de cargas. Por exemplo, imagine que você instale quatro impressoras da mesma marca e modelo em um servidor de impressão. Neste servidor você instala o driver da impressora (logical printer) uma única vez e associa este driver com as quatro impressoras instalados. Com isso você criou um “printer pool”. A medida que os trabalhos de impressão vão chegando, o driver da impressora vai redirecionando os trabalhos sempre para a impressora que estiver com o menor volume de trabalho, ou seja, com a menor fila de impressão. Com isso o trabalho

vai sendo dividido entre as diferentes impressoras que fazem parte do pool. A condição necessária para que seja possível criar um pool é que todas as impressoras utilizem o mesmo driver de impressão. Podem fazer parte do pool impressoras diretamente ligadas ao servidor ou impressoras conectadas diretamente à rede através de uma placa de rede.

Aviso importante sobre compatibilidade de drivers: O Windows Server 2003 trabalha com dois tipos diferentes de drivers de impressora, conhecidos com driver de nível 2 e driver de nível 3. Os drivers de nível 2 são compatíveis com o Windows NT Server 4.0. Os drivers de nível 2 são executados em nível de Kernel do sistema operacional e em caso de problemas podem desestabilizar todo o sistema operacional, sendo necessária uma reinicialização do servidor. Os drivers de nível 2 somente são suportados quando da migração de um servidor com o NT Server 4.0 para o Windows Server 2003. Neste caso, os drivers de impressoras já instalados serão mantidos e estarão disponíveis no Windows Server 2003. Porém você não poderá instalar novos drivers nível 2 no Windows Server 2003. O Windows 2000 Server e o Windows Server 2003 utilizam os drivers de nível 3. Os drivers de nível 3 rodam em modo de usuário protegido. Em caso de problemas com um destes drivers, o máximo que acontece é a desestabilização do serviço Spooler (o qual é o responsável pela impressão no Windows), o qual será automaticamente reinicializado, sem que seja necessário reiniciar o servidor.

## Entendendo o serviço de impressão no Windows Server 2003.

O serviço de impressão do Windows Server 2003 procura auxiliar ao máximo os clientes que utilizam este serviço. Por exemplo, ao instalar uma impressora no Windows Server 2003 (logical driver), o administrador pode instalar também drivers da impressora para outras versões do Windows (NT 4.0, Windows 2000, Windows XP e assim por diante). Quando um destes clientes acessa uma impressora compartilhada no servidor, o respectivo driver é carregado diretamente a partir do servidor, sem que o cliente tenha que fornecer um CD com o driver da impressora.

Outra vantagem do serviço de impressão (vantagem esta do ponto de vista do administrador) é que é possível gerar um log com a descrição detalhada dos trabalhos que estão sendo enviados para a impressora. Com base neste log o administrador pode determinar o volume de impressão por usuário, por impressora e assim por diante.

O Windows Server 2003 fornece suporte a diferentes tipos de conexão entre o servidor e a impressora. O tipo mais comum é a conexão via porta paralela, a já conhecida LPT1. A maioria das impressoras (quase a totalidade) trabalha com este tipo de conexão, via porta paralela. Existem também impressoras que conectam via porta serial, mas normalmente são impressoras utilizadas em estações de trabalho da rede, mais especificamente nos conhecidos PDVs – Pontos de Vendas. Por exemplo, um caixa de supermercado é conhecido como PDV – Ponto de Venda. Existem diversos modelos de impressoras fiscais que utilizam a conexão via porta serial. Dificilmente você terá uma impressora serial conectada a um servidor com o Windows Server 2003. Existem outros tipos de conexão, sendo que um dos que mais vem sendo adotado atualmente é o padrão USB – Universal Serial Bus. Este é um padrão de conexão que vem tendo ampla aceitação da indústria e dos usuários. Todos os novos computadores já vem com uma ou mais portas USB.

Você pode conectar qualquer dispositivo USB em uma porta USB. Existem teclados, mouses, impressoras e inúmeros outros dispositivos já habilitados ao padrão USB. O Windows Server 2003 reconhece e trabalha sem problemas com o padrão USB. Outra forma de conexão é através de conexão direta com a rede. São impressoras que vêm com uma placa de rede, padrão Ethernet instalada e que são conectadas diretamente à rede. Estas impressoras recebem um endereço IP e passam a fazer parte da rede. No Windows Server 2003, ao instalar o driver da impressora, você pode configurar o driver e associá-lo com o endereço IP da impressora. Desta maneira o driver está instalado no Windows Server 2003 e redireciona os trabalhos para a rede, usando o IP configurado na impressora. Mostrarei um exemplo de configuração deste tipo de impressora na parte prática deste capítulo. A vantagem do uso das impressoras de rede (conectadas diretamente à rede) é que a impressora não precisa estar fisicamente junto ao servidor que a controla.

Uma novidade que foi introduzida no Windows 2000 Server e que foi melhorada no Windows Server 2003 é a impressão através da Internet (ou da Intranet da empresa). Você pode configurar uma impressora para que ele seja visível através da Internet ou da Intranet da empresa. Você pode definir quais usuários terão permissão para utilizar esta impressora,

a exemplo do que acontece com qualquer tipo de impressora instalada no Windows Server 2003. A impressão via Internet é feita através do protocolo Internet Printing Protocol – IPP. O suporte ao protocolo IPP depende da impressora. Se a impressora não vier de fábrica com suporte a este protocolo, você deverá instalar o protocolo no Windows Server 2003 e também o IIS para que você possa administrar a impressora usando o Browser. No Capítulo 13 você aprenderá a instalar, utilizar e administrar o IIS 6.0.

As impressoras com suporte ao protocolo IPP, normalmente, vem com uma interface de administração via Browser. Ou seja, você conecta o Browser diretamente com o IP configurado para a impressora e é aberta uma página com uma série de comandos de administração da impressora. Normalmente é exigida uma senha para que possa ser feita a administração da impressora, para evitar que qualquer usuário que conheça o IP da impressora faça a conexão e altere as configurações da impressora.

Depois de instalada uma impressora e habilitada para o protocolo IPP, você pode conectar com a impressora, facilmente, usando o Internet Explorer 4.0 ou superior. Por exemplo, para exibir a lista de impressoras do domínio abc.com, basta utilizar o endereço a seguir:

**`http://abc.com/printers`**

Para fazer a conexão diretamente com uma impressora, cujo nome de compartilhamento seja las-col-01, no domínio abc.com, basta utilizar o endereço a seguir:

**`http://abc.com/ las-col-01`**

Será exibida uma lista de comandos da impressora. Basta clicar em Install e pronto, o driver da impressora será instalado e você poderá imprimir diretamente neste impressora. Para o usuário aparece com mais uma impressora (logical driver) na lista de impressoras instaladas. Quando o usuário envia uma impressão, o protocolo IPP é responsável por enviar os dados para a impressora de destino para que a impressão seja realizada.

## Alguns detalhes sobre o processo de impressão do Windows Server 2003

A seguir descrevo as etapas envolvidas no processo de impressão, desde o momento em que o usuário manda um trabalho para impressão, até o momento em que o trabalho é, efetivamente, impresso. Estes passos são baseados em White Paper sobre impressão publicado no site oficial do Windows Server 2003: [www.microsoft.com/windowsserver2003](http://www.microsoft.com/windowsserver2003) e na Ajuda do Windows Server 2003.

Os passos a seguir exemplificam o que acontece quando um cliente, usando um computador com o Windows XP Professional, envia um documento para impressão em uma impressora instalada e compartilhada em um servidor com o Windows Server 2003 instalado:

1. O usuário abre o Word e utiliza o comando Arquivo -> Imprimir para enviar a impressão para uma impressora compartilhada no servidor Windows Server 2003.
2. O Windows XP detecta o comando de impressão e utiliza a GDI (Graphical Device Interface). A GDI identifica qual o driver de impressão associado com a impressora de destino. A GDI e o driver da impressora trocam informações para formatar os dados do documento no formato de comandos que possam ser interpretados pela linguagem da impressora de destino. Estas informações, já formatadas para o formato adequado, são passadas para o serviço de impressão na estação de trabalho do usuário – no nosso exemplo o serviço spooler na estação de trabalho com o Windows XP.
3. O serviço de impressão do cliente envia o trabalho de impressão para o servidor de impressão. O servidor onde está instalada a impressora de destino.
4. Para pedidos de impressão vindos de clientes com o Windows XP, Windows 2000 ou Windows NT 4.0, são recebidos no formato conhecido como enanchced metafiles (EMF).

5. O serviço de roteamento de impressão no servidor passa os dados da impressão para o provedor de impressão local (que é um dos componentes do serviço spooler no servidor). O provedor de impressão local coloca o trabalho de impressão na fila (em spool), isto é, grava o trabalho em uma pasta específica do disco rígido, reservada para os trabalhos de impressão. Os dados são salvos em um arquivo com a extensão .SPL.
6. Neste momento o pedido de impressão está em uma fila única de impressão. Quando o pedido de impressão chega no início da fila, o sistema de impressão no servidor determina se os dados precisam ser convertidos para um formato diferente, antes de serem enviados para a impressora.
7. Se uma página de separação foi configurada, nas propriedades da impressora, o sistema de impressão providenciará a criação da página separadora.
8. O trabalho é então enviado para a impressora de destino, através da porta configurada para a impressora.
9. A impressora recebe os comandos de impressão e com base destes comandos gera uma imagem no padrão bitmap e então imprime as páginas do documento.

A Figura 7.1, obtida a partir da ajuda do Windows Server 2003, dá uma visão geral deste processo de impressão:

**NOTA:** Caso o usuário esteja utilizando outro sistema operacional que não o Windows, ou uma aplicação não compatível com o Windows, outro componente será utilizado ao invés da GDI.

**NOTA:** Existem aplicações que usam um outro formato conhecido como read to print (RAW). Você pode configurar o formato utilizado pela impressora, nas propriedades da impressora, conforme descreverei na parte prática deste capítulo.

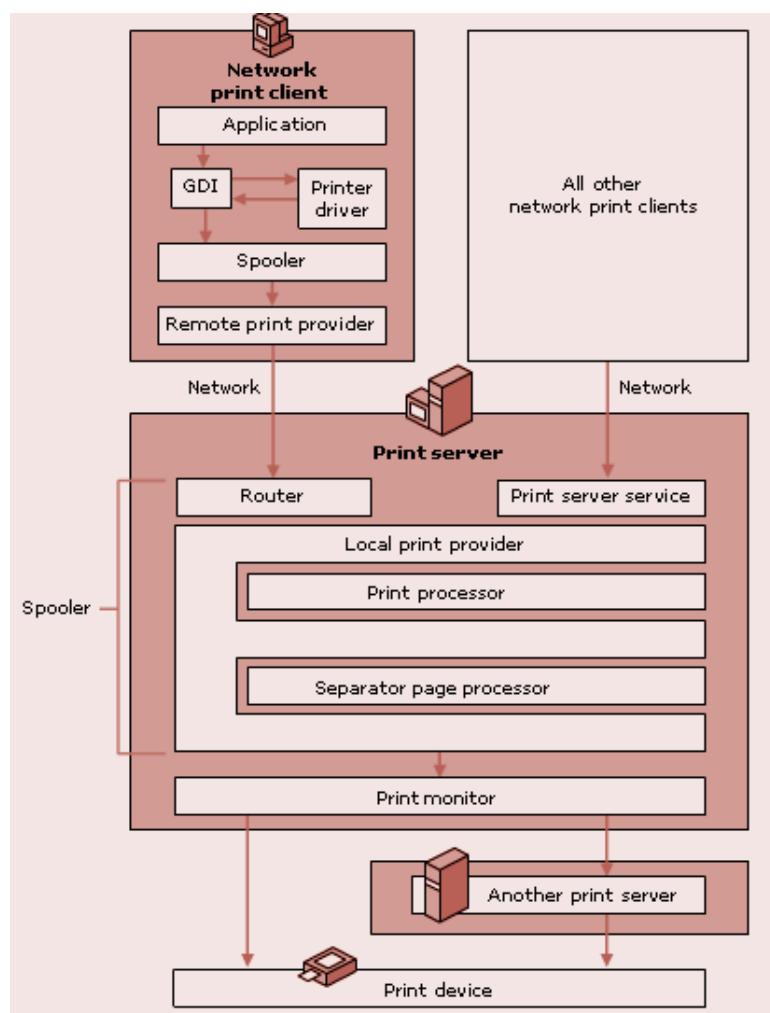


Figura 7.1 Uma visão geral do processo de impressão do Windows Server 2003.

## **Padronização de nomes e outros detalhes importantes para o uso de impressoras em rede.**

O administrador pode selecionar o nome de compartilhamento de cada impressora da rede, bem como definir os comentários, descrição e outras informações sobre cada impressora. Porém é aconselhável que sejam seguidas determinadas recomendações, as quais irão facilitar para o usuário a localização das impressoras através da rede e também as pesquisas no Active Directory. Com a definição de normas para as informações a serem cadastradas para cada impressora, o administrador facilita a vida do usuário, o qual pode fazer pesquisas pelo tipo de impressora (laser, jato de tinta, jato de cera, etc), pela localização, pelas características, pela velocidade e por outros detalhes que possam ser relevantes.

É também importante manter um padrão para a nomeação das impressoras, sempre tendo em mente que o objetivo desta padronização é fazer com que seja fácil para o usuário, localizar uma impressora com as características que ele precisa.

Cada impressora instalada e compartilhada em um servidor tem dois nomes. O primeiro nome é o nome da própria impressora, nome este que é exibido na janela Impressoras ou no Browser, quando o administrador está gerenciando impressoras através do Browser (conforme mostrarei no final deste capítulo). O nome da impressora pode ter até 220 caracteres de comprimento. O outro nome é o nome de compartilhamento. É o nome que é exibido na lista de recursos compartilhados quando o usuário acessa os recursos de um servidor usando o ícone Meus locais de rede ou usando o comando net view \\nome-do-servidor, para exibir a lista de recursos compartilhados em um servidor.

O nome de compartilhamento pode ter até 80 caracteres de comprimento. Porém é importante lembrar que clientes mais antigos, como o Windows 3.x ou MS-DOS, não reconhecem mais do que 8 caracteres como nome de compartilhamento. Somente clientes com o Windows 2000 Server, Windows XP ou Windows Server 2003 são capazes de reconhecer nomes de compartilhamento que contenham espaços. Por isso se você tem clientes baseados no Windows 95/98/Me ou no NT Workstations 4.0, evite utilizar nomes de compartilhamento com espaços.

A idéia básica é que o nome da impressora deve conter informações básicas, tais como o tipo da impressora, localização e indicação de uma característica principal, como nos exemplos a seguir:

- ◆ HP Laser Colorida – Fiscalização
- ◆ Cânon Laser Monocromática – Contabilidade
- ◆ HP Laser – Suporte A3 – Pesquisa

Estes nomes indicam a marca (poderíamos também ter incluído o modelo), uma característica principal (no último exemplo é o suporte a papel tamanho A3) e a localização da impressora.

Os nomes de compartilhamento também deve ser indicativos das características e da localização da impressora. Considere os exemplos a seguir:

- ◆ LasMonoContab
- ◆ LasColPesquisa
- ◆ CeraColRecepção
- ◆ LasColSalaPresidente

## **Considerações sobre o “custo da impressora” e o “custo de impressão”.**

Ao comprar uma impressora, o administrador não pode cometer o erro de considerar apenas o preço de aquisição, ou seja, o preço da Impressora. Deve-se levar em consideração o “custo de propriedade”, o qual leva em consideração o custo de impressão por página. Por exemplo, pode ser que uma impressora tenha um custo de aquisição mais em conta,

porém seja menos econômica do que uma outra. Com isso, a primeira impressora tem um custo de aquisição mais baixo, porém um preço de impressão por página, mais elevado. Ao longo do tempo a primeira impressora, somando o custo de aquisição e o custo de impressão, acaba sendo mais cara do que a segunda.

Na Figura 7.2 mostro uma simulação que demonstra os conceitos de custo de aquisição e custo de propriedade:

|                          | <b>Custo de aquisição</b> | <b>Custo por página</b>   |
|--------------------------|---------------------------|---------------------------|
| IMPRESSORA 1:            | R\$ 500,00                | R\$ 0,05                  |
| IMPRESSORA 2:            | R\$ 1.100,00              | R\$ 0,03                  |
| <b>Páginas impressas</b> | <b>Custo total IMPR1:</b> | <b>Custo total IMPR2:</b> |
| 100                      | R\$ 505,00                | R\$ 1.103,00              |
| 200                      | R\$ 510,00                | R\$ 1.106,00              |
| 500                      | R\$ 525,00                | R\$ 1.115,00              |
| 1000                     | R\$ 550,00                | R\$ 1.130,00              |
| 2000                     | R\$ 600,00                | R\$ 1.160,00              |
| 3000                     | R\$ 650,00                | R\$ 1.190,00              |
| 5000                     | R\$ 750,00                | R\$ 1.250,00              |
| 10000                    | R\$ 1.000,00              | R\$ 1.400,00              |
| 15000                    | R\$ 1.250,00              | R\$ 1.550,00              |
| 20000                    | R\$ 1.500,00              | R\$ 1.700,00              |
| 25000                    | R\$ 1.750,00              | R\$ 1.850,00              |
| <b>30000</b>             | <b>R\$ 2.000,00</b>       | <b>R\$ 2.000,00</b>       |
| 40000                    | R\$ 2.500,00              | R\$ 2.300,00              |
| 50000                    | R\$ 3.000,00              | R\$ 2.600,00              |

Figura 7.2 Custo de aquisição x Custo de propriedade.

Observe que a Impressora1 tem um custo de aquisição menor em comparação à Impressora 2. Já a Impressora2 possui um custo de impressão por página, bem menor. Com isso o custo total da Impressora2 é, inicialmente maior, devido ao seu Custo de aquisição maior; porém a medida que o número de páginas impressas aumenta, esta diferença vai diminuindo, até que o custo total se iguale, para um número de 30000 páginas impressas. A partir deste ponto, a Impressora2 passa a ter um custo Total menor do que a Impressora1. Nesta situação, se estimarmos que, durante a vida útil da impressora, serão impressas mais do que 30000 cópias, é mais barato a opção pela Impressora2, embora esta tenha um custo de aquisição maior, o qual é compensado, ao longo do tempo, pelo custo de impressão menor. O Gráfico da Figura 7.3 ilustra bem os dados da simulação.

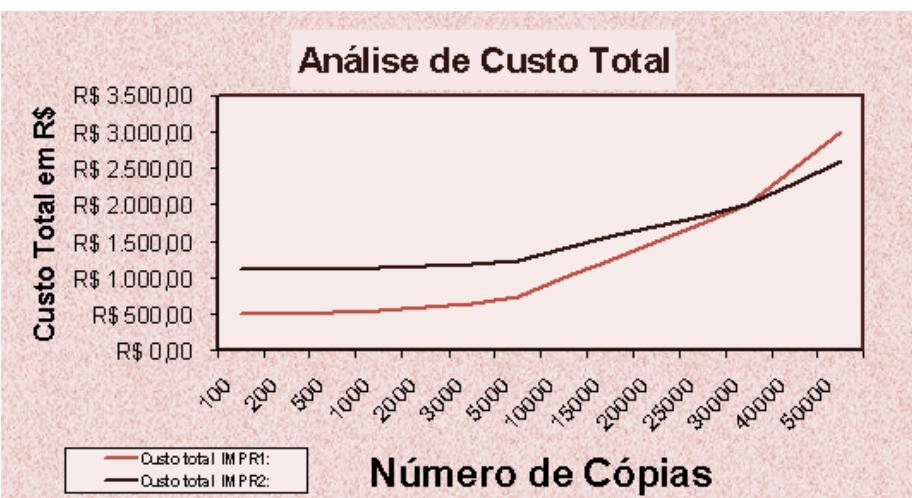


Figura 7.3 Evolução do Custo total em relação ao número de cópias.

# Instalação e Configuração de Impressoras - Prática

Quando o administrador conecta uma nova Impressora, para ser utilizada em um servidor com Windows Server 2003, é preciso instalar o “driver” da impressora (logical printer, na terminologia do Windows Server 2003, conforme descrito no início do capítulo). Um driver nada mais é do que o software que controla a comunicação entre o Windows Server 2003 e a impressora. Cada marca e modelo possui um driver específico para ser usado. Se for instalado o driver incorreto, serão obtidos resultados imprevistos e com certeza a impressora não vai trabalhar corretamente.

O CD de instalação do Windows Server 2003 já vem com milhares de drivers (é isto mesmo: “milhares”) para diferentes marcas e modelos de impressoras. Mas para modelos mais novos, lançados após a disponibilização do Windows Server 2003, pode acontecer do driver não estar no CD do Windows Server 2003. Neste caso o driver vem junto com a impressora ou você pode obtê-lo através do site do fabricante da impressora na Internet.

Então quando digo que vou “instalar” uma impressora, na verdade vou instalar o driver da impressora (logical driver), para que o Windows Server 2003 possa trabalhar corretamente com a impressora. Para instalar uma nova impressora (o driver da impressora), você deve utilizar a opção Iniciar -> Impressoras e aparelhos de Fax. Também existe um atalho para a janela de Impressoras no Painel de controle.

## Instalando uma nova impressora (instalando o driver da impressora)

Neste item mostrarei um exemplo, passo-a-passo de como fazer uma instalação de uma nova impressora. Ou seja, como instalar o driver de uma nova impressora. A medida que você for seguindo as etapas do assistente, farei comentários sobre algumas propriedades e informações relacionadas com a instalação da impressora.

Exemplo: Instalar uma impressora HP Deskjet 660C.

Neste exemplo, você irá instalar uma impressora marca HP, modelo Deskjet 660C, isto é, será instalado o driver para utilizar uma HP Deskjet 660C. A impressora será instalada no computador chamado SRV-Win2003. Substitua SRV-Win2003 pelo nome do servidor que você está utilizando, nesta e nas próximas lições, sempre que for feita alguma referência ao nome SRV-Win2003. Caso a sua impressora seja de uma marca ou modelo diferente, use a marca e modelo adequados para acompanhar este exemplo. Você também pode acompanhar este exemplo, sem ter uma impressora conectada ao seu computador. O Windows Server 2003 instalará o driver e quando você conectar a impressora o driver já estará pronto para ser utilizado.

Para instalar uma nova impressora siga os passos indicados a seguir:

1. Faça o logon com um conta com permissões de Administrador ou com uma conta pertencente ao grupo Oper. de Impressão.
2. Utilize o comando Iniciar -> Impressoras e aparelhos de fax.
3. Será aberta a janela Impressoras e aparelhos de fax, indicada na Figura 6.4, na qual é mostrada uma lista das impressoras instaladas no seu computador.

**IMPORTANTE:** Quando você instala uma impressora, ela pode ser usada por qualquer programa instalado no Windows Server 2003. Se você alterar as configurações da impressora dentro de um programa, como por exemplo o Microsoft Word, estas alterações terão efeito apenas para o documento que está sendo impresso no momento. Ao utilizar um outro programa, serão utilizadas as configurações definidas na própria impressora. Por exemplo, você está imprimindo um documento do Word e seleciona a qualidade de impressão Rascunho. Esta configuração somente será utilizada até que você feche o Word. Agora você fecha o Word e abre o Excel. Ao imprimir uma planilha do Excel, serão utilizadas as configurações definidas nas propriedades da impressora, a não ser que você as altere, no próprio Excel. Para fazer alterações que sejam válidas para todos os programas instalados, estas alterações devem ser feitas acessando as propriedades da impressora. Mostrarei como fazer estas configurações mais adiante, neste capítulo.

**NOTA:** Selecionei um modelo qualquer. Ao acompanhar o exercício, substitua o modelo que eu estou utilizando, pelo modelo que você irá utilizar no seu servidor.

Caso não exista nenhuma impressora instalada, a lista estará vazia, estando disponível apenas a opção Adicionar impressora, que é o caso indicado na Figura 7.4:

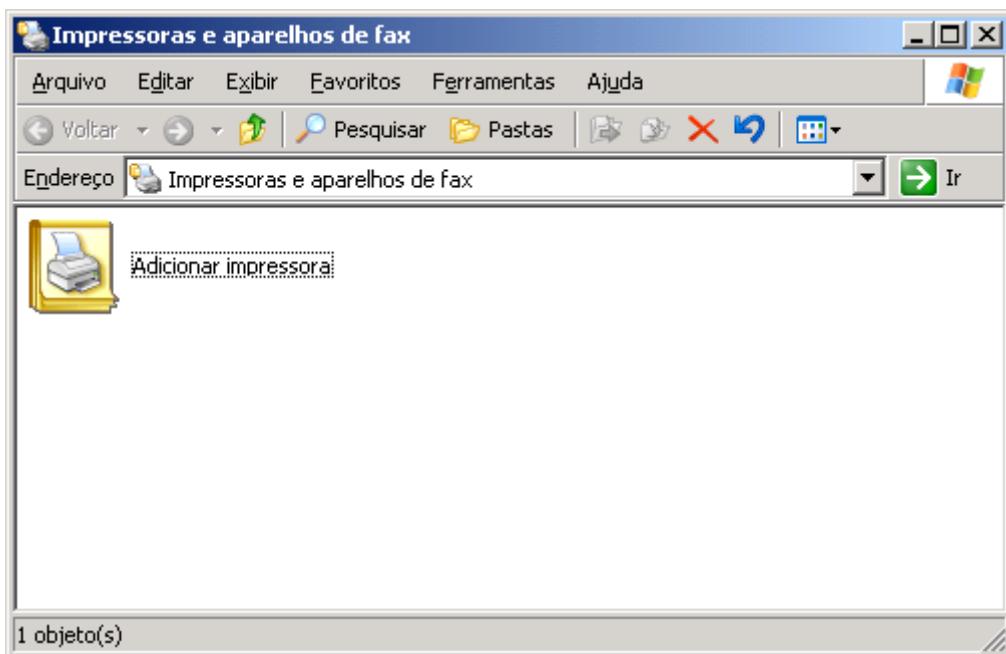


Figura 7.4 A janela Impressoras e aparelhos de fax.

4. Dê um clique duplo no ícone Adicionar impressora.
5. Será aberto o Assistente para adicionar impressora. Este é um assistente que irá guiando você passo a passo na tarefa de instalar o driver para a nova impressora. O assistente solicita diversas informações em cada uma das etapas.
6. Nesta primeira etapa, é exibida uma mensagem explicativa. Dê um clique no botão Avançar para ir para a próxima etapa do assistente.

Na segunda etapa, você deve informar para o Windows Server 2003 se a impressora que está sendo instalada é local (ligada diretamente ao computador) ou é uma impressora da rede (conectada à rede através de uma placa padrão Ethernet ou é uma impressora compartilhada em outro servidor). Você também pode marcar a opção Detectar e instalar automaticamente a impressora Plug and Play, para que o Windows Server 2003 tente detectar a marca/modelo da impressora e instale o driver adequado. Esta opção vem marcada por padrão. Para este exemplo prático, desmarque esta opção.

7. Como estou instalando uma impressora local, certifique-se que a opção Impressora local conectada ao computador esteja marcada e Desmarque a opção Detectar e instalar automaticamente a impressora Plug and Play, conforme indicado na Figura 7.5.
8. Dê um clique no botão Avançar para ir para a terceira etapa do assistente.
9. Na terceira etapa, você tem que escolher a porta onde está ligada a impressora. Uma porta nada mais é do que um meio de comunicação do Windows Server 2003 com os dispositivos ligados ao computador. A grande maioria das impressoras utiliza a porta paralela LPT1 (Line Printer 1).

Certifique-se de que LPT1 esteja selecionada na lista de portas. LPT1 já vem selecionada por padrão, pois é a porta normalmente utilizada pela impressora. A seguir apresento uma descrição dos tipos de portas mais utilizados para conexão de uma impressora com o Windows Server 2003.

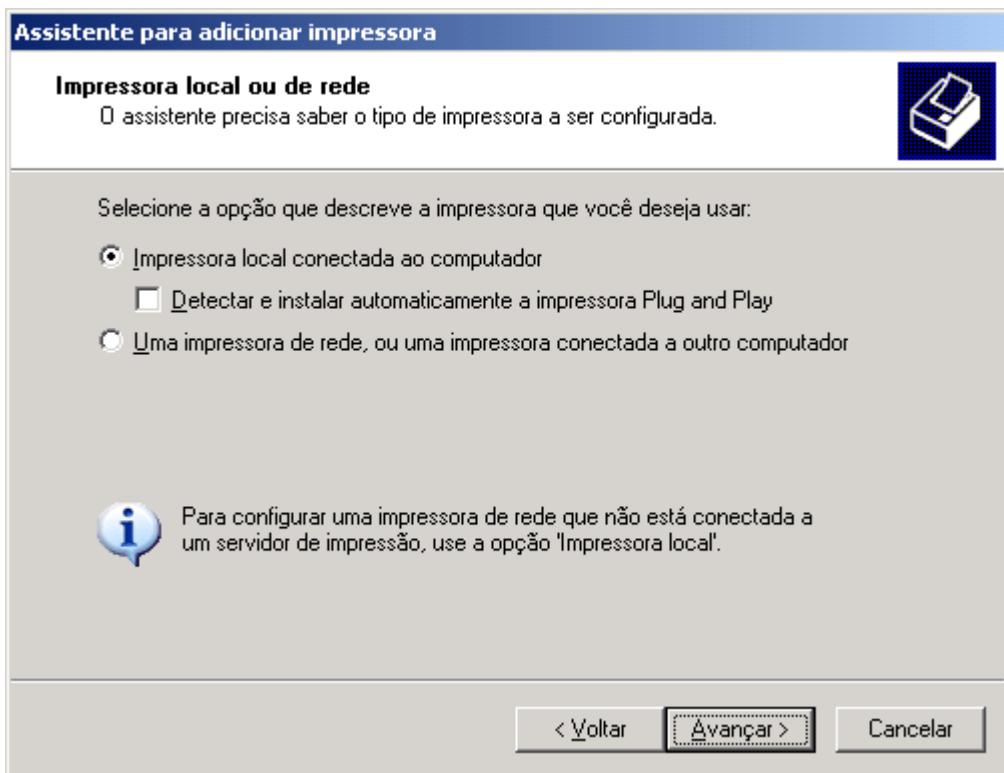


Figura 7.5 - Instalando uma impressora local.

- ◆ **Local Port (Porta Local):** São consideradas portas locais a porta paralela (LPT1, pode haver mais de uma porta paralela, neste caso teremos LPT2, LPT3 e assim por diante), as portas seriais (COM1, COM2 e assim por diante). Uma porta local também pode ser o caminho para um arquivo, como por exemplo C:\trabalhos de impressão\impressão.prn. Neste caso, todos os trabalhos enviados para a porta local serão gravados no arquivo impressão.prn e cada novo trabalho sobrescreve o anterior. Também pode ser utilizada como porta local o caminho UNC para uma impressora compartilhada em outros servidores, como por exemplo \\server02\laser01. Neste caso sempre que a impressão for enviada para esta impressora, será, na prática, redirecionada para \\server02\laser01. NUL é utilizada para criar uma porta nula, ou seja, não ligada a uma impressora. A porta NUL é utilizada apenas para testar se os clientes conseguem enviar os trabalhos de impressão, sem que estes sejam efetivamente impressos. Você também pode utilizar uma porta IR, a qual é utilizada para conexões com impressoras que utilizam o protocolo Infrared Data Association (IrDA). As portas do tipo arquivo, UNC, NUL e IR somente estão disponíveis quando você opta por criar uma nova porta. Na lista de portas locais, por padrão, somente são listadas as portas Paralelas (LPTs) e Seriais (COMs).
- ◆ **Standard TCP/IP port (Porta padrão TCP/IP):** Este tipo de porta é utilizado para acessar impressoras conectadas diretamente à rede e configuradas com um número IP. Mostrarei um exemplo prático deste tipo de porta em um dos próximos exemplos.
- ◆ **AppleTalk printing devices:** Este tipo de porta é utilizada quando você tem clientes de rede baseados no Macintosh. Somente está disponível se o protocolo AppleTalk estiver instalado no servidor.
- ◆ **LPR port:** É utilizada para comunicação com impressoras instaladas em servidores no padrão UNIX, que utilizam o sistema LPD para gerenciamento da impressão. Este tipo de porta somente está disponível quando o Print Services for UNIX (Serviços de Impressão para Unix) estiver instalado.
- ◆ **Port for NetWare:** Utilizada por computadores que usam o Novell Netware. Só está disponível quando o protocolo NWLink e o Client Services for NetWare (Cliente de Serviços para Netware), estiverem instalados.

10. Dê um clique no botão Avançar para ir para a quarta etapa do assistente.

Na quarta etapa você deve escolher a marca e o modelo da impressora, cujo driver está sendo instalado. Na coluna da esquerda existe uma listagem dos fabricantes em ordem alfabética. Quando você seleciona um fabricante na coluna da esquerda, a coluna da direita exibe apenas os modelos do fabricante selecionado.

11. Na coluna da esquerda localize HP e dê um clique nesta opção para selecionar HP. Na coluna da esquerda serão exibidos todos os modelos de impressoras HP para os quais o CD do Windows Server 2003 possuí um driver.  
12. Na coluna da esquerda localize o modelo HP Deskjet 660C, e dê um clique sobre este modelo para marcá-lo, conforme indicado na Figura 7.6:

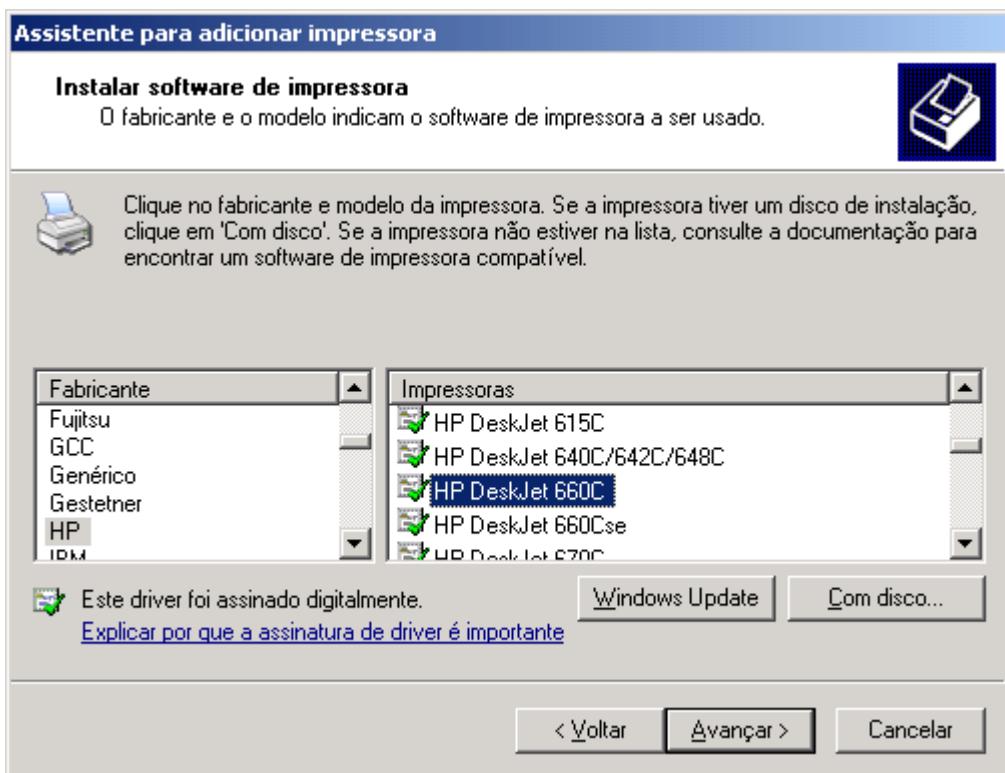


Figura 7.6 Instalando uma HP Deskjet 660C.

13. Dê um clique no botão Avançar para ir para a quinta etapa do assistente.  
14. Na quinta etapa, o Windows Server 2003 pede que você digite um nome para a Impressora. Esse nome é o nome que irá aparecer dentro da janela Impressoras e aparelhos de fax, depois que você tiver concluído a instalação.  
15. No campo Nome da impressora digite o seguinte: HP Deskjet 660 – Colorida - Gerência.  
16. Dê um clique no botão Avançar para ir para a sexta etapa do assistente.  
17. Na sexta etapa, você define se deseja, ou não, compartilhar a impressora. Por padrão vem marcada a opção Nome do compartilhamento, já com uma sugestão de nome para compartilhamento da impressora. Neste momento você não irá compartilhar a impressora. Para isso marque a opção Não compartilhar esta impressora.

**IMPORTANTE:** Você pode utilizar o botão Windows Update para exibir uma lista de drivers de dispositivo que podem ser descarregados do site do Microsoft Windows Update na Internet. Nessa lista, selecione o devido adequado para o dispositivo. Esta opção somente funcionará se você tiver alguma forma de conexão com a Internet. Utilize o botão Com disco..., para instalar o drive da impressora a partir de um CD-ROM ou disquete, ou de um compartilhamento de rede. Ao clicar neste botão será aberta uma janela para que você informe o local onde está disponível o driver da impressora. [www.jehobatista.com.br](http://www.jehobatista.com.br)

18. Dê um clique no botão Avançar para ir para a quinta etapa do assistente.
19. Na sétima etapa surge uma tela perguntando se você deseja imprimir uma página de teste. Caso você tenha uma impressora conectada, escolha Sim, para verificar se a impressora está funcionando corretamente. Caso contrário marque a opção Não.
20. Dê um clique em Avançar para ir para a última etapa do assistente, onde o Windows Server 2003 exibe um resumo das informações fornecidas nas diversas etapas, conforme indicado na Figura 7.7:

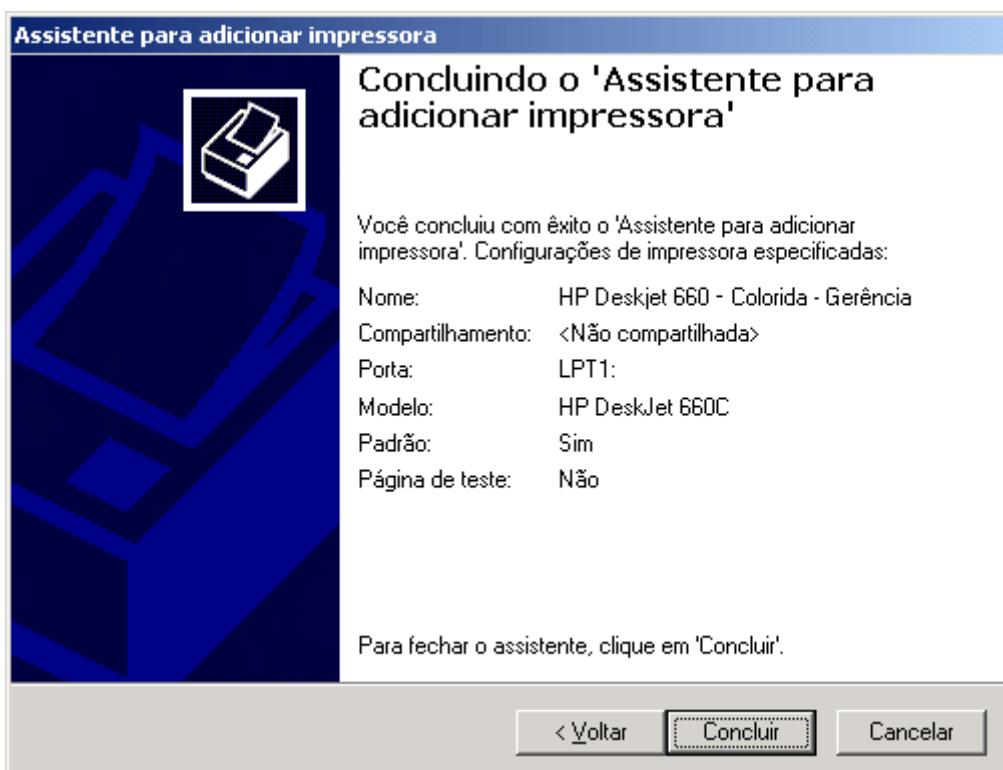


Figura 7.7 Etapa final do Assistente para adicionar impressora.

21. Caso esteja tudo OK, dê um clique no botão Concluir.

O Windows Server 2003 começa a copiar os arquivos necessários. Nesta etapa pode ser que você seja solicitado a colocar o CD do Windows Server 2003 no driver de CD-ROM, caso o Windows Server 2003 não encontre todos os arquivos necessários no disco rígido.

Após concluir a cópia dos arquivos, você estará de volta a janela Impressoras e Aparelhos de fax e a impressora HP Deskjet 660C (ou outra marca e modelo que você tenha instalado), já aparece na janela Impressoras, conforme indicado pela Figura 7.8:

**NOTA:** Caso você constate que existe alguma informação incorreta, você pode usar o botão Voltar para ir até a etapa onde foi fornecida a informação incorreta e corrigi-la.

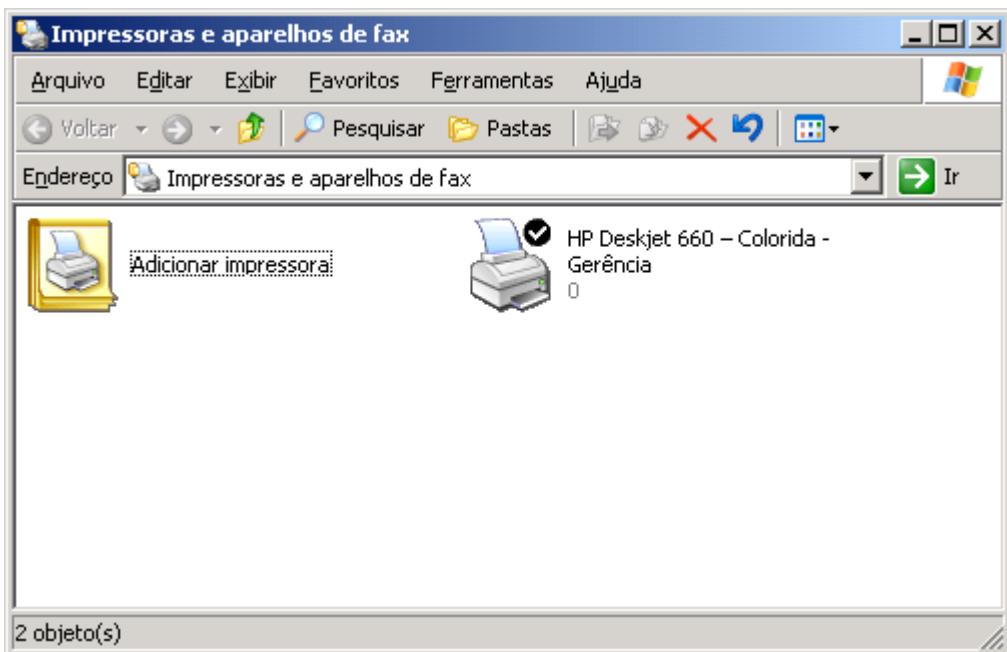


Figura 7.8 Impressora HP Deskjet 660C já aparecendo na janela Impressoras.

Observe que na janela de impressoras, no painel da esquerda já aparece uma série de comandos relacionados com a administração/gerenciamento de impressoras, conforme indicado na Figura 7.9:

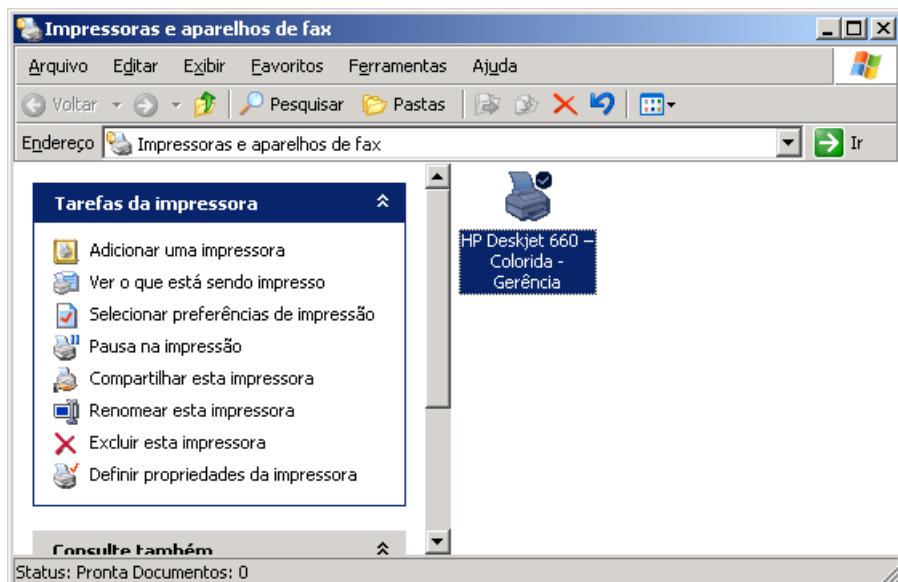


Figura 7.9 O painel Tarefas comuns.

Quando você clica em uma determinada impressora, são exibidos atalhos para diversas tarefas relacionadas com a impressora, tais como:

- ◆ Adicionar uma impressora.
- ◆ Ver o que está sendo impresso.
- ◆ Selecionar preferências de impressão.
- ◆ Pausa na impressão.

**NOTA:** No Windows XP foi introduzida uma funcionalidade bem interessante e bem útil, funcionalidade esta também disponível no Windows Server 2003. É um painel que pode ser exibido nas janelas do Meu computador, do Windows Explorer, na janela de Impressoras, no painel de controle e assim por diante. Este painel, exibido no lado esquerdo da janela, contém uma série de atalhos, relacionados às tarefas mais comuns da janela em questão. Por exemplo, na janela de impressoras, você pode exibir, no lado esquerdo, um painel com atalhos para as tarefas mais comuns, relacionadas com administração de impressoras. Para exibir este painel, na janela Impressoras e aparelhos de fax selecione o comando Ferramentas -> Opções de pasta... Será exibida a janela Opções de pasta. Clique na guia Geral. No grupo Tarefas, marque a opção Show common tasks in folders Mostrar tarefas comuns nas pastas e clique em OK.

- ◆ Compartilhar esta impressora.
- ◆ Renomear esta impressora.
- ◆ Excluir esta impressora.
- ◆ Definir propriedades da impressora.

Você aprenderá a executar estas diversas operações ao longo deste capítulo.

## Compartilhando uma impressora para uso através da rede.

Após ter instalado o driver da impressora, o próximo passo é compartilhar a impressora para que ele possa ser acessada através da rede, pelas estações de trabalho dos usuários. Claro que antes que os usuários começam a utilizar a impressora, é recomendado que você configure as permissões de acesso, mas este já é o assunto de um exemplo mais adiante.

Neste tópico você aprenderá a compartilhar um impressora, para que ela possa ser utilizada por outros computadores da rede. Depois mostrarei diferentes maneiras para você conferir que a impressora realmente foi compartilhada e está disponível para acesso através da rede.

Exemplo: Compartilhando a impressora HP Deskjet 660C, que foi instalada na lição anterior.

Para compartilhar uma impressora, siga os seguintes passos.

1. Faça o logon com um conta com permissões de Administrador ou com uma conta pertencente ao grupo Oper. de Impressão.
2. Utilize o comando Iniciar -> Impressoras e aparelhos de fax. Será exibida a lista das impressoras instaladas no seu computador.
3. Dê um clique na impressora a ser compartilhada, para seleciona-la. No nosso exemplo dê um clique na impressora “HP Deskjet 660 – Colorida – Gerência”.
4. No painel de opções do lado esquerdo da janela Impressoras e aparelhos de fax, dê um clique na opção Compartilhar esta impressora (para detalhes sobre como exibir o painel do lado esquerdo, consulte a nota do exemplo anterior). Você também pode clicar com o botão direito do mouse na impressora a ser compartilhada e, no menu de opções que é exibido, clicar na opção Compartilhamento. Usando qualquer uma destas opções, será exibida a janela com as propriedades da impressora, com a guia Compartilhamento já selecionada
5. Marque a opção Compartilhar esta impressora.
6. Digite um nome para o compartilhamento. De preferência um nome que seja indicativo da marca e modelo da impressora e do computador onde a impressora está instalada. Para o nome, digite hp666-col-geren. Sua janela deve estar conforme indicado na Figura 7.10.

**IMPORTANTE:** Quando for instalada uma nova impressora, sendo que já existe uma ou mais impressoras instaladas, o Windows Server 2003 exibirá uma tela a mais no assistente, perguntando se você deseja definir a impressora que está sendo instalada como a Impressora padrão (Default printer). No Windows Server 2003, o administrador pode ter diversas impressoras instaladas, porém somente uma é definida como padrão. A impressora padrão é aquela para a qual o Windows Server 2003 vai imprimir, a menos que seja explicitamente escolhida uma outra impressora. Você pode, facilmente identificar a impressora padrão na janela Impressoras, uma vez que esta é exibida com um sinalzinho de certo junto ao ícone da impressora.

**NOTA:** Se você estiver utilizando outra impressora, substitua HP Deskjet 660 – Colorida - Gerência, pelo nome da impressora que você estiver utilizando para acompanhar este exemplo.

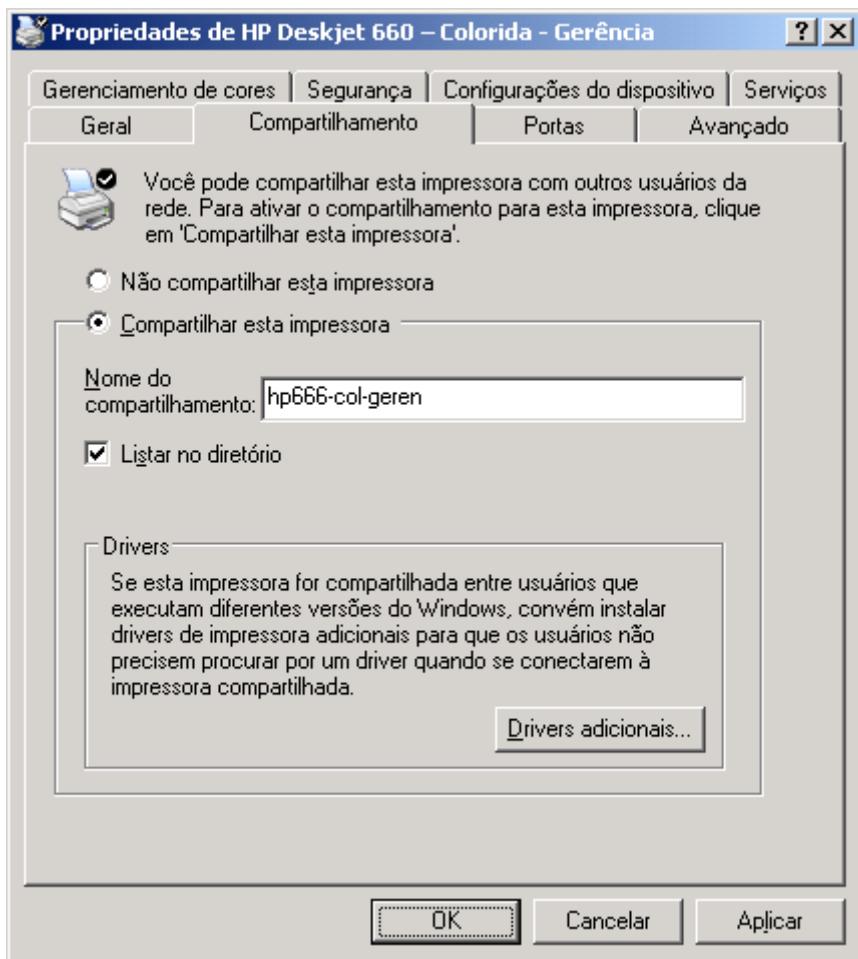


Figura 7.10 Definindo um nome para o compartilhamento.

7. Dê um clique OK para confirmar o compartilhamento da impressora HP Deskjet 660 – Colorida – Gerência, com o nome de compartilhamento hp666-col-geren. Como o nome de compartilhamento tem mais do que 8 caracteres, surge uma mensagem avisando que clientes mais antigos, como o MS-DOS não poderão acessar este compartilhamento. Clique em Sim para manter o nome de compartilhamento que foi definido e fechar a mensagem de aviso.

Você estará de volta a janela impressoras. Observe que aparece uma pequena mão “segurando” a impressora que acabou de ser compartilhada. Você está lembrado que uma essa pequena mão também surge quando compartilhamos uma pasta? A partir deste momento a impressora está compartilhada e pronta para ser acessada através da rede.

Agora você irá confirmar se a impressora realmente foi compartilhada com sucesso. Você tentará localizá-la usando o comando Iniciar -> Executar.

Para verificar se a impressora foi compartilhada com sucesso, faça o seguinte:

1. Faça o logon em um dos computadores da rede.
2. Clique em Iniciar -> Executar
3. No campo Abrir, digite \\nome-do-servidor-onde-está-a-impressora. Para o nosso exemplo digite \\srv-win2003 e clique em OK.

**NOTA:** Você pode utilizar o botão Drivers Adicionais... para, além do drive para o Windows Server 2003, instalar também drivers para outras versões do Windows: 95, 98, Me, 2000 e assim por diante. Esta opção é importante no caso de a impressora ser acessada por computadores que utilizam uma versão do Windows que não o Windows Server 2003. Por exemplo, se um computador com o Windows 95 for acessar uma impressora compartilhada em um computador com o Windows Server 2003 e no computador com o Windows Server 2003, o administrador tiver utilizado o botão Drivers Adicionais..., para adicionar o driver para o Windows 95, este driver será copiado, automaticamente, para o computador do cliente com o Windows 95, quando este computador tentar acessar a impressora. Se o driver não estiver disponível para ser copiado pela rede, ao instalar a impressora no computador com o Windows 95, deverá ser fornecido o CD de instalação do Windows 95 ou um CD com o driver da impressora.

**IMPORTANTE:** Observe que não existe um botão Permissões, para que sejam definidas permissões de compartilhamento para a impressora. Para impressoras compartilhadas não existe o conceito de permissões de compartilhamento, a exemplo do que ocorre com pastas compartilhadas. Para impressoras, existem permissões de acesso que podem ser definidas, conforme mostrarei mais adiante neste capítulo. Estas permissões

4. O Windows Server 2003 abre uma janela exibindo todos os recursos compartilhados disponíveis no servidor srv-win2003. Observe que um dos recursos disponíveis é a impressora hp660-col-geren. Você identifica que é uma impressora, por causa do ícone (uma pequena impressora) próxima ao nome. As pastas compartilhadas também são exibidas, com exceção dos compartilhamentos ocultos. Um compartilhamento torna-se oculto quando o nome do compartilhamento termina com um sinal de \$. Também são exibidas as Tarefas agendadas. Falarei sobre o agendamento de tarefas no Capítulo 8.

Com isso você comprovou que após o compartilhamento a Impressora está disponível para ser acessada através da rede.

Para reforçar: Todo recurso compartilhado em uma rede Microsoft Windows, pode ser acessada através do seu nome UNC – Universal Name Convention. O nome UNC inicia com duas barras invertidas, depois o nome do computador onde está o recurso, mais uma barra invertida e finalmente o nome do compartilhamento. No nosso exemplo temos \\srv-win2003\ hp660-col-geren, o que indica a impressora compartilhada com nome de compartilhamento hp660-col-geren, no computador srv-win2003.

5. Feche a janela srv-win2003.

Por exemplo, o comando a seguir, exibe uma lista dos recursos compartilhados (com exceção dos compartilhamentos ocultos), no servidor cujo nome é srv-win2003, conforme indicado na Figura 7.11.

**net view \\srv-win2003**

| Nome do compartilhamento | Tipo      | Usado como                            |
|--------------------------|-----------|---------------------------------------|
| Documentos               | Disco     | Documentos no computador microxp01    |
| hp660-col-geren          | Impressão | HP Deskjet 660 - Colorida - Gerência  |
| NETLOGON                 | Disco     | Compartilhamento do servidor de logon |
| Novos Documentos         | Disco     | Novos documentos para o projeto XYZ   |
| Programas                | Disco     | Programas compartilhados              |
| SYSVOL                   | Disco     | Compartilhamento do servidor de logon |

Figura 7.11 Usando o comando net view \\nome-do-servidor.

definem o tipo de acesso que cada usuário/grupo pode ter à impressora. Estas permissões são definidas na guia Security (Segurança), da janela de propriedades da impressora.

**NOTA:** A opção Listar no diretório (que vem selecionada por padrão) é utilizada para publicar informações sobre o compartilhamento da impressora no Active Directory. Ao marcar esta opção, serão publicadas informações sobre o compartilhamento e as características da impressora. Estas informações serão publicadas no Active Directory, o que irá facilitar a pesquisa se impressoras no Active Directory, conforme mostrarei mais adiante.

**NOTA:** Caso você tenha acesso a outro computador da rede, faça o logon como Administrador e acompanhe este exercício no outro computador. Para o nosso exemplo, srv-win2003 é o nome do computador onde foi instalada e compartilhada a impressora HP Deskjet 660 – Colorida – Gerência. Caso você tenha criado em um computador com outro nome, substitua srv-win2003 pelo nome do computador que você está utilizando.

**Dica:** Você também pode exibir uma listagem dos recursos compartilhados, disponíveis em um servidor, abrindo um Prompt de comando e executando o seguinte comando: `net view \\nome-do-servidor`

Agora é hora de definir as permissões de acesso à impressora. Mas este já é o assunto do próximo exemplo.

**NOTA:** Observe que ao lado do nome de compartilhamento hp660-col-geren, aparece o tipo Print (Impressora), indicando que esta é uma impressora compartilhada. Ao lado das pastas compartilhadas aparece o tipo Disk.

## Atribuindo permissões de acesso para a impressora.

Neste item mostrarei um exemplo prático de como definir permissões de acesso para uma impressora compartilhada. Também farei uma descrição detalhada dos diferentes níveis de permissão que podem ser definidos para o acesso a uma impressora. As permissões podem ser atribuídas a usuários ou a grupos. A exemplo da recomendação que foi feita para o caso de pastas compartilhadas, para impressoras compartilhadas também é recomendado sempre definir as permissões para grupos, o que simplifica e facilita a administração destas permissões.

Assim como é possível atribuir permissões para uma pasta compartilhada, é possível definir permissões de acesso para uma impressora compartilhada. As permissões definem quais os usuários que podem utilizar a impressora e qual o nível de permissão de cada usuário. Ao definir permissões para um grupo, os membros do grupo herdam as permissões. Se o usuário pertencer a mais de um grupo, a sua permissão efetiva será a soma das permissões atribuídas a todos os grupos aos quais ele pertence. Negar uma permissão de impressão tem precedência sobre todas as demais permissões. Por exemplo, se o usuário pertence a cinco grupos, grupos estes que tem diferentes permissões de acesso a uma impressora compartilhada. Se ele for incluído em um sexto grupo, o qual tem negada a permissão de acesso à impressora, a permissão efetiva do usuário será acesso negado, ou seja, o negar que ele herdou do sexto grupo, tem precedência sobre todas as demais permissões que ele herdou dos demais grupos aos quais ele pertence.

Quando uma impressora é instalada em uma rede, são atribuídas permissões de impressão padrão, as quais permitem que todos os usuários imprimam e que grupos selecionados gerenciem a impressora, documentos enviados a elas ou ambos. Por padrão é definida a permissão Print (Imprimir) para o grupo Everyone (Todos); a permissão Print (Imprimir), Manage Documents (Gerenciar Documentos) e Manage Printers (Gerenciar Impressoras) para os grupos locais do domínio Administrators (Administradores), Server Operators (Operadores de Servidores) e Print Operators (Operadores de Impressão). Também é adicionada permissões totais para o usuário dono da impressora, que é o usuário que estava logado quando a impressora foi instalada. Como a impressora está disponível, por padrão, para todos os usuários na rede (permissão Imprimir para o grupo Todos), convém limitar o acesso de algumas pessoas atribuindo permissões de impressoras específicas. Por exemplo, você pode conceder a permissão Print (Imprimir) a todos os usuários não administrativos de um departamento e as permissões Print (Imprimir) e Manage Documents (Gerenciar documentos) somente para os gerentes. Desse modo, todos os usuários e gerentes poderão imprimir documentos, mas somente os gerentes poderão alterar o status de impressão de qualquer documento enviado à impressora. (gerenciar documentos).

O Windows fornece três níveis de permissões de segurança de impressão: Print (Imprimir), Manage Printers (Gerenciar impressoras) e Manage Documents (Gerenciar documentos). Quando várias permissões são atribuídas a um grupo de usuários, as permissões menos restritivas se aplicam, ou seja, a permissão efetiva do usuário é a soma das permissões atribuídas aos grupos aos quais ele pertence, mas as permissões atribuídas diretamente a sua conta. No entanto, se a opção Negar tiver sido atribuída, ela terá precedência sobre qualquer permissão, a exemplo do que acontece com as permissões de compartilhamento e com as permissões NTFS. Existem três níveis de permissão, conforme detalhado a seguir:

- ◆ **Print (Imprimir):** Permite ao usuário conectar-se à Impressora e imprimir documentos, pausar, reiniciar e continuar a impressão dos documentos por ele enviados para a impressora. Quando um usuário envia um documento para a impressora, o usuário torna-se o dono daquele documento, por isso que ele pode

administrar os documentos por ele enviados. Esta permissão normalmente atribuída para aqueles usuários que simplesmente precisam enviar documentos para a impressora. Por padrão, quando uma nova impressora é instalada, a permissão Print (Imprimir) é atribuída ao grupo Everyone (Todos), conforme descrito anteriormente.

- ◆ **Manage Documents (Gerenciar documentos):** Tem todas as permissões atribuídas a permissão Print (Imprimir), mais Controlar a impressão de todos os documentos (enviados por qualquer usuário) e também pausar, reiniciar e continuar a impressão de qualquer documento enviado por qualquer usuário. Normalmente atribuída para aquele usuário que administra a impressora, resolvendo problemas de impressão, mas sem permissões para alterar propriedades e permissões da impressora. Quando a permissão Manage Documents (Gerenciar documentos) for atribuída a um usuário, ele não poderá acessar documentos existentes que estejam aguardando para serem impressos, na fila de impressão. A permissão se aplicará somente aos documentos enviados para a impressora depois que a permissão tiver sido atribuída ao usuário.
- ◆ **Manage Printers (Gerenciar impressoras):** Todas as permissões de Print (Imprimir) e Manage documents (Gerenciar documentos), mais permissões para cancelar a impressão de todos os documentos pendentes, compartilhar a impressora, alterar as propriedades da impressora, eliminar a impressora e alterar as permissões de impressão. Normalmente atribuída a um usuário que deve ter poderes completos na administração da impressora, inclusive podendo removê-la do sistema. Por padrão, os membros dos grupos Administrators (Administradores), Print Operators (Operadores de Cópia) e Server Operators (Operadores de Servidores) têm esta permissão.

É importante salientar, que as permissões para o uso da impressora tem efeito tanto localmente, quanto para o acesso através da rede. Além disso caso um usuário pertença a mais de um grupo que possui permissões para a impressora, a sua permissão efetiva é a soma das permissões. Também um permissão Negar tem prioridade sobre Permitir (sei que estou repetindo isso pela terceira vez, mas o objetivo é exatamente fazer com que o amigo leitor não esqueça destes detalhes). Por exemplo se o usuário jsilva pertence aos grupos Contabilidade e Marketing. O grupo Contabilidade possui permissão Print (Imprimir), já o grupo Marketing tem permissão Deny Print (Negar Imprimir), então a permissão efetiva do usuário jsilva será Deny Print (Negar Imprimir).

Agora é hora de praticar um pouco e atribuir algumas permissões para a impressora que foi instalada no exemplo anterior e depois você irá testar as permissões atribuídas.

Exemplo: Atribuindo permissões para a impressora HP Deskjet 660 – Colorida - Gerência, instalada anteriormente.

1. Faça o logon com uma conta com permissão de Administrador, ou com uma conta do grupo Operadores de Impressão ou do grupo Operadores de Servidores, no servidor onde está instalada a impressora..
2. Selecione o comando Iniciar -> Impressoras e aparelhos de fax.

Será exibida a janela Impressoras e aparelhos de fax, na qual é mostrada uma lista das impressoras instaladas no seu computador.

3. Dê um clique com o botão direito do mouse na impressora para a qual você deseja definir as permissões.
4. No menu que surge, dê um clique na opção Propriedades. Será exibida uma janela com as propriedades da impressora e a guia Geral selecionada por padrão.
5. Dê um clique na guia Segurança. Será exibida a janela da Figura 7.12:

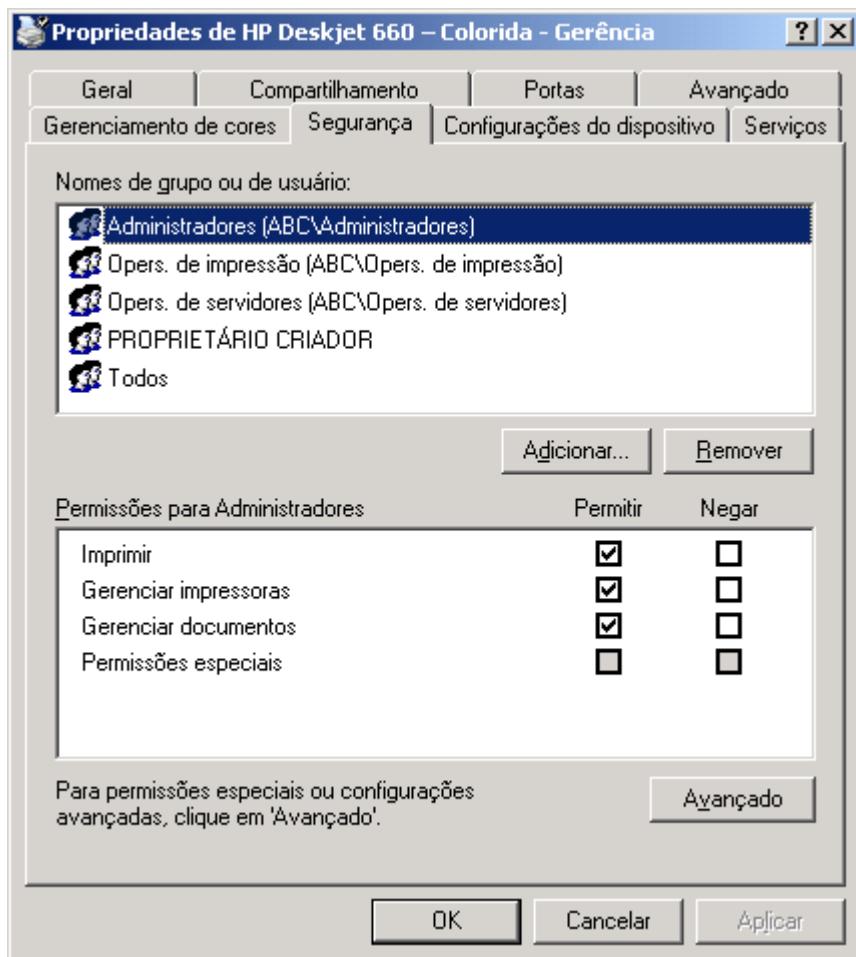


Figura 7.12 Através desta guia, você define as permissões de acesso à impressora.

Nesta guia você irá definir as permissões para a impressora. Vou eliminar todas as permissões que foram automaticamente atribuídas pelo Windows Server 2003, com exceção da permissão para o grupo Administradores.

6. Dê um clique no grupo Todos e depois um clique no botão Remover. Repita a operação com o usuário PROPRIETÁRIO CRIADOR, e para os grupos Oper. de Cópias e Oper. de Servidores.

A janela de permissões deve ter ficado conforme indicado na Figura 7.13.

Agora você definirá permissões de acesso Imprimir, apenas para os usuários user01 e user02 (utilize nomes de usuários do domínio no qual você está trabalhando ou do servidor local no qual você estiver trabalhando). Não darei permissão para o usuário user3. O procedimento para definir permissões para uma impressora é idêntico ao procedimento para definir permissões de compartilhamento ou permissões NTFS. Você clica no botão Adicionar, seleciona um ou mais usuários/grupos e depois define as permissões para cada usuário/grupo que foi adicionado.

7. Clique no botão Adicionar. Será exibida a janela Selecionar Usuários, Computadores ou Grupos, janela esta que você aprendeu a utilizar nos Capítulos 4 e 6.

**IMPORTANTE:** Observe que por padrão o Windows Server 2003 já adiciona permissões para uma série de grupos. O grupo Administradores, o usuário PROPRIETÁRIO CRIADOR (que é o usuário que estava logado e instalou a impressora), o grupo Todos e os grupos Oper. de Cópias e Oper. de Servidores.

**NOTA:** Ao invés de utilizar o botão direito do mouse, você também pode clicar na impressora para marcar-la e no painel de opções no lado esquerdo

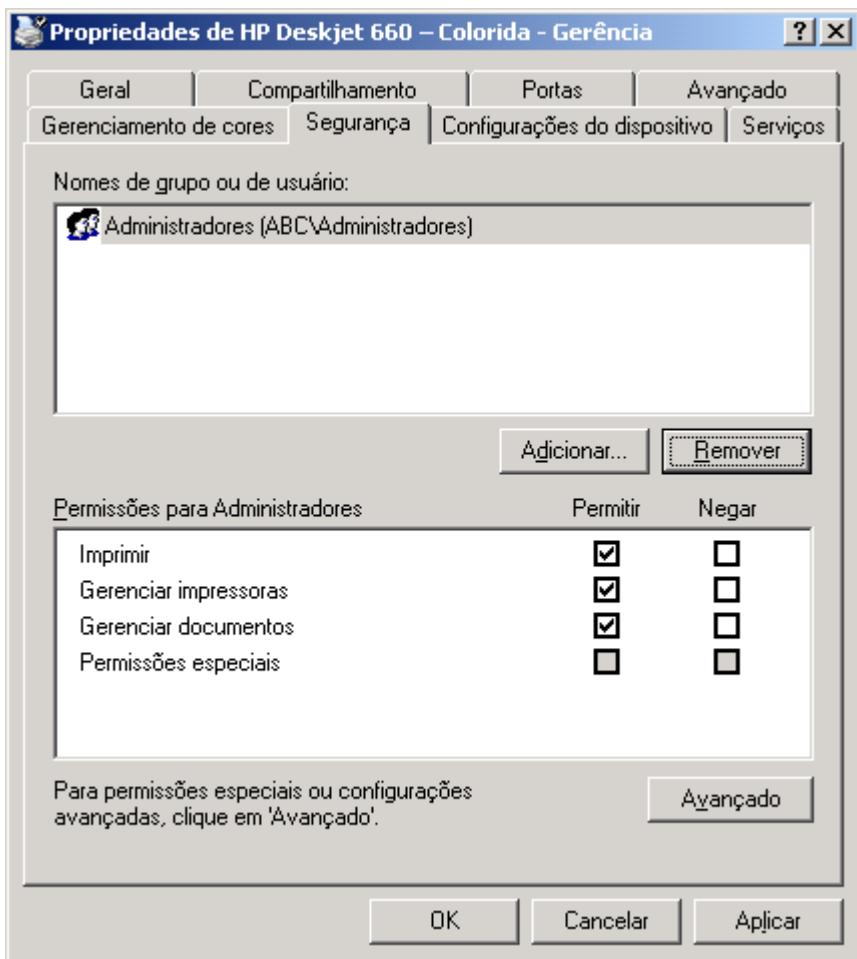


Figura 7.13 Mantendo as permissões padrão apenas para o grupo Administrators.

8. Digite o nome dos usuários que receberão permissões. Separe os nomes por ponto e vírgula, conforme indicado na Figura 7.14.

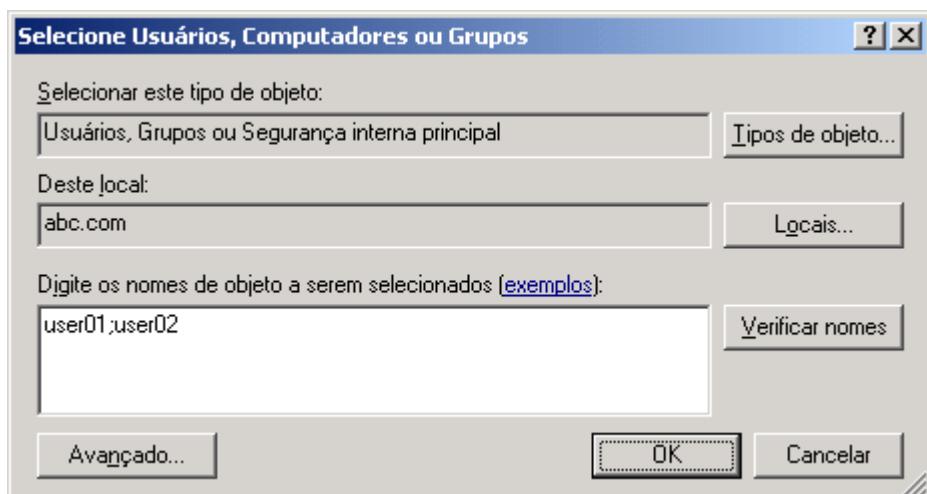


Figura 7.14 Adicionando os usuários user01 e user02.

9. Dê um clique no botão OK e você estará de volta a guia Segurança.

da janela impressoras, dar um clique na opção Definir propriedades da impressora. Será aberta a janela de propriedades da impressora, com a guia Geral selecionada. Dê um clique na guia Segurança e será exibida a janela indicada na Figura 7.12.

Além de adicionar os dois usuários, deve ser configurado o nível de acesso dos usuários. Vou definir uma permissão Imprimir para os dois usuários.

10. Dê um clique em user01 para marcá-lo. Na parte do meio da janela, onde está a lista de permissões, deixe marcada somente a opção Imprimir, da coluna Permitir.
11. Repita a operação para o usuário user02.
12. Dê um clique no botão OK para fechar a janela de propriedades da impressora a aplicar as permissões recém configuradas.
13. Feche a janela de impressoras impressoras.

Em resumo: Para definir permissões de impressão siga os seguintes passos:

1. Acesse a janela de impressoras.
2. Acesse as propriedades da impressora desejada.
3. Clique na guia Segurança.
4. Defina as permissões de impressão.

Agora é hora de testar se as permissões recém definidas já entraram em vigor.

Exemplo - Testando as permissões de impressão definidas anteriormente.

1. Se estiver logado como Administrador faça o logoff do usuário Administrador.
2. Faça o logon como usuário user01.
3. Acesse a janela de impressoras.
4. Localize a impressora para a qual você atribuiu permissões no exercício anterior, dê um clique com o botão direito do mouse na impressora e no menu que surge escolha propriedades. Será aberta a janela de propriedades da impressora.
5. Dê um clique na guia Segurança. Observe que as opções aparecem desabilitadas (acinzentadas), isto é, o usuário user01 não consegue alterá-las, conforme indicado na Figura 7.15. Isto acontece porque o usuário user01 somente tem permissão Imprimir, a qual não permite que ele altere as permissões.

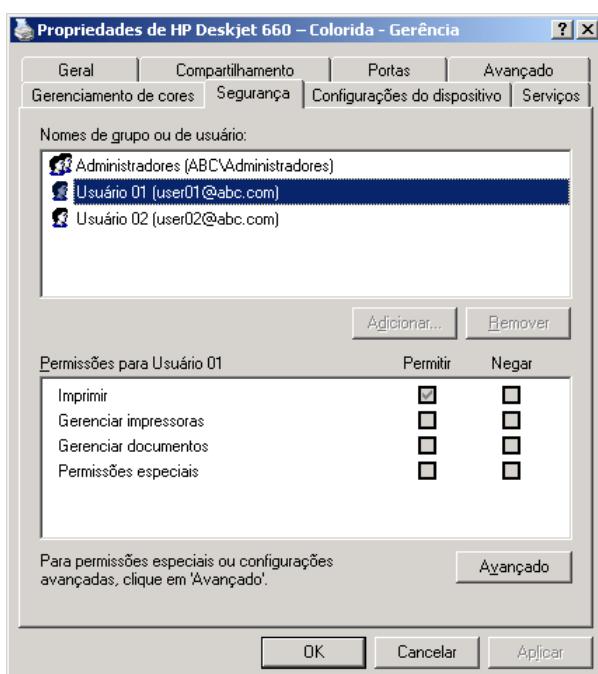


Figura 7.15 Permissões que não podem ser alteradas pelo usuário user1.

Por que está acontecendo isso ? Pensando ...

Muito simples. Isso acontece porque você está logado como user02 e este usuário possui nível de permissão apenas para imprimir documentos – permissão Print (Imprimir). Para que ele pudesse alterar as Permissões de Impressão, ele precisaria de um nível de permissão Manage Printers (Gerenciar impressoras).

6. Dê um clique no botão OK para fechar a janela de propriedades da impressora.
7. Feche a janela de impressoras
8. Faça o logoff do usuário user02.

Teste: Faça o logon como usuário user03. Tente acessar as propriedades da impressora para o qual somente os usuários user01 e user02 tem permissão. Você deverá receber uma mensagem de acesso negado. Tente imprimir um documento nesta impressora. Novamente você receberá uma mensagem de acesso negado, pois o usuário user3 não tem nenhum nível de permissão na impressora do nosso exemplo, nem mesmo permissão para imprimir documentos na impressora.

Nunca é demais salientar que as permissões de impressão tem efeito tanto para o acesso localmente, no servidor onde está instalada a impressora, quanto para o acesso através da rede, usando o compartilhamento da impressora.

## Acessando uma impressora compartilhada através da rede.

Após uma impressora ter sido compartilhada, esta pode ser acessada através da rede, pelas estações de trabalho dos usuários que tem permissão para acessar a impressora. Para que não seja necessário acessar a impressora manualmente, cada vez que o usuário necessitar dela, o usuário pode fazer com que a impressora apareça na pasta impressoras como se fosse uma impressora local, mas na verdade na hora de imprimir, o trabalho é enviado para a impressora compartilhada no servidor. A impressora precisa ser instalada uma única vez, depois passa a estar disponível sempre que for necessária.

Existem três opções para acessar uma impressora compartilhada em um servidor da rede:

- ◆ A opção Adicionar impressora da janela impressoras
- ◆ A opção Meus locais de rede da janela Meu computador.
- ◆ O comando Iniciar -> Executar.

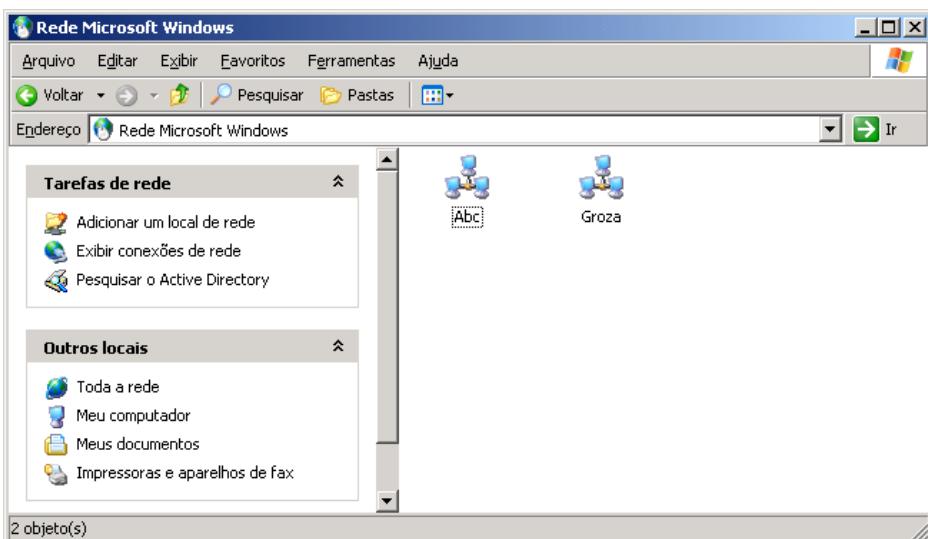
Nesta lição mostrarei como um usuário, em sua estação de trabalho na rede, pode acessar a impressora hp660-col-geren no servidor srv-win2003. Mostrarei como fazer este acesso, utilizando os três métodos descritos anteriormente. Lembre que a impressora HP Deskjet 660C foi instalada em um servidor da rede e compartilhada com o nome de hp660-col-geren.

Método 1 – Usando a opção Meus locais de rede, para acessar uma impressora compartilhada através da rede.

1. Faça o logon com uma conta com permissão de administrador na estação de trabalho a partir do qual você deseja acessar a impressora compartilhada na rede.
2. Abra o Meu computador.
3. No painel de opções que aparece à esquerda, dê um clique na opção Meus locais de rede.

**IMPORTANTE:** Um caso especial é o caso do usuário Administrador ou de qualquer usuário que pertença ao grupo Administradores. Mesmo que um usuário do grupo Administradores não possua nenhuma permissão de acesso à impressora, ele poderá ter acesso a guia segurança e atribuir permissões para si mesmo. Isso é feito para que os Administradores possam ter controle sobre todos os recursos da rede.

- Será exibida a janela Meus locais de rede. Dê um clique na opção Toda a rede (no painel de opções do lado esquerdo).
- Serão exibidas algumas opções. Dê um clique duplo na opção Rede Microsoft Windows.
- Será exibida uma lista dos domínios que fazem parte da sua rede, conforme exemplo da Figura 7.16.



**NOTA:** Caso você tenha acesso a outro comutador da rede, faça o logon como Administrador e acompanhe este exercício no outro computador. **srv70-290** (para este exemplo) é o nome do computador onde foi instalada e compartilhada a impressora HP Deskjet 660C. Caso você tenha criado em um computador com outro nome, substitua **srv70-290** pelo nome do computador que você está utilizando.

Figura 7.16 Relação de domínios da rede.

- O próximo passo é acessar o domínio onde está o servidor com a impressora compartilhada que você quer acessar. Para exibir os recursos de um determinado domínio, basta dar um clique duplo no domínio.
- Será exibida a lista de computadores do domínio. Dê um clique duplo no domínio ABC. Na lista de servidores que é exibida, dê um clique duplo no computador **srv70-290**, que é o computador onde está compartilhada a impressora que a ser acessada.
- Será aberta uma janela com todos os recursos compartilhados do computador **srv70-290**, conforme indicado na Figura 7.17:

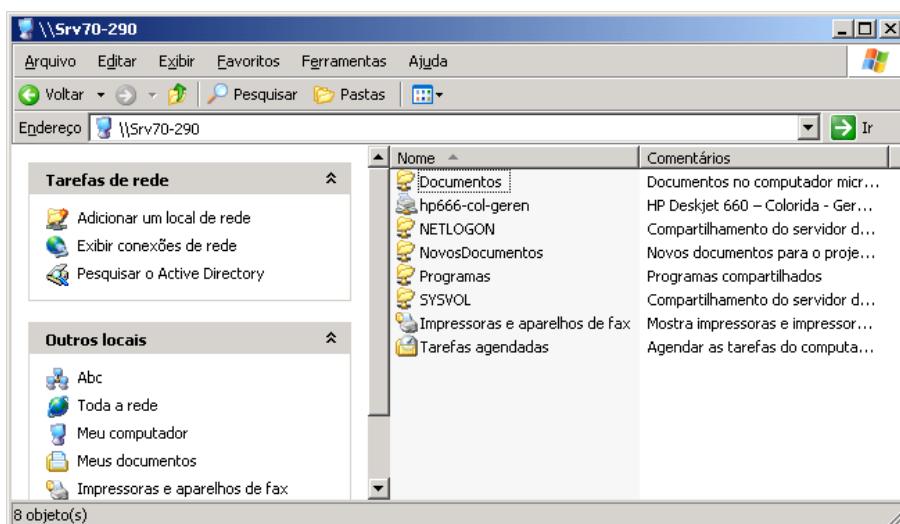


Figura 7.17 Lista de recursos compartilhados em **srv70-290**

10. Clique com o botão direito do mouse na impressora hp660-col-geren. No menu de opções que surge dê um clique na opção Conectar-se... Neste momento o computador que você está utilizando faz a conexão com o servidor srv70-290 e copia e instala o driver para a impressora HP Deskjet 600C do servidor para a estação de trabalho do cliente. Essa operação pode demorar alguns instantes, principalmente se o servidor estiver em uma rede remota, conectada através de um link de WAN.

Pronto, a impressora será instalada na estação de trabalho do usuário como se fosse uma impressora local. A impressora é instalada com o nome de HP Deskjet 660 – Colorida – Gerência em srv-70-290. Observe que abaixo da figura da impressora aparece a figura de um cabo de rede, para indicar que na verdade é uma impressora da rede

11. Selecione o comando Iniciar -> Impressoras e aparelhos...
12. Observe que a impressora já foi instalada. Sabemos que essa é uma impressora da rede pelo ícone com a figura de um cabo de rede ligado a impressora.

Agora toda vez que um usuário fizer o logon na sua estação de trabalho e imprimir na impressora instalada neste exemplo, a impressão será enviada para a impressora compartilhada localizada no servidor srv70-290. Além disso as permissões que foram definidas continuam valendo. Observe que, do ponto de vista do usuário, é como se fosse uma impressora local, porém, na prática, a impressora está conectada com a impressora compartilhada no servidor.

13. Feche a janela de impressoras.

Agora você aprenderá a utilizar os outros dois métodos, para acessar uma impressora compartilhada na rede.

Método 2 – Usando o comando Iniciar -> Executar, para acessar uma impressora compartilhada através da rede.

1. Faça o logon com uma conta com permissão de administrador na estação de trabalho a partir do qual você deseja acessar a impressora compartilhada na rede.
2. Selecione o comando Iniciar -> Executar.
3. Será aberta a janela Executar. No campo Abrir digite: \\srv70-290 e clique no botão OK. Lembre: srv70-290 é o nome do servidor onde está a impressora compartilhada que será acessada.

Será aberta uma janela com todos os recursos compartilhados no computador srv70-290.

4. Localize a impressora que você quer acessar, clique com o botão direito do mouse neste impressora e no menu que é exibido dê um clique na opção Conectar...

Neste momento o computador que você está utilizando faz a conexão com o servidor srv-win2003 e copia e instala o driver para a impressora HP Deskjet 600C do servidor para a estação de trabalho do cliente. Essa operação pode demorar alguns instantes, principalmente se o servidor estiver em uma rede remota, conectada através de um link de WAN.

5. Para conferir se a impressora foi realmente instalada, acessa a pasta impressoras e observe que a impressora já está disponível. Após o nome da impressora, aparece: em srv70-290, informando que a impressora está compartilhada no computador srv70-290.

---

**NOTA:** Se a estação de trabalho estiver com uma versão do Windows para a qual não existe driver disponível no servidor onde a impressora está compartilhada, o Windows solicita que seja inserido o CD-ROM de instalação. Isto acontece quando o Windows não consegue copiar o driver da impressora diretamente do servidor onde a impressora está compartilhada.

---

**NOTA:** Caso você tenha acesso a outro comutador da rede, faça o logon como Administrador e acompanhe este exercício no outro computador. srv70-290 é o nome do computador onde foi instalada e compartilhada a impressora HP Deskjet 660C. Caso você tenha criado em um computador com outro nome, substitua srv70-290 pelo nome do computador que você está utilizando.

---

### Método 3 – Usando o Assistente para adicionar uma nova impressora.

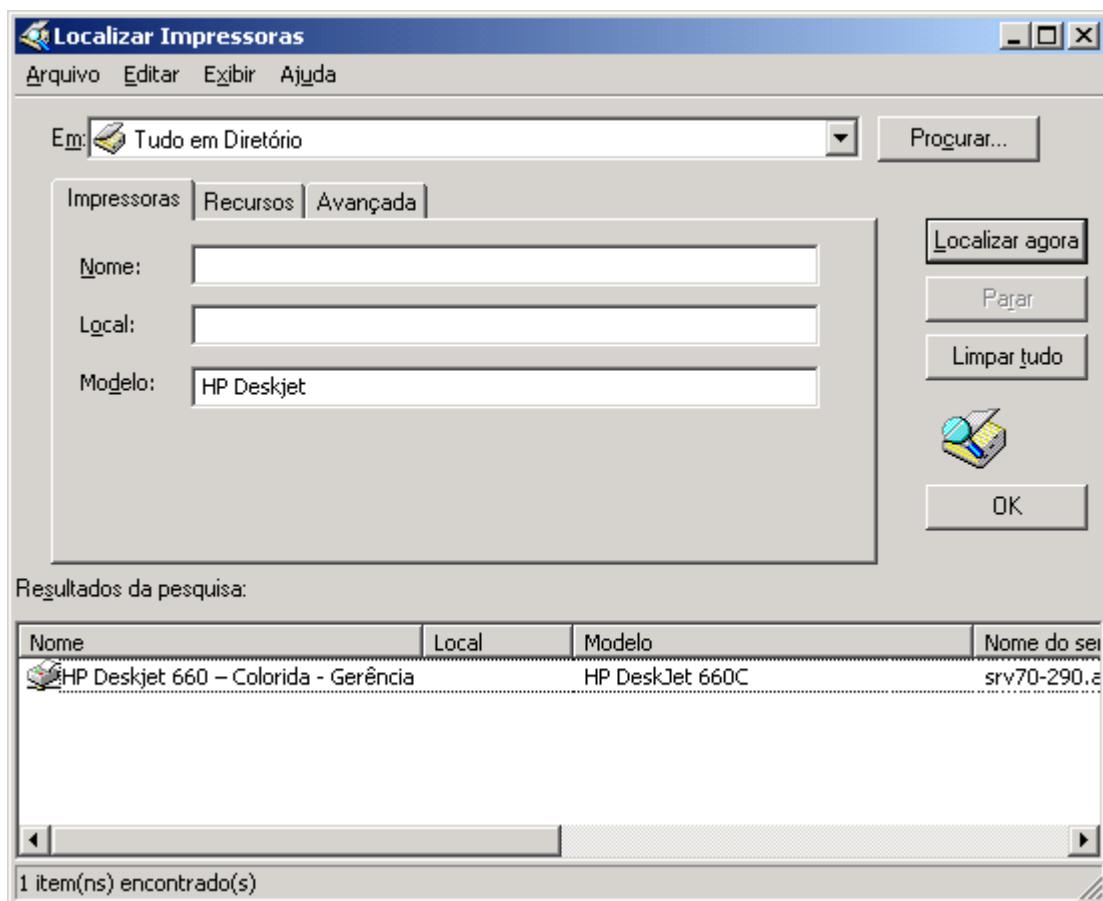
1. Faça o logon com uma conta com permissão de administrador na estação de trabalho onde você deseja instalar a impressora compartilhado no servidor srv70-290.
2. Abra a janela de impressoras.
3. No painel da esquerda, no grupo de opções Tarefas da impressora, dê um clique na opção Adicionar uma impressora. Será exibida a tela inicial do Assistente para adicionar impressora.
4. Dê um clique no botão Avançar, para ir para a próxima etapa do assistente.
5. Nesta etapa você deve informar se a impressora que está sendo adicionada é uma impressora instalada localmente ou se é uma impressora de rede. Marque a opção Uma impressora de rede, ou uma impressora conectada a outro computador.
6. Dê um clique no botão Avançar, para ir para a próxima etapa do assistente.

Nesta etapa são exibidas diversas opções para informar o caminho para a impressora a ser acessada:

- ◆ **Localizar uma impressora no diretório:** Se você marcar esta opção e clicar no botão Próximo, será exibida uma listagem com todos os computadores da domínio, nos quais tem pelo menos uma impressora compartilhada. Ao clicar no sinal de +, ao lado do nome do computador, serão exibidas as impressoras compartilhadas. Para acessar uma destas impressoras, basta clicar para marca-la.
  - ◆ **Conectar-se à impressora....:** Podemos utilizar esta opção para digitar diretamente o caminho da impressora, no padrão UNC: \\nomecomputador\namecompartilhamento.
  - ◆ **Conectar-se à uma Impressora na Internet ou em uma rede doméstica ou no escritório:** Esta opção é utilizada para conectar-se a uma impressora através da Internet, usando um endereço da impressora, como por exemplo: <http://abc.com.br/printers/laser01>.
7. Marque a opção Localizar impressora no diretório e dê um clique no botão Avançar, para ir para a próxima etapa do assistente.
  8. Será aberta a janela Localizar Impressoras. Esta é a janela para pesquisa de impressoras no Active Directory. Somente estão disponíveis para pesquisa as impressoras que ao serem compartilhadas, tiveram a opção Listar no diretório marcada. Você pode fazer uma pesquisa por nome, localização ou modelo, desde que estes campos estejam corretamente preenchidos nas propriedades da impressora, conforme mostrarei nos próximos exemplos.
  9. Por exemplo, no campo Modelo digite HP Deskjet e clique no botão Localizar Agora. Serão localizadas as impressoras que atendem ao critério especificado (modelo = HP Deskjet), conforme indicado na Figura 7.18:

**Dica: Observe que usar o comando Executar é muito mais rápido que navegar pelas opções da janela Meus locais de rede. O único inconveniente do comando Executar é que o usuário tem que saber o nome do servidor onde a impressora está compartilhada, o que muitas vezes, na prática, não acontece. Nestas situações é mais fácil para o usuário navegar pelas opções do domínio (ou pesquisar no Active Directory, conforme mostrarei mais adiante).**

**IMPORTANTE:** Pode parecer que não existe diferença entre uma "Impressora de rede" e uma "Impressora conectada a outro computador". Mas existe sim diferenças. Uma Impressora de rede é uma impressora que tem instalada uma placa de rede e é ligada diretamente na rede, através desta placa de rede, tendo inclusive sido configurada com um endereço IP. Uma impressora de rede não é ligada diretamente a nenhum servidor. Já uma impressora conectada a outro comutador, é uma impressora ligada na porta paralela (ou em outra porta, como por exemplo Serial ou USB) de um servidor da rede. Esta impressora passa a estar acessível pela rede, quando ela é compartilhada.



**Figura 7.18 Pesquisando a impressora no Active Directory.**

10. Clique na impressora a ser instalada e depois clique em OK.
11. Você estará de volta ao assistente de instalação, na etapa que pergunta se você deseja definir esta impressora como a impressora padrão. Marque Sim para defini-la como impressora padrão ou Não caso não queira defini-la como impressora padrão.
12. Clique em Avançar, para seguir para a próxima etapa do assistente.
13. Você estará na etapa final do assistente. Caso queira fazer alguma alteração utilize o botão Voltar. Clique em Concluir para instalar a impressora.
14. A impressora é instalada e passa a estar disponível na pasta impressoras.

## Administrando trabalhos enviados para uma impressora.

Muito bem, você instalou a impressora e a compartilhou no servidor. Você também aprendeu como fazer para que os clientes possam conectar-se com uma impressora compartilhada no servidor. Agora os usuários começarão a enviar os seus trabalhos de impressão. O próximo passo é entender como o Windows Server 2003 trata os trabalhos que enviados para a impressora, uma vez que diversos trabalhos podem ser enviados ao mesmo tempo. Pode acontecer de um trabalho ainda não ter sido concluído e um novo trabalho chegar para impressão. O Windows Server 2003 adota o seguinte procedimento: a medida que as solicitações de impressão vão sendo enviadas, elas vão sendo colocadas em uma fila de impressão, de tal forma que serão impressas conforme a ordem de chegada e levando em consideração a prioridade de cada trabalho.

Esta fila de documentos para impressão pode ser gerenciada. Um usuário, com permissão Gerenciar documentos, pode realizar uma série de ações sobre os documentos que estão em uma fila de impressão. É possível alterar a ordem dos documentos na fila, eliminar documentos da fila, interromper a impressão de um documento e retomá-la novamente, além de cancelar todos os documentos que estão na fila.

Neste item mostrarei como realizar estas tarefas, através de exemplos práticos. Utilizarei a impressora HP Deskjet 660C instalada em um dos exemplos anteriores. Apenas para recordar, instalei esta impressora no servidor com o nome srv70-290. Caso você esteja utilizando uma impressora diferente e um computador com nome diferente, utilize-os para o acompanhamento dos exercícios.

É hora de praticar um pouco e ver, através de exemplos, como gerenciar documentos que estão em uma fila de impressão.

Exemplo: Gerenciando documentos que estão em uma fila de impressão.

**NOTA:** Conforme mostrarei mais adiante, é possível instalar uma mesma impressora duas vezes, definindo compartilhamentos e permissões diferentes para cada instalação. O resultado prático é que o administrador tem condições de definir prioridades diferentes, para diferentes grupos de usuários. Mostrarei estas configurações através de um exemplo prático mais adiante.

1. Faça o logon com uma conta de usuário que tem a permissão Gerenciar documentos, na impressora que será utilizada neste exemplo.
2. Abra a janela de impressoras.
3. Na janela impressoras, dê um clique duplo na impressora onde está a fila de impressão a ser gerenciada. Será exibida uma janela semelhante a indicada na Figura 7.19, onde aparecem uma série de documentos esperando para serem impressos, ou seja, documentos que estão na fila de impressão.

Observe, na Figura 7.19, que existem várias colunas de informação: O nome do documento, o nome do usuário (nome de logon) que enviou o documento para impressão, o status da impressão, o número de páginas, o tamanho e a data e hora de envio.

4. Para excluir um documento da fila de impressão, basta dar um clique com o botão direito do mouse no documento a ser excluído. No menu de opções que é exibido, clique em Cancelar. O Windows pede uma confirmação, se você realmente deseja excluir o documento da fila de impressão. Clique no botão Sim para confirmar a exclusão do documento, da fila de impressão.

**NOTA:** Para os exemplos desta lição, enviei uma série de documentos para a impressora, de tal forma que fosse possível ver uma fila de documentos a serem impressos. A maneira mais rápida de enviar vários documentos de uma só vez é selecionar vários documentos, utilizando o Windows Explorer ou o Meu computador, clicar com o botão direito do mouse na seleção e no menu que aparece clicar em Imprimir. Todos os arquivos selecionados serão enviados para a impressora padrão.

| HP Deskjet 660 - Colorida - Gerência        |            |               |         |                    |                    |       |  |
|---|------------|---------------|---------|--------------------|--------------------|-------|--|
| Nome do documento                           | Status     | Proprietário  | Páginas | Tamanho            | Enviado            | Porta |  |
| CompraramWordAvançado.txt - Bloco de notas  | Imprimindo | Administrador | 1       | 1004 bytes/1,03 KB | 13:31:24 14/2/2004 | LPT1: |  |
| DicasCertificacoes.txt - Bloco de notas     |            | Administrador | 1       | 3,72 KB            | 13:31:25 14/2/2004 |       |  |
| divulga_excel_120.txt - Bloco de notas      |            | Administrador | 1       | 2,64 KB            | 13:31:25 14/2/2004 |       |  |
| elogios no site.txt - Bloco de notas        |            | Administrador | 7       | 33,1 KB            | 13:31:26 14/2/2004 |       |  |
| Endereços de Simulados.txt - Bloco de notas |            | Administrador | 1       | 2,98 KB            | 13:31:27 14/2/2004 |       |  |
| enquete.txt - Bloco de notas                |            | Administrador | 1       | 1,51 KB            | 13:31:27 14/2/2004 |       |  |
| entrega464.txt - Bloco de notas             |            | Administrador | 1       | 5,84 KB            | 13:31:27 14/2/2004 |       |  |
| entrega858.txt - Bloco de notas             |            | Administrador | 1       | 4,96 KB            | 13:31:27 14/2/2004 |       |  |
| enviaEnderecos.txt - Bloco de notas         |            | Administrador | 2       | 9,98 KB            | 13:31:29 14/2/2004 |       |  |
| Envio de CD.txt - Bloco de notas            |            | Administrador | 1       | 2,57 KB            | 13:31:29 14/2/2004 |       |  |
| final.txt - Bloco de notas                  |            | Administrador | 1       | 3,71 KB            | 13:31:30 14/2/2004 |       |  |
| Exclusion List.txt - Bloco de notas         |            | Administrador | 1       | 1,78 KB            | 13:31:30 14/2/2004 |       |  |

Figura 7.19 Documentos na fila de impressão.

5. Para pausar um documento, basta dar um clique com o botão direito do mouse no documento e no menu que surge clicar em Pausar. A impressão do documento será suspensa até que você clique novamente com o botão direito do mouse sobre o documento e no menu que surge, clique na opção Reiniciar.

Quando um documento é enviado para a impressora, existe uma prioridade associada com cada documento. Esta prioridade é baseada no usuário que enviou o documento. Conforme mostrarei mais adiante é possível dar prioridades maiores para determinados usuários ou grupos, com isso as impressões enviadas por estes usuários/grupos serão colocadas no início da fila de impressão, a medida que os trabalhos de impressão forem sendo enviados para a impressora. Documentos de prioridade maior são impressos antes, independente da ordem de chegada. Você pode fazer com que um documento do final da fila seja impresso antes do que os demais, simplesmente aumentando a prioridade deste documento.

6. Para aumentar a prioridade de um documento, clique com o botão direito do mouse no documento e no menu que surge, dê um clique na opção Propriedades. Será exibida uma janela com as propriedades do documento, conforme indicado na Figura 7.20:

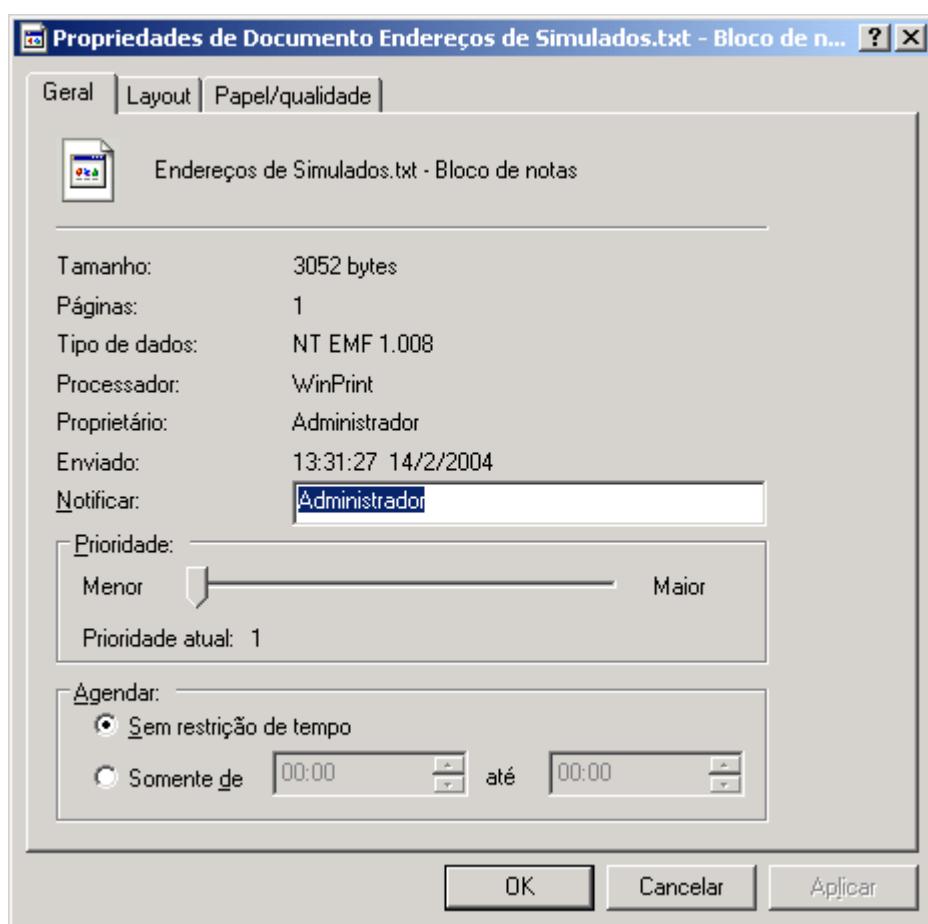


Figura 7.20 Propriedades do documento na fila de impressão.

7. Por padrão a prioridade de todo documento é 1, em uma escala que vai de 1 a 99.

Para aumentar a prioridade do documento, basta clicar no controle deslizante de prioridade e arrastá-lo para a direita. A medida que você vai arrastando o Windows Server 2003 vai indicando qual a prioridade, em uma escala de 1 a 99.

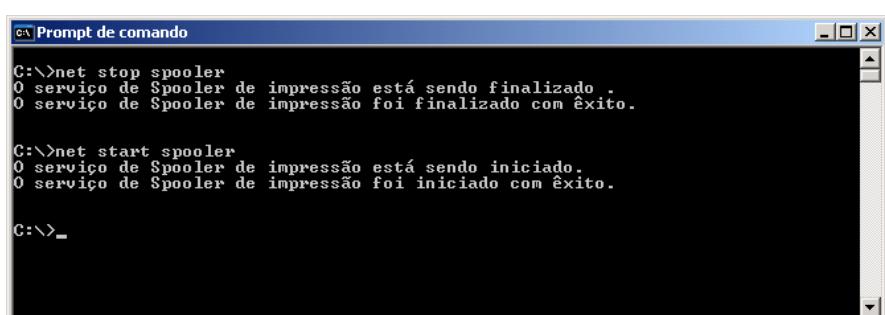
8. Você pode suspender, temporariamente, a impressão de todos os documentos para resolver pequenos problemas do tipo: falta de papel ou trocar o tonner da impressora. Para suspender temporariamente a impressora, selecione o comando Impressora -> Pausar impressão. Observe que na barra de títulos da janela da impressora, ao lado do nome da impressora aparece a expressão Em pausa.
9. Para voltar a imprimir, clique novamente no menu Impressora e depois na opção Pausar impressão, para retirar o sinal de certo do lado desta opção.
10. Para cancelar todos os documentos da fila de impressão, dê um clique no menu Impressoras e depois na opção Cancelar todos os documentos, o Windows Server 2003 exibe uma janela pedindo confirmação, dê um clique em Sim e todos os documentos, com exceção do documento que está sendo impresso atualmente, serão excluídos da fila de impressão.
11. Feche a janela com da impressora.

Quem controla toda a impressão no Windows Server 2003 é um Serviço chamado “Spooler”. Um serviço nada mais é do que um programa que inicializa, automaticamente, quando o Windows Server 2003 é inicializado. O serviço é inicializado e continua operando, sem a necessidade de que ao administrador faça o logon no servidor. Falarei mais sobre serviços no Capítulo 8.

Para eliminar todos os documentos de uma fila de impressão quando a impressão está apresentando problemas maiores, os quais você não consegue solucionar simplesmente administrando a fila de impressão, a maneira mais simples é parar o serviço Spooler e inicializá-lo novamente. Ao fazer isso, todos os documentos que estão na fila de impressão, serão removidos, inclusive o documento que está atualmente sendo impresso.

Para parar o serviço Spooler e inicializá-lo novamente.

1. Abra um Prompt de comando.
2. Para parar o serviço Spooler digite o seguinte comando:  
**net stop spooler**
3. Pressione Enter. O serviço Spooler será finalizado e todos os documentos serão removidos da fila de impressão.
4. Para reiniciar o serviço Spooler digite o seguinte comando:  
**net start spooler**
5. Pressione Enter. O serviço Spooler será reinicializado.
6. Na janela da Figura 7.21, mostro a execução dos dois comandos, onde o serviço Spooler foi “parado” e inicializado novamente:



```
C:\>net stop spooler
O serviço de Spooler de impressão está sendo finalizado .
O serviço de Spooler de impressão foi finalizado com êxito.

C:\>net start spooler
O serviço de Spooler de impressão está sendo iniciado.
O serviço de Spooler de impressão foi iniciado com êxito.

C:\>_
```

**IMPORTANTE:** Quando o Windows terminar de imprimir o documento que está sendo impresso atualmente, o próximo a ser impresso será o de mais alta prioridade, entre os que estão na fila de impressão, independentemente da ordem de chegada do documento na fila de impressão.

**IMPORTANTE:** Podem ocorrer problemas mais sérios, onde o administrador não consegue eliminar os documentos da fila de impressão e a impressora continua imprimindo uma série de páginas com uns caracteres meio estranhos, ou seja, lixo. Muitas vezes o Administrador acaba reinicializando o servidor para poder suspender as impressões com problema.

Figura 7.21 Parando e reinicializando o serviço Spooler.

7. Para sair do Prompt de comando, digite exit e tecle Enter.

## Configurando propriedades importantes e outras ações.

Existem algumas opções e propriedades das impressoras, que são bastante úteis. O administrador deve conhecer e saber configurar estas propriedades, bem como entender em que situações práticas devem ser utilizadas.

Uma das opções importantes é a disponibilidade. Por padrão, quando uma impressora é instalada, ela fica disponível 24 horas por dia, 7 dias por semana. O administrador pode limitar o tempo em que uma impressora fica disponível. Quando um documento é enviado durante um período em que a impressora está configurada para não estar disponível, o documento fica na fila de impressão e quando chegar o horário em que a impressora está configurada para voltar a estar disponível, o documento será impresso, sempre respeitando a ordem de chegada na fila de impressão e a prioridade de cada documento. Configurar o horário de disponibilidade, pode ser usado para evitar que documentos extensos sejam impressos fora do horário do expediente, sem que o administrador tome conhecimento.

Você aprenderá um pouco mais sobre estas propriedades e aprenderá a configura-las, através de um exemplo prático.

Exemplo: Alterando o horário de disponibilidade para impressão.

Para alterar o horário em que uma impressora está disponível para a impressão, siga os seguintes passos:

1. Faça o logon com uma conta que tenha permissão Gerenciar impressoras, na impressora que será configurada.
2. Abra a janela de impressoras.
3. Localize a impressora na qual você deseja alterar o horário de disponibilidade, dê um clique com o botão direito do mouse na impressora e no menu que é exibido dê um clique em Propriedades. Será aberta a janela de Propriedades da impressora.
4. Dê um clique na guia Avançado. Observe que por padrão a impressora está Sempre disponível (Sempre disponível marcado), conforme destacado na Figura 7.22:

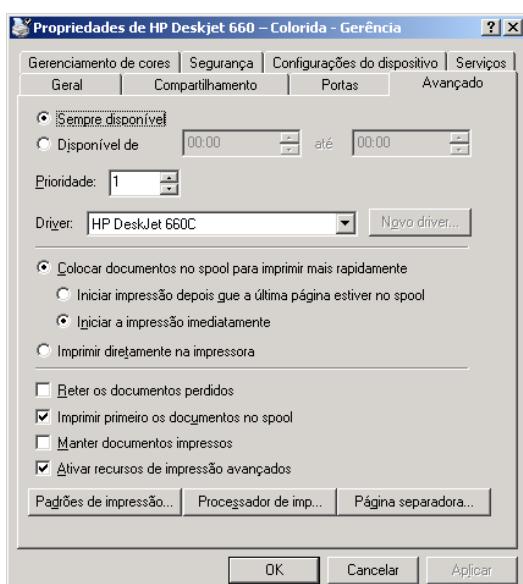


Figura 7.22 Guia Avançado das propriedades da impressora.

**DICA:** Quando uma impressora tem trabalhos em sua fila de impressão, um ícone com uma figura de uma impressora, é exibido ao lado da hora do sistema, bem no canto inferior direito do vídeo. Para abrir a janela que exibe a fila de impressão, basta dar um clique duplo neste ícone. Depois é só utilizar os comandos que você aprendeu no exemplo anterior, para Gerenciar os documentos da fila de impressão.

5. Altere o horário de disponibilidade para que a impressora somente possa ser utilizada, por exemplo, entre as 8:00 e as 18:00 hs. Um documento que for enviado, por exemplo, às 23:00 hs, ficará na fila de impressão até as 8:00 hs, quando então começará a ser impresso. Para fazer esta alteração dê um clique na opção Disponível de: e, no primeiro campo, digite 8:00. No segundo campo digite 18:00
6. Dê um clique no botão OK para aplicar as novas configurações.
7. Feche a janela de impressoras.

Um outro aspecto importante para facilitar a utilização da impressora, é quanto aos clientes que vão acessar a impressora através da rede. Por exemplo, imagine que a sua rede tem estações de trabalho com o Windows 3.11, Windows 95 e Windows 98, Windows NT Workstation 4.0, Windows 2000 Professional e Windows XP Professional (uma verdadeira salada de frutas), todos acessando uma impressora que está compartilhada em um servidor com o Windows Server 2003. O administrador pode armazenar os drivers para cada um destes Sistemas Operacionais, no servidor onde a impressora está compartilhada, conforme já descrito brevemente, no início do Capítulo. Desta forma quando o cliente for conectar-se com a impressora pela primeira vez, ao invés de ter que fornecer um disquete ou CD-ROM com o driver da impressora, o drive será baixado diretamente do servidor onde a impressora está compartilhada.

Exemplo: Como armazenar drivers para outros sistemas operacionais no servidor onde a impressora está compartilhada.

Para adicionar drivers para outros sistemas operacionais, siga os seguintes passos:

1. Faça o logon com uma conta que tenha permissão Gerenciar impressoras, na impressora que será configurada.
2. Abra a janela de impressoras.
3. Localize a impressora para a qual você deseja adicionar drivers para outras versões do Windows, dê um clique com o botão direito do mouse na impressora e no menu que é exibido dê um clique em Propriedades. Será aberta a janela de Propriedades da impressora.
4. Dê um clique na guia Compartilhamento. Veja que na parte de baixo da janela existe um botão Drivers adicionais.... Dê um clique neste botão para abrir a janela indicada na Figura 7.23:



Figura 7.23 Adicionando drivers para diferentes versões do Windows.

5. Marque os sistemas para os quais deseja adicionar drivers e dê um clique no botão OK.
6. Caso o Windows Server 2003 não tenha os arquivos necessários no disco rígido, você será solicitado a fornecer um CD-ROM ou disquete onde está o driver a ser copiado.

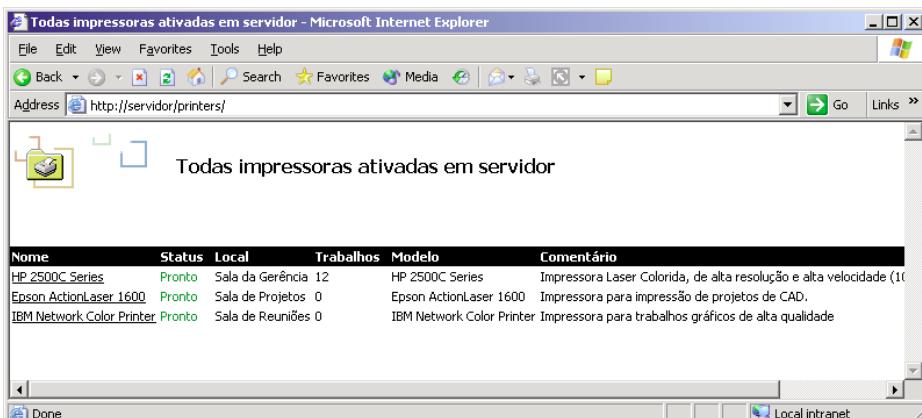
## Administrando a impressora através do navegador.

Uma das grandes melhorias na administração, introduzidas no Windows 2000 Server e também presente no Windows Server 2003, é a possibilidade de administrar uma série de recursos através do navegador (Browser). Um dos recursos que podem ser administrados através do browser são as impressoras instaladas em um computador. Estas facilidades também estão presentes no Windows XP, ou seja, utilizando o Navegador é possível acessar as impressoras compartilhadas em um computador (com o Windows 2000, com o Windows Server 2003 ou com o Windows XP instalado) e realizar uma série de tarefas de administração das impressoras.

Exemplo: Administrando de impressoras usando o Navegador. Neste exemplo você administrará as impressoras de um servidor onde o IIS está instalado, usando o navegador.

Para administrar as impressoras de um computador chamado servidor (onde está instalado o IIS), faça o seguinte:

1. Faça o logon com uma conta que tenha permissão Gerenciar impressoras, na impressora que será acessada. O logon pode ser feito em qualquer estação de trabalho da rede, preferencialmente não no próprio servidor onde estão as impressoras a serem gerenciadas.
2. Abra o Internet Explorer.
3. Na barra de endereços digite: <http://servidor/printers> e tecle Enter. Onde servidor é o nome do servidor onde estão as impressoras a serem administradas.
4. Será exibida uma página com a listagem de todas as impressoras instaladas no computador servidor e com uma série de informações sobre cada impressora. No exemplo da Figura 7.24, accesei um servidor com o Windows Server 2003 em Inglês, onde havia três impressoras instaladas., sendo que na impressora HP existe uma série de trabalhos na fila de impressão.



**NOTA:** Intel, IA64 ou Alpha, indica o tipo de microprocessador. O sistema operacional Windows NT possuí versões: tanto para Alpha quanto para Intel. Processadores da AMD ou Cyrix também se encaixam na categoria Intel, pois são compatíveis com os mesmos. IA64 representa a nova geração de processadores de 64bits, para as quais já existe uma versão do Windows XP de 64 bits. Itanium é a nova geração de processadores baseados em arquitetura de 64 bits. Existe uma versão do Windows Server 2003 específica para esta família de processadores, versão esta também baseada em arquitetura de 64 bits.

**IMPORTANTE:** Para que a administração através do navegador seja possível é necessário que o computador onde a impressora está compartilhada, tenha o servidor Web instalado. O IIS é o servidor Web da Microsoft e é instalado por padrão, quando da instalação do Windows 2000 Server. Já no Windows Server 2003, o IIS não é instalado por padrão. Para maiores detalhes sobre a instalação do IIS 6.0, consulte o Capítulo 13.

Figura 7.24 Impressoras compartilhadas no servidor.

- Dê um clique na impressora que você quer administrar.
- Se existirem documentos na fila de impressão, será exibida uma listagem dos documentos que estão na fila, conforme indicado na Figura 7.25:

The screenshot shows the Microsoft Internet Explorer browser window titled "HP 2500C Series em servidor - Microsoft Internet Explorer". The address bar shows the URL: [http://servidor/printers/ipp\\_0004.asp?view=q&eprinter=HP~202500C~20Series&page=1727](http://servidor/printers/ipp_0004.asp?view=q&eprinter=HP~202500C~20Series&page=1727). The main content area displays the printer status: "Fila da impressora: Pronto" and "Tempo de espera: sobre 2 min". It also shows "Documentos pendentes: 12" and "Tamanho médio: 1 página(s)". On the left, there are three sections: "EXIBIR" with links to "Lista de documentos", "Propriedades", and "Todas impressoras"; "AÇÕES DA IMPRESSORA" with links to "Pausar", "Retomar", "Cancelar todos os documentos", and "Conectar"; and "AÇÕES DE DOCUMENTO" with links to "Pausar", "Retomar", and "Cancelar". A large table lists the 12 pending documents with columns: Documento, Status, Proprietário, Páginas, Tamanho, and Emitido. The table includes rows for various text files like "Endereços de Simulados.txt", "cache.txt", "baboo.txt", etc., each with its status (Imprimindo or Pendente), owner (Administrador), number of pages, file size, and print time.

| Documento                                   | Status     | Proprietário    | Páginas | Tamanho  | Emitido            |
|---|------------|-----------------|---------|----------|--------------------|
| Endereços de Simulados.txt - Bloco de notas | Imprimindo | Administrador 1 | 1       | 56 bytes | 14:57:02 31/5/2003 |
| cache.txt - Bloco de notas                  | Pendente   | Administrador 1 | 1       | 1,8 Kb   | 14:57:02 31/5/2003 |
| baboo.txt - Bloco de notas                  | Pendente   | Administrador 3 | 1       | 12,6 Kb  | 14:57:02 31/5/2003 |
| DicasCertificacoes.txt - Bloco de notas     | Pendente   | Administrador 1 | 1       | 3,7 Kb   | 14:57:02 31/5/2003 |
| compraexav.txt - Bloco de notas             | Pendente   | Administrador 1 | 1       | 2,7 Kb   | 14:57:02 31/5/2003 |
| elogios no site.txt - Bloco de notas        | Pendente   | Administrador 7 | 1       | 33,0 Kb  | 14:57:02 31/5/2003 |
| auto-resposta.txt - Bloco de notas          | Pendente   | Administrador 2 | 1       | 6,3 Kb   | 14:57:02 31/5/2003 |
| enquete.txt - Bloco de notas                | Pendente   | Administrador 1 | 1       | 1,5 Kb   | 14:57:02 31/5/2003 |
|   |            | Administrador 1 | 1       | 1,0 Kb   | 14:57:02 31/5/2003 |

**Figura 7.25 Listagem dos documentos na fila de impressão.**

Nesta página você pode realizar uma série de operações de administração, tanto da impressora quanto dos documentos que estão na fila de impressão.

- Por exemplo, para excluir um documento da fila de impressão, basta marcá-lo dando um clique no documento a ser excluído e depois, no painel da esquerda, clicar no link Cancelar, abaixo de AÇÕES DE DOCUMENTO.
- Para excluir todos os documentos da fila de impressão, com exceção do documento que está sendo impresso, dê um clique no link Cancelar todos os documentos, abaixo de AÇÕES DA IMPRESSORA.

No painel da esquerda temos uma série de opções para gerenciar a impressora e a fila de impressão.

- Feche o navegador.

A possibilidade de administrar recursos através do browser facilita em muito a administração de uma rede baseada no Windows Server 2003.

## Utilizando impressoras de rede.

Anteriormente neste capítulo eu expliquei que existe diferença entre uma impressora que está conectada a uma porta (normalmente a porta paralela) de um servidor e compartilhada neste servidor, em relação a uma impressora de rede. Considera-se uma impressora de rede, uma impressora que tem uma placa padrão Ethernet instalada, que tem um número IP configurado na impressora e que está conectada diretamente à rede, através da placa de rede instalada na impressora. Este tipo de impressora é de uso bastante comum e tem a grande vantagem de não precisar estar localizada, fisicamente,

próxima ao servidor que a controla. Por exemplo, a sala dos servidores pode estar no primeiro andar e a impressora pode estar no vigésimo andar do prédio e mesmo assim estar sendo gerenciada por um servidor da sala de servidores.

Vou dividir este item em duas partes. Na primeira parte, com base em um diagrama de rede, mostrarei como são utilizadas, na prática, as impressoras de rede, ou seja, impressoras conectadas diretamente à rede, através de uma placa de rede. Na segunda parte mostrarei as configurações práticas para colocar a impressora de rede em funcionamento, isto é, disponível para os usuários da rede.

Inicialmente considere o diagrama da Figura 7.26:

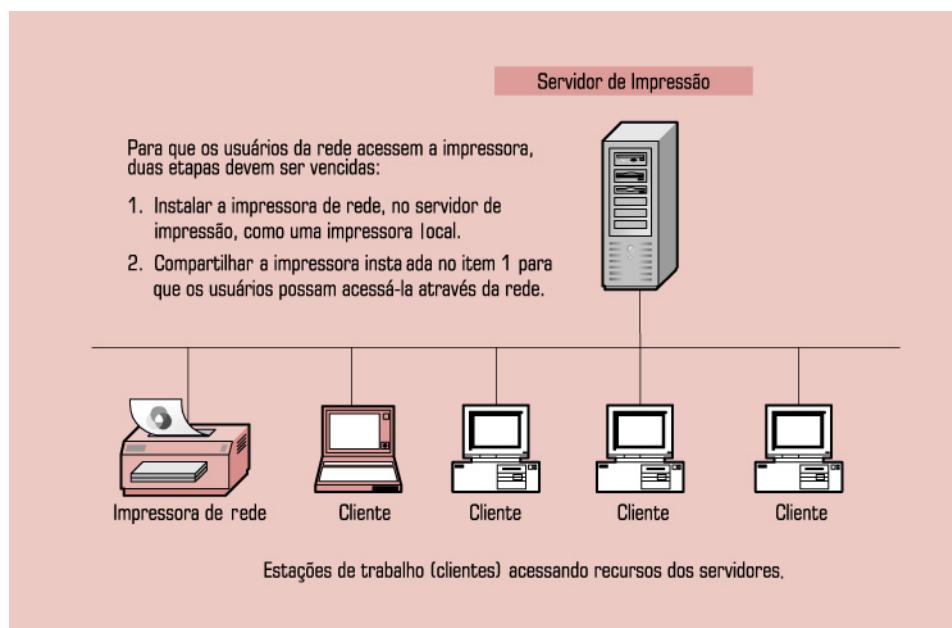


Figura 7.26 Diagrama de uso de uma impressora de rede.

No diagrama da Figura 7.26 é exibida uma impressora conectada diretamente à rede. Esta impressora deve ser configurada com um número IP válido, ou seja, um número IP da rede onde ele está conectada. A configuração do número IP da impressora depende da marca e do modelo da impressora. Após ter sido conectada à rede, para que os usuários possam acessar a impressora, duas etapas devem ser vencidas:

1. Instalar a impressora de rede, no servidor de impressão, como uma impressora Local. Os usuários não irão acessar diretamente a impressora da rede. O acesso será feito através de um servidor de impressão baseado no Windows Server 2003. No servidor, você deve instalar a impressora de rede como sendo uma impressora local. O procedimento é o mesmo de instalar uma impressora local. A diferença é na hora de informar a porta da impressora, quando então, ao invés de LPT1, será informado o número IP da impressora e o nome configurado na impressora. Mostrarei esta etapa no exemplo prático, logo a seguir.
2. Compartilhar a impressora instalada no item 1, para que os usuários possam acessá-la através da rede. Após instalada como impressora local, porém com a porta configurada para o endereço IP da impressora, basta compartilhar a impressora para que esta possa ser acessada através da rede, pelas estações de trabalho dos usuários. Na prática, depois de instalada como uma impressora local, para o Windows Server 2003, é como se fosse uma impressora local. A única diferença é na hora de imprimir, quando os trabalhos são enviados para o endereço IP configurado como porta da impressora e não para uma porta paralela, serial ou USB do próprio servidor. Para os usuários é simplesmente uma impressora compartilhada no servidor, o usuário não sabe se esta impressora está diretamente conectada ao servidor ou se é uma impressora de rede.

Agora é hora de praticar um pouco. Você acompanhará a execução dos dois passos necessários para tornar uma impressora de rede disponível para ser utilizada pelos usuários da rede. Os dois passos são executados no servidor com o Windows Server 2003 instalado, servidor este que irá controlar a impressora.

Passos 1 e 2: Instalar a impressora de rede, no servidor de impressão, como uma impressora Local. Depois compartilhar a impressora para que ela possa ser utilizada pelas estações de trabalho da rede.

Neste exemplo prático você irá executar os dois passos necessários. Para isso, siga as etapas indicadas a seguir:

1. Faça o logon com um conta com permissões de Administrador ou com uma conta pertencente ao grupo Oper. de Impressão, no servidor onde a impressora será instalada.
2. Utilize o comando Iniciar -> Impressoras e aparelhos de fax.
3. Será aberta a janela Impressoras e aparelhos de fax, na qual é mostrada uma lista das impressoras instaladas no seu computador. Caso não exista nenhuma impressora instalada, a lista estará vazia, estando disponível apenas a opção Adicionar Impressora.
4. Dê um clique duplo no ícone Adicionar impressora.
5. Será aberto o Assistente para adicionar impressora. Este é um assistente que irá guiando você passo a passo na tarefa de instalar a nova impressora. O assistente solicita diversas informações em cada uma das etapas.
6. Nesta primeira etapa, é exibida uma mensagem explicativa. Dê um clique no botão Avançar para ir para a próxima etapa do assistente.
7. Como estou instalando uma impressora local (apenas vou redirecionar a porta de conexão da impressora para o número IP da impressora na rede), certifique-se que a opção Impressora local conectada ao computador esteja marcada e desmarque a opção Detectar e instalar automaticamente a impressora Plug and Play.
8. Dê um clique no botão Avançar para ir para a terceira etapa do assistente.
9. Na terceira etapa, você tem que escolher a porta onde está ligada a impressora. Nesta etapa é que você criará uma nova porta e irá associá-la com o número IP da impressora na rede. Clique na opção Criar uma nova porta. Abra a lista de opções disponíveis e selecione Standard TCP/IP Port, conforme indicado na Figura 7.27:

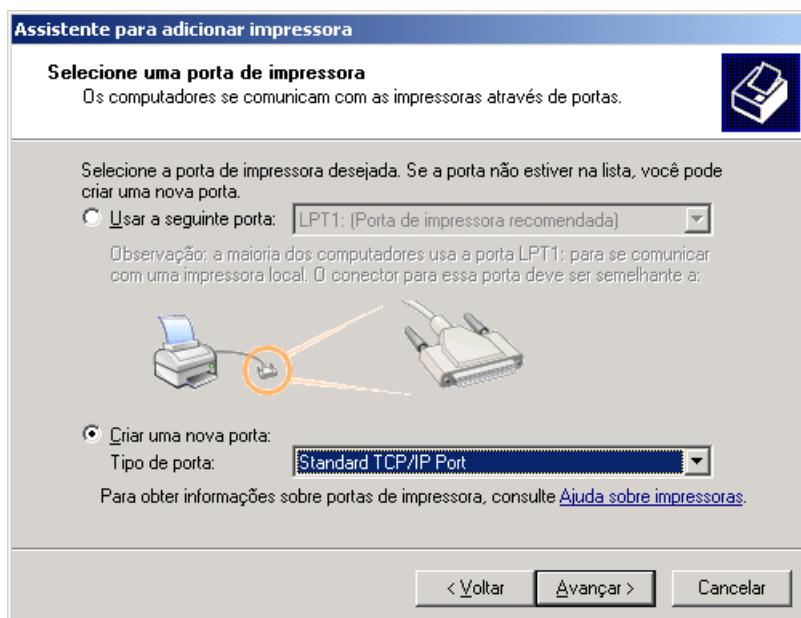
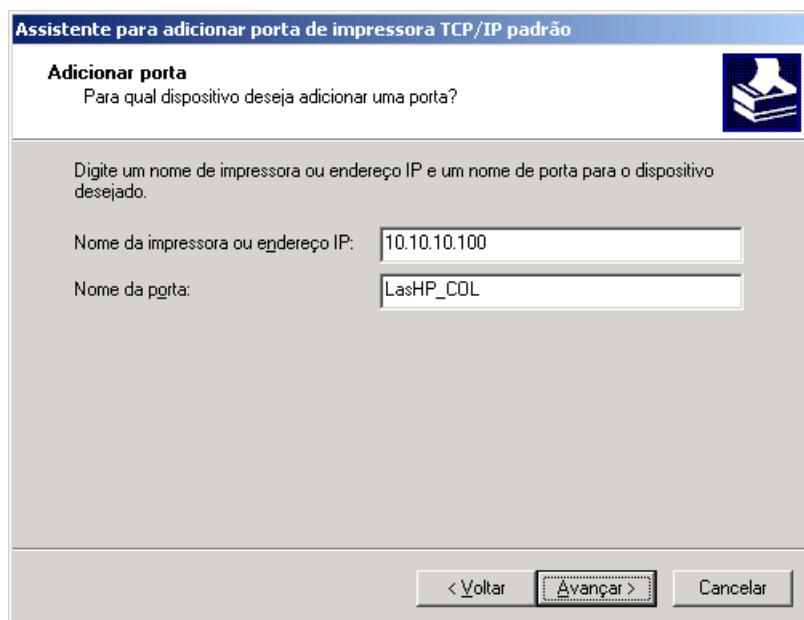


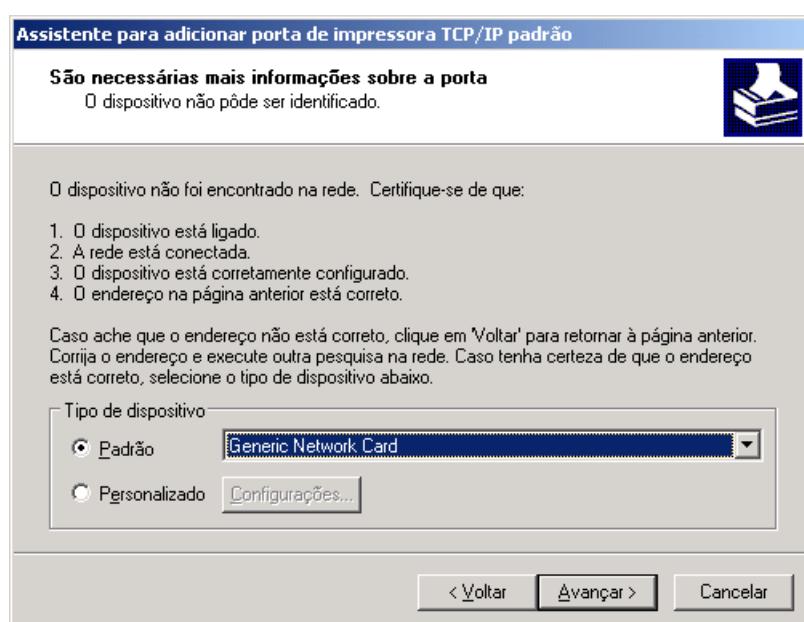
Figura 7.27 Criando uma nova porta padrão TCP/IP.

10. Dê um clique no botão Avançar para ir para a quarta etapa do assistente.
11. Será aberto o Assistente para adicionar porta de impressora TCP/IP padrão. A primeira tela do assistente é apenas informativa. Clique Avançar, para seguir para a próxima etapa.
12. Nesta etapa você deve informar o número IP da impressora (ou o nome, caso o nome esteja corretamente configurado no servidor DNS) e o nome da porta da impressora, conforme exemplo da Figura 7.28:



**Figura 7.28 Informações sobre a porta TCP/IP da impressora de rede.**

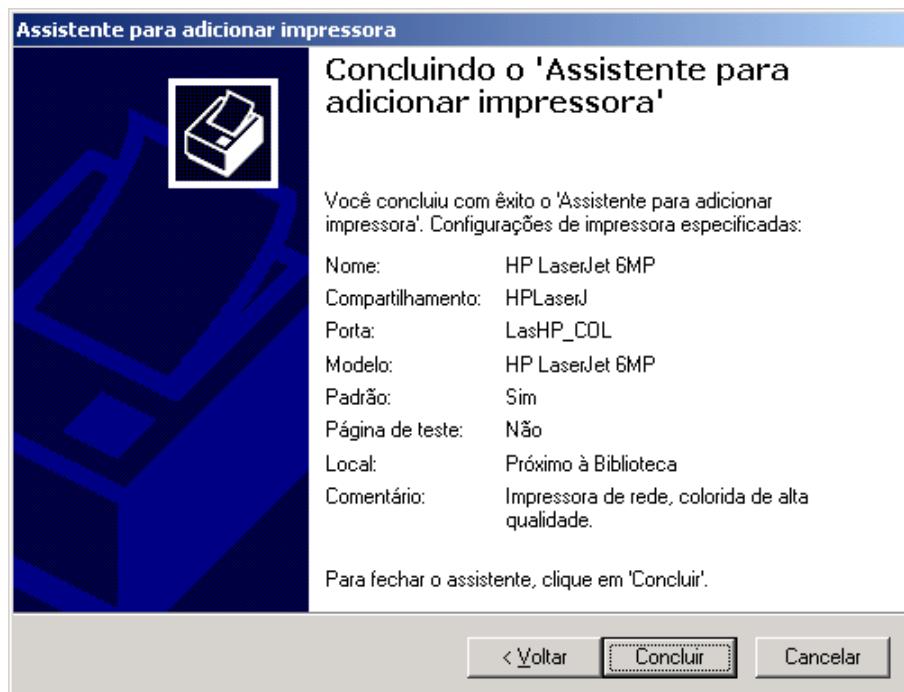
13. Dê um clique no botão Avançar para ir para a próxima etapa.
14. Nesta etapa você pode definir informações adicionais, tais como o tipo, marca e modelo de impressora de rede, selecionando em uma lista de modelos já existentes, ou pode informar um novo tipo/modelo, usando a opção Personalizada, conforme indicado na Figura 7.29:



**Figura 7.29 Informações adicionais sobre a impressora de rede.**

15. Selecione as opções relacionadas com a impressora que você está instalando e clique em Avançar, para seguir para a próxima etapa.
16. Será exibida a etapa final do assistente para adição de uma porta TCP/IP padrão, com um resumo das opções selecionadas. Caso você precise alterar alguma opção, basta clicar em Voltar. Clique em Concluir para finalizar o assistente de adição de porta TCP/IP.
17. Você estará de volta ao assistente para adição de impressoras, agora com a porta TCP/IP da impressora de rede já configurada.
18. Nesta etapa você deve escolher a marca e o modelo da impressora que está sendo instalada. Na coluna da esquerda existe uma listagem dos fabricantes em ordem alfabética. Quando você seleciona um fabricante na coluna da esquerda, a coluna da direita exibe apenas os modelos do fabricante selecionado. Selecione a marca e modelo da impressora que você está instalando.
19. Dê um clique no botão Avançar para ir para a próxima etapa do assistente.
20. Nesta etapa o Windows Server 2003 pede que você digite um nome para a Impressora. Esse nome é o nome que irá aparecer dentro da janela Impressoras e aparelhos de fax, depois que você tiver concluído a instalação.
21. No campo Nome da impressora digite um nome que ajude a identificar a marca, modelo, localização e característica principal da impressora.
22. Dê um clique no botão Avançar para ir para a próxima etapa do assistente.
23. Nesta, você define se deseja, ou não, compartilhar a impressora. Por padrão vem marcada a opção Nome de compartilhamento, já com uma sugestão de nome para compartilhamento da impressora. Neste momento você irá compartilhar a impressora. Com isso você já está cumprindo a segunda etapa, ou seja, compartilhando a impressora para que ele possa ser utilizada pelos usuários da rede. Certifique-se de que a opção Nome de compartilhamento esteja marcada, digite um nome de compartilhamento e dê um clique no botão Next (Avançar)para ir para a próxima etapa do assistente.
24. Nesta etapa surge uma tela para que você preencha os campos Localização e Comentários. É importante que você preencha estes campos para que estas informações estejam disponíveis para os usuários que pesquisam pela impressora na rede. Estas informações ajudam na localização de impressoras próximas ao local de trabalho do usuário. Preencha os campos de informação e clique em Avançar, para seguir para a próxima etapa do assistente.
25. Nesta etapa surge uma tela perguntando se você deseja imprimir uma página de teste. Caso você tenha uma impressora conectada, escolha Sim, para verificar se a impressora está funcionando corretamente. Caso contrário marque a opção Não.
26. Dê um clique em Avançar para ir para a última etapa do assistente, onde o Windows Server 2003 exibe um resumo das informações fornecidas nas diversas etapas, conforme indicado na Figura 7.30:

**NOTA:** Você pode utilizar o botão Windows Update para exibir uma lista de drivers de dispositivo que podem ser descarregados do site do Microsoft Windows Update na Internet. Nessa lista, selecione o dever adequado para o dispositivo. Esta opção somente funcionará se você tiver alguma forma de conexão com a Internet. Utilize o botão Com disco... para instalar o drive da impressora a partir de um CD-ROM ou disquete, ou de um compartilhamento de rede. Ao clicar neste botão será aberta uma janela para que você informe o local onde está disponível o driver da impressora que está sendo instalada.



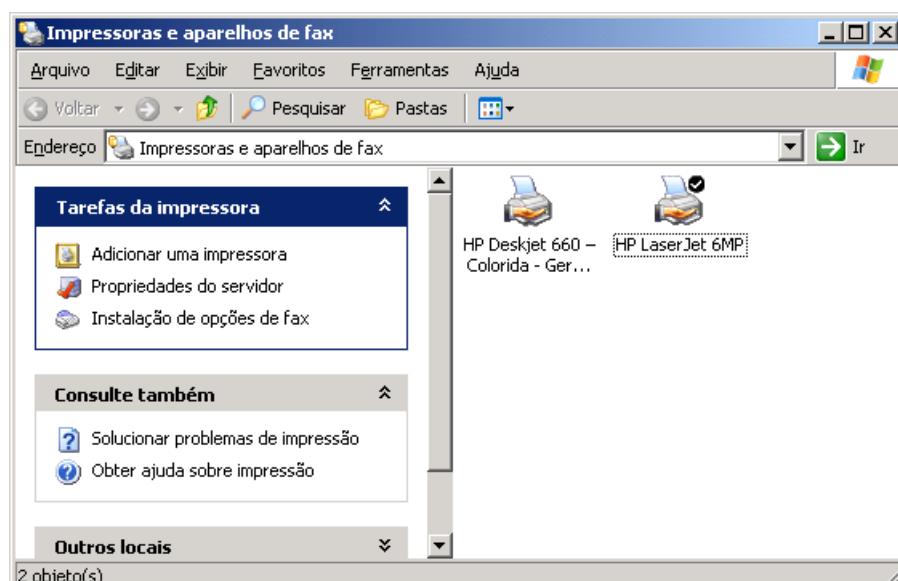
**Figura 7.30** Etapa final do Assistente para adicionar impressora.

27. Caso esteja tudo OK, dê um clique no botão Concluir.

O Windows Server 2003 começa a copiar os arquivos necessários. Nesta etapa pode ser que você seja solicitado a colocar o CD do Windows Server 2003 no driver de CD-ROM, caso o Windows Server 2003 não encontre todos os arquivos necessários no disco rígido.

Após concluir a cópia dos arquivos, você estará de volta a janela Impressoras e aparelhos de fax e a impressora recém instalada, já aparece na janela Impressoras, conforme indicado pela Figura 7.31. No exemplo da Figura, foi adicionada uma HP LaserJet 6MP.

**NOTA:** Caso você constate que existe alguma informação incorreta, você pode usar o botão Voltar para ir até a etapa onde foi fornecida a informação incorreta e corrigi-la.



**Figura 7.31** Impressora de rede instalada como uma impressora local.

Agora a impressora de rede está instalada como se fosse uma impressora local no servidor, apenas com a porta redirecionada para o número IP da impressora na rede e também está compartilhada. Ou seja, é uma impressora compartilhada no servidor como outra qualquer. O administrador pode definir permissões de acesso, gerenciar a fila de impressão e definir propriedades importantes da impressora, como se fosse uma impressora local. Quando o usuário envia um trabalho de impressão, o trabalho é enviado para o servidor Windows Server 2003 onde a impressora foi instalada e compartilhada. O Windows Server 2003 verifica que a porta da impressora está associada com o número IP de uma impressora de rede. O trabalho de impressão é enviado, através da rede, diretamente para a impressora cujo número IP foi informado durante a instalação da impressora no Windows Server 2003. É exatamente o que queríamos, ou seja, o Windows Server 2003 faz todo o gerenciamento da impressão e envia o trabalho de impressão diretamente para a impressora na rede. Como ele “acha” a impressora? Através do número IP configurado durante a instalação da impressora. É isso.

## Diferentes prioridades para diferentes grupos.

Neste item descreverei quais os passos necessários para que o administrador possa definir diferentes prioridades, para diferentes grupos, no uso da mesma impressora. Esta é uma situação bastante comum. Imagine a situação descrita a seguir:

Uma nova impressora Laser, Colorida, de alta resolução e de alta velocidade (15 páginas por minuto) foi instalada no andar da direção. Neste andar, além dos executivos da empresa também trabalham as secretárias e uma equipe de estagiários que fazem uma série de trabalhos de apoio. Todos devem ter permissão para usar a nova impressora, a qual será instalada e compartilhada em um servidor Windows Server 2003 localizado no mesmo andar. Todos os executivos fazem parte do grupo Administração, todas as secretárias fazem parte do grupo Secretárias e todos os estagiários fazem parte do grupo Estagiários. Você, como administrador, foi solicitado para permitir que os grupos Administração, Secretárias e Estagiários tenham acesso a esta nova impressora, porém com diferentes prioridades. O grupo Administração deve ter prioridade Máxima e o grupo Secretárias deve ter uma prioridade menor do que o grupo Administração, porém maior do que o grupo Estagiários. Quais os passos que você deve executar, para implementar a configuração proposta?

Esta é uma questão bastante comum no dia-a-dia da administração de impressoras em uma rede, ou seja, permitir o uso de uma impressora, por diferentes grupos, com diferentes prioridades. Você não tem como definir, nas propriedades da impressora, diferentes prioridades para diferentes grupos. Quando você define uma determinada prioridade para uma impressora (logical printer) você está definindo esta mesma prioridade para todos os usuários que tem permissão de acesso à impressora. Para solucionar esta questão é preciso “apelar” para a criatividade do ser humano. Felizmente somos seres criativos, curiosos por natureza. A resolução deste problema é bastante simples (embora dê um pouco de trabalho manual) e passa pela execução dos seguintes passos:

1. Instale a impressora (instalar o driver da impressora) três vezes, porém com nomes diferentes. No exemplo da Figura 7.32, instalei a impressora HP Deskjet 660C três vezes, porém com nomes diferentes.

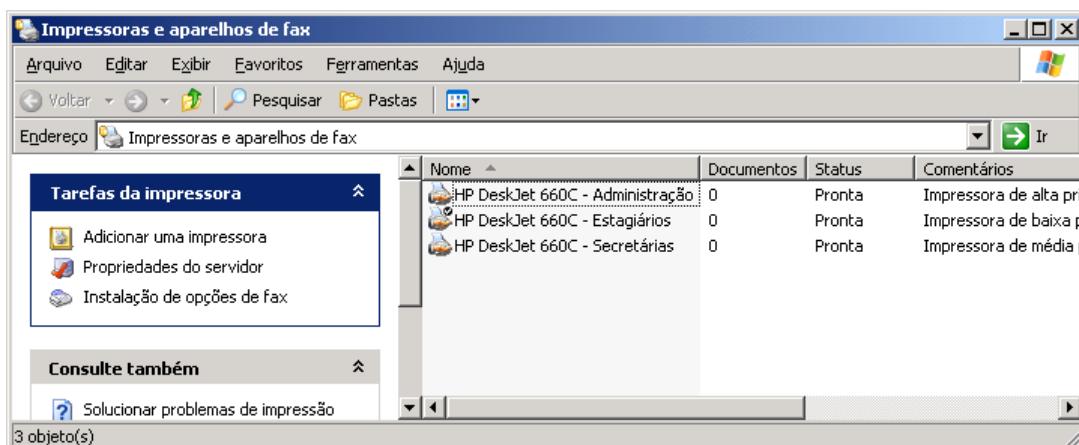


Figura 7.32 - Impressora instalada três vezes com nomes diferentes.

2. As três impressoras também foram compartilhadas com nomes de compartilhamento diferentes, conforme indicado a seguir:

| Grupo         | Nome da impressora              | Nome de compartilhamento |
|---------------|---------------------------------|--------------------------|
| Estagiários   | HP DeskJet 660C – Estagiários   | HP660Est                 |
| Secretárias   | HP Deskjet 660C – Secretárias   | HP660Sec                 |
| Administração | HP DeskJet 660C – Administração | HP660Adm                 |

3. A próxima etapa é definir diferentes propriedades para cada uma das instalações da impressora. Para definir a prioridade de uma instalação basta clicar com o botão direito do mouse na impressora a ser configurada. No menu de opções que é exibido clique em Propriedades. Clique na guia Avançado. No campo Prioridade, informe um valor entre 1 e 99. Quanto maior o valor, maior a prioridade da instalação no uso da fila de impressão. Na Figura 7.33 é exibido o campo para configuração da prioridade da impressora.

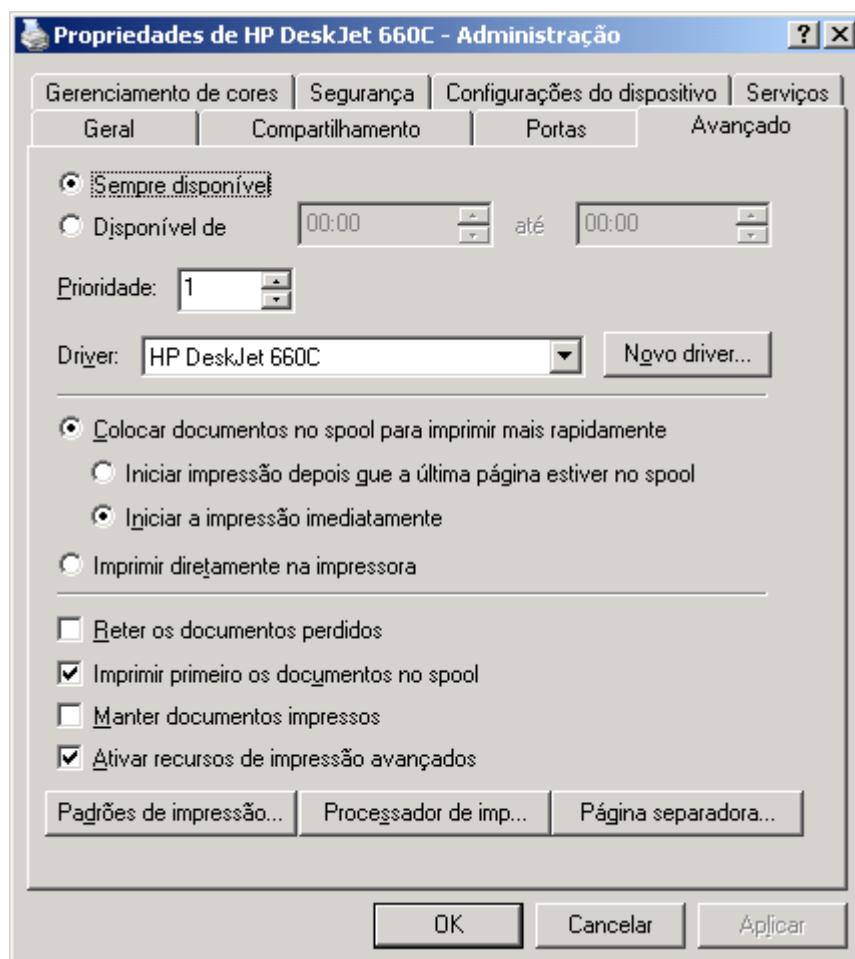


Figura 7.33 – Definindo a prioridade da impressora.

Basta definir a prioridade e clicar em OK. Defina as seguintes prioridades para cada uma das instalações:

| <b>Grupo</b>  | <b>Nome da impressora</b>       | <b>Nome de compartilhamento</b> | <b>Prioridade</b> |
|---------------|---------------------------------|---------------------------------|-------------------|
| Estagiários   | HP DeskJet 660C – Estagiários   | HP660Est                        | 10                |
| Secretárias   | HP Deskjet 660C – Secretárias   | HP660Sec                        | 50                |
| Administração | HP DeskJet 660C – Administração | HP660Adm                        | 99                |

4. Define permissões de acesso específicas em cada instalação, conforme indicado a seguir:

| <b>Grupo</b>  | <b>Nome da impressora</b>       | <b>Permissão para o grupo</b> |
|---------------|---------------------------------|-------------------------------|
| Estagiários   | HP DeskJet 660C – Estagiários   | Estagiários                   |
| Secretárias   | HP Deskjet 660C – Secretárias   | Secretárias                   |
| Administração | HP DeskJet 660C – Administração | Administração.                |

Com isso cada grupo somente poderá acessar a sua respectiva instalação, com o nível de prioridade adequado a cada grupo.

5. Agora configure para que cada usuário accesse o respectivo compartilhamento, conforme indicado a seguir:

| <b>Grupo</b>  | <b>Nome de compartilhamento</b> | <b>Prioridade</b> |
|---------------|---------------------------------|-------------------|
| Estagiários   | HP660Est                        | 10                |
| Secretárias   | HP660Sec                        | 50                |
| Administração | HP660Adm                        | 99                |

Pronto, agora cada usuário somente consegue acessar uma das instalações da impressora e de acordo com o nível de prioridade definido para o respectivo grupo.

Este é um exemplo simples, de uma solução que não existe pronta no Windows Server 2003, mas combinando o conhecimento sobre impressoras, com uma pitada de criatividade, o administrador consegue implementar uma solução para uma demanda real. É um erro esperar por soluções prontas para todas as demandas do mundo real, por que as demandas são muitas e variadas. O trabalho do administrador é utilizar os recursos disponíveis e a sua criatividade para implementar soluções para os problemas reais do dia-a-dia. Até porque, se o sistema operacional já apresentasse soluções prontas para todos os problemas reais, não seria necessária a figura do administrador, ou seja, o próprio sistema operacional tomaria conta de tudo. Bem, deixando a filosofia de lado, vamos a mais uma situação prática que pode ocorrer no caso de grandes volumes de impressão.

**NOTA:** Todos os passos para executar as ações práticas deste exemplo, tais como instalar uma impressora, compartilhar a impressora e definir permissões, foram descritos anteriormente neste capítulo. Em caso de dúvidas na execução de um destes passos é só voltar no capítulo, no respectivo item.

## Criando um “pool” de impressão.

Imagine a situação onde você tem um grande volume de impressão, literalmente milhares de páginas sendo impressas. Neste caso pode ser que uma única impressora não dê conta do recado. Nestas situações você pode instalar duas ou

mais impressoras, da mesma marca e modelo e fazer com que estas impressoras apareçam para o Windows Server 2003 como sendo uma única impressora (um pool de impressão). A medida que os trabalhos de impressão vão chegando, o Windows Server 2003 envia este trabalho para uma das impressoras do pool, sempre tendo como critério a impressora que estiver com a menor carga de trabalho, ou seja, com a menor fila de impressão.

Para criar um pool de impressão é extremamente simples. Basta você instalar a impressora a primeira vez e depois acessar as propriedades da impressora. Na janela de propriedades clique na guia Portas. Nesta guia você pode usar o botão Adicionar Porta... para adicionar novas portas de impressão. No exemplo proposto, você deve adicionar novas portas, associadas com o endereço IP de cada impressora que fará parte do pool de impressão. No exemplo da Figura 7.34, adicionei três novas portas, associadas com o número IP das impressoras:

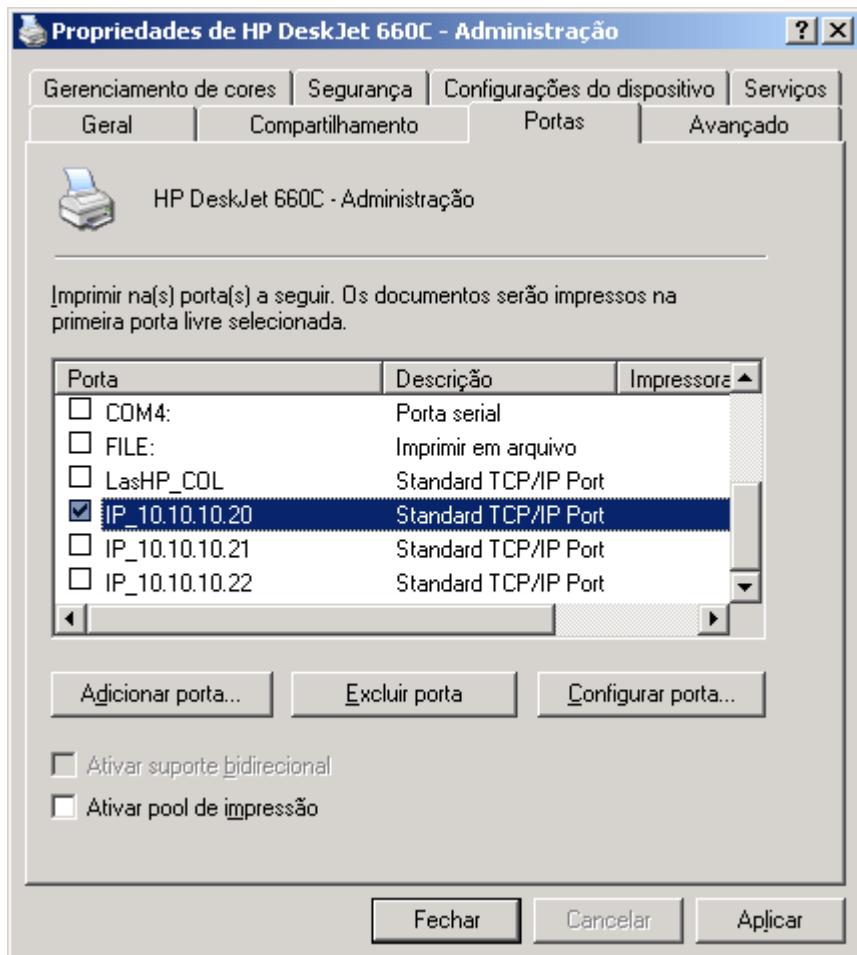


Figura 7.34 – Adicionando novas portas de impressão.

O próximo passo é marcar a opção Ativar pool de impressão. Após ter marcado esta opção, você deve marcar as portas onde estão as impressoras que farão parte do pool. No exemplo da Figura 7.34, quatro impressoras farão parte do pool. Três impressoras conectadas à rede, com as portas associadas ao endereço IP de cada impressora e a quarta impressora ligada a porta serial COM4:

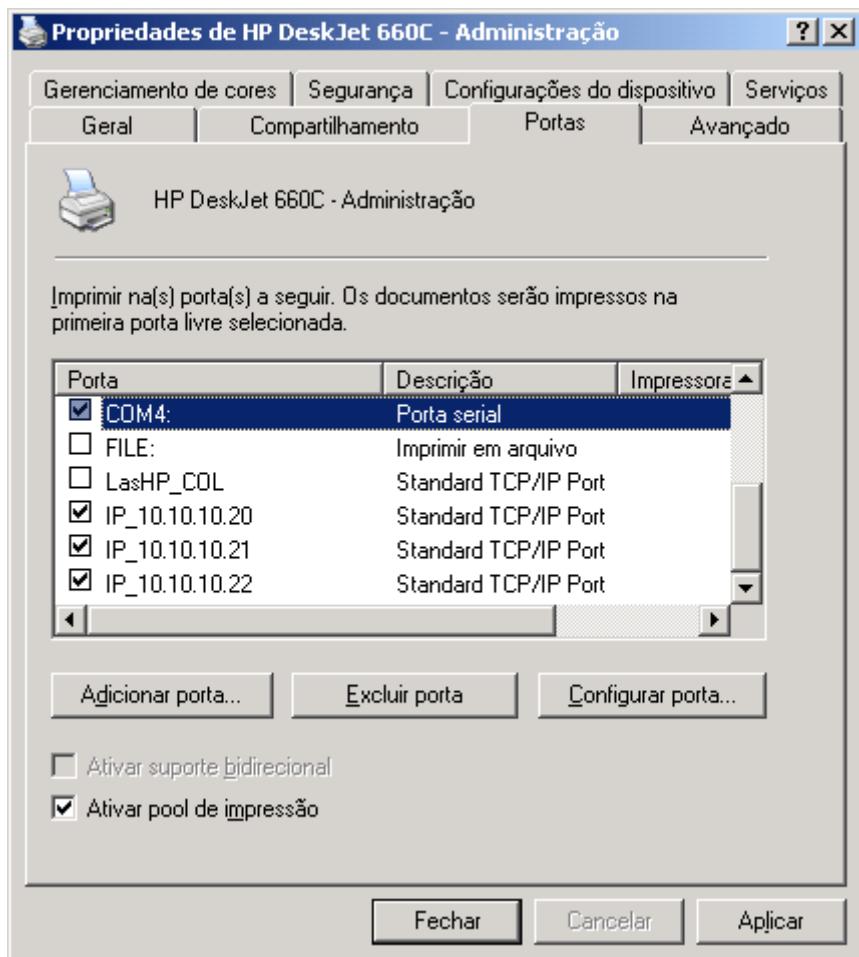


Figura 7.35 – Criando um pool de impressão com quatro impressoras.

Após ter habilitado o pool de impressão e selecionado as portas onde estão as impressoras que farão parte do pool de impressão é só clicar em OK e pronto. A medida que os trabalhos de impressão forem sendo enviados, o Windows Server 2003 irá distribuí-los entre as impressoras do pool.

Este tipo de configuração é recomendado em situações onde existe um grande volume de impressão, conforme descrito anteriormente. Nunca é demais salientar que a condição básica para a criação do pool é que todas as impressoras que farão parte do pool, devem utilizar o mesmo driver de impressão. O driver é instalado no servidor e nas propriedades da impressora, conforme descrito anteriormente, cria-se o pool de impressão, marcando as portas das impressoras que farão parte do pool de impressão. É isso.

## Comandos para o gerenciamento e administração de compartilhamento de impressoras e pastas.

Pode parecer estranho e até mesmo ultrapassado a utilização de comandos para a realização de tarefas administrativas. Afinal porque um Administrador irá querer aprender a sintaxe de uma série de comandos, se tudo pode ser feito com a utilização da interface gráfica, do MMC e dos consoles Administrativos?

**IMPORTANTE:** A condição para criar um pool de impressão e para que ele funcione corretamente é que todas as impressoras do pool devem utilizar o mesmo driver. Claro que sendo impressoras da mesma marca e modelo este não será um problema. Porém impressoras da mesma marca e de modelos diferentes, as vezes utilizam o mesmo driver. Neste caso será possível juntá-las em um pool. Já para impressoras de marcas diferentes, será praticamente impossível que utilizem o mesmo driver e que possam fazer parte do mesmo pool de impressão.

Bem, existem situações em que a utilização de comandos é, mais do que útil, eu diria: INDISPENSÁVEL. A situação mais específica é na resolução de problemas, ou melhor, quando o administrador está na fase de detecção do problema, para uma posterior resolução. Outro situação seria na utilização de scripts para automação de tarefas administrativas.

Neste tópico mostrarei alguns comandos úteis para o gerenciamento e administração de recursos compartilhados, mais especificamente: pastas e impressoras.

## O comando net share

O comando net share permite que o Administrador crie, modifique, visualize ou exclua compartilhamentos. A forma mais simples de utilização deste comando é simplesmente abrir um Prompt de comando, digitar net share e pressionar ENTER. Este comando exibirá todos os recursos compartilhados, disponíveis no servidor onde o comando foi executado, conforme indicado na Figura 7. 36. Observe que inclusive os compartilhamentos ocultos, cujo nome termina com o caractere '\$' são exibidos.

| Nome                         | Recurso                                  | Observação                                  |
|------------------------------|--|---|
| IPC\$                        |  | IPC remoto                                  |
| print\$                      | C:\WINDOWS\system32\spool\drivers        | Drivers de impressora                       |
| ADMIN\$                      | C:\WINDOWS                               | Administração remota                        |
| C\$                          | C:\                                      | Recurso compartilhado padrão                |
| Documentos                   | C:\Documentos                            | Documentos no computador microxp01          |
| NETLOGON                     | C:\WINDOWS\SYSVOL\sysvol\abc.com\SCRIPTS | Compartilhamento do servidor de lo          |
| NovosDocumentos              | C:\NovosDocumentos                       | Novos documentos para o projeto XY          |
| Programas                    | C:\Programas                             | Programas compartilhados                    |
| SYSVOL                       | C:\WINDOWS\SYSVOL\sysvol                 | Compartilhamento do servidor de lo          |
| HP660Adm                     | LPT1:                                    | No spool Impressora de alta prioridade, de  |
| HP660Est                     | LPT1:                                    | No spool Impressora de baixa prioridade, de |
| HP660Sec                     | LPT1:                                    | No spool Impressora de média prioridade, de |
| Comando concluído com êxito. |  |   |

Figura 7.36 O comando net share sem parâmetros.

Se você quiser informações sobre um recurso específico, utilize o seguinte comando:

```
net share nome_do_compartilhamento
```

Por exemplo, para obter informações sobre um compartilhamento chamado Programas, utilize o seguinte comando:

```
net share programas
```

Serão exibidas diversas informações sobre o compartilhamento programas, conforme indicado a seguir:

```
C:\>net share programas
Nome do compartilhamento      Programas
Caminho                         C:\Programas
Observação                      Programas compartilhados
Máx. usuários                  10
Usuários
Cache                           Cache manual dos documentos
Permissões                       ABC\Diretoria, DESCONHECIDO (0x1200a9)
                                    ABC\Empresa, FULL
                                    ABC\Vendas, CHANGE

Comando concluído com êxito.
C:\>
```

Agora vamos obter informações sobre a impressora compartilhada hp660adm. Digite o seguinte comando:

```
net share hp660adm
```

ao pressionar ENTER você deve obter um conjunto de informações semelhante as indicadas a seguir:

```
C:\>net share hp660adm
Nome do compartilhamento      HP660Adm
Caminho                         LPT1:
Observação                      Impressora de alta prioridade, de uso da Administração
Máx. usuários                  Sem limite
Usuários
Cache                           Cache manual dos documentos
Permissões                       Todos, FULL
                                BUILTIN\Administradores, FULL
                                BUILTIN\Oper. de impressão, FULL
                                BUILTIN\Oper. de servidores, FULL

Comando concluído com êxito.
C:\>
```

Para uma listagem completa, com todas as opções do comando net share, execute o seguinte comando:

```
net share /?
```

pressione ENTER. Será exibida a seguinte listagem de opções:

```
C:\>net share /?
```

A sintaxe deste comando é:

```
NET SHARE
compartilhamento
    compartilhamento=unidade:caminho [/USERS:número | /UNLIMITED]
                                    [/REMARK:"texto"]
                                    [/CACHE:Manual | Automatic | No ]
    compartilhamento [/USERS:número | /UNLIMITED]
                    [/REMARK:"texto"]
                    [/CACHE:Manual | Automatic | No ]
{compartilhamento | dispositivo | unidade:caminho} /DELETE
```

Para entender melhor esta sintaxe, vou apresentar alguns exemplos práticos de utilização do comando net share para realizar tarefas tais como:

---

**NOTA:** Entre o share e a barra deve ter um espaço em branco.

---

- ◆ Excluir um compartilhamento.
- ◆ Criar um compartilhamento.
- ◆ Modificar um compartilhamento.

### Compartilhando uma pasta usando o comando net share.

Vamos supor que você queira compartilhar uma pasta C:\publica, com um nome de compartilhamento docpub, com um número máximo de 10 conexões simultâneas e como comentário: Pasta de acesso público. Para criar este compartilhamento, utilize o seguinte comando:

```
net share docpub=C:\publica /Users:10 /remark:"Pasta de acesso público"
```

Ao executar este comando você recebe a seguinte mensagem:

O recurso docpub foi compartilhado com êxito.

Se você abrir o Windows Explorer, poderá observar que a pasta C:\publica foi compartilhada. Clique com o botão direito do mouse nesta pasta e no menu que surge dê um clique na opção Compartilhamento. Observe que o número máximo de 10 usuários simultâneos foi definido, bem como o comentário: Pasta de acesso público.

A seguir descrevo as principais opções do comando net share:

- ◆ **/Users:número:** Define o número máximo de usuários simultâneos no compartilhamento.
- ◆ **/Unlimited:** Define que o compartilhamento não tem limite para usuários simultâneos.
- ◆ **/Remark:"texto do comentário":** Utilizado para definir ou alterar o comentário do compartilhamento.
- ◆ **/Cache:manual, /Cache:documents, /Cache:programs, ou /Cache:no:** Define opções de cache para o compartilhamento. Estas opções foram explicadas no tópico referente ao trabalho com pastas Off-line, anteriormente neste capítulo.

## Modificando um compartilhamento usando o comando net share.

Suponha que você queira alterar o compartilhamento docpub, criado anteriormente. Ao invés de 10 conexões simultâneas você vai permitir apenas 5 conexões. Para alterar o compartilhamento docpub, conforme proposto, utilize o seguinte comando:

```
net share docpub /Users:5
```

Ao executar este comando você recebe a seguinte mensagem:

**Comando concluído com êxito.**

Se você acessar as propriedades de compartilhamento da pasta C:\publica, verá que o limite de usuários simultâneos já foi alterado para 5.

## Excluindo um compartilhamento usando o comando net share.

Agora você irá excluir o compartilhamento docpub criado anteriormente. É importante salientar que, ao excluir um compartilhamento, o administrador apenas está fazendo com que a pasta ou impressora deixe de ser compartilhada. A pasta no disco rígido, com a qual o compartilhamento estava relacionado não será excluída, apenas deixará de estar compartilhada. No nosso exemplo, vou excluir o compartilhamento docpub, porém a pasta C:\publica continuará no drive C:

Para excluir o compartilhamento execute o seguinte comando:

```
net share docpub /delete
```

Ao executar este comando você recebe a seguinte mensagem:

**Êxito na exclusão de docpub.**

Se você abrir o Windows Explorer ou o Meu computador, poderá observar que a pasta C:\publica não está mais compartilhada. Isto é facilmente comprovado, pois não aparece mais uma pequena mão “segurando” a pasta.

## O comando net use.

O comando net use pode ser utilizado para executar uma série de tarefas, tais como:

- ◆ mapear um drive de rede.
- ◆ “desmappear” um drive de rede.
- ◆ exibir um listagem dos recursos de rede aos quais o usuário logado está conectado.

Se você executar o comando net use, sem nenhum parâmetro, será exibida uma listagem com todos os recursos aos quais o usuário está conectado.

Execute o seguinte comando:

```
net use
```

Você obtém uma listagem no seguinte formato:

```
C:\>net use
```

Novas conexões serão lembradas.

| Status                       | Local | Remoto                 | Rede                   |
|------------------------------|-------|------------------------|------------------------|
| Desconectado                 | X:    | \microxp02\Axcel Books | Rede Microsoft Windows |
| OK                           | Z:    | \servidor\Axcel Books  | Rede Microsoft Windows |
| Comando concluído com êxito. |       |                        |                        |

Na listagem anterior, é apresentado um exemplo em que o usuário tem dois drives mapeados. O drive X: que acessa o compartilhamento Axcel Books no computador microxp02. Observe que o status do drive X: é desconectado. Isto pode acontecer se o computador microxp02 estiver desligado ou sem contato com a rede. O drive Z: que acessa o compartilhamento Axcel Books no computador servidor. Observe que o status do drive Z: é OK, ou seja, o usuário pode acessá-lo normalmente, usando o Meu computador ou o Windows Explorer.

Também é possível mapear um drive de rede utilizando o comando net use. Por exemplo, para mapear um drive W: associado ao compartilhamento documentos em um computador chamado servidor, utilizamos o seguinte comando:

```
net use w: \\servidor\documentos
```

Para uma listagem completa, com todas as opções do comando net use, execute o seguinte comando:

```
net use /?
```

pressione ENTER. Será exibida a seguinte listagem de opções:

```
C:\>net use /?
```

A sintaxe deste comando é:

```
NET USE  
[dispositivo[*] [\computador\compartilhamento[\volume] [senha | *]]  
 [/USER:[domínio\]usuário]  
 [/USER:[nome de domínio com ponto\]usuário]  
 [/USER:[nome_usuario@nome de domínio com ponto]]  
 [/SMARTCARD]  
 [/SAVECRED]  
 [[/DELETE] | [/PERSISTENT:{YES | NO}]]  
 NET USE {dispositivo | *} [senha | *] /HOME  
 NET USE [/PERSISTENT:{YES | NO}]
```

Por exemplo, para desconectar o drive w:, mapeado anteriormente, utilize o seguinte comando:

```
net use w: /delete.
```

Se você quiser que um drive seja mapeado toda vez que o usuário faz o logon, utilize a opção: /Persistent:yes. Esta opção é equivalente a marcar a opção Reconectar-se durante o logon, quando mapeamos um drive utilizando o Meu computador ou o Windows Explorer.

**NOTA:** Para executar os comandos descritos neste tópico, abra o Prompt de comando: Iniciar -> Todos os programas -> Acessórios -> Prompt de comando.

**NOTA:** Entre o 'use' e a barra deve ter um espaço em branco.

## O comando net statistics

O Windows Server 2003, a exemplo do que acontece com o Windows 2000, inicializa uma série de serviços, na inicialização do Sistema Operacional. Cada serviço realiza uma tarefa específica. Dois dos serviços mais importantes são os seguintes:

- ◆ Workstation.
- ◆ Server.

O serviço Workstation é o responsável pela interface do Windows Server 2003 com o usuário. É este serviço que carrega e disponibiliza a interface gráfica e todos os seus recursos. Problemas neste serviço podem fazer com que o Windows Server 2003 se torne inoperante.

O serviço Server é responsável por atender requisições de outros computadores da rede, que acessam pastas, impressoras e demais recursos disponíveis.

O comando net statistics pode ser utilizado para fornecer informações sobre estes dois serviços: Workstation e Server.

Para obter informações sobre o serviço Workstation, abra um prompt de comando e execute o seguinte comando:

```
net statistics workstation
```

Serão exibidas uma série de informações, conforme indicado a seguir:

```
C:\>net statistics workstation
Estatísticas da estação de trabalho para \\MICROXP01
Estatísticas desde 4/1/2002 8:36 PM

Bytes recebidos      11366569
Blocos de mensagens de servidor (SMB) recebidos      22514
Bytes transmitidos    18109983
Blocos de mensagens de servidor (SMB) transmitidos    22527
Operações de leitura     2056
Operações de gravação    1965
Leituras não processadas negadas   0
Gravações não processadas negadas   0
Erros de rede          0
Conexões estabelecidas    10
Reconexões estabelecidas   79
O servidor se desconecta    3
Sessões iniciadas        0
Sessões suspensas        0
Sessões falhadas         0
Operações falhadas       11
Contagem de uso           41
Contagem de uso falhada   11
Comando concluído com êxito.
```

Estas informações podem ser muito úteis para o Administrador do sistema. Por exemplo, um grande número de Leituras não processadas negadas ou de Gravações não processadas negadas, pode indicar um usuário tentando acessar recursos para os quais ele não tem permissão. Isso pode caracterizar um ataque, isto é, uma tentativa de quebra de segurança.

Para obter informações sobre o serviço Server, abra um prompt de comando e execute o seguinte comando:

```
net statistics server
```

Serão exibidas uma série de informações, conforme indicado a seguir:

```
C:\>net statistics server
Estatísticas do servidor para \\MICROXP01
Estatísticas desde 4/1/2002 8:36 PM
Sessões aceitas          2
Sessões com tempo limite excedido    0
Sessões com erros         0
KB enviados              6330
KB recebidos              388
Tempo médio de resposta (mseg)  0
Erros de sistema          0
Violações de permissões     0
Violações de senha         0
Acessos a arquivos         263
Acessos a dispositivos de comunicação  0
Trabalhos de impressão no spool  0
Buffers esgotados
  Buffers grandes           0
  Buffers de requisição      0
Comando concluído com êxito.
```

## Pesquisando impressoras no Active Directory

Durante os exemplos práticos deste capítulo, principalmente nos exemplos de instalação de impressoras, salientei a importância da opção Listar no diretório. Ao marcar esta opção, quando uma impressora é instalada, informações sobre a impressora serão publicadas no Active Directory. Isso facilita a pesquisa de impressoras e a localização de uma impressora com as características desejadas. Também salientei a importância de preencher os campos Localização e Comentários. É importante definir um padrão para preenchimento destes campos. Por exemplo, no campo comentários você pode colocar o modelo da impressora, seguida da característica principal e de alguma outra informação relevante. Estas informações são publicadas no Active Directory e facilitam a localização das impressoras disponíveis.

Caso você não tenha preenchido os campos Localização e Comentários ou não tenha marcado a opção Listar no Diretório, durante a instalação da impressora, você poderá configurar estas opções depois da instalação. Para isso basta acessar a pasta impressoras, clicar com o botão direito do mouse na impressora a ser configurada e no menu de opções que é exibido clique em Propriedades. Na janela de propriedades clique na guia Geral. Nesta guia você pode preencher os campos Localização e Comentários, conforme exemplo da Figura 7.37:

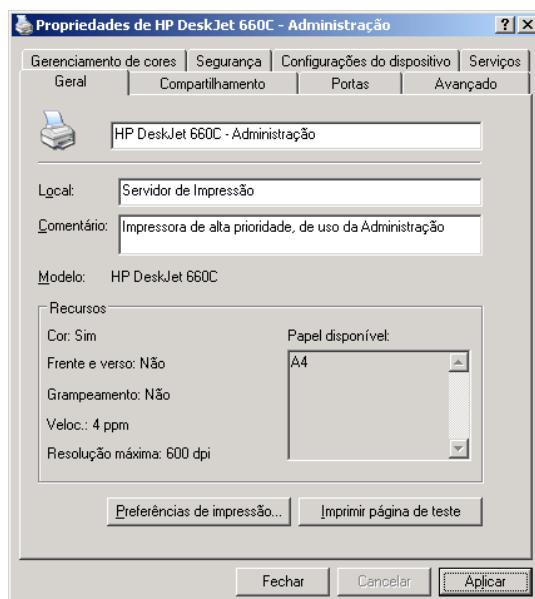


Figura 7.37 Configurando as propriedades da impressora.

A opção Listar no Diretório está disponível na guia Compartilhamento, da janela de propriedades da impressora. Caso você não tenha marcado esta opção durante a instalação da impressora, você pode acessar as propriedades da impressora, clicar na guia Compartilhamento e marcar esta opção.

A seguir apresento um exemplo prático de como pesquisar impressoras no Active Directory.

Exemplo: Para pesquisar impressoras no Active Directory, siga os passos indicados a seguir:

1. Execute o comando Iniciar -> Pesquisar
2. Na janela Resultados da Pesquisa, no painel da esquerda, clique na opção Outras opções de pesquisa.
3. Nas opções que são exibidas no painel da esquerda clique em Impressoras, computadores ou pessoas.
4. Serão exibidas três opções, conforme indicado na Figura 7.38:

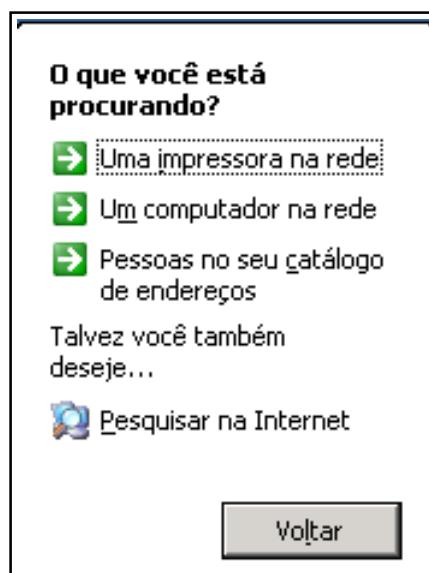


Figura 7.38 Opções de pesquisa.

5. Clique na opção Uma impressora na rede.
6. Será aberta a ferramenta Localizar Impressoras. Nesta ferramenta você pode fazer pesquisa por nome, localização ou modelo. Por exemplo, para pesquisar todas as impressoras HP Deskjet, preencha o campo Modelo, conforme exemplo da Figura 7.39:

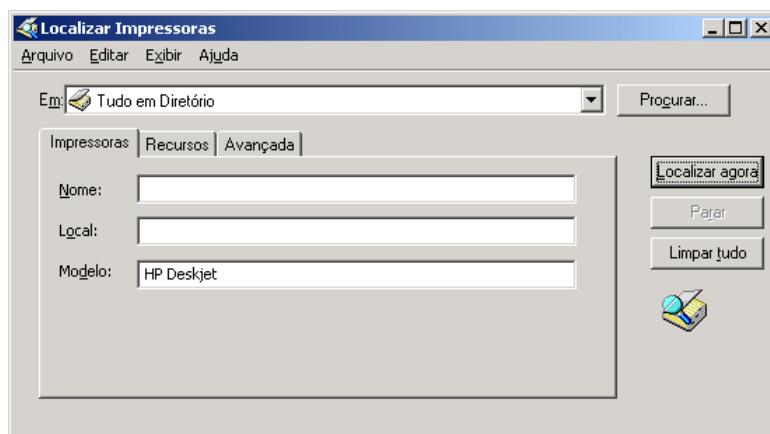
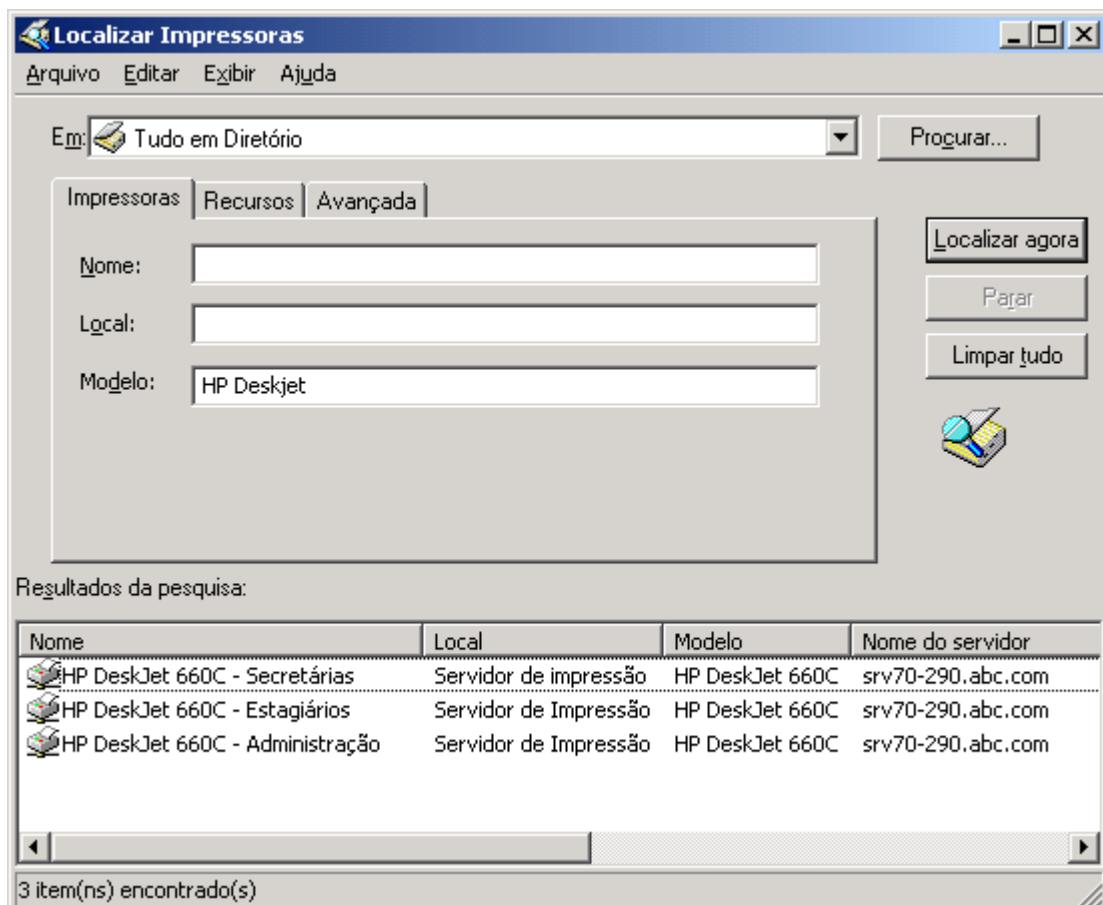


Figura 7.39 Pesquisando por modelo da impressora.

- Clique no botão Localizar agora. A ferramenta pesquisa no Active Directory e retorna a lista de impressoras encontradas, conforme indicado na Figura 7.40:



**Figura 7.40 Impressoras encontradas.**

- Para instalar uma das impressoras localizadas, basta clicar com o botão direito do mouse na impressora a ser utilizada. No menu de opções que é exibido clique em Conectar-se. Pronto, o Windows Server 2003 carrega o driver da impressora a partir do servidor onde a impressora está instalada e instala a impressora para ser utilizada.
- Para limpar os critérios de pesquisa e fazer uma nova pesquisa, clique no botão Limpar tudo. Os critérios definidos anteriormente serão excluídos e a listagem de impressoras será oculta. Agora você pode digitar novos critérios para fazer uma nova pesquisa. Se você deixar todos os campos de pesquisa em branco e clicar no botão Localizar agora, serão exibidas todas as impressoras compartilhadas, disponíveis na rede.
- No campo Em, você pode selecionar onde será feita a pesquisa, se em toda a rede, em um domínio ou servidor específico.
- Você também pode salvar uma pesquisa usando o comando Arquivo -> Salvar pesquisa... A consulta será salva em um arquivo no disco rígido. Quando necessário você pode usar o comando Arquivo -> Abrir para abrir uma consulta salva no disco rígido.
- Após ter feito as consultas e localizado a impressora desejada, feche a ferramenta Localizar Impressoras.
- Você estará de volta à janela Resultados da Pesquisa. Feche esta janela.

# Conclusão

Neste capítulo tratei basicamente de impressão no Windows Server 2003. Abordei uma série de tópicos relacionados com impressão, desde a instalação de uma impressora para uso localmente, até recursos mais sofisticados, como a publicação e pesquisa de impressoras de rede no Active Directory.

Iniciei o capítulo falando sobre o sistema de impressão do Windows Server 2003. Defini termos utilizados quando se trata de impressão no Windows Server 2003. Devido a importância destes termos, repito a terminologia utilizada no Windows Server 2003:

No Windows Server 2003 são utilizados os seguintes termos:

- ◆ **printer (Impressora):** Este termo refere-se a impressora propriamente dita, ao hardware. Ou seja, uma HP Deskjet 660 C, uma Rima Okidata 1100, uma Epson LX 300 e assim por diante (que no Windows NT Server 4.0 e Windows 2000 Server era chamado de print device)
- ◆ **logical printer:** faz referência ao driver da impressora, ao software instalado e que controla a impressora. É o elemento que aparece na pasta Printers (Impressoras). Também aparece, em alguns pontos da documentação oficial, o termo printer driver (driver da impressora).

Neste capítulo utilizei os termos adotados pelo Windows Server 2003, ou seja: printer faz referência ao hardware, a impressora propriamente dita e logical printer faz referência ao driver, ao software que controla a impressora.

Em seguida comecei a mostrar como executar uma série de operações práticas com impressoras. Iniciei mostrando como usar o assistente para instalação de impressoras para instalar o driver de uma impressora para uso local. Falei sobre o conceito de portas de impressão. Em seguida mostrei como compartilhar a impressora para que esta possa ser utilizada por outros computadores da rede. O próximo passo foi mostrar como acessar uma impressora que está compartilhada para uso através da rede.

O próximo passo foi falar sobre a definição de permissões de acesso a impressoras. Você aprendeu que existem diferentes níveis de permissão de acesso, conforme indicado a seguir:

- ◆ **Print (Imprimir):** Permite ao usuário conectar-se à Impressora e imprimir documentos, pausar, reiniciar e continuar a impressão dos documentos por ele enviados para a impressora. Quando um usuário envia um documento para a impressora, o usuário torna-se o dono daquele documento, por isso que ele pode administrar os documentos por ele enviados. Esta permissão normalmente atribuída para aqueles usuários que simplesmente precisam enviar documentos para a impressora. Por padrão, quando uma nova impressora é instalada, a permissão Print (Imprimir) é atribuída ao grupo Everyone (Todos), conforme descrito anteriormente.
- ◆ **Manage Documents (Gerenciar documentos):** Tem todas as permissões atribuídas a permissão Print (Imprimir), mais Controlar a impressão de todos os documentos (enviados por qualquer usuário) e também pausar, reiniciar e continuar a impressão de qualquer documento enviado por qualquer usuário. Normalmente atribuída para aquele usuário que administra a impressora, resolvendo problemas de impressão, mas sem permissões para alterar propriedades e permissões da impressora. Quando a permissão Manage Documents (Gerenciar documentos) for atribuída a um usuário, ele não poderá acessar documentos existentes que estejam aguardando para serem impressos, na fila de impressão. A permissão se aplicará somente aos documentos enviados para a impressora depois que a permissão tiver sido atribuída ao usuário.
- ◆ **Manage Printers (Gerenciar impressoras):** Todas as permissões de Print (Imprimir) e Manage documents (Gerenciar documentos), mais permissões para cancelar a impressão de todos os documentos pendentes, compartilhar a impressora, alterar as propriedades da impressora, eliminar a impressora e alterar as permissões

de impressão. Normalmente atribuída a um usuário que deve ter poderes completos na administração da impressora, inclusive podendo remove-la do sistema. Por padrão, os membros dos grupos Administrators (Administradores), Print Operators (Operadores de Cópia) e Server Operators (Operadores de Servidores) têm esta permissão.

Em seguida você aprendeu a gerenciar a fila de impressão. A medida que os documentos vão sendo enviados para a impressora, eles vão sendo colocados em uma fila de impressão. Também mostrei que é possível gerenciar esta fila utilizando o navegador, desde que o IIS esteja instalado no servidor onde a impressora está compartilhada.

Na seqüência mostrei como configurar opções importantes da impressora, tais com o horário de disponibilidade e a prioridade de uso da impressora.

Em seguida mostrei uma série de exemplos de situações práticas que podem ocorrer no dia-a-dia. Comecei falando sobre como configurar uma impressora para que possa ser utilizada por diferentes grupos de usuários, com diferentes níveis de prioridade. Em seguida mostrei como configurar portas TCP/IP padrão para instalar uma impressora de rede como se fosse uma impressora local. Também mostrei como configurar um pool de impressão.

O próximo passo foi apresentar uma série de comandos para administração de compartilhamentos, tanto de compartilhamentos de pasta quanto de compartilhamentos de impressoras. Para finalizar o capítulo mostrei como pesquisar impressoras no Active Directory.

# Introdução

Nesta capítulo tratarei dos seguintes assuntos:

- ◆ Agendamento de tarefas.
- ◆ Tipos de Backup.
- ◆ Estratégias de backup e restore.
- ◆ Ações práticas de backup e restore.
- ◆ Backup e Restore do Active Directory

Vou iniciar o capítulo tratando sobre: Agendamento de Tarefas. Conforme mostrarei, é possível fazer o agendamento de tarefas, de tal forma que uma determinada tarefa pode ser programada para executar um ou mais passos, em dias e horários previamente configurados pelo Administrador. Posso definir qual ação cada passo de uma tarefa irá realizar. Por exemplo, no primeiro passo verifica se uma determinada pasta já existe, se existir, o segundo passo da tarefa será excluir a pasta e um terceiro passo cria uma nova pasta. Este é apenas um exemplo simples, conforme mostrarei, é possível configurar uma tarefa para executar operações bastante complexas.

Além de definir quais os passos serão executados por uma tarefa, você também pode configura-la para ser executada, automaticamente, em horários e datas definidas. Por exemplo, posso ter uma tarefa que seja iniciada durante os dias de semana (de segunda à sexta-feira), às 23:30 e aos sábados e domingos, às 22:00.

O uso de tarefas agendadas é de grande ajuda para o Administrador, pois permite que ações repetitivas, que tenham que ser executadas diariamente, possam ser agendadas para execução automática. Conforme mostrarei neste capítulo, o agendamento de tarefas é extremamente simples de ser feito com o auxílio de um assistente para a criação e o agendamento de tarefas.

Para finalizar o assunto ‘Tarefas Agendadas’, apresentarei os comandos relacionados com o agendamento de tarefas. Estes comandos são úteis para a criação de scripts, os quais quando executados, criam uma ou mais tarefas agendadas. Por exemplo, o administrador pode criar e distribuir um script que agenda uma determinada tarefa para execução nos vários servidores da rede. Passado o período para execução da tarefa, o administrador pode distribuir um script com comandos que excluem a tarefa agendada. Para criar estes scripts, o administrador tem que conhecer os comandos relacionados à tarefas agendadas.

A próxima etapa será falar sobre a importância das cópias de segurança, o já famoso: Backup. Nunca é demais ressaltar a importância de manter cópias de segurança de todos os arquivos de dados: documentos do Word, planilhas do Excel, bancos de dados, documentos de texto e assim por diante, bem como manter backup da instalação dos servidores e de toda e qualquer informação necessária ao funcionamento da empresa. A cópia de segurança é a única proteção que o Administrador tem para o caso de um dano físico no disco rígido.

# CAPÍTULO

## 8

### Fazendo o Backup dos Dados e Agendando Tarefas

Falarei sobre os diferentes tipos de cópia de segurança (backup) que existem, quais as estratégias de backup/restore que podem ser utilizadas. Na parte prática vou reforçar a importância do planejamento para a criação de um estratégia de backup eficiente. Mostrarei que é possível automatizar as rotinas de backup, mediante o uso de tarefas agendadas. Este é um exemplo típico de tarefa repetitiva, que deve ser executada fora do horário de expediente e que é adequada para a automação por meio do recurso de tarefas agendadas do Windows Server 2003.

## O conceito de Tarefas agendadas

O administrador pode utilizar a opção Tarefas agendadas, do Painel de controle, para agendar tarefas que serão executadas em um determinado horário, em determinados dias da semana e que executarão uma ou mais ações. Você pode agendar qualquer programa que roda no Windows Server 2003 para ser executado através de uma tarefa agendada. Pode agendar uma tarefa de tal forma que ela seja executada uma única vez, ou que seja executada em intervalos regulares ou em um determinado horário especificado.

Você pode utilizar Tarefas agendadas para executar rotinas de manutenção em horários específicos. Por exemplo, é possível criar uma tarefa que efetua cópia de segurança dos arquivos alterados durante o dia, e agenda-la para ser executada as duas horas da madrugada.

Uma tarefa também pode ser programada para ser executada uma única vez e depois de executada, ser automaticamente eliminada da lista de tarefas agendadas. Também é possível executar uma tarefa a qualquer momento, sem ter que esperar que ela seja executada automaticamente, no horário programado. É possível acompanhar o histórico de execução de uma determinada tarefa, para sabermos se ela está sendo executada normalmente ou está apresentando algum problema.

Com o agendador de tarefas, que será visto na parte prática, você pode executar uma série de operações com tarefas agendadas, tais como:

- ◆ Criar e agendar novas tarefas para execução diária, semanal, mensal, em horários específicos ou durante a ocorrência de eventos específicos, tais como a inicialização ou o desligamento do sistema.
- ◆ Alterar o agendamento e as demais configurações de uma tarefa já existente.
- ◆ Parar e desativar uma tarefa agendada.
- ◆ Personalizar a maneira como uma tarefa é executada.

Cada tarefa que você cria é gravada em um arquivo com a extensão .JOB. Estes arquivos são gravados na pasta WINDOWS\TASKS, considerando que o Windows Server 2003 esteja instalado na pasta WINDOWS.

Você pode copiar os arquivos .JOB de um servidor para o outro, dentro da pasta TASKS. O único cuidado que você deve ter é se a conta que foi configurada para execução da tarefa (toda tarefa é executada no contexto de uma conta de usuário ou da conta Local System) é válido no servidor de destino, onde o arquivo .JOB foi copiado.

O agendamento e execução de tarefas é controlado pelo serviço Task Scheduler (Agendador de tarefas), o qual é configurado para inicializar automaticamente, durante a inicialização do Windows Server 2003, conforme indicado na Figura 8.1.

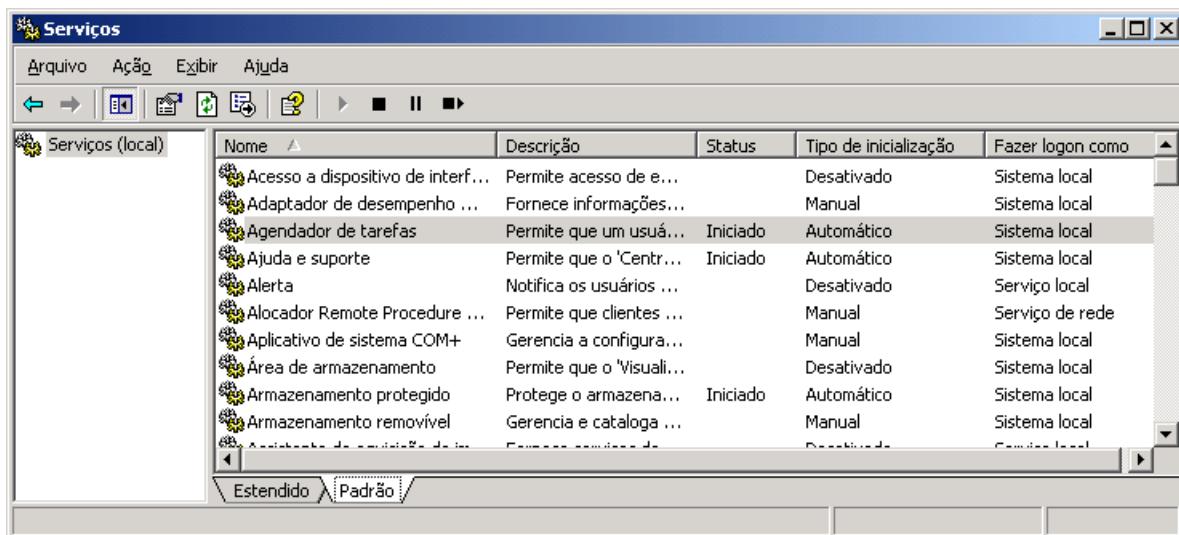
---

**NOTA:** Na prática, além dos usuários com permissões de administrador, os membros dos grupos Backup Operators (Oper. de Cópias) e Server Operators (Oper. de Servidores), também tem permissão para criar e configurar novas tarefas agendadas.

---

**NOTA:** Se você estiver trabalhando em um servidor que foi migrado do NT Server 4.0 ou do Windows 2000 Server, para o Windows Server 2003, é provável que a pasta de instalação do Windows seja a pasta WINNT.

---



**Figura 8.1 Servico Agendador de tarefas, configurado para inicializaco automtica.**

Você pode programar uma tarefa para que execute um programa, como por exemplo o Microsoft Excel ou o Microsoft Access; para que execute um aplicativo com comandos de administração do Windows Server 2003, como por exemplo scripts no padrão WSH – Windows Scripting Host ou os já conhecidos arquivos .bat, os quais contém um comando em cada linha, comandos estes que são executados em seqüência; para que execute um atalho, o que na prática equivale a abrir o programa ao qual o atalho se refere ou para executar um documento, como por exemplo um .doc, o que na prática equivale a dar um clique duplo no documento, ou seja: O Word será aberto e o documento carregado.

É possível agendar tarefas para serem executadas toda vez que o computador é inicializado. Este tipo de tarefa será executado, independentemente de haver ou não um usuário logado. Também é possível agendar uma tarefa para ser executada toda vez que um usuário faz o logon no servidor. Este tipo de tarefa será iniciado quando o primeiro usuário fizer o logon, depois que o servidor tiver sido inicializado. Se o usuário fizer o logoff e outro usuário fizer o logon, a tarefa não será reinicializada, o que só acontece quando o computador for reinicializado e um usuário (qualquer usuário) fizer o logon depois da reinicialização.

**Questões de segurança, relacionadas com tarefas agendadas.**

Toda tarefa agendada deve ser executada no contexto de uma conta de usuário. Quando o administrador cria uma tarefa agendada, ele tem que informar o nome de uma conta de usuário e a respectiva senha. Quando a tarefa for executada, independentemente do usuário que estiver logado ou se não houver nenhum usuário logado, a tarefa é executada como se tivesse sido iniciada pelo usuário cuja conta foi informada durante a criação da tarefa agendada. Isso que significa “executar no contexto de uma conta”.

Por exemplo, se você configurar uma tarefa agendada para rodar com uma conta com permissão de administrador. Quando a tarefa for executada é como se um usuário do grupo administrador estivesse logado e tivesse disparado a tarefa manualmente. Se durante a execução da tarefa um outro usuário estiver logado, a tarefa executa normalmente, porém a sua execução não será visível para o usuário que está logado, pois a tarefa está executando no contexto da conta de usuário que foi informada quando da criação da tarefa.

**NOTA:** Para acessar a lista de serviços disponíveis em um servidor, você usa o console Serviços (Iniciar -> Ferramentas administrativas -> Serviços). Com o console serviços você pode verificar os serviços disponíveis, alterar as configurações do serviço (configurá-lo para inicializar manualmente ou automaticamente), alterar a conta com a qual é executado o serviço e assim por diante.

Para poder criar uma tarefa agendada você deve estar logado com uma conta com permissão de administrador ou com uma conta pertencente a um dos seguintes grupos: Backup Operators (Oper. de Cópia) ou Server Operators (Oper. de Servidores). Você não pode configurar uma tarefa agendada para rodar com uma conta com nível de permissão maior do que o nível de permissão da conta com a qual você está logado. Vou esclarecer esta última informação com um exemplo prático. Imagine que você está logado com uma conta com permissão de Oper. de Cópia e está criando uma tarefa agendada. Você não poderá configurar esta tarefa agendada para executar no contexto de uma conta com permissão de administrador, pois o conjunto de permissões de administrador é maior (tem mais poderes e acesso a mais funções e recursos) do que o conjunto de permissões dos membros do grupo Oper. de Cópia.

O administrador pode atribuir a permissão de criar e agendar tarefas para outros usuários, que não somente os pertencentes aos grupos Administrators (Administradores), Backup Operators (Oper. de Cópia) ou Server Operators (Oper. de Servidores). Para isso basta alterar as permissões NTFS da pasta Tasks, a qual fica dentro da pasta onde o Windows Server 2003 está instalado, normalmente \WINDOWS\TASKS ou \WINNT\TASKS.

No Windows Server 2003, conforme descrito no Capítulo 4, a senha das contas de usuários tem que ser alteradas de tempos em tempos, de acordo com as definições das diretivas de senhas do domínio. Quando você cria uma tarefa agendada, você informa o nome de uma conta e a respectiva senha. Quando a senha desta conta for alterada, no Active Directory, a alteração não será feita também na tarefa agendada. Com isso, nas propriedades da tarefa agendada, estará sendo informada uma senha que não é mais válida. O efeito prático disso é que a tarefa deixará de ser executada. Quando o Windows Server 2003 tenta executar a tarefa, ele verifica se a senha informada está correta. Como a senha foi alterada, na conta do usuário, a senha informada nas propriedades da tarefa agendada estará diferente e a tarefa não poderá ser executada. Para evitar este problema é indicado que você crie uma conta especificamente para ser usada por uma ou mais tarefas agendadas e que marque a opção A senha nunca expira, para a conta que está sendo criada, conforme exemplo da Figura 8.2:

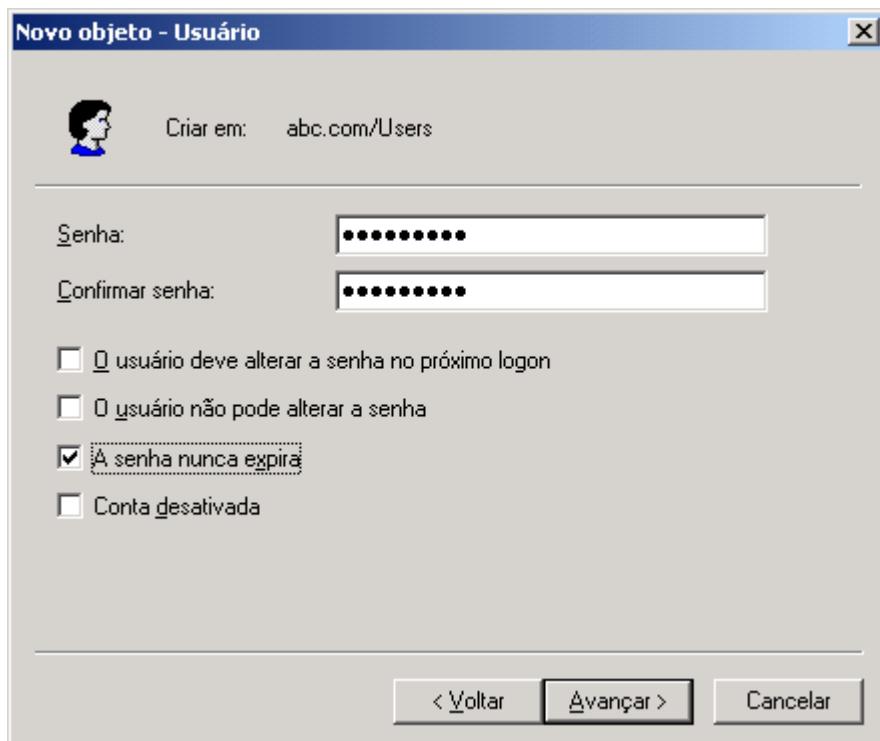


Figura 8.2 A opção “A senha nunca expira”.

Outro detalhe importante é que a conta com a qual a tarefa foi configurada para execução, deve ter permissão para executar os programas e dados acessados durante a execução da tarefa. Caso contrário a execução da Tarefa agendada irá falhar.

## Criação e Administração de Tarefas agendadas.

A criação, configuração e administração das tarefas agendadas é feita através da opção Tarefas agendadas, do Painel de Controle. Na verdade esta opção é simplesmente um atalho para a pasta TASKS já citada anteriormente.

Abra o Painel de controle: Iniciar -> Painel de controle e dê um clique duplo na opção Tarefas agendadas. Será aberta a janela Tarefas agendadas, indicada na Figura 8.3. Observe que, por padrão, em um novo servidor, não existe nenhuma tarefa agendada. Existe apenas a opção Adicionar tarefa agendada.

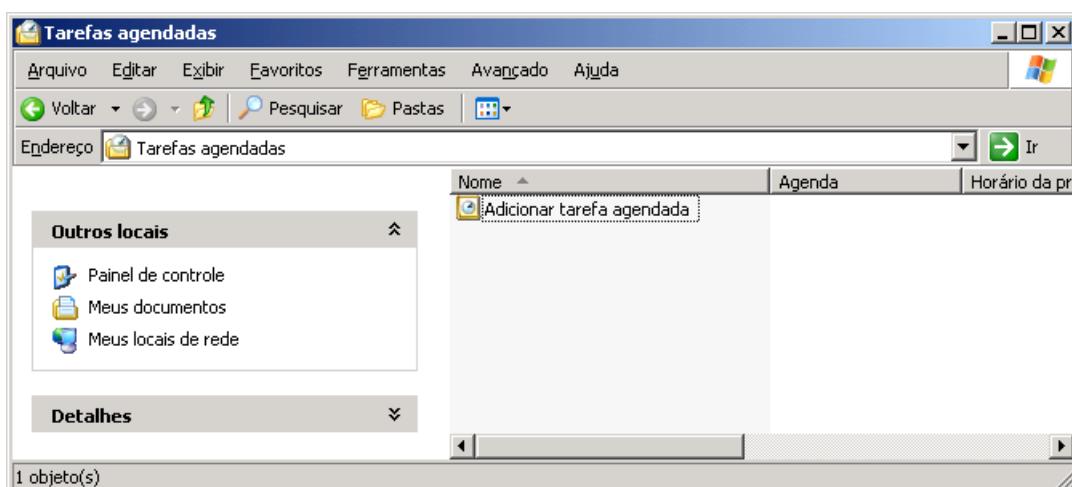


Figura 8.3 A janela para criação e administração de tarefas agendadas.

Na seqüência, apresentarei uma série de exemplos onde você aprenderá a criar, configurar e a administrar tarefas agendadas.

No exemplo a seguir você aprenderá a criar uma tarefa agendada simples. A tarefa será programada para executar a ferramenta Limpeza de disco, toda sexta-feira, as 16:30.

### Exemplo: Criando e agendando uma tarefa para execução automática.

1. Faça o logon como Administrador ou com uma conta com permissão de administrador. Também pode ser uma conta do grupo Oper. de Cópia ou Oper. de Servidores.
2. Abra o Painel de controle. Dê um clique duplo na opção Tarefas agendadas. Observe que existe somente um ícone: Adicionar tarefa agendada, conforme indicado anteriormente, na Figura 8.3, a não ser que você já tenha criado tarefas agendadas anteriormente. Caso já tenha sido agendada alguma tarefa, aparecerá um ícone para cada uma das tarefas agendadas.

---

**NOTA:** Você também poderia utilizar o Windows Explorer ou o Meu computador para abrir diretamente a pastas TASKS, a qual fica no caminho WINDOWS\TASKS, onde WINDOWS é a pasta onde está instalado o Windows Server 2003.

3. Dê um clique duplo no ícone Adicionar tarefa agendada. Será iniciado um assistente chamado Assistente de tarefa agendada. Este assistente o conduzirá passo-a-passo, na trabalho de criar e agendar uma tarefa.
4. A primeira tela do assistente é apenas informativa. Dê um clique no botão Avançar para seguir para a segunda etapa do assistente.
5. Surge uma tela, com uma listagem dos programas instalados no seu computador. Caso o programa que você deseja que seja executado pela tarefa, não apareça na listagem, você pode utilizar o botão Procurar, para indicar ao Windows Server 2003 a pasta e o nome do programa a ser executado pela tarefa agendada que está sendo criada.
6. Na Listagem de programas, selecione opção Limpeza de disco, conforme indicado na Figura 8.4 e dê um clique no botão Avançar para ir para a próxima etapa do assistente.

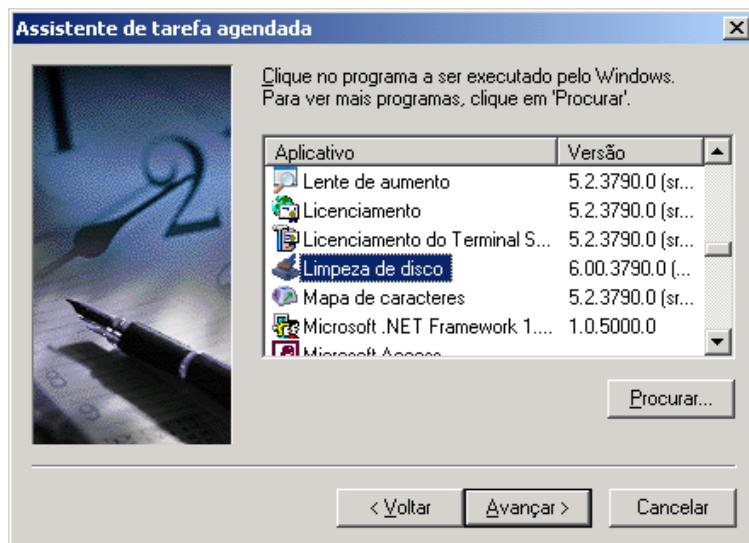


Figura 8.4 Agendando o utilitário Limpeza de disco, para ser executada automaticamente.

7. Surge uma tela pedindo para que você digite um nome para a tarefa que está sendo criada e que seja escolhida uma periodicidade para a execução. Configure as opções, conforme indicado na Figura 8.5, depois dê um clique no botão Avançar para ir para a próxima etapa do assistente.

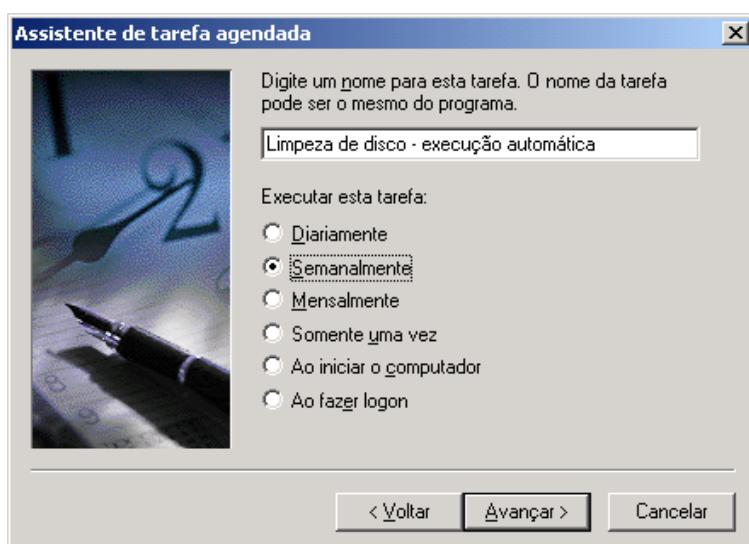


Figura 8.5 Atribuindo um nome para a tarefa e configurando a periodicidade.

8. Na tela desta etapa você pode configurar a Hora de início da tarefa, quais os dias em que a tarefa deve ser executada e se semanalmente (valor 1 no campo A cada), de duas em duas semanas (valor 2 no campo A cada) e assim por diante. Configura as opções conforme indicado na Figura 8.6 e depois dê um clique no botão Avançar para ir para a próxima etapa do assistente.

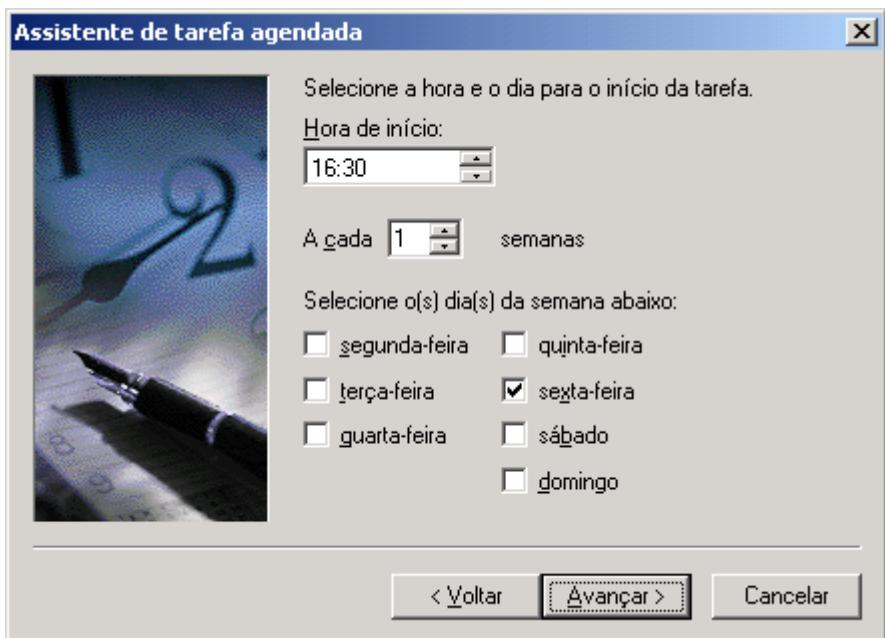


Figura 8.6 Configurando a Hora e os dias de execução da tarefa.

**NOTA:** Estou selecionando o agendamento Semanalmente, pois de acordo com o exemplo proposto, quero que a tarefa seja executada somente nas sextas-feiras. Ao selecionar Semanalmente, em uma das próximas etapas do assistente, o Windows Server 2003 possibilitará que eu selecione os dias e horários desejados.

9. Na tela desta etapa, você deve fornecer o nome de uma conta de usuário e a respectiva senha. Deve ser um usuário que tenha permissão para executar o programa que está sendo agendado, no nosso exemplo a ferramenta Limpeza de disco. Por exemplo, não são todos os usuários que tem permissões para fazer Cópias de Segurança das informações. Caso você crie uma tarefa para fazer Cópia de segurança (mais conhecida por Backup), nesta tela deve ser fornecido o nome e a senha de um usuário que tem a permissão para fazer a Cópia de segurança, pois caso contrário, a execução da tarefa irá falhar. Forneça o nome de um usuário, e digite a senha duas vezes. O nome do usuário é no formato “NOME DO COMPUTADOR \Nome do usuário” se você estiver utilizando uma conta local (no caso de um standalone Server – servidor que não faz parte do domínio) ou “NOME DO DOMÍNIO \Nome do usuário” se você estiver utilizando uma conta do Domínio. Vamos utilizar a conta Administrador do domínio ABC. Digite as informações para esta etapa, conforme indicado na Figura 8.7 e dê um clique no botão Avançar para ir para a sexta etapa do assistente.
10. Na tela desta etapa, o Windows Server 2003 exibe informações sobre a tarefa que está sendo agendada, com detalhes sobre as opções selecionadas nas etapas anteriores. Marque a opção Abrir as propriedades avançadas desta tarefa ao clicar em ‘Concluir’. Ao marcar esta opção, quando você clicar em Concluir, será aberta uma janela com opções de configuração avançadas da tarefa. Dê um clique no botão Finish (Concluir), para exibir a janela com as propriedades avançadas, conforme indicado na Figura 8.8.

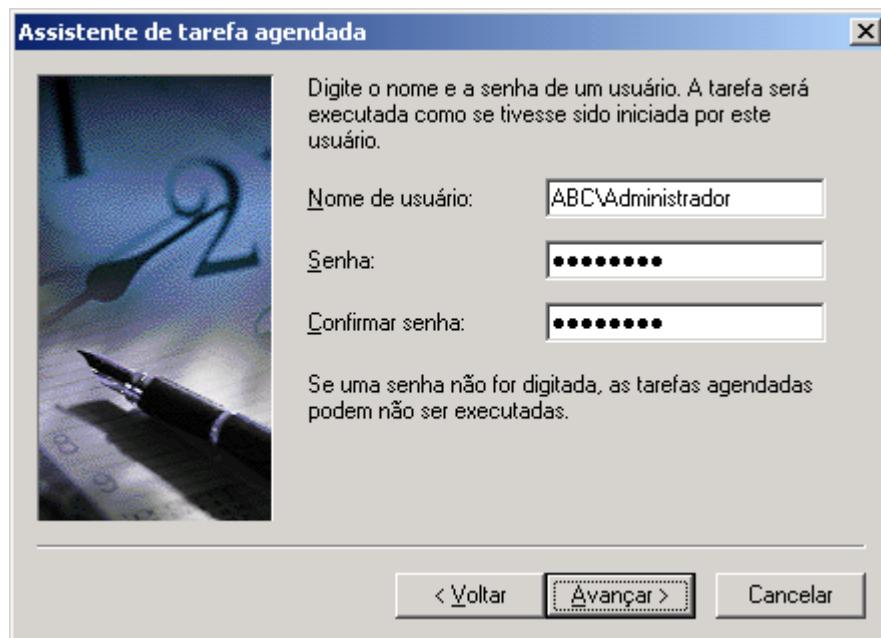


Figura 8.7 Toda tarefa agendada, exige o nome e senha de um usuário do domínio.

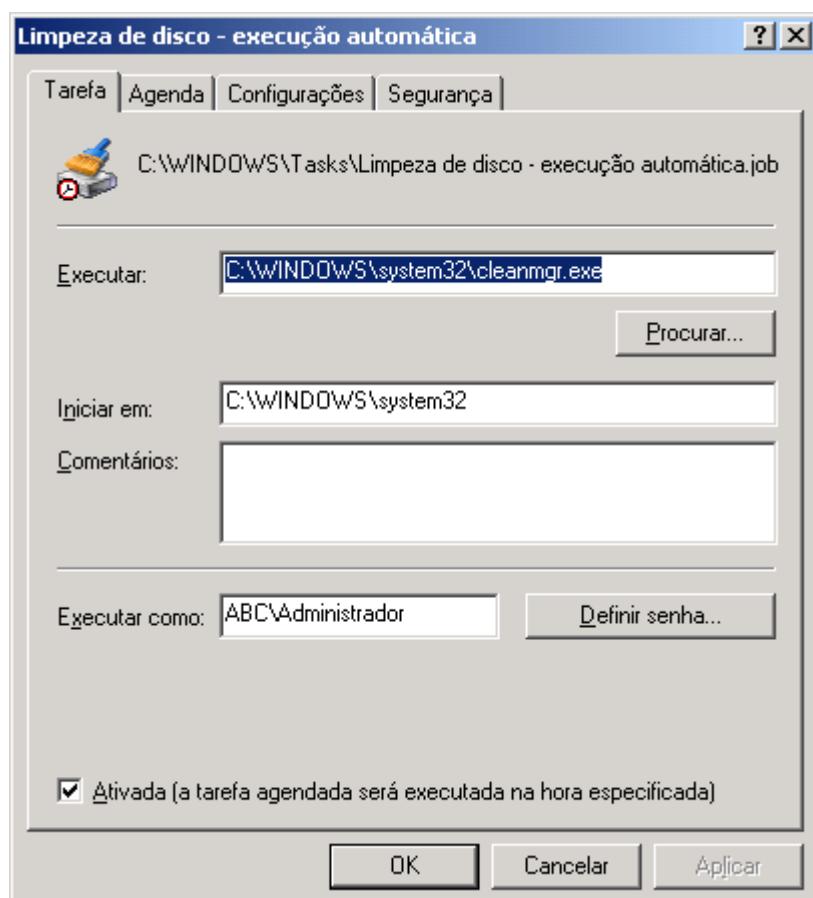


Figura 8.8 Janela com propriedades avançadas, da tarefa que está sendo criada.

Na janela de configurações avançadas, são exibidas as guias: Tarefa, Agenda, Configurações e Segurança. Na guia Tarefa são exibidas informações sobre o programa que será executado (campo Executar), a pasta base Iniciar em,

Comentários sobre a tarefa, o nome do usuário que será utilizado para execução da tarefa Executar como e uma caixa de seleção para Ativar/Desativar a tarefa.

Dê um clique na guia Agenda. Nesta guia você pode alterar o agendamento da tarefa, configurar opções avançadas do agendamento (botão Avançado...) e configurar múltiplos agendamentos.

Na guia Configurações, estão disponíveis as seguintes opções:

- ◆ **Excluir a tarefa se ela não estiver agendada para nova execução:** Esta opção é utilizada para criar tarefas que devem ser executadas uma única vez. Se você marcar esta opção, após a execução da tarefa com sucesso, o Windows Server 2003 se encarrega de excluir a tarefa. Essa opção é útil para as tarefas agendadas para uma única execução, como por exemplo, uma tarefa que irá copiar arquivos de um computador para o outro e que deve ser executada uma única vez.
- ◆ **Interromper a tarefa se ela for executada por:** Especifica se a tarefa é interrompida após estar em execução durante o período especificado e ainda não ter sido concluída. Esta opção é utilizada para evitar que a tarefa fique executando indefinidamente, caso aconteça algum problema com a execução da tarefa. Esta execução, mesmo com problemas, pode comprometer o desempenho do sistema como um todo.
- ◆ **Só iniciar a tarefa se o computador ficar ocioso no mínimo por:** Especifica que a tarefa agendada é iniciada apenas se você não tiver usado o teclado ou o mouse durante o período de tempo especificado. Se a tarefa for agendada para se repetir, sua primeira execução somente ocorrerá se o computador estiver ocioso durante o período especificado. Se o computador não estiver ocioso quando a tarefa efetuar sua primeira tentativa de inicialização, o Agendador de tarefas continuará verificando se o computador está ocioso pelo período especificado neste campo. Se o computador não se tornar ocioso durante esse período, nenhuma ocorrência da tarefa será executada. Pode ser utilizada para tarefas que não são urgentes e podem ser adiadas, a espera de um período de ociosidade do servidor.
- ◆ **Se o computador não estiver ocioso por tanto tempo, tentar novamente por até:** Fornece um espaço para você digitar o tempo (em minutos) no qual o Agendador de tarefas continuará verificando se o computador está ocioso. Se você tiver selecionado esta opção e o computador não estiver ocioso no horário agendado, você também poderá clicar nas setas de rolagem para selecionar uma nova configuração. Se o computador não se tornar ocioso durante esse período, nenhuma ocorrência da tarefa será executada.
- ◆ **Interromper a tarefa se o computador não estiver ocioso:** Especifica que a tarefa agendada deve ser interrompida se você começar a usar o computador durante a execução da tarefa, isto é, se o computador deixar de estar ocioso.
- ◆ **Não iniciar a tarefa se o computador estiver usando baterias:** Especifica se o início da tarefa agendada será desabilitado e não poderá executar as tarefas, enquanto o computador usa baterias. Por exemplo, pode ter havido uma queda de luz e o servidor estar sendo mantido por no-break. Alguns programas acessam com

**IMPORTANTE:** Em determinadas situações pode ser necessária a criação de múltiplos agendamentos. Por exemplo, vamos supor que uma tarefa deva ser executada todos os dias, às 23:30 hs. e também nos sábados e domingos às 11:30 hs. Neste caso é necessário a criação de dois agendamentos: um para executar a tarefa diariamente, às 23:30 hs. e outro para executar a tarefa aos sábados e domingos, às 11:30 hs.

frequência o disco rígido, causando um maior consumo de bateria. Você pode aumentar a vida útil das baterias marcando essa caixa de seleção.

- ◆ **Interromper a tarefa se o computador começar a usar baterias:** Especifica se a execução da tarefa agendada será interrompida quando o computador começar a usar baterias.
- ◆ **Acordar o computador para executar esta tarefa:** Especifica se o computador é ativado para a execução da tarefa no horário agendado, mesmo que esteja no modo de dormir e use o gerenciamento de energia OnNow. Clique na guia Segurança. Nesta guia você define quais usuários e grupos terão acesso e qual o nível de permissão de acesso à tarefa agendada que está sendo criada. Esta guia é muito semelhante à guia para definição de permissões NTFS em pastas e arquivos. Você utiliza o botão Adicionar... para incluir novos usuários ou grupos, o botão Remover para excluir usuários ou grupos e o botão Avançado..., para definir permissões especiais. Na prática, ao definir estas permissões, você está definindo as permissões de acesso ao arquivo .JOB, que é gravado na pasta TASKS. É importante lembrar que para cada tarefa agendada, o Windows Server 2003 cria um arquivo .JOB, o qual é gravado na pasta TASKS já descrita anteriormente. O arquivo .JOB contém todas as informações sobre a tarefa agendada.

11. Você não fará nenhuma alteração na janela de configurações avançadas. Clique em OK para fechá-la.
12. Você deve ter voltado à janela das tarefas agendadas. Observe que já existe um novo ícone para a tarefa recém criada, com o nome que você deu para a tarefa: Limpeza de disco - execução automática, conforme indicado pela figura 8.9:

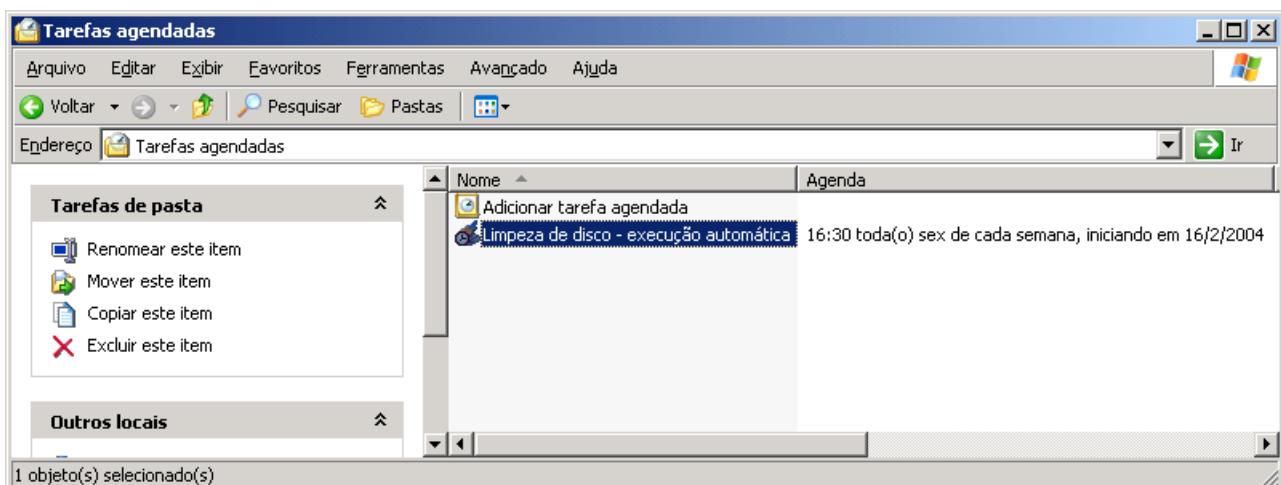


Figura 8.9 A nova tarefa já criada - Limpeza de disco - execução automática.

## Alterando uma tarefa agendada.

Após a criação de uma tarefa, o administrador ou um usuário com as devidas permissões, pode executar uma série de configurações na tarefa, inclusive o próprio agendamento da tarefa pode ser alterado. Neste tópico você aprenderá a fazer as seguintes alterações em uma tarefa agendada:

- ◆ Executar uma tarefa imediatamente, sem esperar pelo horário do agendamento.
- ◆ Renomear uma tarefa.
- ◆ Alterar a conta de usuário com a qual a tarefa é agendada.
- ◆ Alterar o agendamento da tarefa.
- ◆ Alterar opções avançadas do agendamento.

- ◆ Criar múltiplos agendamentos.
- ◆ Verificar o log do Agendador de tarefas.
- ◆ Excluir uma tarefa agendada.

### **Para executar uma tarefa imediatamente siga os passos indicados a seguir:**

1. Faça o logon como Administrador ou com uma conta com permissão de administrador ou com uma conta que tenha permissão para executar a tarefa agendada.
  2. Abra o Painel de controle. Dê um clique duplo na opção Tarefas agendadas.
  3. Clique com o botão direito do mouse na tarefa a ser executada e no menu de opções que é exibido, clique na opção Executar.
- ou
3. Clique na tarefa a ser executada para marca-la e selecione o comando Arquivo -> Executar.
  4. O Windows inicia a execução da tarefa. Por exemplo, se você executar a tarefa criada no exemplo anterior, a ferramenta Limpeza de disco será executada. Isto comprova que a tarefa foi executada com sucesso.

### **Para renomear uma tarefa agendada, siga os passos indicados a seguir:**

1. Faça o logon como Administrador ou com uma conta com permissão de administrador ou com uma conta que tenha permissão para alterar a tarefa agendada.
2. Abra o Painel de controle. Dê um clique duplo na opção Tarefas agendadas.
3. Clique com o botão direito do mouse na tarefa a ser renomeada e no menu de opções que é exibido, clique na opção Renomear.
4. Digite o novo nome e pressione Enter. Observe que quando você digita a primeira letra do novo nome, o nome antigo é excluído.

### **Alterar a conta com a qual a tarefa é executada.**

É importante salientar que a conta que está configurada para execução de uma tarefa, deve ter as devidas permissões para executar o programa ou comandos definidos para a tarefa. Se a conta não tiver as devidas permissões, a tarefa irá falhar, isto é, não será executada. A falha ou sucesso na execução é registrada em um log do Agendador de tarefas. Este log é um arquivo de texto, conforme mostrarei mais adiante.

Para alterar a conta com a qual a tarefa é executada, faça o seguinte:

1. Faça o logon como Administrador ou com uma conta com permissão de administrador ou com uma conta que tenha permissão para alterar a tarefa agendada.
2. Abra o Painel de controle. Dê um clique duplo na opção Tarefas agendadas.
3. Na janela Tarefas agendadas dê um clique duplo na tarefa a ser alterada. Será exibida a janela de propriedades da tarefa.
4. A guia Tarefa vem selecionada por padrão. No campo Executar como, você digita o nome da conta a ser utilizada, em um dos seguintes formatos:

**Nome\_do\_computador\Nome\_da\_conta**

ou

**Nome\_do\_Domínio\Nome\_da\_conta**

5. Clique no botão Definir senha... Será aberta a janela Definir senha, onde você deve informar a senha do usuário duas vezes, para confirmação, conforme indicado na Figura 8.10:

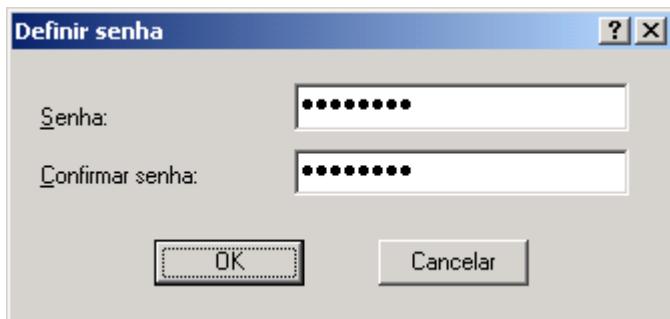


Figura 8.10 Informando a senha da conta com a qual será executada a tarefa.

6. Informe a senha duas vezes e clique em OK para fechar a janela Definir senha.  
7. Você estará de volta à janela de propriedades da tarefa. Clique em OK para fechá-la. Feito isso a conta de execução da tarefa terá sido alterada.

## Alterar o agendamento da tarefa.

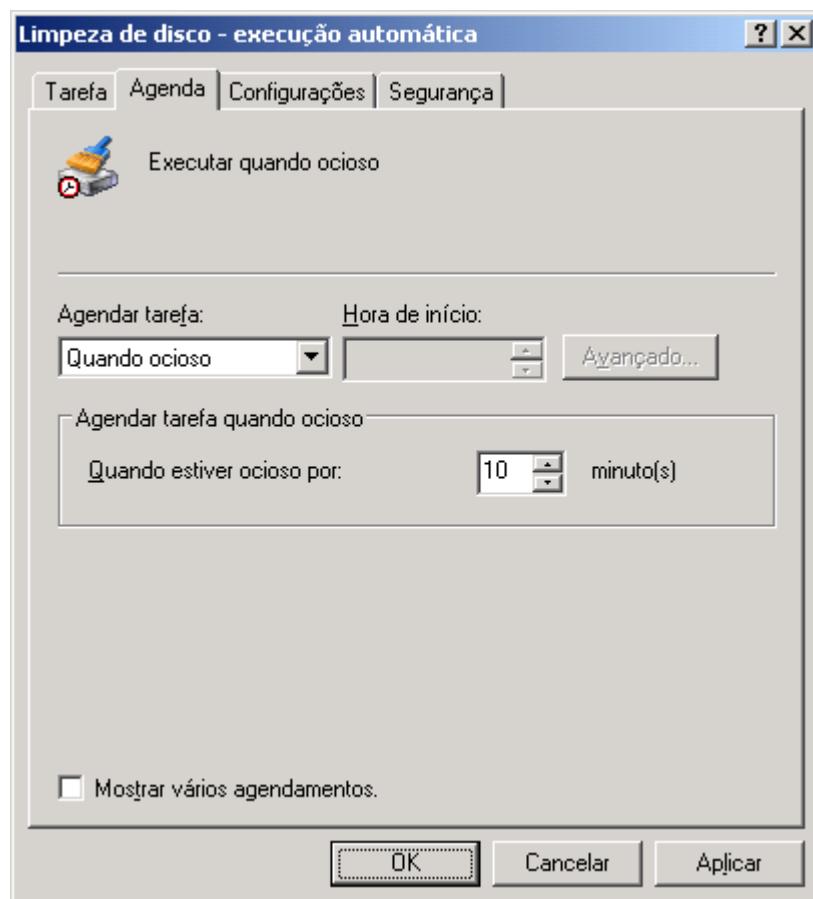
Você pode alterar o agendamento programado para uma tarefa. Por exemplo, você pode ter agendado uma cópia de segurança para iniciar às 2:00 da madrugada, porém, devido ao grande volume de dados, a cópia não está sendo concluída até às 8:00 da manhã. Você pode alterar o agendamento da tarefa que executa a cópia de segurança, para que inicie, por exemplo, a 1:00 da madrugada, para que possa ser concluída antes das 8:00 da manhã.

Para alterar o agendamento de uma tarefa, faça o seguinte:

1. Faça o logon como Administrador ou com uma conta com permissão de administrador ou com uma conta que tenha permissão para alterar a tarefa agendada.
2. Abra o Painel de controle. Dê um clique duplo na opção Tarefas Agendadas.
3. Na janela de tarefas agendadas dê um clique duplo na tarefa a ser alterada. Será exibida a janela de propriedades da tarefa.
4. A guia Tarefa vem selecionada por padrão. Clique na guia Agenda.
5. Nesta guia você pode alterar o agendamento da tarefa. A seguir apresento uma descrição das principais opções desta guia. As opções Mostrar vários agendamentos e Avançado..., serão descritas nos próximos tópicos.
  - ◆ **Agendar tarefa:** Nesta lista você especifica a freqüência de execução da tarefa: Semanalmente, mensalmente, Uma vez, Ao inicializar o sistema, No logon e Quando ocioso.
  - ◆ **No campo Hora de início, você define o horário em que a tarefa deve ser iniciada.** Este campo não será exibido quando você selecionar uma das seguintes opções de freqüência: Ao inicializar o sistema, No logon e Quando ocioso. Ao selecionar uma destas opções, as caixas de seleção com os nomes dos dias da semana também serão ocultas.

**IMPORTANTE:** Se você alterar a senha de uma conta de usuário, no Active Directory, esta alteração não é feita na tarefa agendada. Ou seja, após alterar a senha de uma conta de usuário, conta esta que é utilizada por uma tarefa agendada, você deve acessar as propriedades da tarefa agendada e fazer a alteração na senha. Esta sincronização é manual, ou seja, quando trocamos a senha de uma conta no Windows Server 2003, a nova senha não é informada às tarefas agendadas que utilizam a conta. Com isso a tarefa irá falhar na próxima execução, pois estará utilizando a senha antiga. Neste caso você deve utilizar os procedimentos indicados neste tópico, para alterar a senha em cada tarefa onde a conta for utilizada. Uma opção menos trabalhosa seria criar uma conta especificamente para ser utilizada pelas tarefas agendadas e marcar a opção Senha nunca expira, conforme já descrito anteriormente. [www.julio battisti.com.br](http://www.julio battisti.com.br)

- ◆ Ao selecionar as opções Ao inicializar o sistema e No logon, as demais opções serão ocultadas. Ao selecionar a opção Quando ocioso, você poderá definir quantos minutos o computador deve ficar ocioso, até que a tarefa comece a ser executada, conforme exemplo da Figura 8.11:



**Figura 8.11 Executando uma tarefa quando o sistema fica ocioso por 10 minutos.**

- Defina as configurações desejadas para o agendamento e clique em OK para aplicá-las. A partir de agora a tarefa passará a ser executada de acordo com as novas configurações de agendamento.

### Alterar opções avançadas do agendamento.

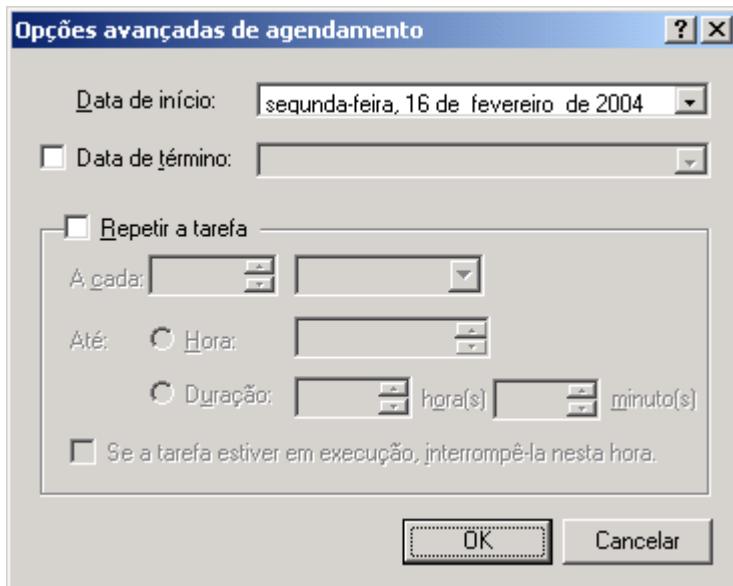
Você pode utilizar as opções avançadas de agendamento para definir as seguintes configurações para uma tarefa:

- ◆ Uma data de início.
- ◆ Uma data final, a partir da qual a tarefa não será mais executada.
- ◆ Um intervalo de repetição da tarefa, por exemplo de hora em hora.

Para configurar as opções avançadas de agendamento, siga os passos indicados a seguir:

1. Faça o logon como Administrador ou com uma conta com permissão de administrador ou com uma conta que tenha permissão para alterar a tarefa agendada.
2. Abra o Painel de controle. Dê um clique duplo na opção Tarefas agendadas.

3. Na janela Tarefas agendadas dê um clique duplo na tarefa a ser alterada. Será exibida a janela de propriedades da tarefa.
4. A guia Tarefa vem selecionada por padrão. Clique na guia Agenda.
5. Clique no botão Avançado. Será aberta a janela Opções avançadas de agendamento, indicada na Figura 8.12:



**Figura 8.12 Opções avançadas de agendamento.**

Nesta janela estão disponíveis as seguintes opções:

- ◆ **Data de início:** define uma data a partir da qual a tarefa começará a ser executada, de acordo com o agendamento programado. Por padrão esta é a data de criação da tarefa, mas você pode configurar esta data para uma data futura, para o caso de a tarefa que só deva começar a ser executada em uma data futura. Ao abrir a lista Data de início, será exibido um controle do tipo calendário, com o calendário do mês atual. Você pode clicar diretamente na data desejada, o que é bem mais fácil do que digitar a data.
  - ◆ **Data de término:** Neste campo você pode definir uma data de término, a partir da qual a tarefa não será mais executada. Por padrão não é definida uma data de término, ou seja, a tarefa continua sendo executada de acordo com o agendamento configurado, até que a tarefa seja excluída pelo administrador.
  - ◆ **Repetir a tarefa:** Se você marcar esta opção, serão habilitados campos para que você defina um intervalo de repetição para a tarefa, por exemplo de 20 em 20 minutos ou a cada hora e assim por diante.
  - ◆ **Se a tarefa estiver em execução, interrompê-la nesta hora:** Especifica se todas as ocorrências da tarefa agendada que ainda estão sendo executadas no prazo final em Tempo ou Duração devem ser interrompidas. Esta opção é útil quando suas tarefas não são interrompidas automaticamente. Se esta caixa de seleção não estiver marcada, a tarefa continuará em execução, mesmo após o prazo final. Por exemplo, pode ser preciso marcar esta caixa de seleção se uma tarefa leva uma hora para ser executada, mas é iniciada 15 minutos antes do prazo final e não é interrompida automaticamente quando termina a execução.
6. Selecione as opções desejadas e clique em OK. Você estará de volta a janela de propriedades da tarefa.
  7. Clique em OK para aplicar as novas configurações. A partir de agora a tarefa passará a ser executada de acordo com as novas configurações avançadas de agendamento.

## Criar múltiplos agendamentos.

É possível criar múltiplos agendamentos para uma mesma tarefa. Podem existir situações em que uma determinada tarefa tenha que ser executada em diversos horários, os quais é impossível configurar em um único agendamento. Por exemplo, você pode ter que agendar uma tarefa de backup para rodar todos os dias, às 2:00 hs. da madrugada e nas segundas, quartas e sextas, além das duas da madrugada, também no horário do almoço, por exemplo, às 12:00 hs. Neste exemplo, você terá que criar dois agendamentos: Um com programação semanal, para todos os dias da semana, com execução para as 2:00 hs. da manhã. Outro com programação semanal, para execução às segundas, quartas e sextas-feiras às 12:00 hs.

Para configurar múltiplos agendamentos, siga os passos indicados a seguir:

1. Faça o logon como Administrador ou com uma conta com permissão de administrador ou com uma conta que tenha permissão para alterar a tarefa agendada.
2. Abra o Painel de controle. Dê um clique duplo na opção Tarefas agendadas.
3. Na janela de tarefas agendadas dê um clique duplo na tarefa a ser alterada. Será exibida a janela de propriedades da tarefa.
4. A guia Tarefa vem selecionada por padrão. Clique na guia Agenda.
5. Marque a opção Mostrar vários agendamentos. Ao marcar esta opção, surge uma lista, na parte de cima da janela, com o agendamento atual. Para criar um novo agendamento, basta clicar no botão Novo, em destaque na Figura 8.13:

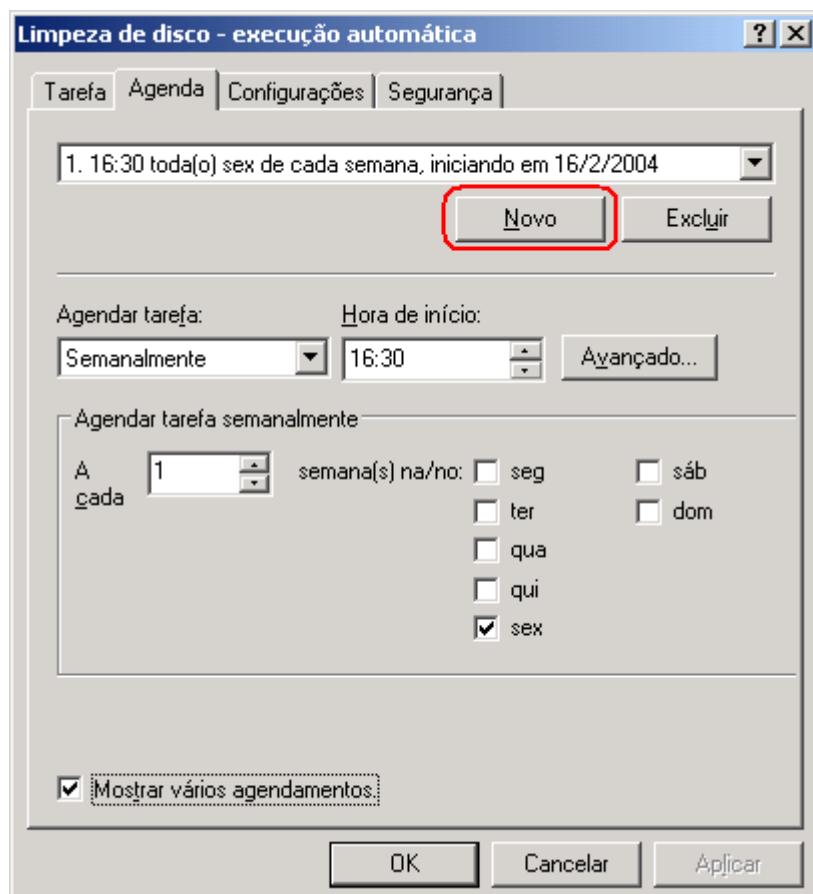
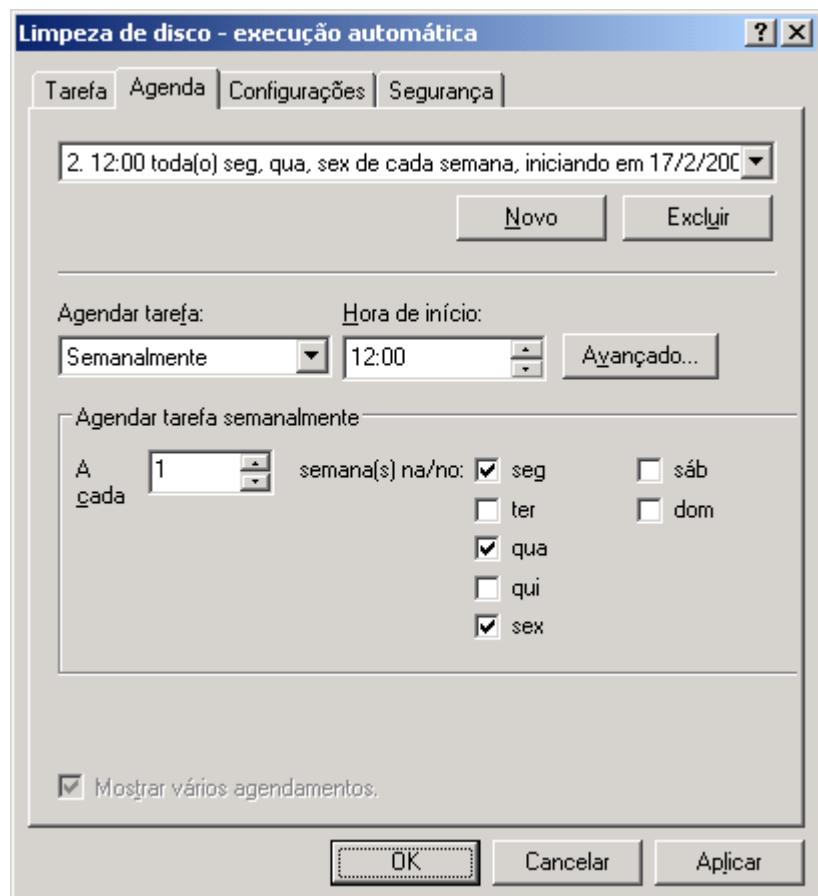


Figura 8.13 Criando um novo agendamento.

6. Clique no botão Novo . Na guia Agenda serão exibidas as configurações para que você defina o novo agendamento. Observe que na lista, na parte superior da guia, aparece o número “2”. ao lado das informações sobre o agendamento. Este número indica que este é o segundo agendamento que está sendo configurado para esta tarefa. Você pode utilizar esta lista, para alternar entre os vários agendamentos configurados para uma determinada tarefa.
7. Por exemplo, para criar um segundo agendamento, para execução às segundas, quartas e sextas-feiras, às 12:00 hs., defina as configurações conforme exemplo da Figura 8.14:



**Figura 8.14 Definindo um novo agendamento.**

8. Defina os agendamentos desejados e clique em OK para salvar as alterações.

### Verificar o log do Agendador de tarefas.

O serviço Agendador de tarefas mantém um log, no qual são gravadas informações sobre a execução das diversas tarefas agendadas. As informações de log são salvas em um arquivo de texto, com o nome SchedLgU.Txt. Neste arquivo estão informações tais como:

- ◆ O nome da tarefa que foi executada.
- ◆ A hora de início da tarefa.
- ◆ A hora de conclusão da tarefa.
- ◆ O resultado da execução da tarefa.

A seguir apresento um trecho do arquivo de log, onde você pode observar as informações descritas anteriormente:

---

**NOTA:** Para excluir um agendamento, basta selecioná-lo na lista de agendamentos e clicar no botão Excluir.

---

**IMPORTANTE:** As configurações avançadas são individualizadas para cada agendamento, ou seja, você pode definir diferentes

```

"IdleTask" (TaskId1)
    Iniciado em 3/4/2002 19:29:26
"IdleTask" (TaskId1)
    Concluído em 3/4/2002 19:29:26
    Resultado: A tarefa foi concluída com o código de saída
(0).

```

Para acessar o log de informações sobre a execução das tarefas agendadas, faça o seguinte:

1. Faça o logon como Administrador ou com uma conta com permissão de administrador ou com uma conta que tenha permissão para alterar a tarefa agendada.
2. Abra o Painel de controle. Dê um clique duplo na opção Tarefas agendadas.
3. Selecione o comando Avançado -> Exibir log.

O Bloco de notas será aberto e o arquivo SchedLgU.Txt será carregado. A seguir listo um exemplo de um arquivo de log das tarefas agendadas. Observe que, na parte final do trecho, são exibidas informações sobre a tarefa que criamos para executar a ferramenta de limpeza de disco.

```

***** TRECHO DO ARQUIVO DE LOG - EXEMPLO *****
...
"IdleTask" (TaskId1)
    Iniciado em 15/4/2002 18:28:58
"IdleTask" (TaskId1)
    Concluído em 15/4/2002 18:29:05
    Resultado: A tarefa foi concluída com o código de saída (0).
"IdleTask" (TaskId5)
    Iniciado em 15/4/2002 18:29:35
"IdleTask" (TaskId5)
    Concluído em 15/4/2002 18:29:35
    Resultado: A tarefa foi concluída com o código de saída (0).
"IdleTask" (TaskId1)
    Iniciado em 15/4/2002 18:43:47
"IdleTask" (TaskId1)
    Concluído em 15/4/2002 18:43:56
    Resultado: A tarefa foi concluída com o código de saída (0).
"IdleTask" (TaskId1)
    Iniciado em 15/4/2002 19:13:46
"IdleTask" (TaskId1)
    Concluído em 15/4/2002 19:13:46
    Resultado: A tarefa foi concluída com o código de saída (0).
"IdleTask" (TaskId1)
    Iniciado em 15/4/2002 19:43:46
"IdleTask" (TaskId1)
    Concluído em 15/4/2002 19:43:46
    Resultado: A tarefa foi concluída com o código de saída (0).
"IdleTask" (TaskId1)
    Iniciado em 15/4/2002 20:58:47
"IdleTask" (TaskId1)
    Concluído em 15/4/2002 20:58:47
    Resultado: A tarefa foi concluída com o código de saída (0).
"IdleTask" (TaskId2)
    Iniciado em 15/4/2002 20:59:17
"IdleTask" (TaskId2)
    Concluído em 15/4/2002 20:59:55
    Resultado: A tarefa foi concluída com o código de saída (0).
"Limpeza de disco - Execução automática.job" (cleanmgr.exe)
    Iniciado em 15/4/2002 23:10:16
"Limpeza de disco - Execução automática.job" (cleanmgr.exe)

```

configurações avançadas para diferentes agendamentos. Por exemplo, um agendamento pode ter uma data de término definida, enquanto outro agendamento da mesma tarefa, não tem uma data de término definida.

```

Concluído em 15/4/2002 23:13:27
Resultado: A tarefa foi concluída com o código de saída (0).
"Limpeza de disco - Execução automática.job" (cleanmgr.exe)
    Iniciado em 15/4/2002 23:15:28
"Limpeza de disco - Execução automática.job" (cleanmgr.exe)
    Concluído em 15/4/2002 23:15:32
    Resultado: A tarefa foi concluída com o código de saída (0).
"Serviço agendador de tarefas"
    Finalizado em 16/4/2002 00:58:25
"Serviço agendador de tarefas"
    Iniciado em 16/4/2002 23:23:46
[ ***** A entrada mais recente está acima desta linha ***** ]

.....
***** FINAL DO TRECHO DO ARQUIVO DE LOG *****

```

## Comandos at para agendamento de comandos.

O comando at pode ser utilizado para agendar um determinado programa ou script para ser executado em um horário específico e em datas determinadas. Você somente poderá usar o comando at se o serviço Task Scheduler estiver rodando normalmente. Ao utilizar o comando at sem nenhum parâmetro, será exibida uma tela de ajuda com as opções do comando, conforme descrevo logo a seguir.

Sintaxe do comando AT:

```

at [\ComputerName] [{[ID] [/delete] | /delete [/yes]}]
at [[\ComputerName] Hours:Minutes [/interactive] {[/every:Date[,...] | /next:Date[,...]}]
Command]

```

Parâmetros do comando AT:

- ◆ **\ComputerName:** Este parâmetro define o nome do servidor onde a tarefa será agendada para execução. Se for omitido, a tarefa será agendada no para executar no servidor onde o comando at está sendo executado.
- ◆ **ID:** Associa um número de identificação com o comando.
- ◆ **/delete:** É utilizado para cancelar um agendamento. Se o ID do agendamento for omitido, todos os comandos agendados no servidor, serão cancelados.
- ◆ **/yes:** Automaticamente responde Yes para todas as mensagens de confirmação que são emitidas quando você usa /delete sem informar um ID, para excluir todos os agendamentos.
- ◆ **Hours:Minutes:** Define o horário de execução do comando que será agendado para execução. A hora é informada no formato hh:mm e o relógio utilizado é o relógio de 24 horas, ou seja 16:00 horas e não 4:00 PM (pós meia-dia).
- ◆ **/interactive:** Permite que a execução do comando agendado interaja com o console do usuário que está logado. Isto é, mensagens de execução serão exibidas pelo comando, no vídeo do usuário.
- ◆ **/every:** Utilizado para agendar a execução do comando em determinados dias da semana. Por exemplo, toda segunda, quarta e sexta-feira.
- ◆ **Date:** Define a data para execução do comando. Você pode especificar um ou mais dias da semana (abreviatura em inglês, começando pela segunda feira: M,T,W,Th,F,S,Su) ou um ou mais dia do mês (utilizando números de 1 até 31). Separe múltiplas entradas com vírgula. Se a data não for informada, o comando AT agendará o comando para ser executado na data atual.

- ◆ **/next:** Executa o comando na próxima ocorrência do dia atual. Por exemplo, na próxima terça-feira (suponde que hoje seja terça-feira).
- ◆ **Command:** Define o comando ou programa (.exe ou .com), ou arquivo de lote (.bat ou .cmd) que será executado. Se o comando exige o caminho de um arquivo como argumento, utilize sempre o caminho completo, inclusive com a unidade, como no exemplo a seguir: C:\rotinasdebackup\backup01.bat. Se o comando estiver sendo agendado para execução em um computador remoto, use a convenção de nomes UNC, já descrita anteriormente.
- ◆ **/?:** Exibe uma tela de ajuda sobre o comando at.

Para visualizar os comandos que foram agendados para execução, usando o comando at, basta executar o comando at sem nenhum parâmetro. A seguir mostro um exemplo da execução do comando at sem nenhum parâmetro:

| Status | ID | Day    | Time     | Command Line                    |
|--------|----|--------|----------|---------------------------------|
| OK     | 1  | Each F | 4:30 PM  | net send group leads status due |
| OK     | 2  | Each M | 12:00 AM | chkstor > check.file            |
| OK     | 3  | Each F | 11:59 PM | backup2.bat                     |

Exemplos de utilização do comando at:

Para exibir a lista de comandos agendadas para execução em um servidor chamado SRV01, utilize o seguinte comando:

```
at \\SRV01
```

Para exibir informações sobre um comando que foi agendado para execução e para o qual foi atribuído o ID 3, utilize o seguinte comando:

```
at 3
```

Para agendar o comando net share, para rodar no servidor chamado SRV01, as 8:00 da manhã e para redirecionar a lista de saída para o arquivo result.txt, no compartilhamento Relatórios, do servidor SRVM, utilize o seguinte comando:

```
at \\SRV01 08:00 cmd /c "net share  
relatorios=d:\marketing\relatorios >>  
\SRVM\relatorios\result.txt"
```

## Estratégias de backup e restore.

Fazer o “Backup”, significa fazer uma ou mais cópias de segurança dos dados dos servidores e também da instalação do Windows Server 2003 das configurações do servidor (Backup do Estado do Sistema). Muitos usuários e até mesmo pequenas empresas simplesmente ignoram a necessidade de implementar uma política de Backup. Muitas vezes os usuários só se dão conta do problema quando é tarde demais, ou seja, quando houve uma perda de dados importantes. É o usuário que perdeu os documentos do Word e figuras da sua tese de mestrado, é a vídeo locadora que perdeu os dados de anos de locações, é o Dentista que perdeu as informações sobre as fichas dos pacientes, sobre quais pacientes deviam e assim por diante. Claro que na rede da sua empresa, a necessidade de backup é indiscutível. Perder dados significa sistemas fora do ar, perda de clientes, e assim por diante. Em resumo: grandes dores de cabeça e prejuízos. Fazer cópia de segurança é uma

**NOTA:** No Windows Server 2003 está disponível um novo comando: schtasks. Este comando pode ser utilizado para criar, gerenciar e administrar tarefas agendadas. Tudo o que você aprendeu a fazer na interface gráfica, é possível ser feito com o comando schtasks. Para detalhes sobre este comando basta abrir a ajuda do Windows Server 2003 e pesquisar pelo nome deste comando.

**IMPORTANTE:** Para utilizar o comando at você deve ter permissão de administrador.

**IMPORTANTE:** Os comandos no Windows Server 2003 são executados no prompt de comando. O prompt de comando é o cmd.exe. Quando você usa o at para agendar a execução de um comando que deve ser executado no prompt de comando, você deve também agendar a execução do cmd.exe, caso contrário a execução do comando irá falhar. Veja o exemplo a seguir, onde primeiro é executado o comando cmd e é passado para este comando, como parâmetro, o comando que será efetivamente executado. Observe que é utilizado o caminho completo: cmd /c dir > c:\test.out

necessidade real, não temos como fugir deste fato. Além disso o custo é insignificante, isto mesmo: insignificante se compararmos com os prejuízos que podem ser causados pela perda de dados.

Neste tópico apresentarei alguns detalhes sobre os tipos de backup existentes e sobre estratégias de backup que podem ser implementadas. Também darei algumas sugestões sobre os dispositivos de Backup que você pode utilizar caso nos servidores da rede da sua empresa.

**IMPORTANTE:** Conheça bem os tipos de backup, as diferenças entre os tipos e em que situações práticas cada tipo deve ser utilizado. Este é um dos tópicos fundamentais para o Exame 70-290.

## Definindo o tipo de Backup a ser utilizado.

Dependendo da quantidade de dados e do tempo disponível para o backup, podem ser utilizadas diferentes estratégias de backup. As estratégias de backup são baseadas em um ou mais tipos de backup. Você pode ter estratégias bastante simples, baseadas na cópia completa de todos os arquivos, até estratégias mais sofisticadas, baseadas na combinação entre diferentes tipos de backup. Vou, inicialmente apresentar os diferentes tipos de backup.

No Windows Server 2003 podemos utilizar os seguintes tipos de backup:

- ◆ **Normal (Normal):** Com este tipo de backup todos os arquivos são copiados, toda vez que o backup for executado, independentemente de os arquivos terem sido alterados ou não. O arquivo é marcado como tendo sido feito o backup, ou seja, o atributo de arquivamento é desmarcado. Cada arquivo tem um atributo que pode ser marcado ou desmarcado. Este atributo serve para informar ao Windows Server 2003 se o arquivo foi ou não modificado desde o último backup normal. A principal vantagem do backup normal é a facilidade para fazer a restauração dos arquivos, quando necessário. Com o backup do tipo normal, para restaurar os dados, você precisa apenas do último backup normal que foi criado. A desvantagem é o tamanho do backup e o tempo para execução. Em cada execução do backup, todos os arquivos e pastas serão copiados, independentemente de terem sido alterados ou não, desde que o último backup normal foi efetuado. Geralmente, o backup normal é executado quando você cria um conjunto de backup pela primeira vez. Nos backup subsequentes é comum a utilização de outros tipos de backup, conforme descreverei logo a seguir.
- ◆ **Copy (Cópia):** Backup que copia todos os arquivos selecionados, mas não marca cada arquivo como tendo sofrido backup (em outras palavras, o atributo de arquivamento não é desmarcado). É idêntico ao backup Normal, com a diferença de que os arquivos não são marcados como tendo sido copiados. A cópia é útil caso você queira fazer backup de arquivos entre os backups normal e incremental (veja descrição do backup incremental logo a seguir), pois ela não afeta essas outras operações de backup ou quando você precisa fazer uma cópia extra dos dados para enviar para um filial da empresa ou para manter a cópia armazenada em um local seguro.
- ◆ **Incremental (Incremental):** Este tipo de backup copia somente os arquivos criados ou alterados desde o último backup normal ou desde o último backup incremental. Os arquivos copiados para o backup são marcados (ou seja, o atributo de arquivamento é desmarcado). Se você utilizar uma combinação de backups normais e incrementais para restaurar os seus dados, será preciso ter o último backup normal e todos os conjuntos de backups incrementais feitos após este backup normal e restaurá-los na seqüência correta. A grande vantagem do backup incremental é que ele reduz o tempo necessário para a execução do backup, pois somente é feita a cópia dos arquivos que foram criados ou modificados desde o último backup normal ou incremental. A grande desvantagem é que para fazer a restauração é necessário o último backup normal e todos os backups incrementais

**NOTA:** Neste tópico utilizarei a palavra Backup como sinônimo de Cópia de segurança, por ser este termo já conhecido e consagrado.

subseqüentes. Os backups incrementais devem ser restaurados na seqüência cronológica em que foram criados. Além disso, se um dos backups incrementais apresentar problemas, não será possível restaurar os dados até o ponto do último backup incremental.

- ◆ **Differential (Diferencial):** Este tipo de backup faz a cópia de todos os arquivos criados ou alterados desde o último backup normal ou incremental. Os arquivos que sofreram backup não são marcados como tal (ou seja, o atributo de arquivamento não é desmarcado). Com isso cada backup diferencial, copia todos os arquivos que foram modificados desde o último backup normal (ou incremental, caso algum tenha sido feito). Se você estiver executando uma combinação de backups normal e diferencial, a restauração de arquivos e pastas exigirá que você tenha o último backup normal e o último backup diferencial. A restauração é mais rápida do que quando você usa backups incrementais, pois somente é necessário o último backup diferencial, porém cada backup diferencial passa a ser maior, pois contém a cópia de todos os arquivos criados ou modificados desde o último backup normal ou incremental.
- ◆ **Daily (Diário):** Este tipo de backup copia todos os arquivos selecionados que forem alterados no dia de execução do backup diário. Os arquivos que sofreram backup não são marcados como tal (ou seja, o atributo de arquivamento não é desmarcado). Não é um tipo muito utilizado. Pode ser utilizado em conjunto com backups do tipo normal e incremental.

O tipo ou tipos de backup que estão sendo utilizados, definem as estratégias de restauração (restore) que serão utilizadas, em caso de perda dos dados originais. A estratégia a ser utilizada depende do volume de dados e do valor dos dados a serem protegidos. Por exemplo, para um usuário doméstico que não tem um grande volume de dados, pode ser suficiente uma estratégia de backup normal todos os dias. Já para os servidores com dados de missão crítica da sua empresa, toda proteção adicional é bem vinda.

Porém você tem que estar atentos a alguns detalhes importantes. Por exemplo, não adianta você fazer o backup dos arquivos, no mesmo disco rígido onde estão gravados os arquivos originais (pois você pode fazer o backup em fita, em disco rígido e em vários outros tipos de mídia suportados pelo Windows Server 2003). Neste caso se o disco rígido “pifar”, ou seja, for danificado e não puder ser recuperado, você perderá os arquivos e também o backup. Para usuários domésticos e pequenas empresas, os quais não tem grandes volumes de dados, a utilização de um segundo disco rígido, no qual serão feitas as cópias de backup, pode ser uma estratégia eficiente. A possibilidade de os dois discos rígidos apresentarem problemas ao mesmo tempo é muito pequena. Já para empresas de grande porte o ideal é ter um conjunto de mídias separado dos servidores e dedicado ao backup. Pode ser uma biblioteca de fitas de backup ou um espaço de armazenamento em disco rígido.

Uma opção muito utilizada é o uso de drives de fita como por exemplo do tipo DLT4 de 40 ou 80 GB (já existem padrões de maior capacidade e maior velocidade do que a DLT4). Além disso após feito o backup, as fitas devem ser armazenadas em local separado da sala dos servidores. Se armazenarmos as fitas, na mesma sala onde estão os dados, corremos o risco de perder os dados e também o backup, em caso de incêndio, inundação ou outro desastre. Claro que uma estratégia deste tipo requer investimentos consideráveis, mas com certeza são investimentos plenamente justificados pela importância dos dados para a empresa.

Outro detalhe importante é que as cópias de segurança devem ser sempre testadas. Após fazer o backup, você deve fazer um teste de restauração para verificar se a cópia realmente foi feita com sucesso. Nada pior do que descobrir, na hora do restore, que o backup não foi feito adequadamente. Existe até um piada bastante conhecida entre os administradores de rede e de bancos de dados: “O backup sempre funciona, o que não funciona, às vezes, é o restore”. Ou seja, o objetivo não é o sucesso do backup e sim que, quando necessário, seja possível fazer o restore dos dados a

partir do backup. Para garantir que isto seja possível, é preciso que exista uma definição de uma política para testes periódicos do backup.

## Exemplos de estratégias de backup/restore.

Agora irei analisar algumas estratégias de backup/restore, baseadas nos diferentes tipos de backup, descritos anteriormente.

Exemplo 1: É feito diariamente um backup Normal, as 23:00 da pasta Meus documentos. Na sexta-feira, as 14:30 ocorre um problema e a pasta Meus documentos é excluída.

Nesta situação você tem que restaurar o backup Normal feito na quinta-feira. Todos as alterações feitas na sexta-feira serão perdidas, ou seja, os arquivos voltarão a situação que estavam na quinta-feira, quando foi feito o último backup normal.

Exemplo 2: No domingo é feito um backup normal. De segunda a sábado é feito um backup Incremental à noite. Na quinta-feira, as 16:00 ocorre um problema e os dados são excluídos.

Você deve restaurar o backup normal do domingo, o backup incremental da segunda-feira, o backup incremental da terça-feira e o backup incremental da quarta-feira, nesta seqüência. Todas as alterações feitas na quinta-feira serão perdidas.

Exemplo 3: É feito um backup normal aos domingos. De segunda a sábado são feitos os seguintes backups incrementais: 2:00, 9:00, 12:00, 15:00, 17:00 e 21:00 hs. Na quarta-feira, as 14:30 ocorre um problema e os dados tem que ser restaurados do backup.

Você deve restaurar o backup normal do domingo e todos os backups incrementais, em ordem cronológica, até o backup incremental da quarta-feira as 12:00, que é o último backup incremental feito antes da ocorrência do problema as 14:30. Todas as alterações feitas entre as 12:00 hs. e as 14:30 serão perdidas. Observe que com a utilização de backups incrementais durante o dia, você reduz a possibilidade de perda de dados, porém a restauração torna-se mais trabalhosa, pois existe um grande número de backups incrementais a serem restaurados. Uma estratégia deste tipo é normalmente utilizada por grandes empresas, que trabalham com grande volumes de dados e não podem nem sequer pensar em perda de dados.

Exemplo 4: É feito um backup normal aos domingos. De segunda a sábado são feitos backups incrementais as 2:00 da madrugada. Toda quarta-feira é feito um backup diferencial as 3:00 da madrugada. Na sexta-feira, as 14:30 ocorre um problema e os dados tem que ser restaurados do backup.

Você deve restaurar o backup normal do domingo, o backup diferencial da quarta-feira e o backup incremental da quinta-feira, nesta seqüência. Todas as alterações feitas na sexta-feira serão perdidas.

Observe que a utilização de um backup diferencial, em conjunto com os backups incrementais, reduziu o número de backups a serem restaurados. Neste caso somente foi necessário restaurar o último backup normal, o último diferencial e os backups incrementais posteriores. Esta é a estratégia mais complexa, mas que ao mesmo tempo otimiza o tempo de backup e o tempo de restauração. É especialmente indicada para grandes volumes de dados, onde o tempo de parada é um fator crítico.

**IMPORTANTE:** Entenda bem as diferentes políticas de Backup/Restore, com base nos diferentes tipos de Backup, disponíveis no Windows Server 2003.

## Questões de segurança relacionadas ao Backup

O usuário que irá realizar o backup ou a conta com a qual será executada a tarefa agendada, responsável pelo Backup, deve ter algumas permissões especiais. A principal delas é poder fazer o backup, mesmo de pastas e arquivos para os quais a conta não tem permissões NTFS de acesso. Se não fosse dessa forma, o usuário responsável pelo backup deveria ter permissão, pelo menos de leitura, em todos os arquivos e pastas da rede, o que não seria uma medida muito aconselhável em termos de segurança. Se a conta pertencer ao grupo local Administrators (Administradores) ou ao grupo local do domínio Backup Operators (Oper. de Cópia), ela poderá ser utilizada para fazer o backup de qualquer arquivo ou pasta no servidor local. Se for uma conta de domínio, que pertencer ao grupo Administrators (Administradores) ou ao grupo Backup Operators (Oper. de Cópia), esta conta terá permissão para fazer o backup de qualquer arquivo ou pasta, localizado em qualquer computador (servidor ou estação de trabalho) que faça parte do domínio ou, inclusive, em qualquer computador ou servidor de domínios que mantém uma relação de confiança bidirecional com o domínio da conta que está sendo utilizada para o backup.

Se a conta com a qual será executado o backup, não pertencer a um dos grupos descritos no parágrafo anterior, ela deverá ser dona dos arquivos e pastas que serão copiados para o backup ou, pelo menos, ter uma das seguintes permissões nos arquivos e pastas a serem copiados para o backup: Read (Leitura) , Read and execute (Leitura e execução) , Modify (Modificar) ou Full Control (Controle Total)

Você também pode restringir o acesso aos dados do backup. Para fazer isso basta selecionar a opção Permitir que apenas o dono e o Administrador tenham acesso aos dados do backup. Ao marcar esta opção (que você aprenderá a configurar na parte prática, logo a seguir) somente um usuário com perfil de Administrador e o usuário que criou o backup, poderão restaurar os arquivos e pastas do backup.

Agora que aprendemos sobre os tipos de backup e sobre estratégias de restore, bem como sobre questões relacionadas a segurança do backup, é hora de aprender a criar e restaurar um backup, utilizando o utilitário de backup do Windows Server 2003.

A seguir descrevo quais os itens que serão incluídos no Backup, quando você faz o Backup do Estado do Sistema.

### Dados do estado do sistema:

Com o utilitário de backup, você pode fazer backup dos seguintes componentes de sistema e restaurá-los para fazer backup do estado do sistema. estado do sistema. O estado do sistema é uma coleção de dados específicos do sistema mantidos pelo sistema operacional dos quais deve ser feito backup como um todo. Não é um backup de todo o sistema. Os dados do estado do sistema incluem o Registro, o banco de dados de registro de classe COM+, os arquivos do sistema, os arquivos de inicialização e os arquivos sob a Proteção de arquivos do Windows. Para servidores, os dados do estado do sistema também incluem o banco de dados dos serviços de certificados (se o servidor for um servidor de certificados). Se o servidor for um controlador de domínio, os dados do estado do sistema incluirão o banco de dados do Active Directory e o diretório SYSVOL. Se o servidor for um nó em um cluster, ele incluirá as informações do banco de dados do cluster. A metabase IIS estará incluída se o IIS estiver instalado.

---

**NOTA:** Se você for fazer o backup em disco, você deve verificar se a conta com a qual está sendo feito o backup, não tem restrição de cotas no disco de destino, onde será gravado o backup. Se houver uma restrição de cota, o backup irá falhar.

---

**NOTA:** Você somente pode fazer o backup e o restore dos dados do sistema (instalação do Windows Server 2003) localmente, no próprio servidor. Não é possível fazer o backup e o restore dos dados do Estado do sistema remotamente, através da rede, mesmo que você tenha permissões de administrador no servidor remoto. Por exemplo, não é possível fazer o backup dos dados do sistema do servidor SRV01 em uma unidade de fita instalada no servidor SRV02.

---

Na Tabela a seguir, descrevo os componentes do Estado do sistema e quando eles são incluídos no Backup do Estado do sistema.

| Componente  | Quando este componente é incluído no estado do sistema? |
|---|---|
| Registro  | Sempre  |
| Banco de dados de registro de classe COM+                       | Sempre  |
| Arquivos de inicialização, incluindo os arquivos de sistema     | Sempre  |
| Banco de dados de serviços de certificados                      | Se for um servidor de serviços de certificados          |
| Serviço de diretório Active Directory                           | Se for um controlador de domínio                        |
| Pasta SYSVOL  | Somente se for um controlador de domínio                |
| Informações do serviço de cluster                               | Se estiver dentro de um cluster                         |
| Metadiretório IIS (Metabase)                                    | Se estiver instalado o IIS                              |
| Arquivos de sistema que estão na Proteção de arquivo do Windows | Sempre  |

O utilitário de backup se refere a esses componentes de sistema como os dados do estado do sistema. O total de componentes do sistema que constituem os dados do estado do sistema depende do sistema operacional e da configuração do computador.

## Fazendo o backup e o restore de pastas e arquivos com o Windows Server 2003.

### Introdução

Para fazer o backup e o restore de pastas e arquivos, é utilizado o utilitário de backup do Windows Server 2003, o qual é acessado através do seguinte caminho: Iniciar -> Todos os programas -> Acessórios -> Ferramentas do sistema -> Backup.

Você deve estar logado com a conta com permissão de administrador, ou com uma conta que pertença ao grupo Backup Operators (Operadores de cópia), para fazer backup de todos os arquivos e pastas. Usuários com permissões de administrador ou pertencentes ao grupo Backup Operators (Operadores de cópia), poderão fazer o backup de qualquer arquivo ou pasta, mesmo de arquivos e pastas para os quais o usuário não tenha permissões NTFS de acesso. Este mecanismo permite que um único usuário, normalmente o administrador, possa fazer o backup de todos os arquivos e pastas, mesmo daqueles para os quais ele não tem permissões de acesso.

**NOTA:** Você também pode abrir o utilitário de backup, utilizando o seguinte comando: Iniciar -> Executar. No campo Abrir digite ntbackup.exe e clique em OK. Será aberto o utilitário de backup, o qual detalharei logo a seguir.

Ao abrir o utilitário de backup pela primeira vez (usando um dos métodos descritos anteriormente) ele será aberto, por padrão, no modo de Assistente, conforme indicado na Figura 8.15.

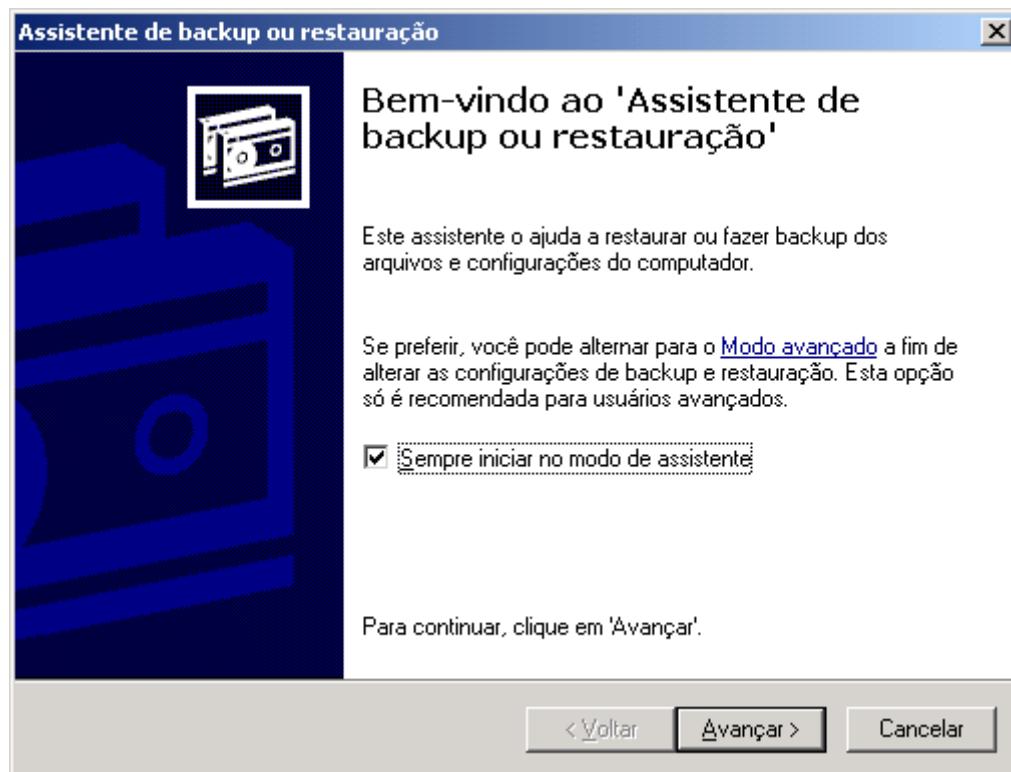


Figura 8.15 Modo de assistente – modo padrão do utilitário de backup.

Se a caixa Sempre iniciar no modo assistente estiver marcada, o utilitário de backup sempre será inicializado no modo de assistente. Se você desmarcar esta opção, o utilitário será aberto no modo completo. Se você clicar na opção Modo avançado, será exibida a interface completa do utilitário de backup.

O utilitário de backup permite que você faça backup de dados em um arquivo no disco rígido ou em uma fita de backup. Para fazer backup de dados em um arquivo, é preciso designar um nome e um local para o arquivo a ser salvo. Geralmente, os arquivos de backup possuem a extensão .bkf, mas você pode alterá-la para qualquer outra extensão. O arquivo de backup pode ser salvo em um disco rígido, um disquete ou qualquer outra mídia, removível ou não removível, na qual seja possível salvar arquivos. No caso de backup para um arquivo em disco é importante que o arquivo de backup (.bkf) não seja gravado no mesmo disco rígido onde estão os arquivos que estão sendo copiados para o backup, pois se o disco rígido apresentar problemas e for danificado, você perderá os dados originais e também o backup, ou seja, não haverá como restaurar os dados.

Para fazer backup de dados em uma fita, você precisa ter um dispositivo de fita (drive de fita) conectado ao servidor. Existem diversos modelos de drives de fita, com diferentes capacidades e velocidades. O modelo a ser escolhido, depende do volume de dados que farão parte do backup e do tempo disponível para o backup.

O utilitário de backup também é utilizado para fazer a restauração (restore) das informações, caso algum problema ocorra com os dados originais. Na verdade o utilitário de backup é um utilitário de backup e restore. Quando ocorre algum problema com os dados e estes precisam ser restaurados, você utiliza o utilitário de backup para ler os dados a partir do backup (arquivo .bkf ou unidade de fita ou em disco) e restaura-los para o local de origem. É possível restaurar os dados para o local original ou para um local alternativo, onde você pode analisar os arquivos para conferir se está tudo OK e somente então copiar para o local original.

Também é possível agendar tarefas de backup para que sejam executadas automaticamente em determinados horários e dias. Por exemplo, você pode agendar uma tarefa de backup para que faça um backup incremental de determinadas pastas e arquivos, diariamente, as 2:00 da madrugada.

Agora é hora de aprender a executar uma série de operações de backup e restore, através de exemplos práticos.

## Fazendo o backup de pastas e arquivos utilizando o modo assistente de backup.

Neste exemplo prático, vou usar o utilitário de backup no modo assistente, para fazer o backup da pasta C:\Documentos (utilize como exemplo uma pasta do servidor no qual você está trabalhando ou um drive de rede mapeado no servidor no qual você está trabalhando). Também vou usar o assistente para criar e agendar uma tarefa que executa este backup, diariamente, as 2:00 da manhã. Vou criar um backup do tipo normal. O backup será feito na unidade de disco F: (utilize uma unidade do servidor no qual você está trabalhando), em uma pasta chamada backups, com o nome de documentos.bkf. Observe que estou fazendo o backup em uma unidade de disco rígido diferente da unidade onde estão os arquivos que serão copiados para o backup.

Para criar o backup proposto e agenda-lo, siga os passos indicados a seguir:

1. Faça o logon com uma conta com permissão de administrador ou com uma conta pertencente ao grupo Backup operators (Oper. de cópia).
2. Abra o utilitário de backup, utilizando um dos seguintes procedimentos:  
Iniciar -> Todos os programas -> Acessórios -> Ferramentas do sistema -> Backup  
Ou  
Iniciar -> Executar. No campo Abrir digite ntbackup.exe e clique em OK.  
Será aberto o utilitário de backup no modo assistente, conforme indicado na Figura 8.15, anteriormente.
3. A primeira tela do assistente é apenas informativa. Para acessar o modo avançado, ou seja, a interface completa do utilitário de backup, basta clicar na opção Modo avançado. No nosso exemplo vamos utilizar o Modo Assistente. Clique no botão Avançar, para ir para a próxima etapa do assistente.
4. Nesta etapa você define se deseja fazer um backup – Fazer backup de arquivos e configurações ou se deseja restaurar arquivos a partir de um backup feito anteriormente –Restaurar arquivos e configurações. Marque a opção Fazer backup de arquivos e configurações. Clique no botão Avançar, para ir para a próxima etapa do assistente.
5. Nesta etapa do assistente, estão disponíveis as duas opções descritas a seguir:
  - ◆ **Todas as informações disponíveis neste computador:** Selecione esta opção para fazer um backup completo, de todos os volumes do servidor. Esta opção também gera um disco de recuperação, o qual pode ser utilizado para recuperação do Windows Server 2003 em caso de falhas mais graves, como quando um dos arquivos do sistema é corrompido.
6. Certifique-se de que a opção Eu escolherei os itens para backup: Esta opção permite que você selecione as pastas e arquivos as quais farão parte do backup.

---

**NOTA: No Capítulo 12 você aprenderá a planejar e a implementar uma política de recuperação à desastres no Windows Server 2003.**

---

**Eu escolherei os itens para backup:**  
Esta opção permite que você selecione as pastas e arquivos as quais farão parte do backup.

---

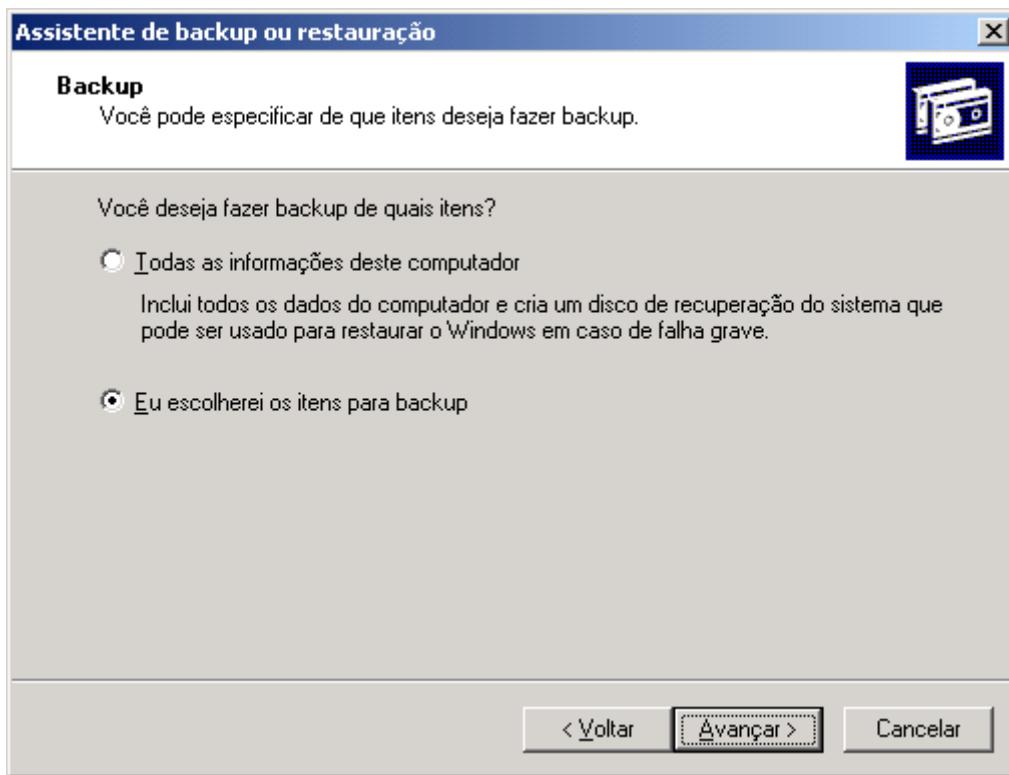


Figura 8.16 O usuário definirá os arquivos e pastas que farão parte do backup.

7. Nesta etapa você define quais arquivos e pastas farão parte do backup. No painel da esquerda é exibida uma estrutura de navegação na forma de árvore, idêntica a estrutura utilizada no Windows Explorer. Navegue até a pasta C:\Documentos e marque a caixa de opção ao lado desta pasta, conforme indicado na Figura 8.17 e clique no botão Avançar, para ir para a próxima etapa do assistente.

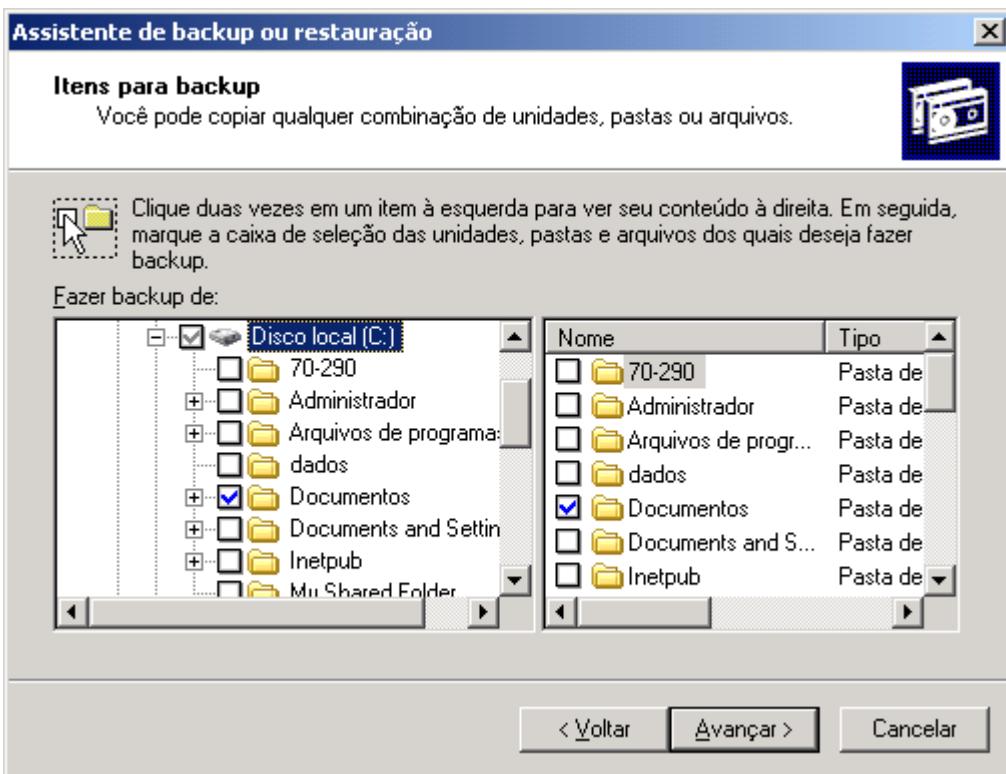
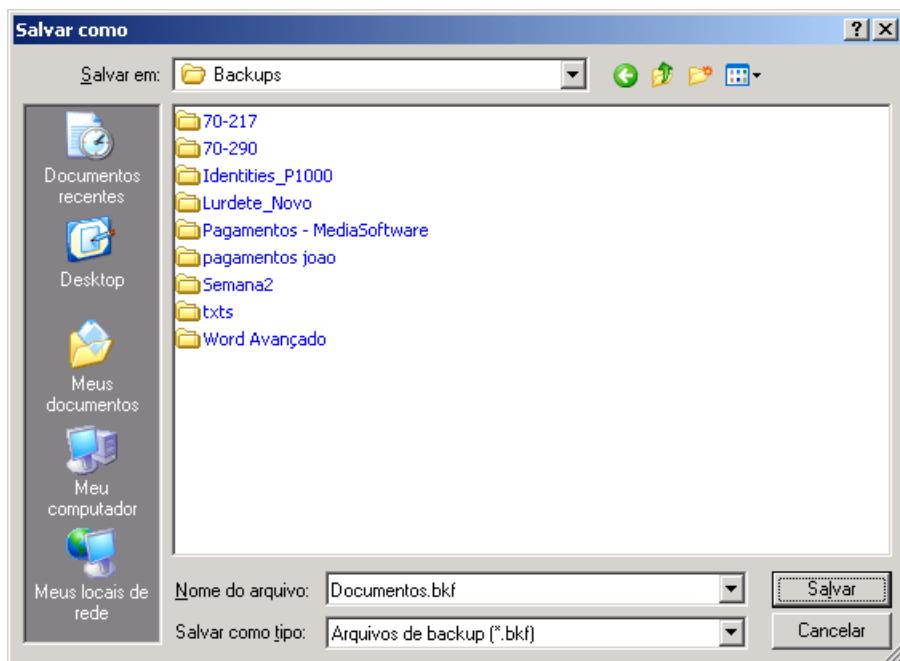


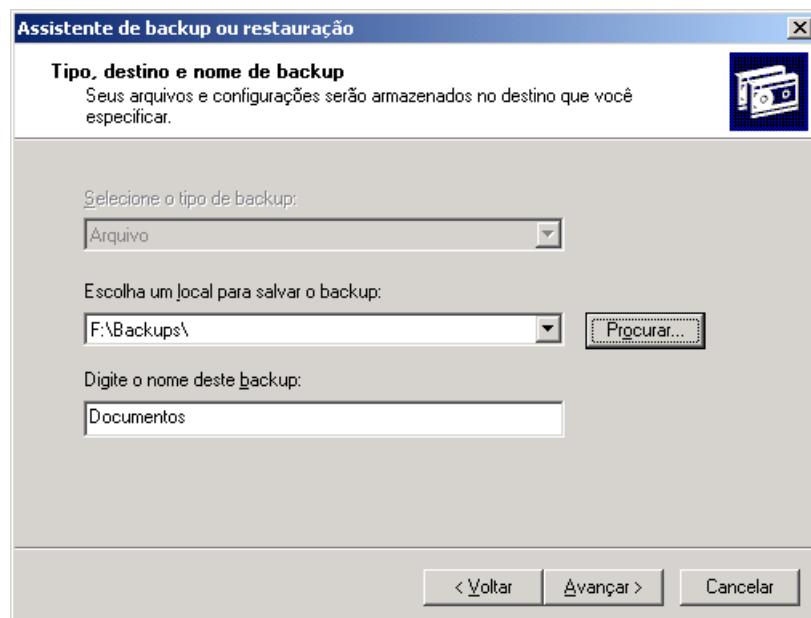
Figura 8.17 Selecionando as pastas que farão parte do backup.

8. Nesta etapa você define o local de destino para o backup. Observe que na lista Selecionar tipo de backup, já vem selecionada a opção Arquivo e esta lista está desabilitada. Isto acontece porque não tenho um drive de fita instalado no servidor utilizado no exemplo. Neste caso somente está disponível a opção Arquivo. Para definir o local de destino clique no botão Procurar.. Será exibida a janela Salvar como, na qual você seleciona a pasta de destino e o nome do arquivo que conterá o backup. Selecione a pasta de destino e defina o nome do arquivo, conforme exemplo indicado na Figura 8.18:



**Figura 8.18 Definindo a pasta de destino e o nome do arquivo de backup.**

9. Clique no botão Salvar, você estará de volta ao Assistente de backup, com as opções selecionadas na janela Salvar como, já definidas no assistente de backup, conforme indicado na Figura 8.19.



**Figura 8.19 Informações de destino já definidas.**

10. Clique no botão Avançar, para ir para a próxima etapa do assistente.
11. Será exibida a tela final do Assistente. Nesta tela será apresentado um resumo das opções selecionadas nos passos anteriores. Para alterar alguma opção utilize o botão Voltar. Para definir o agendamento e o tipo de backup a ser utilizado clique no botão Avançado... Ao clicar no botão Avançado..., serão disponibilizadas etapas adicionais do assistente. Clique no botão Avançado...
12. Será aberto um novo assistente, para configuração das opções avançadas do Backup. Na primeira etapa será exibida uma lista para que você selecione o tipo de backup. Por padrão vem selecionado o tipo Normal que é o tipo que será utilizado no nosso exemplo. Certifique-se de que esteja selecionada a opção Normal e clique no botão Avançar, para ir para a próxima etapa do assistente.

Nesta etapa você pode definir as seguintes opções:

- ◆ **Verificar dados após o backup:** Se você marcar esta opção, os dados serão verificados após ter sido feito o backup. A verificação é feita para garantir que os dados que foram copiados para o backup são idênticos aos dados originais. Ao ativar a verificação, o backup irá demorar bem mais para ser concluído, porém você terá a confirmação de que o backup está sendo feito corretamente e que os dados estão corretos.
  - ◆ **Usar compactação por hardware, se disponível:** Esta opção permite que você utilize a capacidade de compactação de alguns drives de fita de backup. Somente estará disponível se você tiver um drive de fita instalado e estiver fazendo o backup para o drive de fita.
  - ◆ **Desativar a cópia de sombra de volume:** Sombra de volume é uma “horrível” tradução para o recurso de Shadow Copies, o qual será apresentado no final do Capítulo. As cópias de sombra de volume permitem que seja feito o backup de arquivos, mesmo que algumas informações ainda estejam sendo gravadas no disco rígido.
13. Certifique-se de que as opções desta etapa estejam todas desmarcadas e clique no botão Avançar, para ir para a próxima etapa do assistente.
- Nesta etapa do assistente você pode definir as seguintes opções:
- ◆ **Acrescentar este backup aos backups existentes:** Esta opção permite que sejam mantidos diferentes backups (por exemplo, backups feitos em diferentes datas) em um mesmo arquivo de backup (.bkf) ou em uma fita de backup.
  - ◆ **Substituir os backups existentes:** Se você marcar esta opção, todos os backups anteriores, caso exista algum, no arquivo Documentos.bkf (ou na fita que estiver sendo utilizado, no caso de um backup em fita), serão excluídos e somente o backup que está sendo feito será gravado. Ao marcar esta opção, a opção Permitir que somente o proprietário e o administrador tenham acesso aos dados de backup e a todos os backups acrescentados a este mídia, será habilitada. Esta opção é utilizada para impedir que qualquer outro usuário possa restaurar os dados do backup, mesmo não tendo permissões sobre os arquivos originais. É uma proteção adicional aos dados.
14. Certifique-se de que as opções Substituir os backups existentes e Permitir que somente o proprietário e o administrador tenham acesso aos dados de backup e a todos os backups acrescentados a este mídia estejam marcadas, conforme indicado na Figura 8.20:

**IMPORTANTE: Permita-me enfatizar este ponto, pela terceira vez. É fundamental que você entenda claramente os diferentes tipos de backup e em que situações eles são utilizados, bem como as estratégias de restore a serem utilizadas, com base nos tipos de backups que foram efetuados. Revise bem este item, apresentado anteriormente neste capítulo.**

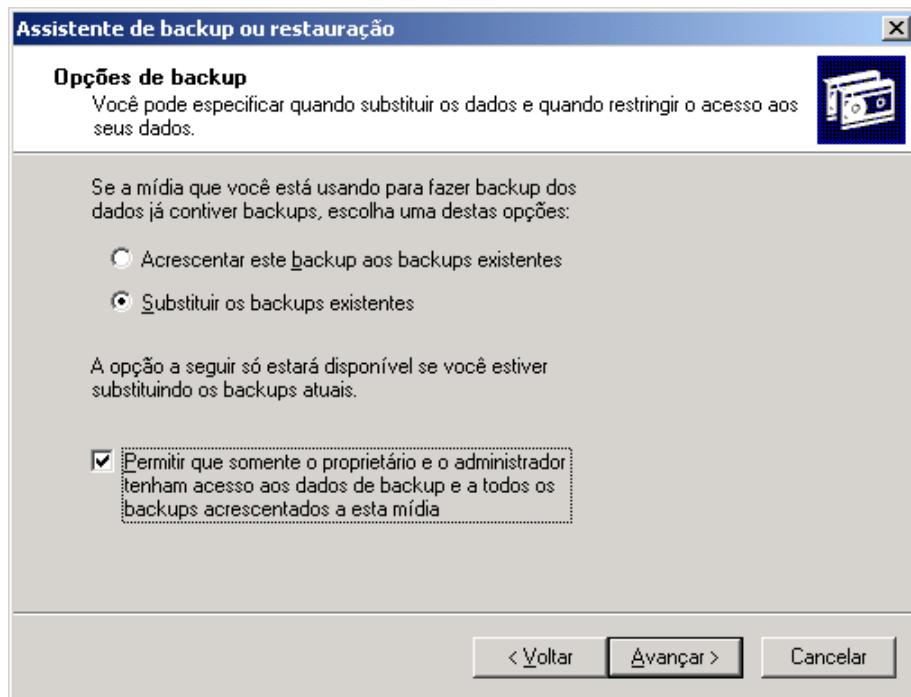


Figura 8.20 Definindo opções de Backup.

15. Clique no botão Avançar, para ir para a próxima etapa do assistente.
16. Nesta etapa podemos definir um agendamento para o Backup. Ao definir um agendamento, será criada uma Tarefa agendada, a qual executará o backup com as opções escolhidas, nos horários programados. Para definir um agendamento marque a opção Mais tarde. Para nome da tarefa agendada digite Backup de Documentos do drive C, conforme indicado na Figura 8.21:

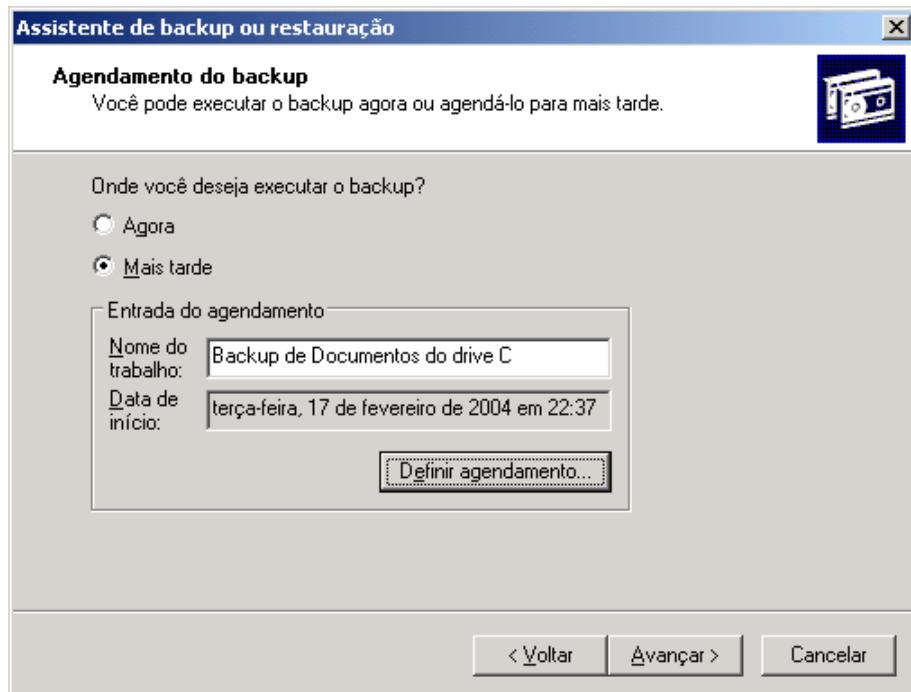


Figura 8.21 Habilitando o agendamento.

17. Para definir os dias e horários de execução da tarefa, clique no botão Definir agendamento... Será exibida a janela Agendar trabalho, já descrita no início do Capítulo, onde tratei sobre a configuração do Agendamento de Tarefas agendadas. Selecione as opções indicadas na Figura 8.22 e clique em OK.

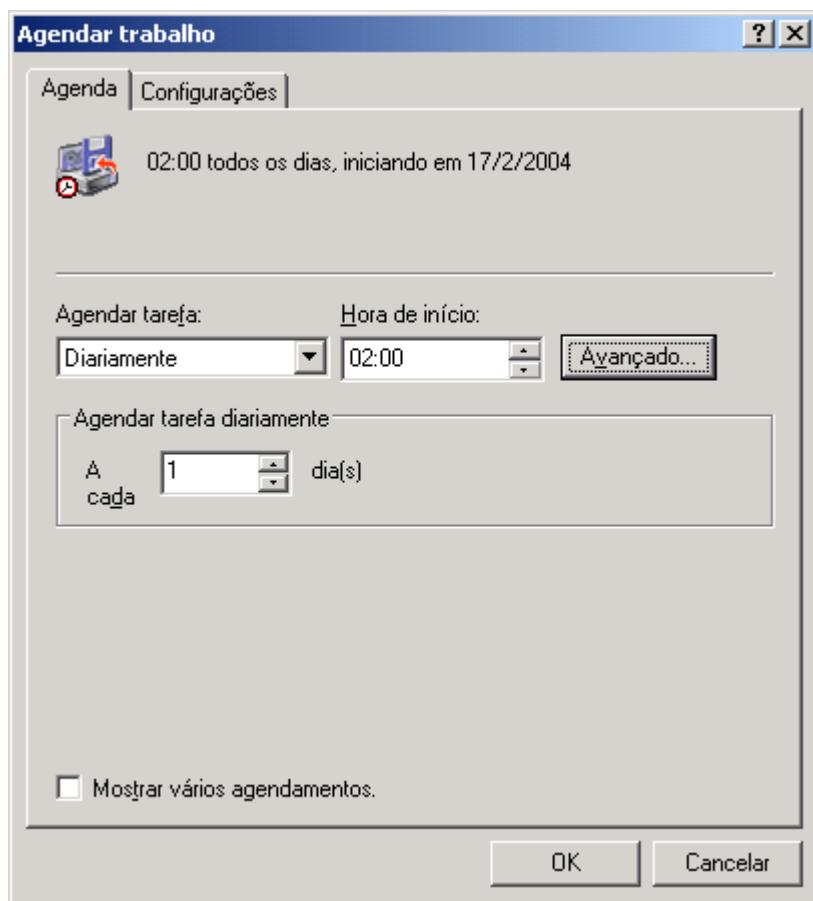


Figura 8.22 Configurando as opções de agendamento.

18. Você estará de volta ao Assistente de backup. Clique no botão Avançar, para ir para a próxima etapa do assistente.
19. Será exibida a janela para definir informações de conta, na qual você precisa informar o nome e senha da conta que será utilizada para a execução da tarefa agendada responsável pela execução do backup. Digite o nome da conta e a senha duas vezes, conforme indicado na Figura 8.23 e clique em OK.
20. Você estará na tela final do assistente. Será exibido um resumo das opções selecionadas. Utilize o botão Voltar, caso você precise alterar alguma opção. Para finalizar o assistente e criar a tarefa agendada responsável pela execução do backup, clique no botão Concluir.

A tarefa é criada e todos os dias, às 2:00 da madrugada a tarefa será executada e o backup da pasta C:\documentos será feito. Você pode fazer com que a tarefa seja executada imediatamente, para testar se o backup será feito corretamente.

**IMPORTANTE:** Pode haver situações práticas onde você terá que executar um Backup com periodicidades diferentes, como por exemplo: todos os dias às 2:00 da madrugada e somente no Sábado às 8:00 da manhã. Nestas situações você tem que criar múltiplos agendamentos. Um agendamento para fazer o backup de segunda a sexta, às 2:00 da madrugada e um segundo agendamento para fazer o backup, aos Sábados, às 8:00 da manhã. Para criar múltiplos agendamentos você usa a opção "Mostrar vários agendamentos", a qual já foi descrita no tópico sobre Tarefas agendadas, no início do capítulo

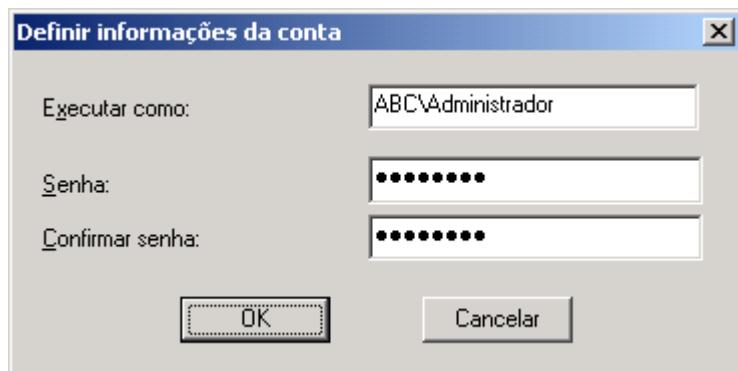


Figura 8.23 Conta para a execução da tarefa agendada.

Para executar a tarefa manualmente e fazer o backup, siga os passos indicados a seguir:

1. Abra o Painel de controle: Iniciar -> Painel de controle.
2. Abra a opção Tarefas agendadas.
3. A tarefa Backup de Documentos do drive C já deve aparecer na lista de tarefas agendadas, conforme indicado na Figura 8.24:

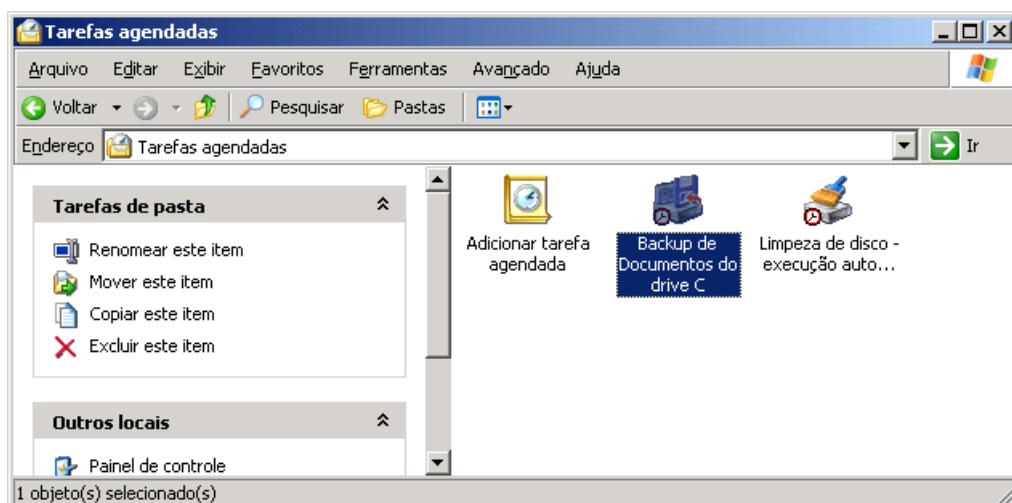
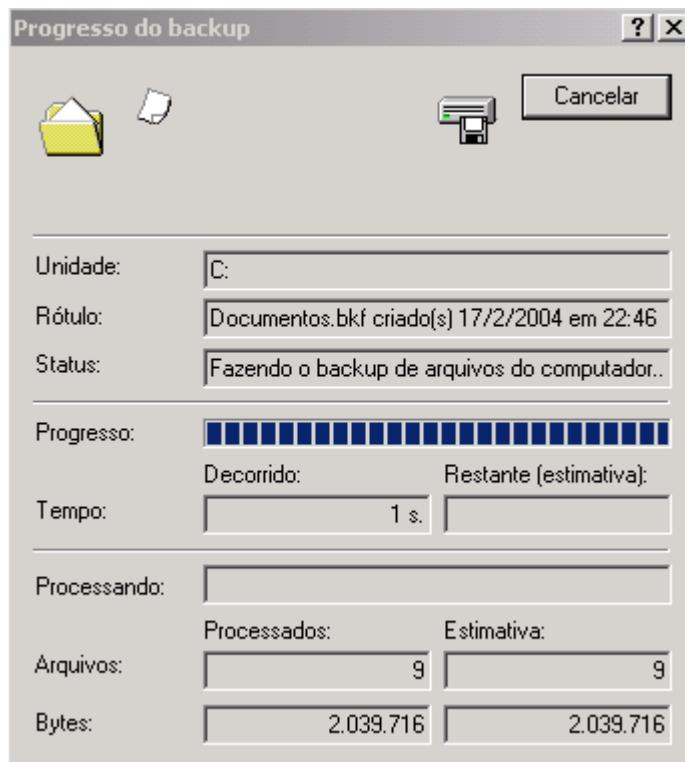


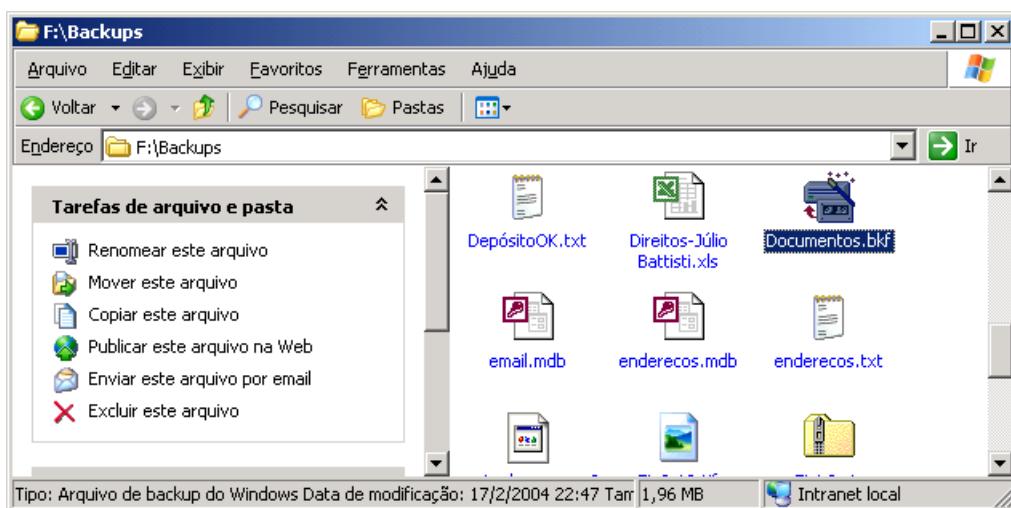
Figura 8.24 A tarefa Backup de Documentos do drive C.

4. Clique na tarefa Backup de Documentos do drive C para marca-la e selecione o comando Arquivo -> Executar.
5. O utilitário de backup será inicializado e o backup da pasta C:\Documentos começará a ser feito, conforme indicado na Figura 8.25:



**Figura 8.25 O backup da pasta C:\Documentos sendo feito.**

6. Após o encerramento do backup a janela do utilitário de backup é automaticamente fechada e você estará de volta à janela Tarefas agendadas. Feche a janela Tarefas agendadas.
7. Abra o Windows Explorer e navegue até a pasta onde foi feito o backup e verifique se o arquivo Documentos.bkf foi criado, conforme exemplo da Figura 8.26:



**Figura 8.26 O arquivo Documentos.bkf.**

O arquivo Documentos.bkf contém todo o conteúdo da pasta C:\Documentos e poderá ser utilizado para restaurar o conteúdo desta pasta em caso de perda dos dados.

Agora você aprenderá um pouco mais sobre a interface completa do utilitário de backup do Windows Server 2003.

## Fazendo o backup de pastas e arquivos utilizando a interface completa.

Neste exemplo prático, vou utilizar o utilitário de backup no modo completo, para fazer o

backup da pasta Meus documentos do usuário Logado. Também vou criar e agendar uma tarefa que executa este backup, diariamente, as 22:00 hs. Vou criar um backup do tipo normal. O backup será feito na unidade de disco F:, em uma pasta chamada backups, com o nome de Meus documentos.bkf. Observe que estou fazendo o backup em uma unidade de disco rígido diferente da unidade onde estão os arquivos que farão parte do backup.

Para criar o backup proposto e agenda-lo, siga os passos indicados a seguir:

1. Faça o logon com uma conta do usuário para o qual você deseja fazer o backup da pasta Meus documentos.
2. Abra o utilitário de backup, utilizando um dos procedimentos descritos anteriormente. Será aberto o utilitário de backup no modo assistente.
3. A primeira tela do assistente é apenas informativa. Para acessar o modo avançado, ou seja, a interface completa do utilitário de backup dê um clique na opção Modo avançado.
4. Será aberta a janela do utilitário de backup, com a guia Bem-vindo selecionada, conforme indicado na Figura 8.27:

**NOTA:** As opções que foram explicadas no exemplo anterior, não serão explicadas novamente. Irei focar mais na utilização da interface completa, do utilitário de backup.

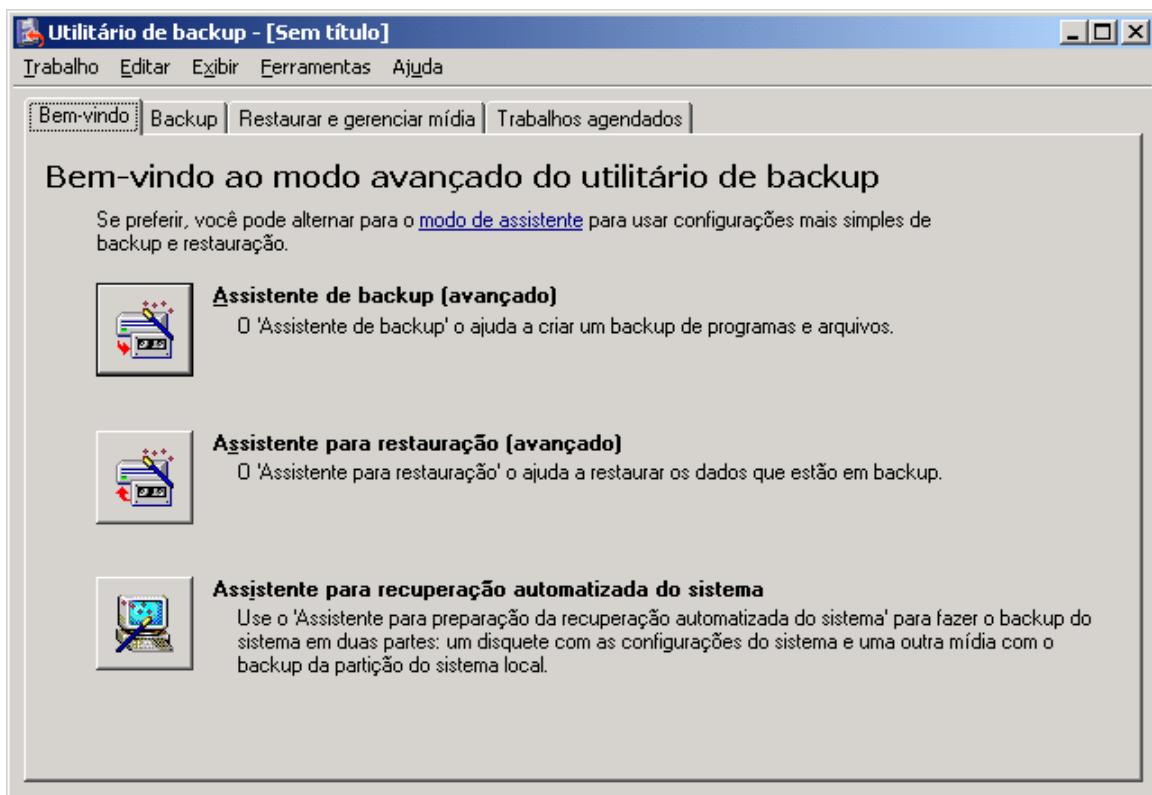


Figura 8.27 O utilitário de backup no modo de interface completa.

Na guia Bem-vindo você tem a opção de iniciar o Assistente de backup (Avançado), o Assistente para restauração (Avançado) ou o Assistente Para Recuperação Automatizada do Sistema, o qual será visto no Capítulo 12. O assistente para restauração será visto mais adiante, ainda neste capítulo. Você utiliza a guia Backup para criar um novo backup. No exemplo proposto, utilizarei a guia Backup. A guia Restaurar e gerenciar mídia será vista no próximo tópico. A

guia Trabalhos agendados exibe o calendário do mês e um indicativo das tarefas agendadas para cada dia. Esta guia também pode ser utilizada para adicionar novas tarefas agendadas.

5. Dê um clique na guia Backup. No painel da esquerda você pode navegar pelos volumes e pastas de cada volume do computador ou da rede, selecionando os arquivos e pastas que farão parte do Backup. Para o nosso exemplo, marque a pasta Meus documentos, conforme indicado na Figura 8.28. No campo Mídia de backup ou nome do arquivo, digite F:\Backups\Meus documentos.bkf, conforme indicado na Figura 8.28.

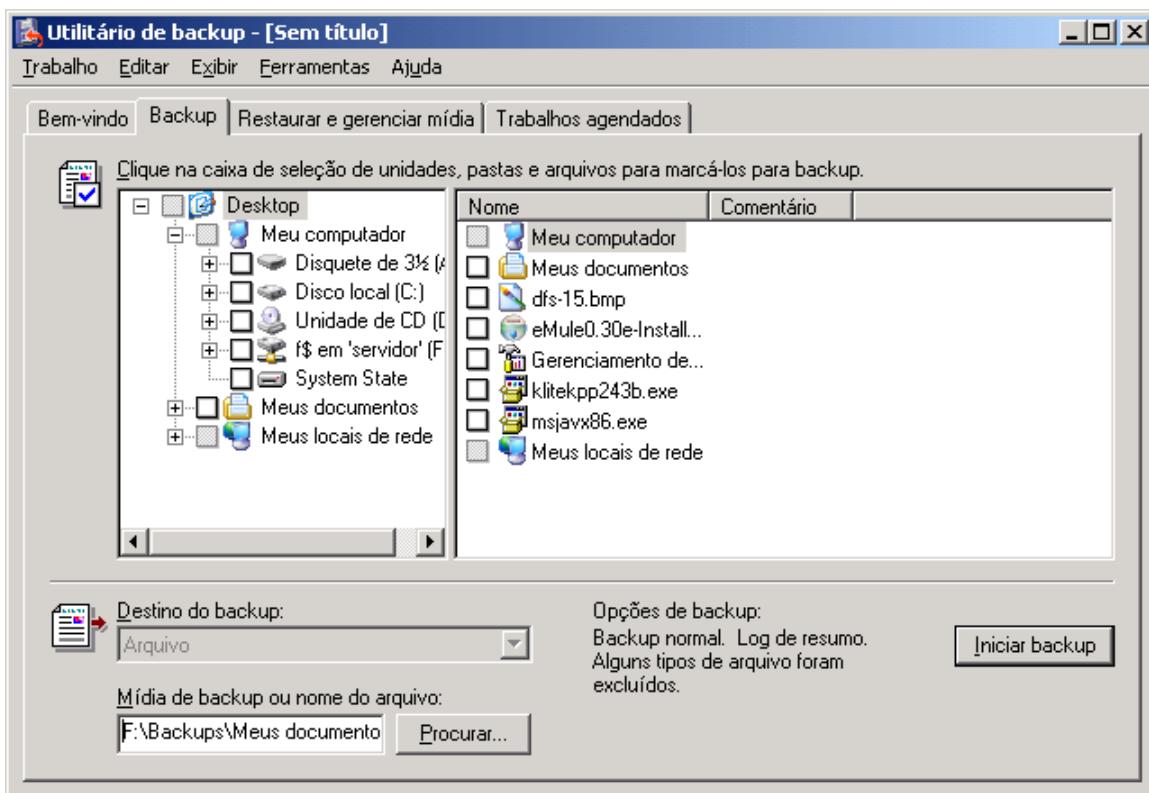
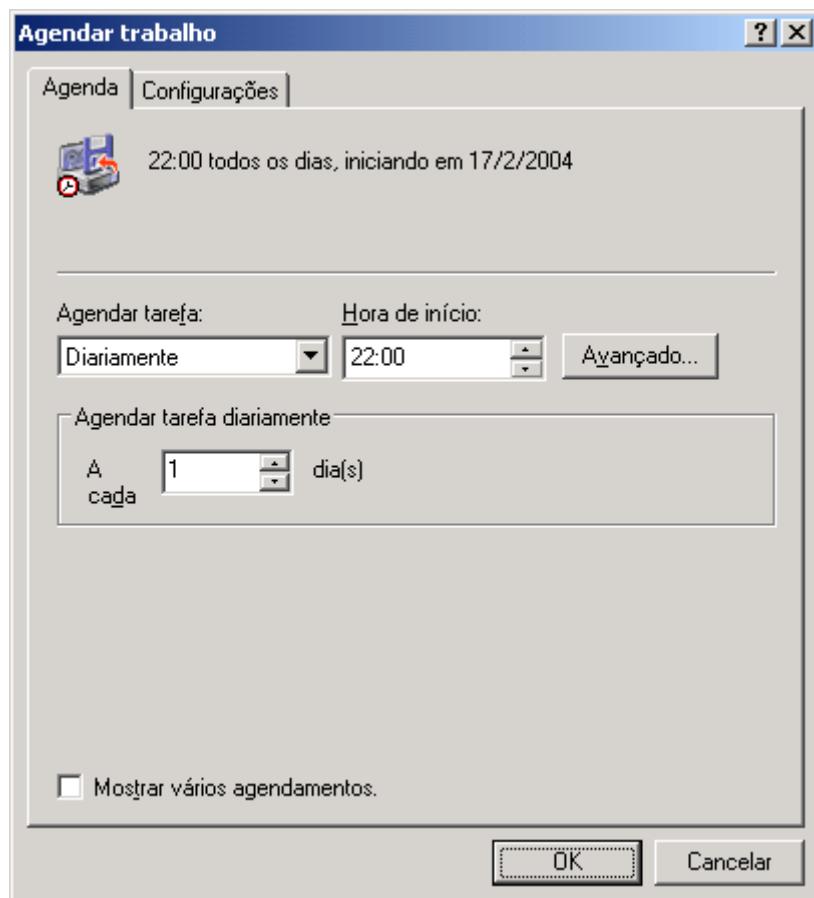


Figura 8.28 Selecionando a pasta Meus documentos, do usuário logado.

6. Para definir o tipo de backup selecione o comando Ferramentas -> Opções. Será exibida a janela Opções com a guia Tipo de backup já selecionada. Certifique-se de que a opção Normal esteja selecionada e clique em OK.
7. Você estará de volta a janela do utilitário de backup. Agora vou definir um agendamento para o backup. Para isso vou alternar para o Assistente de backup, porém mantendo as configurações que já foram feitas. Selecione o comando Ferramentas -> Assistente de backup. Surge uma janela pedindo se você deseja manter as configurações já efetuadas. Clique em Sim para manter as configurações.
8. O assistente é aberto. Clique no botão Avançar, para ir para a próxima etapa do assistente.
9. Observe que na segunda etapa já aparece selecionada a pasta Meus documentos. Clique no botão Avançar, para ir para a próxima etapa do assistente.
10. Nesta etapa você precisa redefinir o arquivo de destino, pois esta configuração não é mantida. Para o nosso exemplo vou definir o destino como sendo o drive F:\Backups\Meus documentos.bkf. Utilize o destino que for mais adequado para o seu caso. Para definir o destino utilizamos o botão Procurar..., conforme descrito no exemplo anterior. Defina o arquivo de destino para o backup e clique no botão Avançar, para ir para a próxima etapa do assistente.
11. Nesta etapa clique no botão Avançado... para definir o agendamento.

12. É exibida uma lista para que você defina o tipo de Backup. Certifique-se de que a opção Normal esteja selecionada e clique no botão Avançar, para ir para a próxima etapa do assistente.
13. Nesta etapa certifique-se de que todas as opções (já descritas no exemplo anterior) estejam desmarcadas e clique no botão Avançar, para ir para a próxima etapa do assistente.
14. Nesta etapa certifique-se de que as opções Substituir os backups existentes e Permitir que somente o proprietário e o administrador tenham acesso aos dados de backup e a todos os backups acrescentados a este mídia, estejam marcadas e clique no botão Avançar, para ir para a próxima etapa do assistente.
15. Nesta etapa vou definir o agendamento. Clique na opção Mais tarde. No campo Entrada de agendamento digite: Backup de Meus documentos. Clique no botão Definir agendamento... e defina as opções indicadas na Figura 8.29. Depois clique em OK.



**Figura 8.29 Backup diários às 22:00 hs.**

16. Você estará de volta ao Assistente de backup. Clique no botão Avançar, para ir para a próxima etapa do assistente.
17. Será exibida a janela Definir informações de conta, na qual você precisa informar o nome e senha da conta que será utilizada para a execução da tarefa agendada responsável pela execução do backup. Digite o nome da conta e a senha duas vezes e clique em OK.
18. Você estará na tela final do assistente. Será exibido um resumo das opções selecionadas. Utilize o botão Voltar caso você precise alterar alguma opção. Para finalizar o assistente e criar a tarefa agendada responsável pela execução do backup, clique no botão Concluir.

19. Você estará de volta à janela Utilitário de backup. Clique na guia Trabalhos agendados. Observe que existem dois trabalhos de backup (tarefas) agendados para executar diariamente, conforme indicado na Figura 8.30:



Figura 8.30 Duas tarefas agendadas para execução diária.

As duas tarefas diárias são resultado dos dois exemplos que fizemos até agora. Se você deixar o mouse sobre uma das tarefas, aparece uma pequena descrição da tarefa. Se você der um clique duplo em uma dia no calendário mensal, será aberto o assistente de backup, para que você crie uma nova tarefa de backup..

#### 20. Feche o utilitário de backup.

A tarefa é criada e agendada para executar todos os dias, a partir da data de criação, as 22:00 hs. a tarefa será executada e o backup da pasta Meus documentos será feito. Você pode fazer com que a tarefa seja executada imediatamente, para testar se o backup será feito corretamente, conforme descrito no exemplo anterior.

Observe que a criação de uma tarefa para execução do backup consiste basicamente na utilização do assistente de backup.

Agora você aprenderá a fazer o restore a partir de um arquivo de backup.

## Fazendo o restore das informações a partir do backup.

Neste exemplo prático, vou utilizar o utilitário de backup/restore para fazer o restore da pasta C:\Documentos a partir do backup E:\Backups\Documentos.bkf. Observe que estou simulando uma situação onde houve um problema com a pasta C:\Documentos e é necessário restaurá-la a partir do backup. Vou fazer a restauração para um local alternativo, ou seja, não para a pasta original. No nosso exemplo farei a restauração para o drive E:\Documentos. Apenas para lembrar, os arquivos originais que foram copiados para o backup estão em C:\Documentos.

Com o Assistente de restauração que será utilizado neste exemplo, é possível restaurar a pasta C:\Documentos completa ou apenas parte do seu conteúdo. Por exemplo, pode ser que um determinado arquivo da pasta Documentos tenha sido excluído por engano. Neste caso basta restaurar a penas o arquivo que foi excluído por engano e não toda a pasta Documentos.

Também é possível fazer a restauração para outra pasta que não para a localização original. Neste caso faríamos o restore para uma pasta alternativa, verificaríamos se os arquivos foram restaurados com sucesso e então copiaríamos os arquivos para a pasta Documentos original.

Para fazer o restore da pasta C:\Documentos a partir do arquivo de backup Documentos.bkf, siga os passos indicados a seguir:

1. Faça o logon com uma conta com permissão de administrador ou com uma conta do grupo Backup Operators (Oper. de Cópia).
2. Abra o utilitário de backup, utilizando um dos procedimentos descritos anteriormente. Será aberto o utilitário de backup no modo assistente.
3. A primeira tela do assistente é apenas informativa. Para acessar o modo avançado, ou seja, a interface completa do utilitário de backup dê um clique na opção Modo avançado.
4. Será aberta a janela do utilitário de backup, com a guia Bem-vindo selecionada.
5. Clique no botão ao lado da opção Assistente para restauração (avançado).
6. Será aberto o Assistente para restauração. A primeira tela é apenas informativa. Clique no botão Avançar, para ir para a próxima etapa do assistente.

Surge a janela Itens a serem restaurados. Nesta etapa você define o drive de fita ou o arquivo .bkf a partir do qual os dados serão restaurados.

7. Clique no botão Procurar... Surge a janela Abrir arquivo de backup. Nesta janela você pode digitar o caminho completo para o arquivo .bkf, que no nosso exemplo é: E:\Backups\Documentos.bkf, conforme indicado na Figura 15.31:

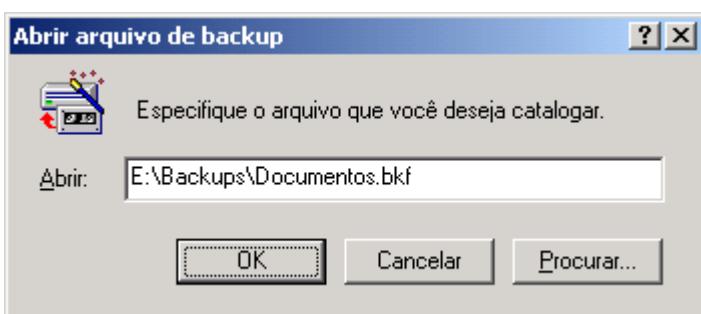


Figura 8.31 Informando o caminho para o arquivo .bkf.

8. Após digitar o caminho para o arquivo .bkf clique em OK. Dependendo do tamanho do arquivo o Windows Server 2003 pode demorar alguns instantes para acessá-lo. Você estará de volta à janela do assistente e o arquivo Documentos.bkf já aparece no Painel da esquerda. Clique no sinal de + ao lado de Documentos.bkf para expandi-lo. Marque a caixa de seleção ao lado do drive C, conforme indicado na Figura 8.32:

**NOTA:** Ao invés de digitar o caminho para o arquivo .bkf você pode utilizar o botão Procurar..., da janela Abrir arquivo de backup). Ao clicar neste botão será aberta a janela Selecione o arquivo para catalogar. Nesta janela você pode navegar até a pasta onde está o arquivo .bkf, clicar nele para marcá-lo e clicar no botão Abrir. O Windows Server 2003 voltará para a janela Abrir arquivo de backup, com o caminho para o arquivo já preenchido.

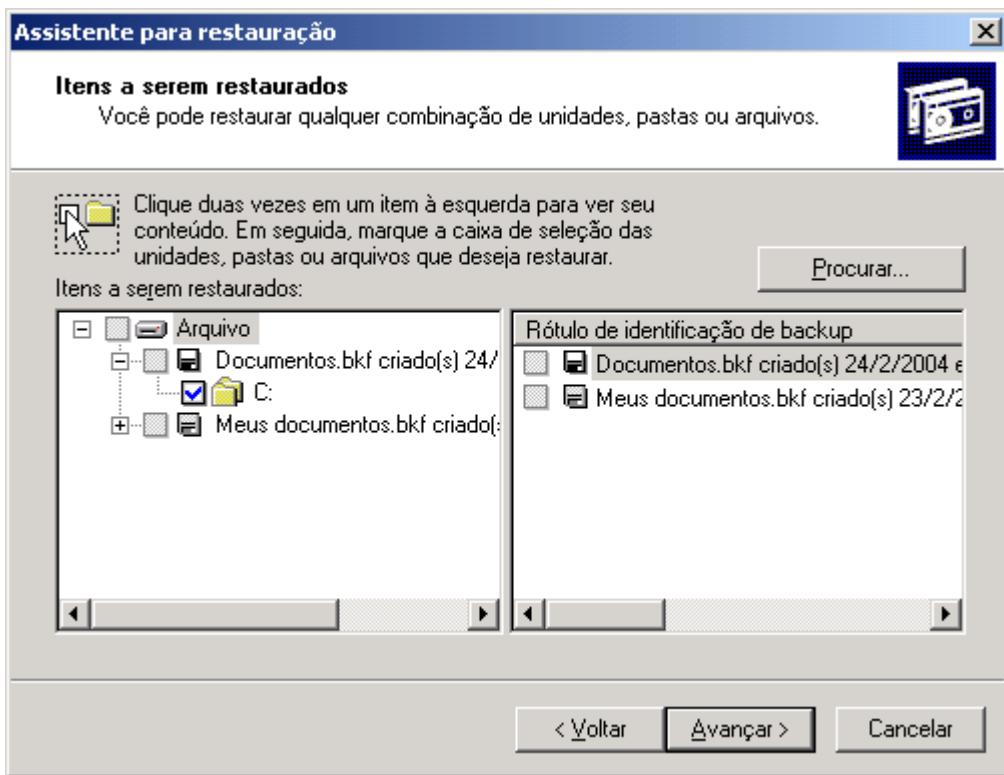


Figura 8.32 Selecionando o arquivo de backup a ser restaurado.

9. Clique no botão Avançar, para ir para a próxima etapa do assistente.
  10. Será exibida a tela final do Assistente com um resumo das opções selecionadas. Caso você queira alterar alguma opção, utilize o botão Voltar. Se você encerrar o assistente neste momento, o Windows Server 2003 irá restaurar os arquivos para os locais originais, isto é, para as pastas onde estes estavam gravados quando foram copiados para o backup. Se quiser fazer a restauração para um local alternativo, você deve que utilizar o botão Avançado...
  11. Clique no botão Avançado..., para especificar um local alternativo para a restauração do backup.
  12. Será exibida a janela Onde restaurar. Na lista Restaurar os arquivos em vem selecionado, por padrão, a opção Local original. Se você escolher esta opção os arquivos serão restaurados para a pasta de origem. Selecione a opção Local alternativo. Observe que ao selecionar esta opção, é exibido o campo Local alternativo, no qual você pode especificar o novo local para restauração dos arquivos. Digite E:\Documentos, conforme indicado na Figura 8.33.
  9. Clique no botão Avançar, para ir para a próxima etapa do assistente.
  10. Surge a janela Como restaurar. Nesta etapa você tem as seguintes opções:
    - ◆ **Manter os arquivos existentes (recomendável):** Se você selecionar esta opção, os arquivos já existentes no local de destino, não serão sobreescritos pelos arquivos copiados a partir do backup. Esta opção é indicada quando você está restaurando um backup para recuperar um ou mais arquivos que
- NOTA:** Ao marcar a caixa de seleção ao lado de Documentos.bkf estamos solicitando ao Windows Server 2003 que restaure todo o conteúdo deste arquivo de backup. Porém poderíamos restaurar apenas uma ou mais pasta ou um ou mais arquivos e não todo o conteúdo. Por exemplo, pode ser que o usuário tenha excluído por engano, um único arquivo. Neste caso não é necessária a restauração de todo o backup e sim apenas do arquivo que foi perdido. Para restaurar apenas parte do backup, basta clicar no sinal de + ao lado de Documentos.bkf. Será exibida a lista de drives a partir dos quais foram copiados dados para o backup. No nosso exemplo surgirá o drive C. Clique no sinal de mais ao lado de drive C. Serão exibidas as pastas do drive C que foram copiadas para o backup. Agora é só ir navegando e marcando as pastas e/ou arquivos a serem restaurados.

foram excluídos por engano. Se o número de arquivos excluídos por engano for pequeno é mais vantagem selecionar apenas os arquivos a serem recuperados, conforme descrito anteriormente.

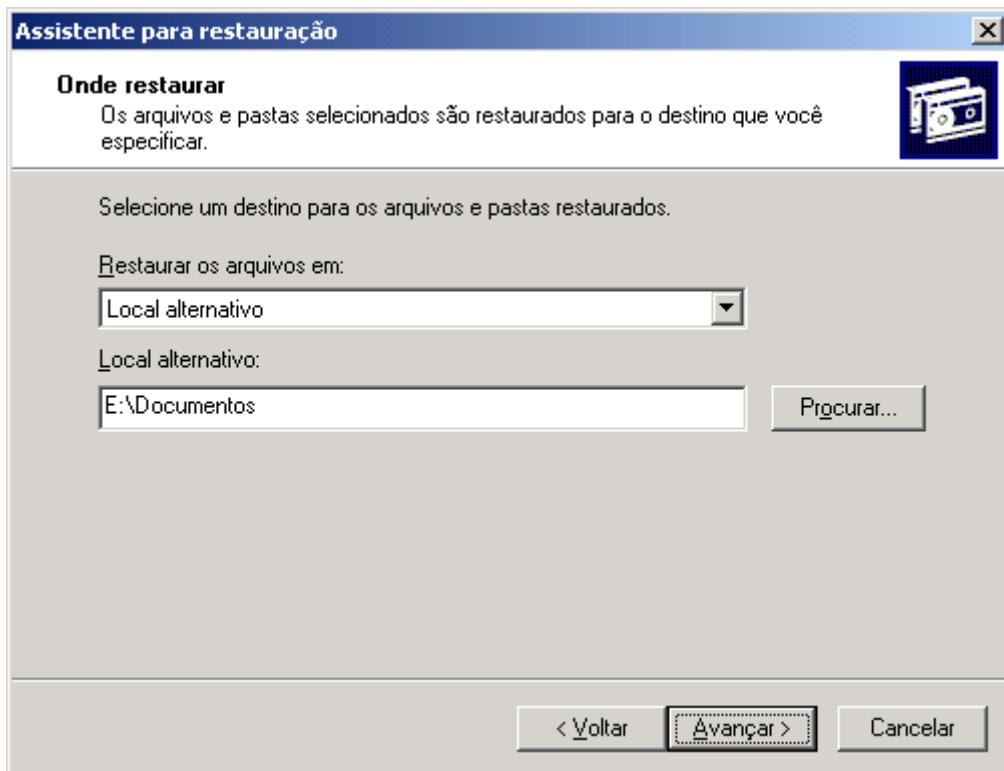
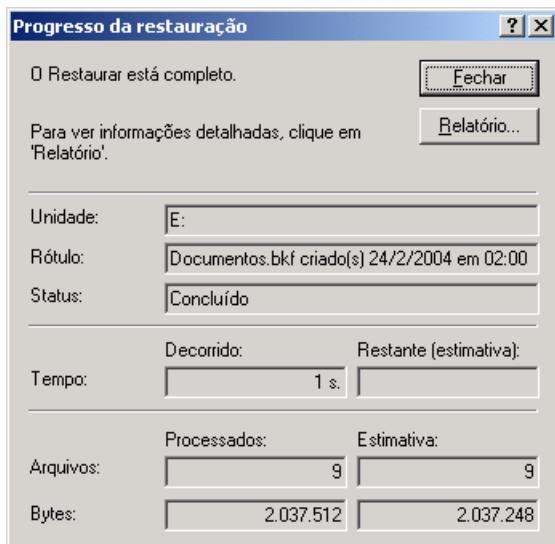


Figura 8.33 Especificando um local alternativo para a restauração.

- ◆ **Substituir os arquivos existentes se eles forem mais antigos do que o backup:** Se você marcar esta opção, os arquivos que já existirem na pasta de destino, somente serão substituídos se forem mais antigos do que os arquivos que estão sendo restaurados a partir do backup.
  - ◆ **Sempre substituir arquivos:** Se você selecionar esta opção, todos os arquivos que já existirem na pasta de destino serão substituídos pelos arquivos do backup, independente de serem mais antigos ou não. Utilize esta opção com cuidado.
11. Certifique-se de que a opção Manter os arquivos existentes (recomendado) esteja selecionada e clique no botão Avançar, para ir para a próxima etapa do assistente.
  12. Nesta etapa você define se deseja ou não Restaurar configurações de segurança. Certifique-se de que a opção Restaurar configurações de segurança esteja selecionada. Esta opção garante que as permissões NTFS e demais opções de segurança como criptografia, sejam mantidas ao restaurar o backup. Clique no botão Avançar, para ir para a próxima etapa do assistente.
  13. Será exibida a tela final do Assistente com um resumo das opções selecionadas. Caso você queira alterar alguma opção, utilize o botão Voltar. Para iniciar o processo de restauração clique no botão Concluir.
- O processo de restauração é inicializado, conforme indicado na Figura 8.34.
14. Ao final do processo de restauração a janela de restauração é mantida aberta com uma mensagem informando que a restauração foi efetuada com sucesso. Clique em Fechar, para sair da janela de restauração.
  15. Você estará de volta à janela do utilitário de backup. Feche-o.



**Figura 8.34 Restauração dos arquivos.**

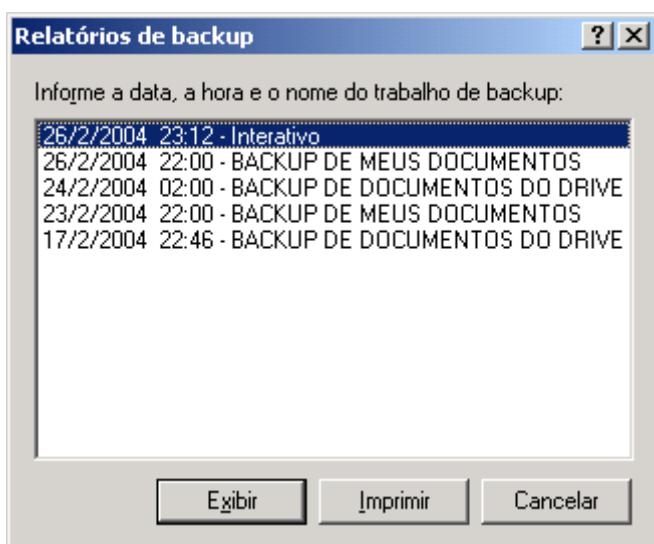
16. Abra o Windows Explorer e navegue para a pasta onde você fez a restauração. Observe se os arquivos foram restaurados com sucesso.
17. Feche o Windows Explorer.

## O log do backup.

O Windows Server 2003 mantém um registro das operações de backup e restauração. Este registro pode ser utilizado pelo Administrador para verificar se as tarefas de backup estão sendo executadas com sucesso.

Para acessar informações sobre as operações de backup, siga os seguintes passos:

1. Faça o logon como Administrador ou com uma conta com permissão de administrador.
2. Abra o utilitário de backup no modo avançado, conforme explicado anteriormente.
3. Selecione o comando Ferramentas -> Relatório...
4. Será exibida a janela Relatórios de Backup, conforme indicado na Figura 8.35:



**Figura 8.35 A janela de relatórios de backup.**

**IMPORTANTE: O log de Backup é gravado como parte da Profile da conta com a qual está sendo executado o Backup. Por exemplo, se o usuário jsilva estiver em sua estação de trabalho – micro01, fazendo o backup de pastas de um Servidor server02, o log de backup será gravado na Profile do usuário jsilva, no computador micro01.**

5. Os nomes que aparecem nesta listagem estão relacionados com os nomes que você definiu para o backup. O nome Interativo será exibido para os backups que foram feitos utilizando a interface completa ao invés do assistente de backup. Selecione um backup na lista e clique em Exibir. O Bloco de Notas será aberto com um relatório de todas as operações efetuadas, conforme exemplo indicado a seguir:

**Status da restauração**  
**Operação: restauração**

```
Backup de "C:", restaurado para "E: Dados\Documentos\"  
Conjunto de backup nº1 na mídia nº1  
Descrição do backup: "Conjunto criado em 20/4/2002 às 22:22"  
  
A restauração foi iniciada no(a) 21/4/2002 às 08:27.  
Restauração concluída no(a) 21/4/2002 às 08:28.  
Pastas: 31  
Arquivos: 753  
Bytes: 69.618.787  
Tempo: 48 segundos
```

---

6. Feche o Bloco de notas. Você estará de volta à janela de relatórios de backup. Clique em Cancelar para fechá-la. Você estará de volta ao utilitário de backup.

## Definindo opções padrão de backup e restore.

Ao utilizar o assistente de backup e/ou restore, você deve ter notado que algumas opções vêm selecionadas por padrão. É possível alterar algumas destas opções, definindo novos padrões. Isto é feito através do comando Ferramentas -> Opções... do utilitário de backup.

Para configurar opções padrão de backup/restore, faça o seguinte:

1. Faça o logon como Administrador ou com uma com permissão de administrador
2. Abra o utilitário de backup.
3. Selecione o comando Ferramentas -> Opções...
4. A janela Opções será exibida. Dê um clique na guia Geral. Serão exibidas as opções indicadas na Figura 8.36:

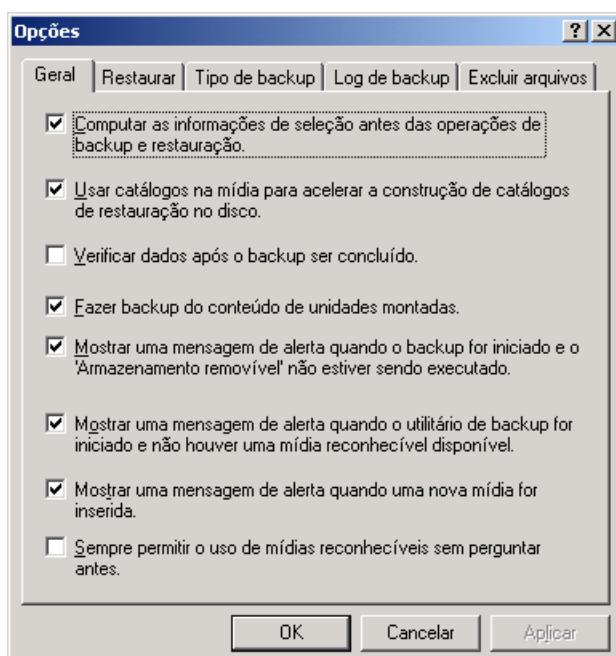


Figura 8.36 A guia geral da janela de opções.

Na guia Geral podem ser configuradas as seguintes opções:

- ◆ **Computar as informações de seleção antes das operações de backup e restauração:** Estima o número de arquivos e bytes que serão copiados ou restaurados durante a operação de backup ou restauração atual. Estas informações serão calculadas e exibidas antes do início do backup ou da restauração.
  - ◆ **Usar catálogos na mídia para acelerar a constituição de catálogos de restauração no disco:** De uma maneira simplificada, um catálogo contém as informações que o utilitário de backup usa para gerenciar um ou mais backups efetuados na mesma fita ou no mesmo arquivo .bkf. Esta opção, quando marcada, indica que você deseja usar o catálogo em mídia para construir o catálogo em disco para restaurar os arquivos e pastas selecionados. Esse é o modo mais fácil de criar um catálogo em disco. Se você desejar restaurar dados de várias fitas e a fita com o catálogo em mídia estiver faltando ou desejar restaurar dados da mídia que está danificada, não deverá selecionar esta opção. O backup verificará todo o conjunto de backup (ou o que você tiver) e criará um catálogo em disco. Este procedimento poderá demorar várias horas se o conjunto de backup for muito extenso.
  - ◆ **Verificar dados após o backup ser concluído:** Verifica os dados de backup comparando-os com os dados originais no disco rígido para certificar-se de que sejam os mesmos. Se não forem, pode haver um problema com a mídia ou com o arquivo que você está usando para fazer backup dos dados. Caso algum problema seja detectado você deve usar uma mídia diferente ou designar outro arquivo e executar a operação de backup novamente.
  - ◆ **Fazer o backup do conteúdo de unidades montadas:** Faz backup dos dados que estiverem em uma unidade montada. Se você selecionar esta opção e fizer backup de uma unidade montada, será efetuado o backup dos dados nessa unidade montada. Se você não selecionar essa opção e fizer backup de uma unidade montada, será efetuado o backup somente das informações do caminho para essa unidade.
  - ◆ **Mostrar uma mensagem de alerta quando o backup for iniciado e o ‘Armazenamento removível’ não estiver sendo executado:** Exibe uma caixa de diálogo quando você iniciar o backup e o armazenamento removível não estiver em execução. Se você fizer backup de dados principalmente em um arquivo e salvar o arquivo em um disquete, disco rígido ou qualquer tipo de disco removível, não precisará marcar esta caixa de seleção. Se você fizer backup de dados principalmente em uma fita ou outra mídia gerenciada pelo armazenamento removível, como por exemplo um zip drive, deverá marcar esta caixa de seleção.
  - ◆ **Mostrar uma mensagem de alerta quando o backup for iniciado e não houver uma mídia de importação compatível disponível:** Exibe uma caixa de diálogo quando você iniciar o backup e existir uma nova mídia disponível no pool de importação de armazenamento removível. Se você fizer backup de dados principalmente em um arquivo e salvar o arquivo em um disquete, disco rígido ou qualquer tipo de disco removível, não precisará marcar esta caixa de seleção. Se você fizer backup de dados principalmente em uma fita ou outra mídia que seja gerenciada pelo armazenamento removível, deverá marcar esta caixa de seleção.
  - ◆ **Mostrar uma mensagem de alerta quando uma nova mídia for inserida:** Exibe uma caixa de diálogo quando a nova mídia for detectada pelo armazenamento removível.
  - ◆ **Sempre permitir o uso de mídias reconhecíveis sem perguntar antes:** Move automaticamente a nova mídia detectada pelo armazenamento removível para o pool de backup. Se você fizer backup de dados principalmente em um arquivo e salvar o arquivo em um disquete, disco rígido ou qualquer tipo de disco removível, não precisará marcar esta caixa de seleção. Se você usar o armazenamento removível para gerenciar a mídia e desejar que todas as novas mídias estejam disponíveis somente para o programa de backup, deverá marcar esta caixa de diálogo.
5. Dê um clique na guia Restaurar. Serão exibidas as opções indicadas na Figura 8.37:

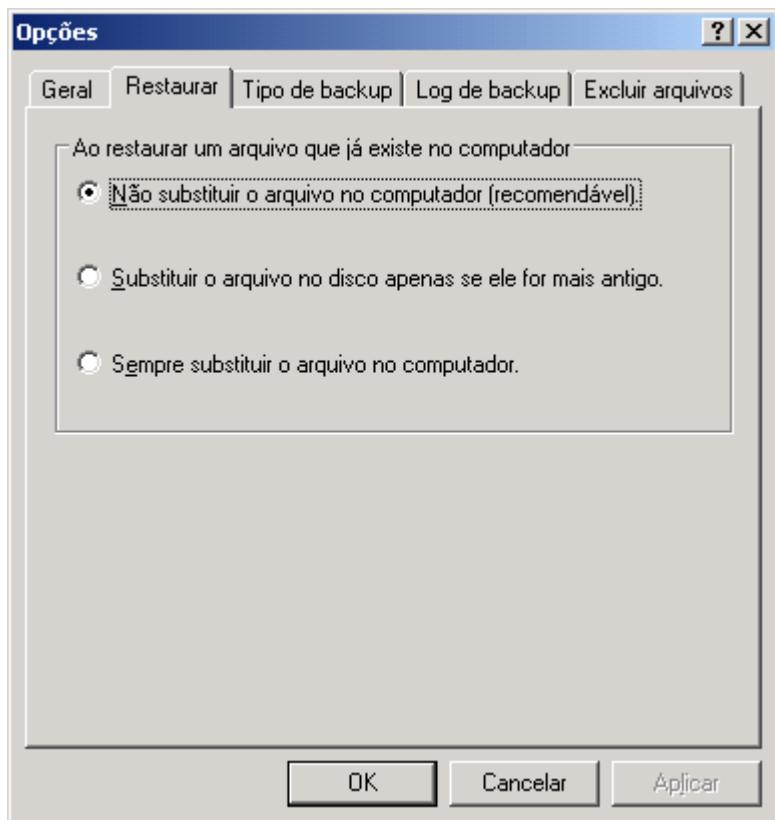


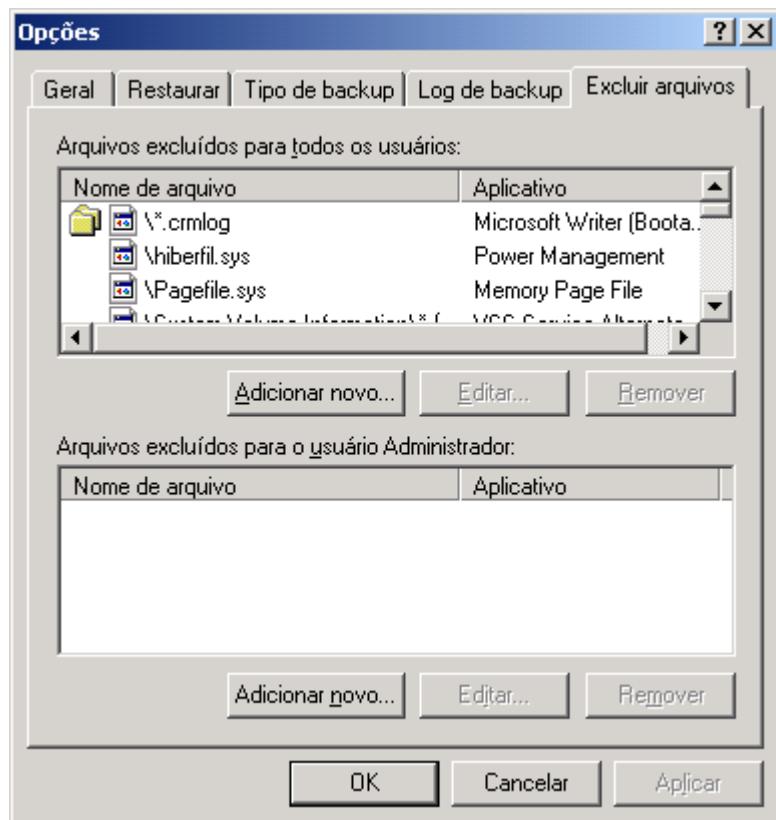
Figura 8.37 A guia Restaurar da janela de opções.

Nesta guia você pode definir um dos seguintes padrões, já descritos anteriormente:

- ◆ Não substituir o arquivo no computador (recomendável). Esta é a opção definida por padrão.
  - ◆ Substituir o arquivo no disco somente se ele for mais antigo.
  - ◆ Sempre substituir os arquivos no computador.
6. Dê um clique na guia Tipo de backup. Nesta guia está disponível uma lista para que você selecione o tipo padrão de Backup. O padrão está definido como Normal. Utilize a lista Tipo de backup padrão, para definir um novo padrão.
7. Dê um clique na guia Log de backup. Nesta guia você pode definir uma das seguintes opções para o log de backup.
  - ◆ **Detalhado:** Salva um registro detalhado das operações de backup e restauração que você executar. Este é o arquivo de log mais informativo que o backup pode criar.
  - ◆ **Resumido:** Salva um resumo das operações de backup e restauração que você executar. Esse é o arquivo de log menos informativo que o backup pode criar.
  - ◆ **Nenhum:** Especifica que você não deseja criar um arquivo de log das operações de backup e restauração.

Por padrão é selecionado o tipo Resumido.
8. Dê um clique na guia Excluir Arquivos. Será exibida a janela indicada na Figura 8.38.

Nesta guia você define quais arquivos não deverão fazer parte do backup, mesmo que o usuário opte por fazer o backup de todo o drive C. Existem duas listas de exclusão: Uma para todos os usuários logados no computador e uma que somente será aplicada para o usuário atual. Esta segunda lista é personalizada para cada usuário.



**Figura 8.38 A guia Excluir arquivos da janela opções.**

Observe que dentre os vários arquivos que estão na lista de arquivos que não farão parte do backup, está o arquivo Pagefile.sys, que é ao arquivo de troca (Swap) do Windows Server 2003. Falarei mais sobre este arquivo no Capítulo 12.

9. Selecione as opções desejadas e clique em OK para aplicá-las. Para os próximos backups estas serão as opções padrão.
10. Feche o utilitário de backup.

## Fazendo o Backup e o Restore do Active Directory..

A base de dados do Active Directory contém informações das quais depende todo o funcionamento da rede. Apenas para citar as mais conhecidas, é no Active Directory que ficam armazenadas informações sobre todas as contas de usuários do domínio, sobre todos os grupos, sobre relações de confiança, sobre contas de computadores, sobre OUs, enfim, informações das quais depende o funcionamento da rede.

É claro que o fato de existir vários DCs em um domínio, cada DC com uma cópia completa do Active Directory, reduz os riscos de perdas destas informações. Em caso de catástrofe, tal como a perda do HD onde está instalado o Windows Server 2003, sempre será possível reinstalar o Windows Server 2003 e, através da replicação, obter uma cópia integral do Active Directory a partir de outros DCs do domínio. O Backup é útil para agilizar este processo, uma vez que, dependendo do volume de dados do Active Directory, pode demorar algum tempo (até mesmo alguns dias), até que o DC consiga receber uma cópia completa do Active Directory, através da replicação de outros DCs do domínio.

Neste tópico você aprenderá sobre como realizar o Backup do Active Directory, sobre conceitos tais como Backup com e sem autoridade e como fazer o restore do Active Directory. O backup do Active Directory é feito com o utilitário de backup, discutido nos tópicos anteriores. O restore é feito com este mesmo utilitário em conjunto com o comando Ntdsutil, o qual pode ser utilizado para fazer um restore seletivo, apenas de partes específicas do Active Directory.

## **Backup do Active Directory:**

Com o utilitário de Backup do Windows Server 2003 você pode fazer o backup do Active Directory com o DC estando ligado e na rede e pode ser feito o backup somente do Active Directory ou do Active Directory juntamente com os dados do servidor. O backup pode ser feito em disco ou em qualquer mídia suportada pelo utilitário de backup do Windows Server 2003.

Um detalhe importante a ser observado é que quando é feito o backup do Active Directory, o único tipo de backup suportado é o backup normal. Ou seja, não podem ser utilizados os backups do tipo incremental, diferencial, cópia ou diário, quando é feito o backup do Active Directory. Para detalhes sobre cada tipo de backup e estratégias de backup/restore, consulte a parte inicial deste Capítulo. O backup normal faz uma cópia de todo o conteúdo do servidor. Na hora de fazer o restore basta ter disponível o último backup normal que foi efetuado.

Ao fazer o backup do Active Directory, o utilitário de backup do Windows Server 2003 também realiza o backup de todas as informações das quais depende o funcionamento do Active Directory, tais como registros de componentes e DLLs, registry do sistema e assim por diante. Este conjunto de informações é conhecido como estado do sistema. As informações que compõem o estado do sistema são as seguintes:

- ◆ Arquivos de inicialização
- ◆ Registros de componentes COM+
- ◆ Pasta SYSVOL
- ◆ Base de dados do Certificados Digitais (se instalado o Certificate Services)
- ◆ Base do DNS (se instalado)
- ◆ Informações de cluster (se o servidor participa de um cluster)
- ◆ Active Directory

## **Restore do Active Directory**

Existem duas abordagens diferentes que podem ser utilizadas para restaurar os dados do Active Directory, em caso de falhas que provoquem perda ou corrupção dos dados do Active Directory:

1. Reinstalar o Windows Server 2003, promovê-lo a DC e deixar que o mecanismo padrão de replicação entre DCs se encarregue de restaurar a base completa do Active Directory. Esta opção pode ser inviável para escritórios ligados à rede da empresa através de links de WAN de baixa velocidade, principalmente se a base de dados do Active Directory for grande (1 GB ou mais).

Ou

2. Fazer o restore a partir de um backup efetuado previamente. No caso do restore a partir do backup, existem dois métodos diferentes de restore que podem ser executados, conforme descrito a seguir:
  21. Nonauthoritative (Sem autoridade): Este é um restore normal. Os dados serão restaurados a partir do backup. Uma vez concluída a restauração, o DC passará a receber as atualizações dos outros DCs. Sempre que um outro DC contiver informações mais atualizadas do que as que foram restauradas do backup, estas informações serão replicadas para o DC onde foi feito o restore. É o processo padrão de restore.

---

**IMPORTANTE:** Lembre-se de que para fazer um Backup do Certificate Services você precisa fazer o Backup do Estado do Sistema.

**2.2. Authoritative (Com autoridade):** Esta é uma situação especial. Para ilustrar este tipo de restore, vou utilizar uma situação prática onde ele seria necessário. Imagine que, por engano, um administrador excluiu uma OU e todo o seu conteúdo. Esta informação (ou seja a informação de que a OU foi excluída) será replicada para os demais DCs do domínio. O efeito prático é que esta OU será excluída em todos os DCs do domínio. Você pode imaginar o seguinte: Basta restaurar a OU a partir do Backup e pronto, as informações da OU serão replicadas para os demais DCs e os dados serão recuperados. Nada disso. Ao restaurar a OU usando o método normal (Nonauthoritative), os dados da OU serão considerados mais antigos do que a informação de que não existe a OU. Quando houver a replicação entre o DC onde foi feito o restore da OU e qualquer outro DC do domínio, o que irá acontecer é que a OU será novamente excluída e não enviada para os outros DCs, pois a informação de que ela foi excluída, é mais recente do que os dados da OU. Com o uso de um restore Authoritative é possível recuperar esta informação. Nesta situação, o administrador utiliza o comando Ntdsutil para fazer um restore Authoritative (Com autoridade) da OU que foi excluída. Fazer um restore authoritative significa alterar o número de série dos dados que estão sendo restaurados, de tal maneira que eles sejam considerados as atualizações mais recentes. Com isso, quando houver a replicação entre o DC onde foi feito o restore e os demais DCs, os dados da OU serão considerados mais recentes e a OU e todo o seu conteúdo será replicada para os demais DCs. O efeito prático é que os dados da OU serão recuperados.

Quem tem permissão para fazer o backup do estado do sistema?

Para fazer o backup ou um restore do tipo nonauthoritative, o usuário deve ter as seguintes permissões e direitos de usuário:

- ◆ Para fazer o backup do estado do sistema, o usuário deve pertencer ao grupo Backup Operators (Oper. de cópia) ou ao grupo Local do domínio Administrators (Administradores).
- ◆ Para fazer o restore do estado do sistema, o usuário deve pertencer ao grupo Local do domínio Administrators (Administradores).

Bem, esta é a teoria sobre o Backup/Restore do Active Directory. A seguir descreverei as operações práticas de backup/restore do Active Directory.

## Fazendo o backup do Active Directory.

Neste item mostrarei como fazer o backup do Active Directory utilizando o utilitário de backup do Windows Server 2003. A base de dados do Active Directory é composta dos seguintes arquivos, localizados na pasta %windir%\ntds (a não ser que você tenha especificado um caminho diferente quando o servidor foi promovido a DC), onde %windir% refere-se a pasta onde o Windows Server 2003 está instalado:

- ◆ **Ntds.dit:** Este é o banco de dados do Active Directory.
- ◆ **Ebb.chk:** O arquivo de checkpoint, utilizado pelo mecanismo de banco de dados do Active Directory.
- ◆ **Ebb\*.log:** Arquivos onde são registrados os logs de transações do banco de dados do Active Directory. A cada 10 MB é iniciado um novo arquivo de log.
- ◆ **Res1.log e Res2.log:** Log de transações, reservado.

Fazer o backup do Active Directory, significa fazer o backup do Estado do Sistema, conforme descrito no exemplo prático logo a seguir.

Exercício: Para fazer o backup do estado do sistema (no qual está incluído o backup do Active Directory), siga os passos indicados a seguir:

1. Faça o logon no DC onde o backup será efetuado, com uma conta pertencente ao grupo Administrators (Administradores) ou ao grupo Backup Operators (Oper. de cópias).
2. Abra o utilitário de backup: Iniciar -> Todos os programas -> Acessórios -> Ferramentas do sistema -> Backup.
3. Será aberta a tela inicial do assistente de backup. A primeira tela é apenas informativa. Clique em Avançar, para seguir para a próxima etapa do assistente.
4. Na segunda etapa você deve informar se será feito um backup ou um restore. Marque a opção Fazer o backup dos arquivos e configurações e clique em Avançar, para seguir para a próxima etapa do assistente.
5. Nesta etapa você tem duas opções: Todas as informações neste computador ou Eu escolherei os itens para backup. Selecione a opção Eu escolherei os itens para backup e clique em Avançar, para seguir para a próxima etapa do assistente.
6. Nesta etapa você deve selecionar quais os itens serão incluídos no Backup. Clique no sinal de + ao lado de Meu computador, no painel da esquerda. Nas opções que são exibidas, marque a opção System State, conforme indicado na Figura 8.39:

**IMPORTANTE:** Você não pode fazer o backup do Estado do Sistema remotamente através da rede. Ou seja, para fazer o backup do Estado do Sistema de um servidor, por exemplo o servidor SRV01, você tem que estar logado localmente neste servidor ou o script que faz o backup tem que estar agendado para execução no servidor SRV01. Os dados do backup podem ser gravados em um volume do próprio servidor SRV01 ou em um drive de rede ou fita de backup, mas a tarefa que executa o backup tem que ser executada no próprio servidor.

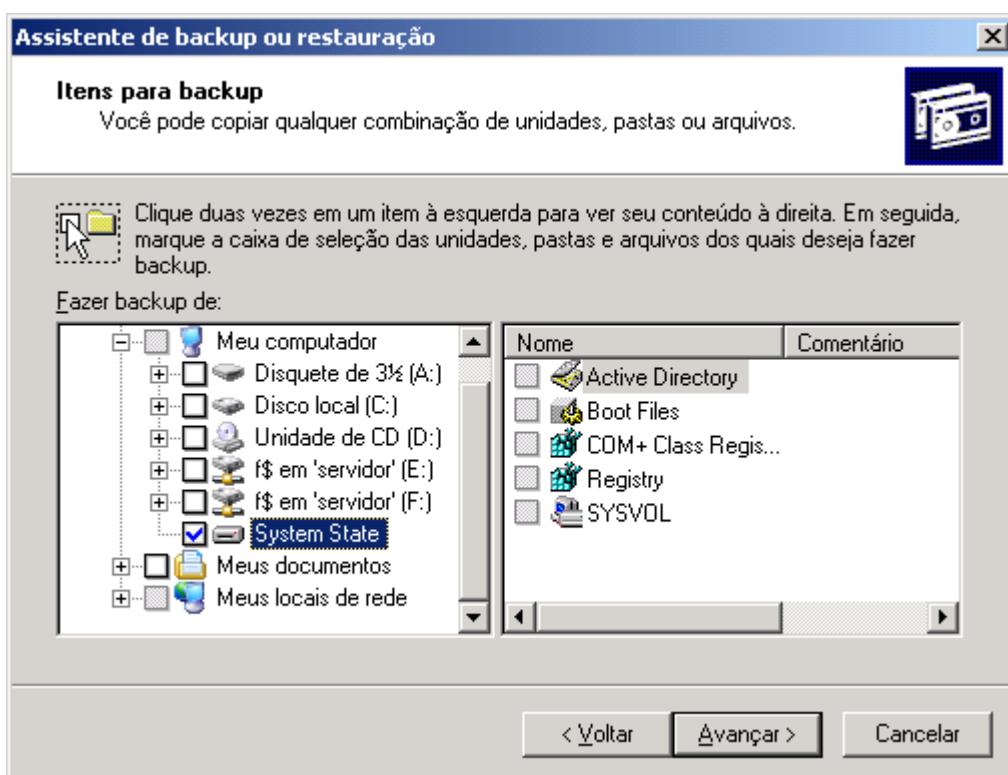


Figura 8.39 Fazendo o backup do estado do sistema.

7. Clique em Avançar, para seguir para a próxima etapa do assistente.

8. Nesta etapa você deve informar onde será feito o backup (em disco, em fita ou em outro meio disponível no servidor). Se for em disco você deve informar a pasta onde será feito o backup e o nome do arquivo de backup. Forneça as informações de acordo com a mídia de backup que você está utilizando e clique em Avançar, para seguir para a próxima etapa do assistente.
9. Será exibida a tela final do assistente. Nesta etapa você pode clicar no botão Avançado..., para que sejam exibidas opções para agendamento do backup. Ao definir o agendamento do backup será criada uma Tarefa agendada, a qual executa o backup de acordo com o agendamento criado pelo administrador. Clique no botão Avançado...
10. Será exibida uma tela para que você selecione o tipo de backup. Por padrão já vem selecionado o tipo Normal. Para o backup do Active Directory deve ser utilizado o tipo Normal. Vamos aceitar a sugestão do assistente. Clique em Avançar, para seguir para a próxima etapa do assistente.
11. Nesta etapa você tem a opção de definir se os dados devem ser verificados após o backup ou não. Se você habilitar a verificação, o processo de backup ficará mais demorado, pois após ter sido feita a cópia dos dados, estes serão verificados e comparados com os dados originais. Certifique-se de que a opção para habilitar a verificação dos dados após o backup esteja desmarcada e clique em Avançar, para seguir para a próxima etapa do assistente.
12. Nesta etapa você pode definir se o backup será anexado a um outro backup já existente ou se deve substituir os backups já existentes. Por exemplo, se você está fazendo o backup do Active Directory em disco, na pasta C:\backups\bad.bkf. Se você escolher a opção Acrescentar este backup aos backups existentes, será mantido cada backup do Active Directory e o novo backup será acrescentado ao anterior. Você ficará com um histórico das várias versões do Active Directory. Se você selecionar a opção Substituir os backups existentes, todos os backups anteriores serão excluídos e será mantido apenas o último backup. Esta é a opção normalmente utilizada para backup do estado do sistema, uma vez que o que interessa é apenas o estado atual, ou seja, o último backup. Selecione a opção Substituir os backups existentes e clique em Avançar, para seguir para a próxima etapa do assistente.

**NOTA:** Para maiores detalhes sobre mídias de backup, backup em fita e backup em disco, consulte a parte inicial deste capítulo.

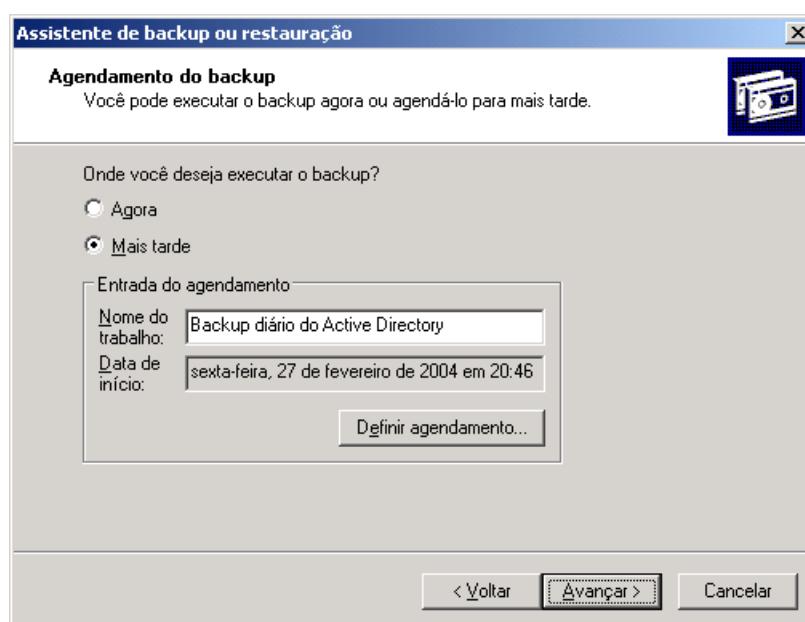
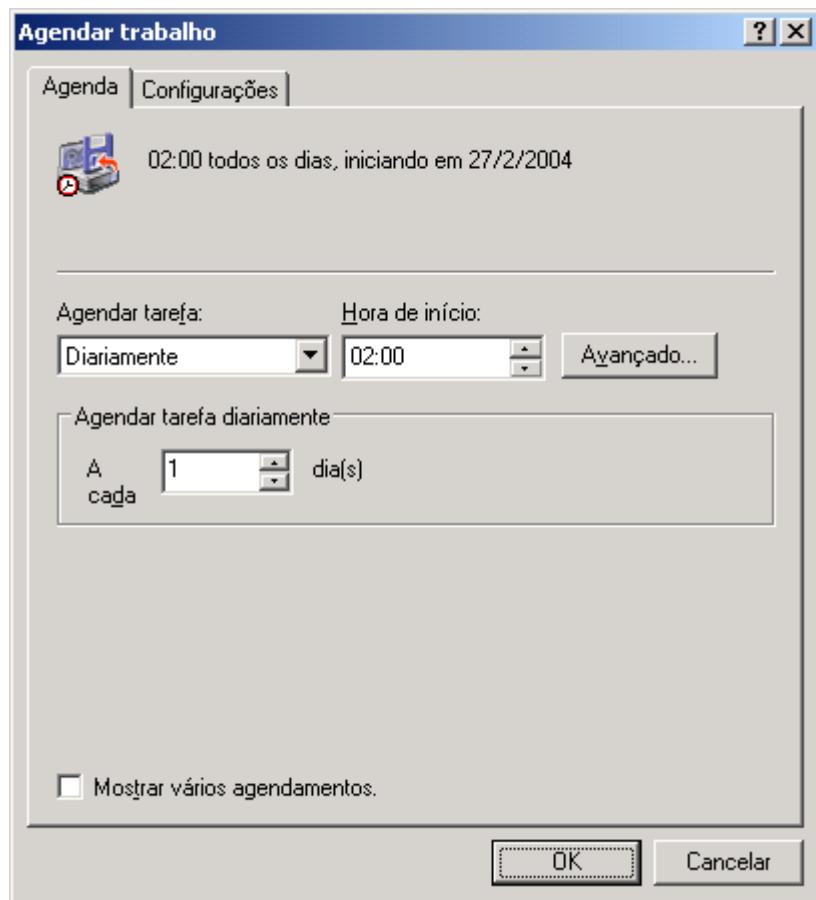


Figura 8.40 Informando que será criado um agendamento.

13. Nesta etapa você pode definir se deseja executar o backup imediatamente após a conclusão do assistente – Agora ou se deseja criar uma tarefa que executa o backup de acordo com um agendamento, como por exemplo, diariamente as 2:00 da manhã – Mais tarde. Marque a opção Mais tarde e digite um nome para a tarefa agendada que será criada, conforme exemplo da Figura 8.40.
14. Clique no Definir agendamento... Será aberta a janela Agendar trabalho, a qual você aprendeu utilizar no início deste Capítulo. Defina as opções indicadas na Figura 8.41, para definir um backup diário do Active Directory, as 2:00 da madrugada e clique em OK.



**Figura 8.41 Definindo um agendamento para o backup do Active Directory.**

15. Será exibida a janela solicitando informações sobre a conta com a qual deverá ser executada a tarefa agendada que irá fazer o backup. Informe uma conta com permissão de Administrador ou pertencente ao grupo Oper. de Cópia. A conta deve ser informada no formato DOMÍNIO\NomeDaConta. Informe a conta e a senha e clique em OK.
16. Clique em Avançar, para seguir para a próxima etapa do assistente. Se forem solicitadas novamente as informações da conta para execução da tarefa agendada, informe novamente e clique em OK.
17. Se você quiser fazer alguma alteração utilize o botão Voltar. Clique em Concluir, para encerrar o assistente e criar a tarefa agendada, a qual fará o backup do Active Directory.
18. Agora vamos verificar se a tarefa foi realmente criada.
19. Abra o Painel de controle e dê um clique duplo na opção Tarefas agendadas. A tarefa Backup diário do Active Directory já deve estar sendo exibida, conforme indicado na Figura 8.42:

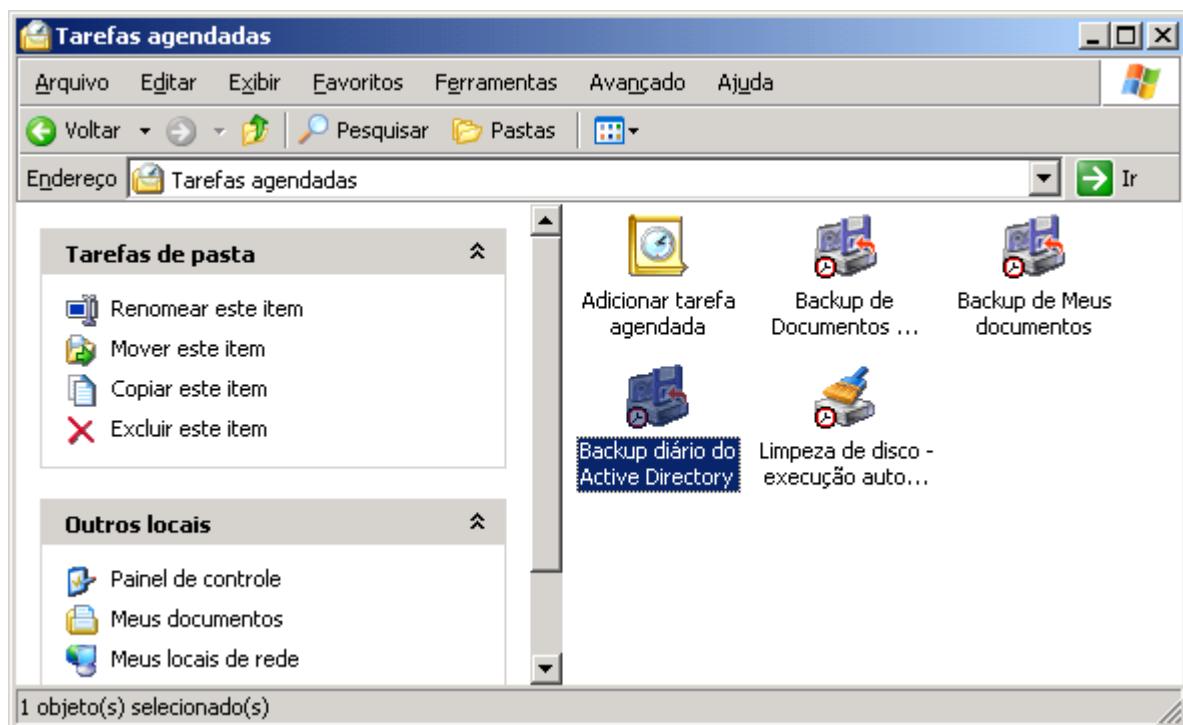


Figura 8.42 A tarefa “Backup diário do Active Directory”.

20. A partir de agora, será feito um backup diário do Active Directory, sempre às 2:00 da madrugada. Você pode iniciar um backup manualmente, a qualquer momento. Para isso basta clicar com o botão direito do mouse na tarefa Backup diário do Active Directory e, no menu de opções que é exibido, clicar em Executar. A tarefa será iniciada e o backup do estado do sistema (no qual está incluído o Active Directory) é inicializado.

Sobre backup do Active Directory é isso, ou seja, basicamente executar o assistente de backup (como você aprendeu no início do capítulo), apenas com o detalhe de marcar a opção System State. Para fazer o restore existem alguns detalhes adicionais que devem ser observados, conforme descreverei logo a seguir.

## Fazendo o restore do Active Directory.

Conforme descrito anteriormente existem dois métodos para fazer o restore do Active Directory. O primeiro é reinstalar o Windows Server 2003, usar o comando `dcpromo` para instalar o Active Directory e deixar que o processo de replicação entre os DCs do domínio se encarregue de sincronizar o novo DC com os demais DCs do domínio. Com este método o Active Directory é restaurado e sincronizado com as últimas alterações do domínio. Outro método é restaurar o Active Directory a partir de um backup. Este método restaura o Active Directory até a situação do momento em que foi feito o backup. Alterações que foram efetuadas após o backup, serão recebidas a partir dos outros DCs, através do processo de replicação. Observe que com este segundo método, somente serão replicadas as alterações que foram efetuadas após o backup.

Ao fazer o restore a partir do backup você também tem a disposição diferentes métodos. Um dos métodos é conhecido como nonauthoritative (sem autoridade). Este é o método que será utilizado normalmente. O restore é feito a partir de um backup feito previamente. O restore é feito utilizando o utilitário de backup do Windows Server 2003. Por exemplo, imagine que houve um problema com o disco rígido onde estava instalado o Windows Server 2003, em um DC do domínio. Neste caso você pode substituir o HD, reinstalar o Windows Server 2003 e depois restaurar o backup do estado do sistema. Com isso o Active Directory também será restaurado. As alterações que foram efetuadas após o backup, serão repassadas para o DC através do mecanismo de replicação. Observe que este método tem a vantagem de

reduzir a quantidade de tráfego gerado na WAN, em relação ao método que restaura toda a base de dados usando replicação. Neste método, grande parte da base de dados do Active Directory é restaurada a partir do backup. Somente as alterações efetuadas após o backup ter sido feito é que serão replicadas.

Conforme descrito anteriormente, outro método de fazer o restore é o restore authoritative (com autoridade), na qual você marca uma parte do Active Directory para ser restaurada com autoridade, o que significa que esta informação será considerada como sendo a mais atualizada e será replicada para os demais DCs. Para fazer um backup authoritative, o administrador tem de utilizar o comando Ntdsutil.

## Efetuando um restore nonauthoritative, usando o utilitário de backup.

Neste item mostrarei como fazer um restore do Active Directory usando o utilitário de backup. Será feito um restore nonauthoritative, usando o backup criado no item anterior. Para fazer o restore do Active Directory, você precisa reinicializar o DC em um modo especial, conhecido como Directory Services Restore Mode. Ou seja, o restore não é feito no modo normal, com o DC inicializado normalmente. É preciso reinicializar o servidor e entrar no modo especial Directory Services Restore Mode.

Para colocar o servidor no modo especial Directory Services Restore Mode, siga os passos indicados a seguir:

1. Reinicie o DC.
2. Ao ser reinicializado, ainda no modo caractere, logo após terminar a contagem da memória RAM do servidor, pressione repetidamente a tecla de Função F8, até que seja exibido o menu de inicialização avançado (sobre o qual falarei no Capítulo 12).
3. Neste menu selecione a opção Directory Services Restore Mode (Domain controllers only) e pressione Enter.
4. O DC será reinicializado no modo de restauração do Active Directory. Neste modo o Active Directory não é inicializado e, portanto, você não poderá usar as contas do Active Directory para fazer o logon. Mas se não posso usar as contas do Active Directory para fazer o logon, que contas vou utilizar? A conta local de administrador que foi definida quando o servidor ainda era um Member server. Use esta conta e a respectiva senha para fazer o logon.
5. Pronto, o DC está no modo de restauração do Active Directory. Agora é só seguir os passos do próximo exemplo.

Exemplo: Para fazer um restore nonauthoritative, usando o utilitário de backup, siga os passos indicados a seguir:

1. Faça o logon no DC onde o restore será efetuado, com uma conta pertencente ao grupo Administrators (Administradores).
2. Abra o utilitário de backup: Iniciar -> Todos os programas -> Acessórios -> Ferramentas do sistema -> Backup.
3. Será aberta a tela inicial do assistente de backup. A primeira tela é apenas informativa. Clique em Avançar, para seguir para a próxima etapa do assistente.
4. Nesta etapa você deve definir se será feito um Backup ou um Restore. Marque a segunda opção Restaurar arquivos e configurações e clique em Avançar, para seguir para a próxima etapa do assistente.
5. Nesta etapa será exibida a lista de backups disponíveis. Dê um clique duplo no backup do Active Directory, feito anteriormente. Abaixo do nome do backup marque a opção System State, conforme indicado na Figura 8.43.
6. Clique em Avançar, para seguir para a próxima etapa do assistente.
7. Será exibida a tela final do assistente. Clique em Concluir para iniciar o processo de restore. Uma vez concluído o processo feche o utilitário de backup e reinicie o DC no modo Normal.
8. O Active Directory terá sido restaurado até o estado de quando foi feito o backup e o processo de replicação se encarregará de atualizar o DC com as mudanças que foram feitas entre o momento do backup e o momento do restore.

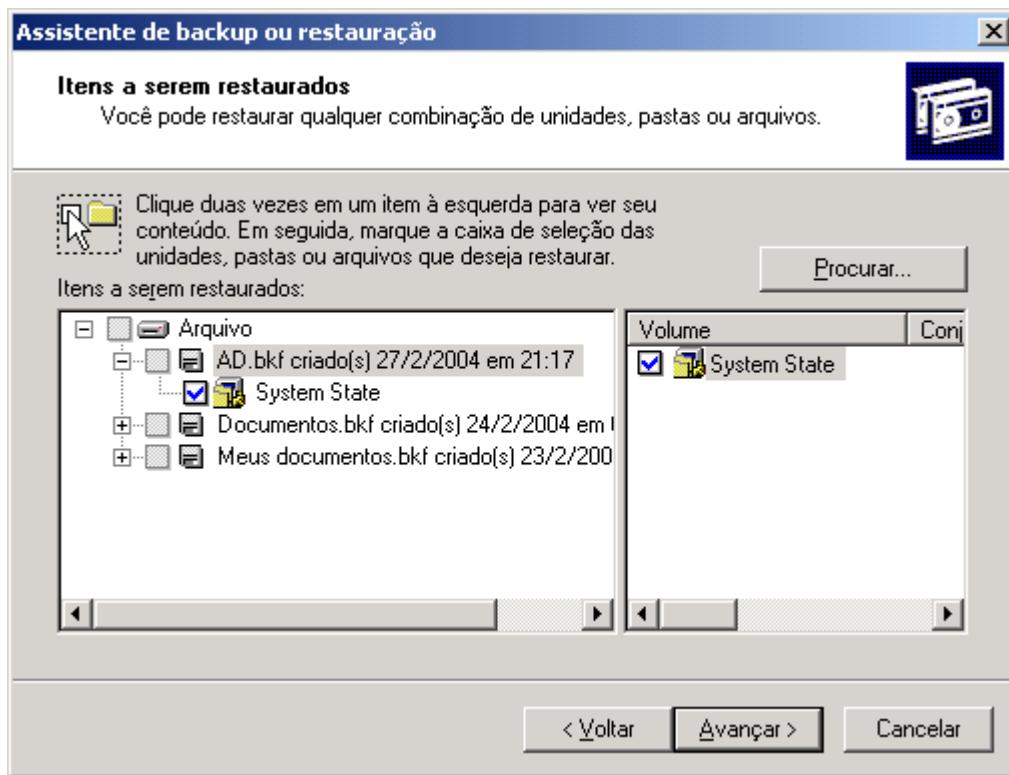


Figura 8.43 Fazendo o restore do System State.

### Efetuando um authoritative restore.

Você pode fazer um authoritative restore para todo o Active Directory ou apenas para partes específicas, tais como um ou mais OUs. Para ilustrar este tipo de restore, vou utilizar uma situação prática onde ele seria necessário. Imagine que, por engano, um administrador excluiu uma OU e todo o seu conteúdo. Esta informação (ou seja a informação de que a OU foi excluída) será replicada para os demais DCs do domínio. O efeito prático é que esta OU será excluída em todos os DCs do domínio. Você pode imaginar o seguinte: Basta restaurar a OU a partir do Backup e pronto (restore do tipo nonauthoritative), as informações da OU serão replicadas para os demais DCs e os dados serão recuperados. Nada disso. Ao restaurar a OU usando o método normal (nonauthoritative), os dados da OU serão considerados mais antigos do que a informação de que não existe a OU. Quando houver a replicação entre o DC onde foi feito o restore da OU e qualquer outro DC do domínio, o que irá acontecer é que a OU será novamente excluída e não enviada para os outros DCs, pois a informação de que ela foi excluída, é mais recente do que os dados da OU. Com o uso de um restore authoritative é possível recuperar esta informação. Nesta situação, o administrador utiliza o comando Ntdsutil para fazer um restore authoritative (com autoridade) da OU que foi excluída. Fazer um restore authoritative significa alterar o número de série dos dados que estão sendo restaurados, de tal maneira que eles sejam considerados as atualizações mais recentes. Com isso, quando houver a replicação entre o DC onde foi feito o restore e os demais DCs, os dados da OU que está sendo restaurada serão considerados mais recentes e a OU e todo o seu conteúdo será replicada para os demais DCs. O efeito prático é que os dados da OU serão recuperados.

**NOTA:** Por padrão os dados do estado do sistema são restaurados para a pasta systemroot, ou seja, a pasta onde está instalado o Windows Server 2003. Com isso os dados do backup irão substituir os dados atualmente no disco. Você pode fazer com que alguns dados do estado do sistema sejam restaurados para um pasta diferente. Para isso clique no botão Avançado..., na etapa final do assistente e, na janela que é exibida, especifique o novo local para fazer o restore. Os dados que são copiados para a nova localização são os seguintes: arquivos de inicialização, os arquivos que compõem a Registry do sistema, a pasta SYSVOL e todo o seu conteúdo e informações de cluster (se for o caso). Já as informações do Active Directory, do registro dos componentes COM+ e do Certificate Services (se este estiver instalado) não serão restaurados para o local alternativo.

O processo é bastante simples. Inicialmente você faz um restore nonauthoritative usando o utilitário de backup, estando o DC no modo Directory Services Restore Mode, conforme descrito no item anterior. Em seguida, antes de reiniciar o DC, você utiliza o comando ntdsutil para marcar objetos do Active Directory (como por exemplo uma OU) como sendo authoritative, ou seja, devem ser replicados para os demais DCs, atualizando outras cópias destes objetos que existam nos demais DCs do domínio. O que o comando Ntdsutil faz para tornar um determinado objeto authoritative é atribuir a este objeto um número de série bem elevado, muito acima da faixa normal utilizada para número de série dos objetos. Com isso o objeto marcado como authoritative será considerado mais atualizado que a cópia que está nos demais DCs e a cópia restaurada como authoritative será replicada para todos os demais DCs do domínio.

Exemplo: Efetuar um restore authoritative para uma OU chamada teste. Para fazer este restore dois passos devem ser executados. Primeiro será feito o restore normal do Active Directory, usando o utilitário de backup. Em seguida utilizaremos o comando ntdsutil para marcar a ou teste como authoritative.

Para fazer o restore proposto pelo exemplo siga os passos indicados a seguir:

Etapa 1: Fazer o restore nonauthoritative usando o utilitário de backup. Para isso, siga os passos indicados a seguir:

1. Reinicie o DC.
2. Ao ser reiniciado, ainda no modo caractere, logo após terminar a contagem da memória RAM do servidor, pressione repetidamente a tecla de Função F8, até que seja exibido o menu de inicialização avançado (sobre o qual falarei no Capítulo 12).
3. Neste menu selecione a opção Directory Services Restore Mode (Domain controllers only) e pressione Enter.
4. O DC será reiniciado no modo de restauração do Active Directory. Neste modo o Active Directory não é inicializado e, portanto, você não poderá usar as contas do Active Directory para fazer o logon. Mas se não posso usar as contas do Active Directory para fazer o logon, que contas vou utilizar? A conta local de administrador que foi definida quando o servidor ainda era um Member server. Use esta conta e a respectiva senha para fazer o logon.
5. Pronto, o DC foi inicializado no modo de restauração do Active Directory.
6. Faça o logon no DC onde o restore será efetuado, com uma conta local do administrador.
7. Abra o utilitário de backup: Iniciar -> Todos os programas -> Acessórios -> Ferramentas do sistema -> Backup.
8. Será aberta a tela inicial do assistente de backup. A primeira tela é apenas informativa. Clique em Avançar, para seguir para a próxima etapa do assistente.
9. Nesta etapa você deve definir se será feito um Backup ou um Restore. Marque a segunda opção Restaurar arquivos e configurações e clique em Avançar, para seguir para a próxima etapa do assistente.
10. Nesta etapa será exibida a lista de backups disponíveis. Dê um clique duplo no backup do Active Directory, feito anteriormente. Abaixo do nome do backup marque a opção System State.
11. Clique em Avançar, para seguir para a próxima etapa do assistente.
12. Será exibida a tela final do assistente. Clique em Concluir para iniciar o processo de restore. Uma vez concluído o processo feche o utilitário de backup. A próxima etapa é utilizar o utilitário Ntdsutil para marcar a OU teste para ser um restore do tipo authoritative.

Etapa 2: utilizar o utilitário Ntdsutil para marcar a OU teste para ser um restore do tipo authoritative e reiniciar o DC:

1. Após ter feito o restore nonauthoritative descrito na Etapa 1, desconecte o cabo de rede do DC e reinicie-o no modo Directory Services Restore Mode novamente.
2. Faça o logon com a conta de administrador local.
3. Abra um Prompt de comando.

4. Digite ntdsutil e pressione Enter.
5. Será exibido o prompt do comando ntdsutil.
6. digite authoritative restore e pressione Enter.
- 6.1. Para fazer um restore authoritative de todo o Active Directory, digite o seguinte comando: Restore database e pressione Enter.
- 6.2. Para restaurar apenas parte do Active Directory, utilize o comando Restore subtree <nome LDAP da parte a ser restaurada>. Por exemplo, para restaurar authoritatively a OU teste, do domínio abc.com, digite o seguinte comando:  
**Restore Subtree OU=teste,DC=abc,DC=com**

Ao executar este comando o utilitário ntdsutil acessa os dados do arquivo ntds.dit e aumenta o número de versão dos objetos que estão sendo restaurados de maneira authoritative, no nosso exemplo a OU teste e todos os objetos que estiverem nesta OU..

7. Para sair do utilitário ntdsutil digite quit e pressione Enter.
8. Agora é só reiniciar o DC no modo normal e conectá-la a rede.

Ao ser reiniciado o DC passa a receber as atualizações dos demais DCs da rede, atualizações que foram feitas entre o momento do backup e o momento do restore. As porções que foram marcadas como authoritative, usando o comando ntdsutil serão replicadas para os demais DCs do domínio.

## Os comandos Ldifde e Dsadd.

Neste item falarei sobre mais dois comandos que são utilizados para administração do Active Directory. São eles:

- ◆ **Comando Ldifde:** É utilizado para criar, modificar e excluir objetos no Active Directory. Este comando também pode ser utilizado para fazer alterações no schema, exportar informações sobre usuários e grupos do Active Directory para outras aplicações ou serviços e para criar objetos no Active Directory, com base em dados de outros serviços de diretório.

Por exemplo, você pode exportar informações completas sobre o domínio, usando o seguinte comando:

```
ldifde -f teste.txt
```

Este comando irá exportar informações do Active Directory para um arquivo de texto chamado teste.txt. A seguir mostro um trecho deste arquivo onde são exibidas informações sobre os usuários user01 e user02:

```
*****
```

```
dn: CN=Usuário 01,CN=Users,DC=abc,DC=com
changetype: add
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: user
cn:: VXN1w6FyaW8gMDE=
sn: 01
c: BR
l:: Qm9xdWVpcsojbyBkbyBMZcOjbw==
st: RS
postalCode: 11111-111
postOfficeBox: 202
givenName:: VXN1w6FyaW8=
distinguishedName:: Q049VXN1w6FyaW8gMDEsQ049VXN1cnMsREM9YWJjLERDPWNvbQ==
instanceType: 4
```

```
whenCreated: 20030521203529.0Z
whenChanged: 20030622220300.0Z
displayName:: VXN1w6FyaW8gMDE=
uSNCreated: 28821
memberOf: CN=Empresa,CN=Users,DC=abc,DC=com
memberOf: CN=Remote Desktop Users,CN=Builtin,DC=abc,DC=com
uSNChanged: 192555
co: Brazil
name:: VXN1w6FyaW8gMDE=
objectGUID:: EBaU6VS8pEC7TC+AX71sRA==
userAccountControl: 512
badPwdCount: 0
codePage: 0
countryCode: 76
badPasswordTime: 127007929242509392
lastLogoff: 0
lastLogon: 127007929904160800
pwdLastSet: 127007929802114064
primaryGroupID: 513
objectSid:: AQUAAAAAAAUVAAAos6r3/QHf9F2488HWAQAAA==
accountExpires: 9223372036854775807
logonCount: 12
sAMAccountName: user01
sAMAccountType: 805306368
userPrincipalName: user01@abc.com
objectCategory: CN=Person,CN=Schema,CN=Configuration,DC=abc,DC=com
lastLogonTimestamp: 127007929166900672

dn: CN=Usuário 02,CN=Users,DC=abc,DC=com
changetype: add
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: user
cn:: VXN1w6FyaW8gMDI=
sn: 02
c: BR
l:: Qm9xdWVpcosObjyBkbyBMZcOjbw==
st: RS
postalCode: 11111-111
postOfficeBox: 202
givenName:: VXN1w6FyaW8=
distinguishedName:: Q049VXN1w6FyaW8gMDIsQ049VXN1cnMsREM9YWJjLERDPWNvbQ==
instanceType: 4
whenCreated: 20030521203549.0Z
whenChanged: 20030527171532.0Z
displayName:: VXN1w6FyaW8gMDI=
uSNCreated: 28828
memberOf: CN=Empresa,CN=Users,DC=abc,DC=com
memberOf: CN=Diretoria,CN=Users,DC=abc,DC=com
memberOf: CN=Remote Desktop Users,CN=Builtin,DC=abc,DC=com
uSNChanged: 69655
co: Brazil
name:: VXN1w6FyaW8gMDI=
objectGUID:: QkTGRkqTJ0q0G2f39TBrqQ==
userAccountControl: 512
badPwdCount: 2
codePage: 0
countryCode: 76
badPasswordTime: 127010648937117488
lastLogoff: 0
lastLogon: 126989930258144832
pwdLastSet: 126980229491607312
primaryGroupID: 513
```

```
objectSid:: AQUAAAAAAAUVAAAAos6r3/QHf9F2488HWQQAAA==  
accountExpires: 9223372036854775807  
logonCount: 6  
sAMAccountName: user02  
sAMAccountType: 805306368  
userPrincipalName: user02@abc.com  
objectCategory: CN=Person,CN=Schema,CN=Configuration,DC=abc,DC=com
```

\*\*\*\*\*

Observe que inclusive o SID dos usuários é exportado, conforme indicado no trecho a seguir, onde é exibido o SID do usuário user01:

```
dn: CN=Usuário 01,CN=Users,DC=abc,DC=com  
objectSid:: AQUAAAAAAAUVAAAAos6r3/QHf9F2488HWAQAAA==
```

Para ver a lista completa de opções do comando ldifde sem nenhum parâmetro. É só digitar ldifde e pressionar Enter.

- ◆ **O comando Dsadd:** Este comando é utilizado para adicionar usuários, grupos, computadores, contatos e OUs no Active Directory.

Por exemplo, o comando a seguir é utilizado para adicionar o usuário jsilva5, ao domínio abc.com, com o primeiro nome (-fn) Jose, o nome do meio (-mi) da e o último nome (-ln) silva, sendo a senha (-pwd) definida como senha;;123

```
dsadd user CN=jsilva5,DC=abc,DC=com -fn Jose -mi da -ln Silva -pwd senha;;123
```

Ao executar este comando você receberá a mensagem indicada a seguir.

```
dsadd succeeded:CN=jsilva5,DC=abc,DC=com
```

Para exibir todas as opções do comando dsadd user, basta digitar o seguinte comando:

```
dsadd user /?
```

e pressionar Enter.

Outras variações do comando dsadd são as seguintes:

|                |    |  |
|----------------|----|--|
| dsadd computer | -> | Para adicionar uma conta de computador |
| dsadd group    | -> | Para criar um novo grupo               |
| dsadd ou       | -> | Para criar uma nova OU                 |

## Conclusão

Neste capítulo tratamos de tarefas importantes para o administrador, tarefas que fazem parte do seu trabalho diário.

Iniciei o capítulo falando sobre o Agendamento de tarefas. Através do agendamento de tarefas o administrador pode configurar ações que serão executadas em horários e dias específicos, de acordo com a programação da tarefa. Você também aprendeu a executar uma tarefa manualmente e a consultar o log da tarefa para acompanhar o seu histórico de execução.

Na segunda parte do capítulo tratou sobre o backup e o restore de informações.

Fazer o “Backup”, significa fazer uma ou mais cópias de segurança dos arquivos e pasta dos volumes do servidor e da instalação do Windows Server 2003 (assunto que veremos no Capítulo 12). Muitos usuários e até mesmo pequenas

empresas simplesmente ignoram a necessidade de implementar uma política de Backup. Muitas vezes os usuários só se dão conta do problema quando é tarde demais, ou seja, quando houve uma perda de dados importantes. É o usuário que perdeu os documentos do Word e figuras da sua tese de mestrado, é a vídeo locadora que perdeu os dados de anos de locações, é o Dentista que perdeu as informações sobre as fichas dos pacientes, sobre quais pacientes deviam e assim por diante. Em resumo: grandes dores de cabeça e prejuízos. Fazer cópia de segurança é uma necessidade real, não tem como fugir deste fato. Além disso o custo é insignificante, isto mesmo: insignificante se compararmos com os prejuízos que podem ser causados pela perda de dados.

Você aprendeu sobre os tipos de backup e sobre estratégias de backup/restore. Foi salientada a importância de se implementar uma política de backup como forma de proteger os dados.

Na seqüência mostrei como fazer o backup e o restore das informações utilizando os assistentes disponíveis e também o utilitário de backup.

Na parte final do Capítulo você aprendeu sobre o Backup do estado do sistema – System State, do qual faz parte do Active Directory. Você também aprendeu sobre o restore do Active directory e sobre os diferentes tipos de Restore.

---

**IMPORTANTE:** Para o exame 70-290 é de fundamental importância que você conheça, bem, os diferentes tipos de backup, quais as características de cada um e as diferentes estratégias de backup/restore que podem ser utilizadas, com base nos diferentes tipos de backups.

---

# Introdução

Este é um capítulo que eu chamo do tipo “Salada de Fruta”. Me explico melhor. Neste capítulo, abordarei uma série de assuntos, relevantes para o Exame 70-290, ou seja, assuntos que fazem parte do programa oficial do exame, mas que não estão diretamente relacionados. Usarei uma abordagem de descrever os tópicos de cada assunto, especificamente relacionados com o Exame 70-290.

Nesta capítulo tratarei dos seguintes assuntos:

- ◆ O uso do Terminal Services
- ◆ O Recurso de Desktop Remoto
- ◆ O Recurso de Shadow Copies
- ◆ Noções Básicas sobre GPO – Group Policy Objects
- ◆ Gerenciamento de Hardware e de Drives
- ◆ Resolução de Problemas de Hardware e Drives.

Vou iniciar o capítulo tratando sobre o Terminal Services. Você aprenderá sobre a utilização deste recurso, os diferentes modos no qual ele pode ser utilizado – Modo de Administração ou Modo de Compartilhamento de Aplicações, aprenderá a instalar e a configurar o Terminal Services e mais algumas questões relevantes para o Exame 70-290, tais como a quais grupos um usuário deve pertencer para poder fazer logon no Terminal Services e outras configurações relacionadas a permissão de acesso ao Terminal Services.

Em seguida vou apresentar o recurso de Área de Trabalho Remota (Remote Desktop). A Área de trabalho remota para administração (conhecida anteriormente como Serviços de terminal no modo de Administração remota) fornece acesso remoto à área de trabalho de qualquer computador que esteja executando um sistema operacional da família Microsoft Windows Server 2003, permitindo administrar o servidor a partir de virtualmente qualquer computador na rede.

Também falarei sobre o recurso de Assistência Remota, , recurso este que é uma novidade introduzida com o Windows XP e que está também presente no Windows Server 2003. A assistência remota permite que uma pessoa de confiança (um amigo, uma pessoa do suporte ou um administrador do setor de informática) auxilie de forma remota e ativa uma outra pessoa com problema no computador. O assistente (também chamado de especialista) poderá ver a tela do usuário que está solicitando assistência e dar algum conselho. Com a permissão do usuário, o assistente poderá inclusive assumir o controle do computador do usuário e executar tarefas remotamente.

A assistência remota normalmente inicia com uma solicitação de ajuda do usuário, através de email, do Windows Messenger ou de um convite salvo como um arquivo. Entretanto, um assistente também poderá oferecer ajuda sem que tenha recebido primeiro uma solicitação de um usuário. A assistência remota exige que os dois computadores estejam executando o Windows XP ou um produto da família Windows Server 2003.

# CAPÍTULO

## 9

### Manutenção do Windows 2003 Server e Gerenciamento de Hardware

Em seguida, vamos falar sobre um dos novos recursos do Windows Server 2003 – Shadow Copies (maravilhosamente traduzidas como Cópias de Sombras). Você verá o que este recurso, qual a sua utilização e quais as configurações necessárias (nos servidores e nos clientes), para que este recurso possa ser utilizado.

Mais um tópico importante será o assunto de GPO – Group Policy Objects. Você aprenderá o que é exatamente uma GPO, como e quando utilizá-la e como as GPOs são aplicadas a um domínio, Unidade Organizacional ou Site. Neste tópico não farei um estudo completo sobre GPOs, abordarei apenas os tópicos cobrados no Exame 70-290. Para um estudo completo sobre GPOs, com mais de 100 páginas de conteúdo, consulte o Capítulo 18 do meu livro: Windows Server 2003 – Curso Completo, 1568 páginas.

Para finalizar a nossa “Salada de Frutas”, falarei sobre a instalação, configuração, administração resolução de problemas relacionados com Hardware. Você aprenderá a utilizar as ferramentas de gerenciamento de hardware do Windows Server 2003 e a resolver problemas com dispositivos que não estão funcionando corretamente. Também falarei sobre o conceito de Assinatura de Drivers.

Então vamos lá, a nossa “saudável” Salada de Fruta. Embora seja um capítulo de tópicos diversos, é um capítulo muito importante para o Exame 70-290, pois aborda tópicos que muito provavelmente estarão no exame.

## **Uma Introdução ao Terminal Services.**

No Capítulo 2, quando fiz um retrospecto desde a época em que havia apenas o Mainframe, depois passamos pelo Cliente Servidor e agora modelo Web e Internet, fiz o seguinte comentário:

“O Júlio ficou louco ou estamos voltando ao Mainframe?

Amigo leitor, nem uma, nem outra. Você deve estar utilizando os seguintes passos de raciocínio, baseado no texto que acabou de ler (texto do Capítulo 2):

1. Na época do Mainframe os aplicativos e os dados ficavam no Mainframe. O acesso era feito através de terminais, conhecidos como terminais burros. A administração era feita centralizadamente, o que facilitava a atualização e manutenção das aplicações.
2. No modelo Cliente/Servidor clássico a aplicação e a lógica ficava no programa instalado na estação de trabalho cliente e os dados no servidor de banco de dados. Isso gera dificuldades para atualização das aplicações e um elevado custo para manter este modelo funcionando.
3. A nova tendência é portar as aplicações para um modelo de n camadas, onde as aplicações, a lógica e os dados ficam em servidores (de aplicações, Web e de banco de dados) e o acesso é feito através de um Navegador.
4. Puxa, mas o modelo em n camadas é praticamente o mesmo modelo do Mainframe, com aplicações e dados no servidor, administração centralizada e redução no custo de propriedade (TCO) em relação ao modelo Cliente/Servidor tradicional? É isso mesmo, este modelo é muito próximo do modelo do Mainframe, porém com todas as vantagens da evolução da informática nestas últimas décadas, tais como interfaces gráficas, programas mais poderosos e por aí vai.

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 da época do Mainframe.

Posso citar o exemplo de um dos bancos com os quais trabalho. Quando vou ao banco renovar um seguro ou tratar algum assunto diretamente com o gerente, vejo que ele tem na sua estação de trabalho, aplicativos de produção do dia-a-dia, tais como o Microsoft Word, Microsoft Excel, um aplicativo de cálculos e análise de crédito e assim por diante. Este mesmo gerente utiliza o site da empresa para fornecer informações. Ele também utiliza a Internet da empresa para se manter atualizado. Além disso ele utiliza alguns sistemas que ainda residem no bom e velho mainframe. Por exemplo, quando eu peço que ele faça uma alteração no meu endereço de correspondência, ela acessa a famosa telinha verde, de um programa emulador de terminal, que acessa uma aplicação que está no Mainframe da empresa.

Este caminho me parece muito mais sensato, ou seja, não precisa ser um ou outro modelo, mas sim o melhor dos dois mundos.”

Este trecho do Capítulo 2 reflete, perfeitamente, a idéia do Terminal Services. Ele foi criado para ser uma ferramenta que facilite a administração dos servidores com o Windows 2000 Server e também com o Windows Server 2003, mas também para ser uma ferramenta de compartilhamento de aplicações, conforme descreverei neste capítulo.

A primeira versão do que hoje é a tecnologia do Terminal Services foi introduzida com o Windows NT Server 4.0, em uma versão separada do NT 4.0, conhecida como: Terminal Server Edition. A partir do Windows 2000 Server e também no Windows Server 2003, o Terminal Services (a partir do Windows 2000 os serviços deixaram de ter a nomenclatura Server para ter a nomenclatura Services) faz parte do próprio sistema operacional.

O Terminal Services trabalha em um modelo Cliente/Servidor, onde o serviço fica instalado em servidores com o Windows Server 2003 ou Windows 2000 Services e diferentes clientes podem se conectar ao servidor. Existe também uma versão reduzida do Terminal Services que é disponibilizada com o Windows XP. Esta versão permite apenas um único usuário conectado ao Windows XP, no recurso conhecido como Desktop Remoto.

## Como funciona o Terminal Services.

A idéia básica do Terminal Services é bastante simples. Usando um software cliente, como por exemplo o Terminal Services Client no Windows 2000 Server ou o Remote Desktop no Windows Server 2003, você pode se conectar a um servidor no qual está rodando o Terminal Services. A se conectar ao servidor, você recebe uma tela de logon, conforme exemplo da Figura 9.1, onde estou fazendo a conexão usando o cliente Remote Desktop em um computador com o Windows Server 2003, para me conectar a um servidor com o Windows 2000 Server, onde está instalado o Terminal Services.

O usuário fornece as informações de logon e clica em OK e pronto. A conexão com o Terminal Services é efetuada e o console (a área de trabalho) do servidor é carregada no computador do cliente, conforme indicado na Figura 9.2. Ou seja, é como se você estivesse localmente conectado e tivesse feito o logon diretamente no servidor de destino, onde Terminal Services está instalado. Na prática é muito parecido com o que acontece quando você usa o comando telnet para fazer uma conexão com um servidor UNIX ou Linux, só que com o Terminal Services o console é gráfico.

Uma vez feita a conexão, é como se você tivesse localmente logado no servidor remoto. Exatamente a mesma área de trabalho é carregada, com botão Iniciar, barra de tarefas e tudo mais. Observe que com o Terminal Services o administrador pode se conectar a qualquer servidor da rede (desde que o servidor tenha o Terminal Services instalado) e administrá-lo como se estivesse localmente logado. Por exemplo, o administrador, da matriz da empresa em São Paulo, pode se conectar, via Terminal Services, com um servidor da filial no Rio de Janeiro e trabalhar como se estivesse “sentado” na frente do servidor no Rio de Janeiro.

---

**NOTA:** Para detalhes sobre a configuração e utilização do Desktop Remoto no Windows XP, consulte o Capítulo 17 do livro: “Windows XP Home & Professional Para Usuários e Administradores”, 820 páginas, Axel Books.

---

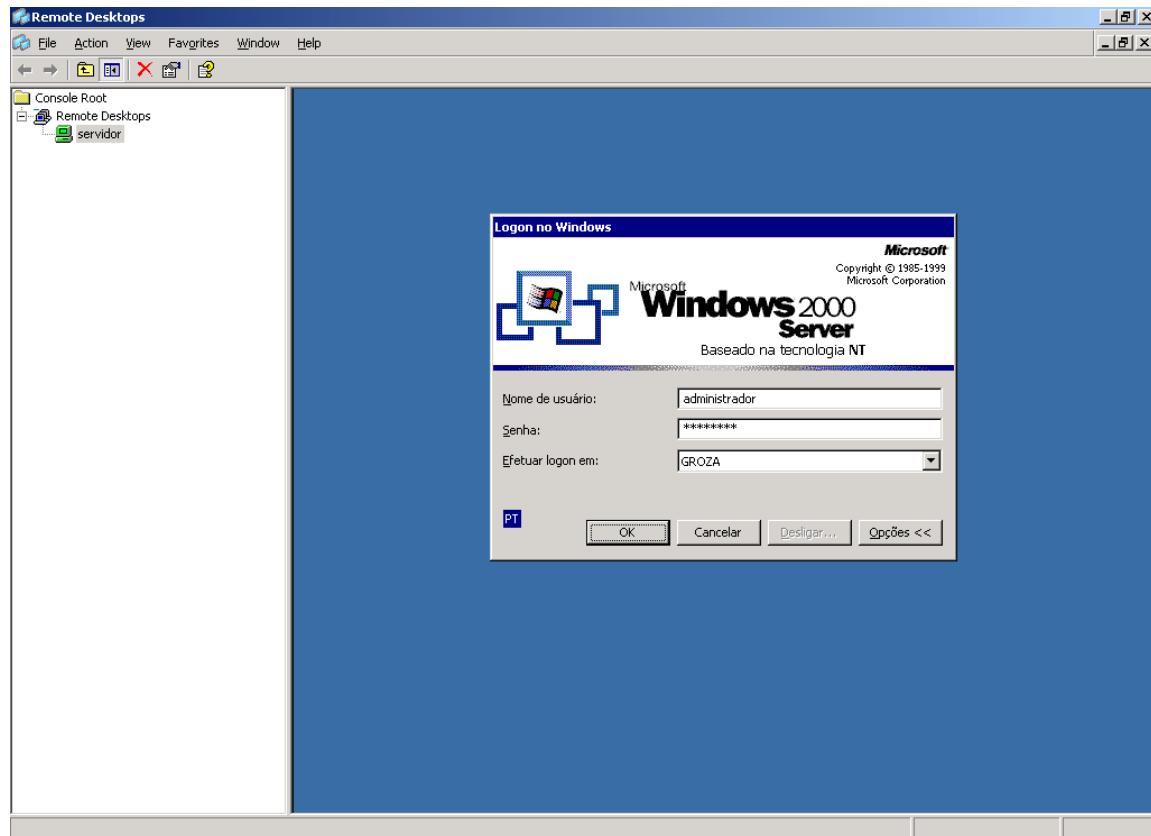


Figura 9.1 A tela de logon ao se conectar com o Terminal Services.

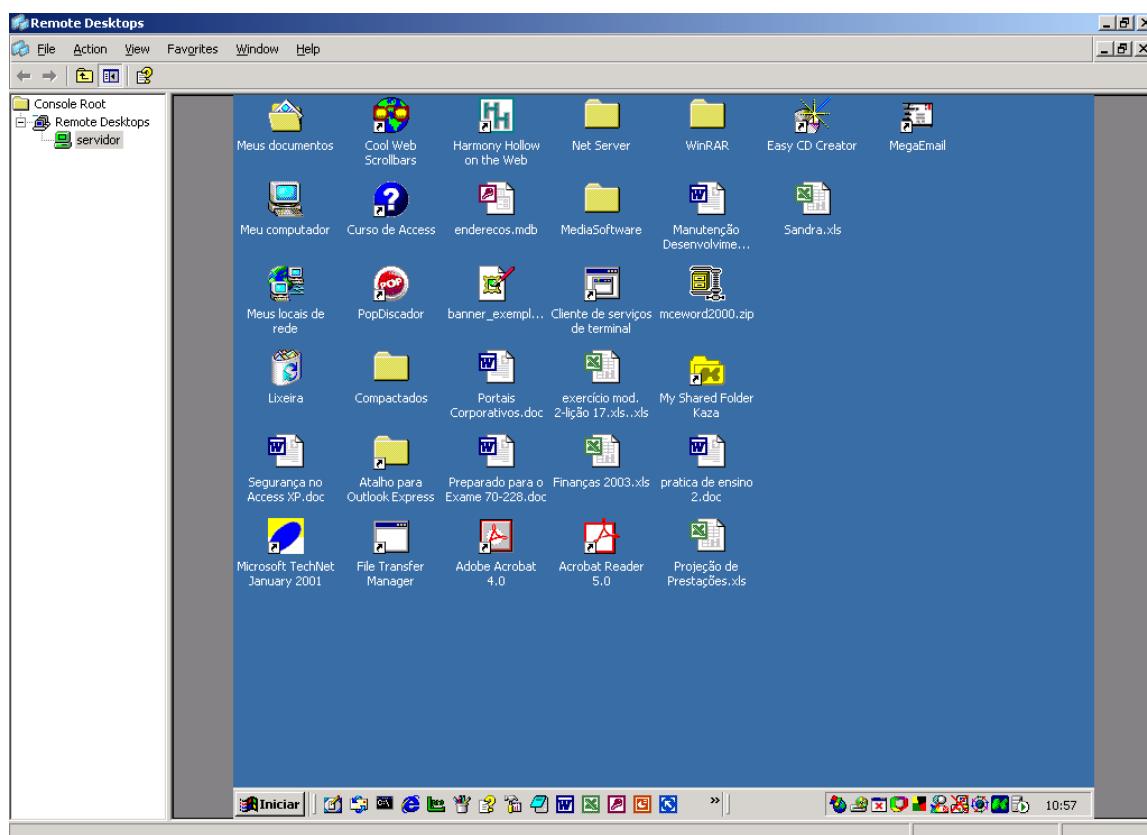


Figura 9.2 A área de trabalho do servidor, carregada via Terminal Services.

A tecnologia do Terminal Services oferece eficientes mecanismos de compactação e cache de telas, transmitindo somente o que muda de uma tela para outra, o que permite que o acesso via Terminal Services tenha desempenho bastante satisfatório, mesmo para conexões remotas, feitas via links de WAN de baixa velocidade.

O cliente envia para o servidor, através da rede, apenas os toques de teclado e as ações de mouse e recebe apenas as atualizações de tela. Este mecanismo de funcionamento, juntamente com a possibilidade de compactação dos dados que são transmitidos e do cache de telas no cliente, faz com que o Terminal Services gere uma quantidade reduzida de tráfego na rede e por isso possa trabalhar com desempenho aceitável, mesmo através de links de WAN de baixa velocidade.

O Terminal Services pode ser utilizado em dois modos diferentes:

- ◆ **Modo de Administração Remota:** Neste modo o Terminal Services é utilizado pelos administradores da rede, para se conectar remotamente aos servidores da rede e executar tarefas administrativas remotamente, como se estivessem localmente logados nos respectivos servidores. Para utilizar o Terminal Services neste modo, basta instalar o serviço nos servidores que deverão ser administrados remotamente e instalar o cliente em sua estação de trabalho (Remote Desktop no Windows XP e no Windows Server 2003 ou o Terminal Services Cliente no Windows 2000). Ao instalar o Terminal Services no modo de Administração Remota, este é instalado com licença para até duas conexões simultâneas. Você não precisa adquirir nenhuma licença adicional e não tem prazo de validade para estas licenças.
- ◆ **Modo de Compartilhamento de Aplicações:** Neste modo, o Terminal Services é utilizado para o compartilhamento de aplicações. Por exemplo, você pode querer instalar o Terminal Services no modo de Compartilhamento de Aplicações, para instalar o Microsoft Office no servidor. Desta maneira, os clientes poderão se conectar, até mesmo usando estações de trabalho mais antigas, como por exemplo um 486, apenas com um cliente de acesso ao Terminal Services instalado. O cliente faz a conexão e tem acesso à área de trabalho do servidor, na qual ele pode usar os aplicativos instalados no servidor, tais como o Word, Excel, Access e PowerPoint, ou quaisquer outros aplicativos instalados para o modo de Compartilhamento de Aplicações. O cliente pode usar os programas no servidor e gravar os dados em sua pasta home (home folder) na rede ou em disquete. A grande vantagem deste procedimento, é que o cliente poderá se conectar ao Terminal Services, usando qualquer computador da rede, no qual exista um cliente de conexão com o Terminal Services. Ao se conectar, usando qualquer um dos computadores da rede, ele receberá sempre a mesma área de trabalho (com os mesmos ícones e configurações) e terá acesso aos seus arquivos de dados. Quando um cliente faz uma conexão com o Terminal Services e faz alguma alteração no ambiente de trabalho, como por exemplo, adicionar um atalho à Área de trabalho, esta alteração é mantida e estará disponível na próxima conexão que o usuário fizer. Com isso é possível manter o ambiente do usuário e este ambiente “acompanha-o” em qualquer computador no qual ele fizer a conexão com o Terminal Services, porque na verdade todas as configurações estão no servidor. Para utilizar o Terminal Services neste modo, você deve adquirir uma licença de conexão para cada usuário que irá utilizar o Terminal Services no modo de Compartilhamento de Aplicações. Mais adiante falarei um pouco mais sobre o licenciamento neste modo.

O uso do Terminal Services traz inúmeras vantagens, dentre as quais podemos destacar as seguintes:

1. O administrador pode se conectar a qualquer servidor da rede, com o Terminal Services instalado e administrar este servidor como se estivesse localmente logado.
2. Com o uso do Terminal Services no modo de compartilhamento de aplicações, você pode criar um ambiente mais seguro e padronizado, onde os usuários acessam suas aplicações diretamente do servidor e gravam seus dados na rede.

3. Com o uso do Terminal Services no modo de compartilhamento de aplicações, fica mais fácil para instalar aplicações e mantê-las atualizadas, uma vez que a instalação e futuras atualizações precisam ser feitas apenas no servidor e não em cada estação de trabalho individualmente.
4. Com o uso do Terminal Services no modo de compartilhamento de aplicações, você pode utilizar clientes de menor capacidade de processamento, os quais não seriam mais aproveitados no modelo tradicional, onde o Windows e todos os aplicativos são instalados na estação de trabalho do cliente.
5. O cliente pode rodar, inclusive, em outros sistemas operacionais. Por exemplo, existem programas clientes para o Terminal Services, fornecido por terceiros, para se conectar através de uma estação de trabalho com o UNIX, Linux, Macintosh e assim por diante. Ou seja, pode haver um cliente UNIX na rede, conectado ao Terminal Services e utilizando o Word.
6. É possível também criar um modelo “misto” de estação de trabalho, na qual o cliente tem o Windows instalado e alguns programas de uso específico, instalados localmente. Já programas de uso geral na empresa, tais como o Word, Excel, Email, etc, o cliente acessa via Terminal Services. Com isso é possível manter um ambiente padronizado e de fácil manutenção para as aplicações utilizadas por todos na empresa, ao mesmo tempo que permite que cada usuário tenha acesso a aplicações específicas, relacionadas com o seu trabalho diário.
7. Redução do tráfego de WAN: Por exemplo, vamos imaginar uma empresa com o servidor de email na sede da empresa e os clientes das filiais com suas caixas de correio neste servidor de email. No modelo tradicional, cada cliente teria o software de email instalado em sua estação de trabalho e acessaria o servidor de email da matriz, através do link de WAN. Neste modelo, todas as mensagens e demais informações são transmitidas do servidor de email para o cliente e de volta para o servidor de email, através do link de WAN. Quem já tentou utilizar um cliente de email como o Lotus Notes, para acessar um servidor que está do outro lado de um link de WAN de 64 ou 129 Kbps, sabe o quanto é penosa esta operação. São minutos para abrir uma única mensagem. Já com o Terminal Services, o cliente abriria o programa de email diretamente no servidor, no mesmo servidor onde está o servidor de email. Com isso, só é transmitido através do link de WAN, os toques de teclado e mouse do cliente e as atualizações de tela do servidor para o cliente. Além de uma considerável redução no tráfego de WAN, o acesso ao email e demais aplicações fica muito mais rápido.

Para cada usuário que se conecta via Terminal Services é criada uma sessão completamente isolada das demais sessões. Ou seja, se um programa apresentar problemas e travar a sessão de um dos usuários conectados, as demais sessões continuarão funcionando normalmente e não serão afetadas. O Windows Server 2003 também grava informações sobre o ambiente de trabalho de cada usuário quando ele se conecta via Terminal Services. Ou seja, o conceito de Profiles, visto no Capítulo 4 é válido também para conexões via Terminal Services.

Outra área onde o Terminal Services pode ser utilizado com grandes vantagens é para oferecer acesso a usuários remotos, tais como vendedores que trabalham usando um Notebook para acessar a rede da empresa ou funcionários que trabalham em casa mas precisam ter acesso aos recursos da rede da empresa. Estes usuários podem fazer a conexão à rede da empresa usando uma linha discada e ter acesso aos aplicativos que precisam via Terminal Services. Este meio de acesso é bem mais eficiente e rápido do que o acesso através de programas clientes instalados no próprio Notebook e através de drives de redes mapeados, uma vez que neste modo é como se o usuário estivesse diretamente conectado ao servidor da empresa, sendo transmitido através da conexão discada, somente os toques de teclado e mouse do usuário e as atualizações de tela do servidor. Muito mais rápido do que

**IMPORTANTE:** Quando o usuário conecta com o Terminal Services ele está utilizando recursos tais como memória RAM e processador, do Servidor. Por isso, se você pretende utilizar o Terminal Services no modo de Compartilhamento de Aplicações, é importante fazer um planejamento cuidadoso da quantidade de recursos de hardware, necessária no servidor. Mais adiante apresentarei mais detalhes sobre a quantidade média de recursos de hardware necessária para cada cliente.

fazer a conexão e depois usar um programa cliente, instalado no próprio Notebook, para fazer conexão com os aplicativos e dados da empresa. Neste segundo modelo, toda a informação e os dados são transmitidos através da conexão discada, o que gera um grande tráfego e tempos de respostas bem mais altos do que com o uso do Terminal Services.

## Recursos de hardware necessários para o funcionamento do Terminal Services.

Os recursos de hardware necessários para dar suporte a instalação do Terminal Services variam, dependendo do modo no qual ele é instalado. No modo de administração, com suporte a no máximo duas conexões simultâneas, o único requisito adicional é cerca de 20 MB de espaço em discos para instalação do Terminal Services. Não será necessário fazer atualização de memória ou processador. Basta instalar o Terminal Services e o administrador poderá usar o Terminal Services Cliente (se estiver usando uma estação de trabalho com o Windows 2000) ou o Remote Desktop (se estiver usando um computador com o Windows Server 2003), para se conectar com o Terminal Services.

Já no modo de compartilhamento de aplicações são necessários recursos adicionais de hardware, principalmente memória RAM e processador. O hardware necessário varia com a quantidade de usuários que irão fazer a conexão simultaneamente e com o tipo de aplicação que estiver sendo compartilhada. Por isso não é possível definir um valor exato, mas apenas apresentar algumas sugestões (com base no que é colocado na Ajuda do Windows Server 2003) com base no número de usuários conectados.

- ◆ **Memória RAM:** Somente para fazer o logon e carregar a área de trabalho, via Terminal Services, você deve prever um adicional de 20 MB de RAM, por usuário conectado. Para um usuário utilizando o Excel mais um programa de email como o Outlook são necessários mais 20 MB. Neste cenário você já teria uma necessidade de 40 MB por usuário. Por exemplo, se você tem uma previsão de ter cerca de 10 usuários conectados simultaneamente, o ideal é providenciar um adicional de, pelo menos, 400 MB. Este é o valor do adicional de memória necessário, além da memória já utilizada, normalmente, pelo Windows Server 2003. Por exemplo, se você tem um servidor com 512 MB de memória e pretende instalar o Terminal Services para dar suporte para 10 usuários simultâneos, você deve adicionar mais cerca de 400 MB de memória (40 MB por usuário), ficando com um total de 912 MB de memória. Na prática, nesta situação, você faria um upgrade para 1GB de memória (1024 MB).
- ◆ **Processador:** Esta, definitivamente, não é uma ciência exata. Ou seja, não existe uma planilha ou uma metodologia de cálculo que permita definir, exatamente, qual a necessidade de processamento para cada usuário. Isso acontece porque cada usuário irá utilizar um conjunto diferente de aplicações, em momentos diferentes e com diferentes necessidades de processamento. Em média, um servidor com um processador Pentium III de 1 GHz é capaz de atender, bem, algo entre 10 e 20 usuários. Eu coloco entre 10 e 20 usuários porque se forem 10 usuários utilizando uma aplicação gráfica pesada, provavelmente o Pentium III de 1 GHz não dará conta; já se forem 20 usuários utilizando apenas o Word, provavelmente o Pentium III de 1 GHZ dará conta com sobra. Creio que isso demonstra bem que, de maneira alguma, existe uma regra geral e uma fórmula fácil para determinar a necessidade de processamento exata. O que acontece, na prática, é que se faz uma estimativa e, com base na estimativa, coloca-se o servidor em produção. Se o processador (ou processadores) não estiver dando conta faz-se uma atualização. Ou seja, mais ou menos na tentativa e erro.
- ◆ **Utilização da rede:** O Terminal Services tem muitos recursos para reduzir a quantidade de informação transmitida entre o cliente e o servidor, através da rede. Por exemplo, são transmitidas, do cliente para o servidor, apenas os toques de teclado e mouse. Do servidor para o cliente são transmitidas apenas as atualizações de tela. Os dados que são transmitidos podem ser compactados e pode ser habilitado um cachê de telas no cliente. Além disso, resoluções menores, tais como 800x600, transmitem uma quantidade bem menor de informações de atualização das telas do que resoluções maiores. Em média, cada cliente conectado, necessita de algo entre 4

e 8 KBps (estimativas da Microsoft). Estas estimativas confirmam o fato de que o Terminal Services realmente optimiza a utilização da rede e dos links de WAN, reduzindo tanto quanto possível o volume de informações a ser transmitido entre o cliente e o servidor.

Claro que estes são valores apenas aproximados e com base em estimativas das necessidades de um usuário típico. O ideal é que você possa fazer um laboratório de testes, com os usuários típicos que irão utilizar aplicações via Terminal Services, para que você possa ter uma idéia mais aproximada das necessidades de hardware, para a situação específica da sua rede. Ao fazer esta estimativa, existem alguns fatores que devem ser levados em consideração, tais como:

- ◆ Quais aplicações serão utilizadas pelos usuários, via Terminal Services. Eles irão utilizar aplicações tais como Word, Excel, email e Internet ou vão utilizar alguma aplicação com necessidades intensivas de hardware, tais como uma aplicação gráfica de CAD?
- ◆ Os usuários que irão acessar aplicações via Terminal Services são usuários experientes, que tiram o máximo de cada aplicação ou são usuários sem maiores conhecimentos de informática, que utilizam sistemas específicos para realizar tarefas específicas. No segundo caso fica bem mais fácil estimar a necessidade de hardware. Basta determinar as necessidades para um dos usuários e multiplicar pelo número de usuários. Já para o primeiro caso, com usuários mais especializados, é melhor por uma boa margem de segurança para as suas estimativas.
- ◆ Os acessos serão feitos via rede local ou você terá usuários móveis, fazendo o acesso através de conexões discadas ou usuários de outros escritórios da empresa, fazendo a conexão via links de WAN?

## Implementação e Administração do Terminal Services.

Para utilizar o Terminal Services no modo de administração remota, com suporte a duas conexões simultâneas, não é preciso instalar o serviço do Terminal Services. Para isso basta habilitar o recurso de Desktop Remoto, que é uma novidade introduzida no Windows XP (com suporte a uma única conexão) e que também está presente no Windows Server 2003 (com suporte a duas conexões simultâneas).

Para habilitar o recurso de Desktop Remoto siga os passos indicados a seguir:

1. Faça o logon com administrador ou com uma conta com permissão de administrador.
2. Abra o Painel de controle: Iniciar -> Painel de controle.
3. Dê um clique duplo na opção Sistema.
4. Será aberta a janela de propriedades do sistema, com a guia Geral selecionada por padrão. Dê um clique na guia Remoto. Será exibida a janela indicada na Figura 9.3.
5. Observe que, por padrão, as duas opções da guia Remoto vêm desmarcadas. Marque a opção Permitir que usuários se conectem remotamente a este computador. Ao marcar esta opção você está habilitando outros usuários a se conectarrem remotamente ao servidor, ou seja, que outros usuários, desde que devidamente habilitados, possam acessar o console do servidor, remotamente. Esta opção habilita até duas conexões simultâneas, ou seja, é exatamente a mesma funcionalidade do Terminal Services em modo de administração, no Windows 2000 Server.

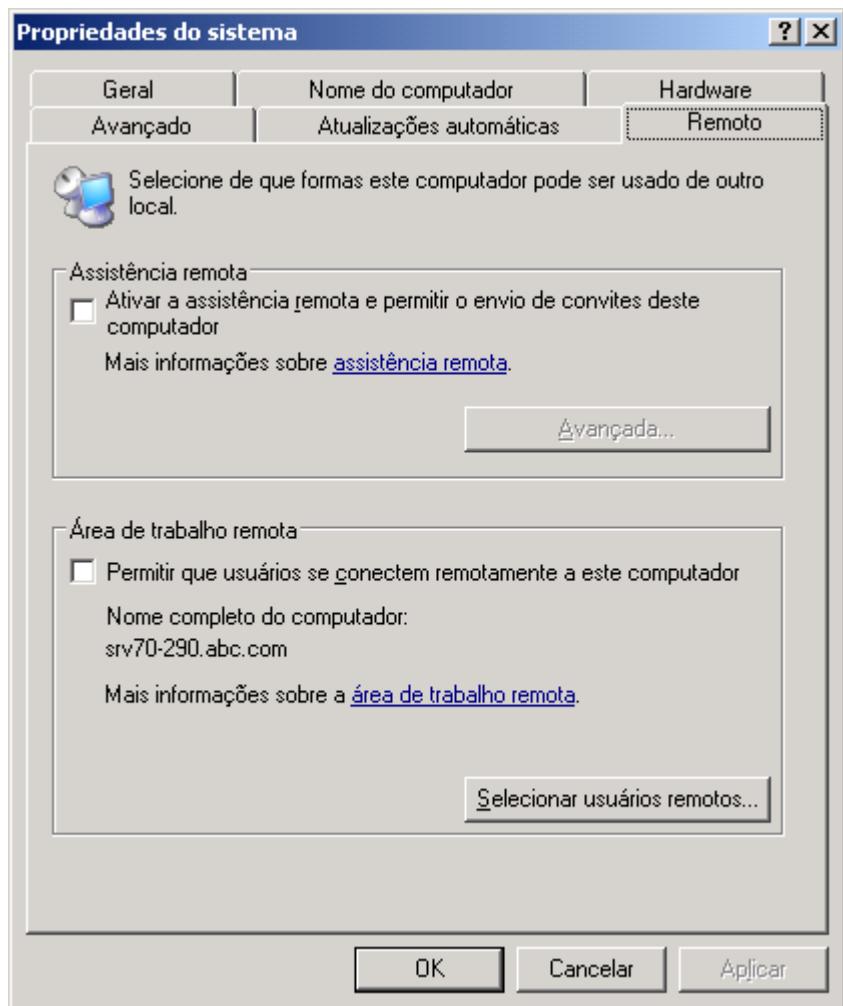


Figura 9.3 Habilitando o recurso de Desktop Remoto.

6. Por padrão somente o usuário Administrador terá permissão para fazer a conexão remota. Você poderá adicionar outros usuários com permissão para fazer a conexão remota. Para isso clique no botão Selecionar usuários remotos...
7. Será exibida a janela Usuários da área de trabalho remota. Observe a mensagem nesta janela, informando que o usuário Administrador já tem permissão de conexão remota, por padrão. Para adicionar novos usuários clique em Adicionar... Será aberta a janela Selecionar usuários ou Grupos, já descrita no Capítulo 4. Informe o nome dos usuários que terão permissão de conexão remota, digitando os nomes separando-os por ponto-e-vírgula, conforme exemplo da Figura 9.4, ou utilize o botão Avançado..., para selecionar os usuários da lista de usuários do Active Directory.

**IMPORTANTE:** Caso alguma das contas de usuário esteja com senha em branco, será exibida uma mensagem de advertência. Clique em OK para fechá-la. Estas contas não poderão ser utilizadas para fazer a conexão remota, já que o Windows Server 2003 exige que as contas que se conectam remotamente, tenham uma senha definida.

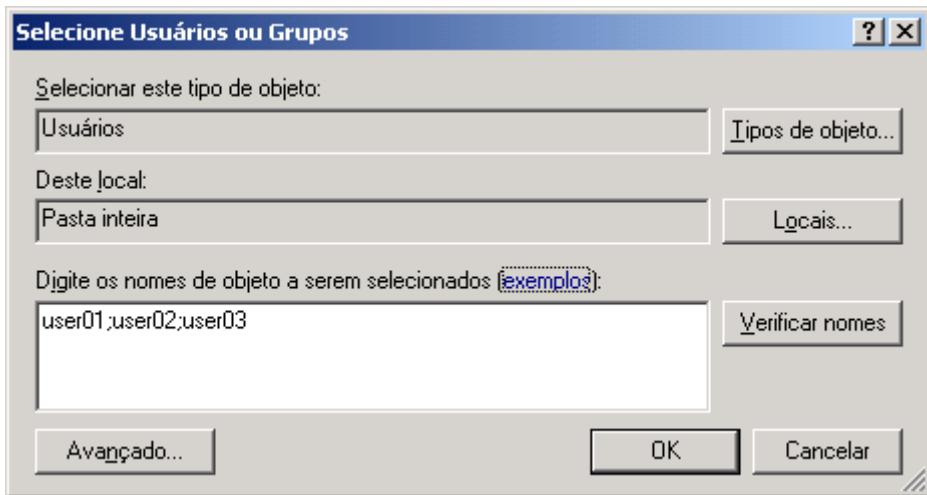


Figura 9.4 Definindo os usuários que terão permissão de se conectar remotamente.

8. Clique em OK. Você estará de volta a guia Usuários da área de trabalho remota, com os usuários selecionados já adicionados à lista, conforme indicado na Figura 9.5:

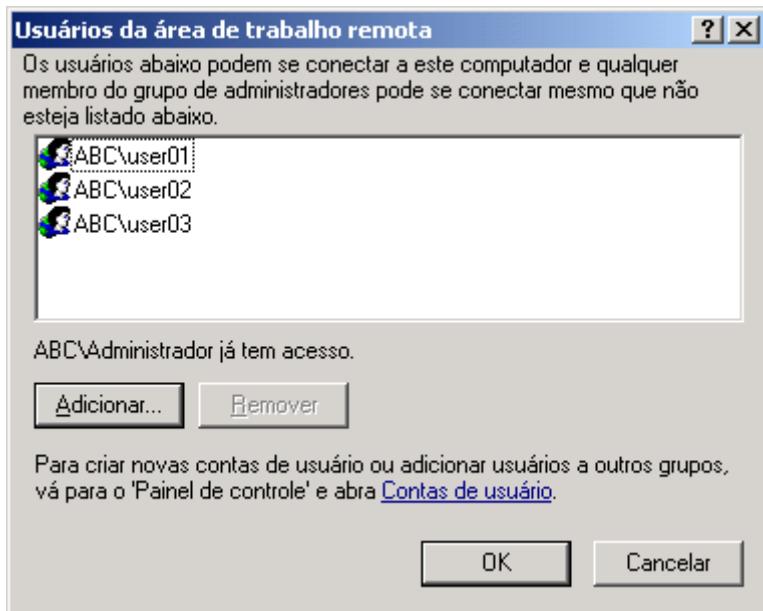
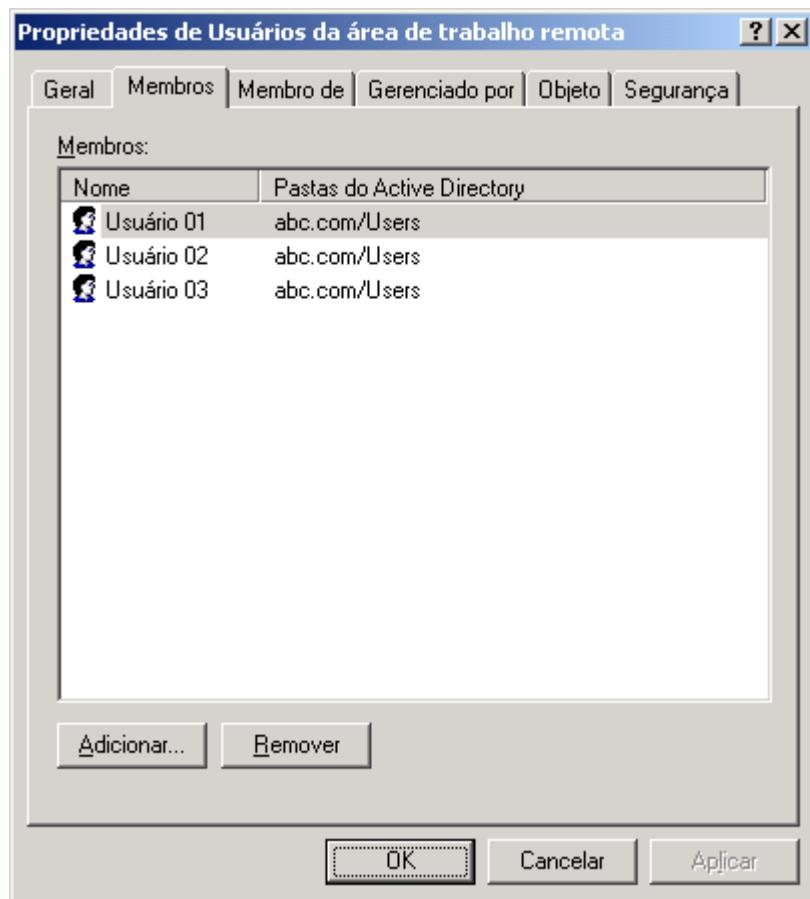


Figura 9.5 Lista de usuários com permissão de acesso remoto.

---

**IMPORTANTE:** Ao adicionar usuários, com permissão para fazer o acesso remoto, na verdade, você estará adicionando estes usuários, como membros do grupo: Usuários da área de trabalho remota. Ou seja, na prática, para dar permissão a uma conta de usuário, para fazer a conexão remota, basta incluir a referida conta, como membro do grupo Usuários da área de trabalho remota. Na Figura 9.6, mostro que a lista de membros do grupo Usuários da área de trabalho remota, ou seja, é exatamente a lista de usuários indicada na Figura 9.5.

---



**Figura 9.6 Membros do grupo Usuários da área de trabalho remota.**

9. Clique em OK para fechá-la. Você estará de volta à janela de propriedades do sistema. Clique em OK para fechá-la.

Pronto, agora o servidor está configurado para ser acessado remotamente, com permissão para até duas conexões simultâneas. A seguir mostrarei como fazer um conexão com este servidor, utilizando o Terminal Services Cliente, em um computador com o Windows 2000 Server instalado. Caso o Terminal Services Cliente não esteja instalado, no Windows 2000, você pode instalá-lo a partir do arquivo adminpak.msi, o qual encontra-se na pasta onde o Windows 2000 Server está instalado, dentro da subpasta system32 . Este arquivo contém um pacote de ferramentas administrativas para o Windows 2000 Server, dentre as quais o Terminal Services Client. Para instalar este pacote de ferramentas, basta dar um clique duplo no arquivo adminpak.msi e seguir as instruções do assistente de instalação.

Para se conectar remotamente ao console de um servidor com o Windows Server 2003, com o recurso da Área de Trabalho Remota, habilitado, usando o Terminal Services Cliente, siga os passos indicados a seguir:

1. Faça o logon no computador onde está instalado o Terminal Services Client. Faça o logon utilizando uma conta com permissão de logon remoto, ou seja, com uma conta pertencente ao grupo Usuários da área de trabalho remota.
2. Abra o Terminal Services Cliente: Iniciar -> Programas -> Ferramentas administrativas -> Cliente dos serviços de terminal -> Cliente de serviços de terminal (lembre-se que estou fazendo o teste em um cliente com o Windows 2000 Server instalado e vou me conectar com um servidor com o Windows Server 2003, instalado).
3. Será aberta a janela Cliente de serviços de terminal, indicada na Figura 9.7. Nesta janela você deve informar o nome ou o número IP do servidor com o qual você deseja se conectar (campo Servidor). Você deve selecionar a resolução a ser utilizada (800x600 no exemplo da Figura 9.7). Você também pode habilitar as opções Ativar

compactação de dados e Armazenar bitmap em cache em disco. Estas duas opções ajudam a reduzir a quantidade de informações que é enviada através da rede, entre o cliente e o servidor. Marque as opções desejadas, conforme exemplo da Figura 9.7 e clique em Conectar-se.

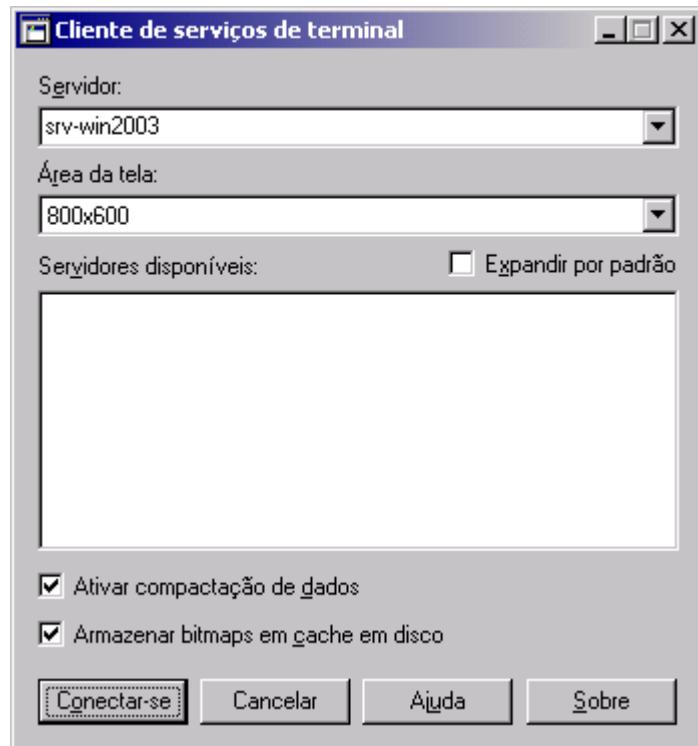


Figura 9.7 Informações para conexão.

4. Será exibida a tela de logon do servidor com o qual você está fazendo a conexão. Informe o nome de usuário e senha para logon, conforme exemplo da Figura 9.8 e clique em OK, para fazer a conexão remotamente.

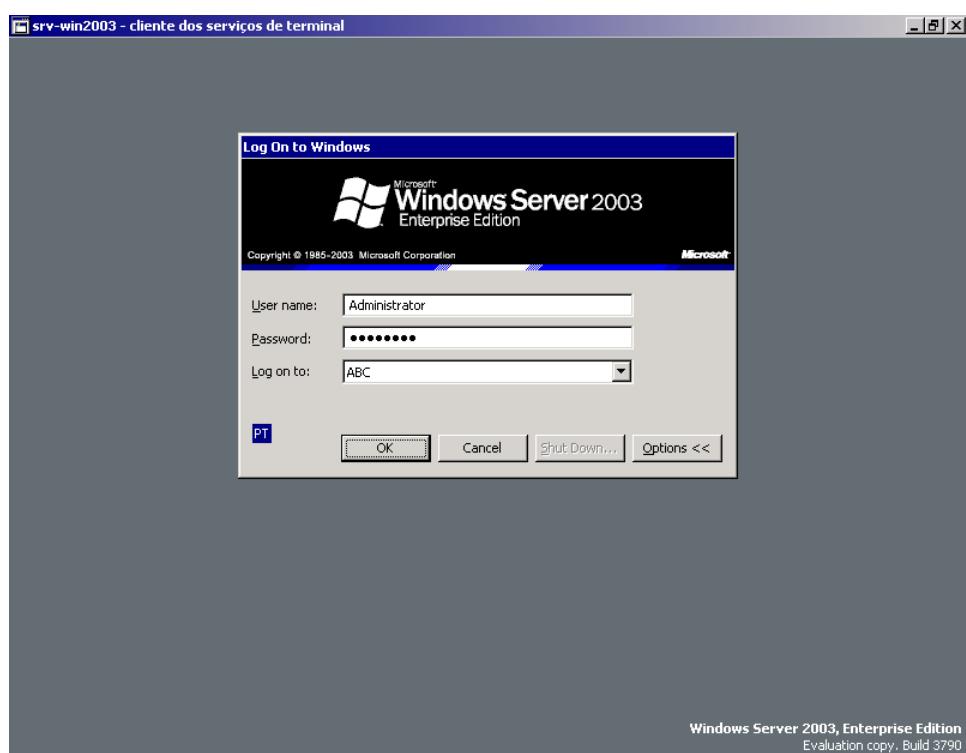
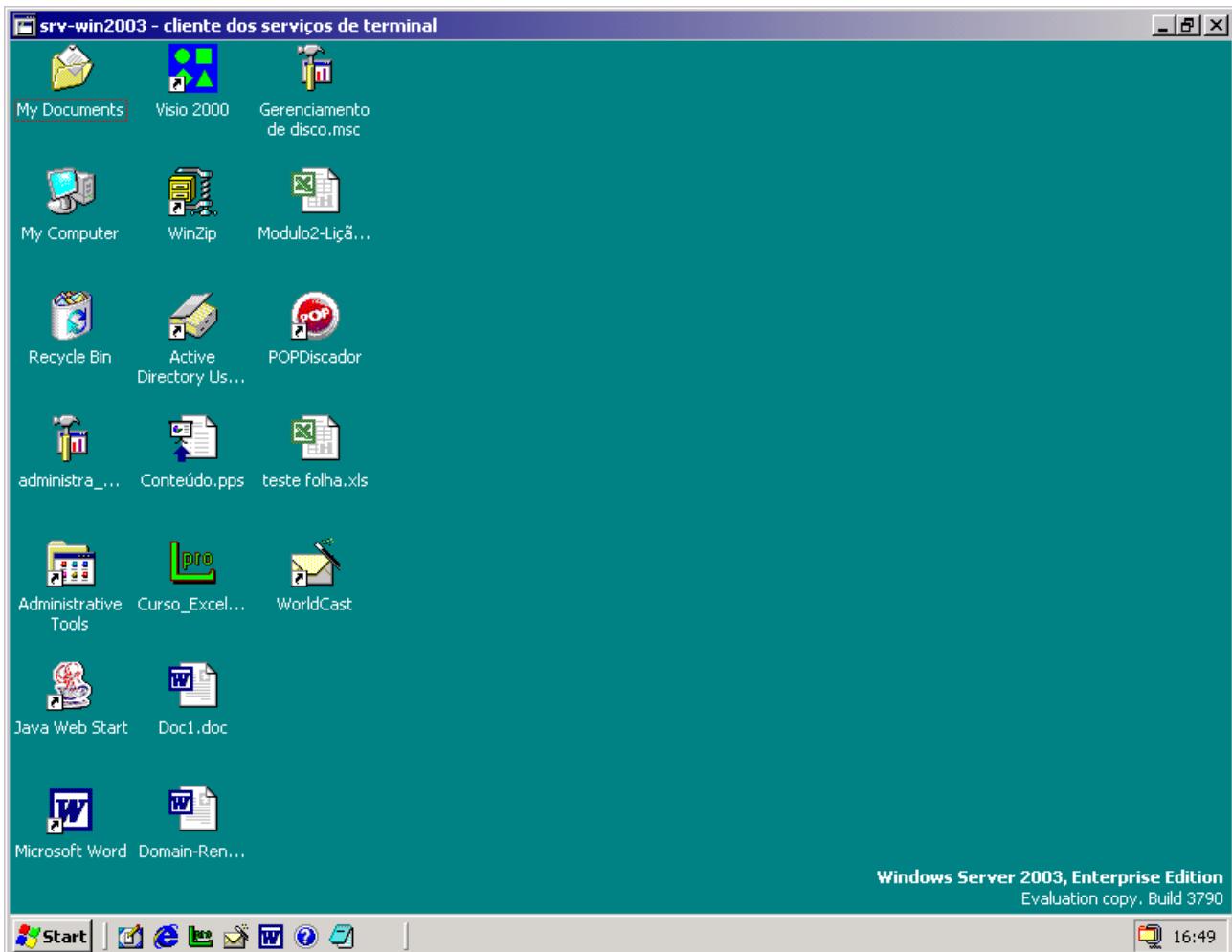


Figura 9.8 Fazendo o logon remotamente.

- Preencha as informações de logon e clique em OK. Pronto, agora é só aguardar. O logon será efetuado e a área de trabalho do servidor remoto será carregada, como se você tivesse feito o logon localmente, conforme indicado na Figura 9.9:



**Figura 9.9 Conexão efetuada com o desktop remoto.**

O desktop remoto passa a ser apenas mais uma janela dentro da sua área de trabalho. Você pode alternar entre o desktop remoto e a área de trabalho do computador local, com um simples clique de mouse. A partir deste momento é como se você estivesse “em frente” ao servidor remoto, como se tivesse feito o logon localmente neste servidor.

- Para encerrar a conexão, faça um log off. Não utiliza a opção Desligar, senão você irá realmente desligar, dar um shutdown no servidor remoto. Lembre-se que a conexão via desktop remoto é como se você estivesse localmente logado no servidor. Ao fazer o logoff será exibida novamente a janela de conexão, da Figura 9.7. Para fechá-la clique em Cancelar.

Observe que com esta funcionalidade, a partir da sua estação de trabalho, o administrador poderá se conectar a qualquer servidor com o recurso de Desktop Remoto (Área de Trabalho Remota) habilitado. É realmente uma ferramenta de administração muito poderosa e que facilita, e muito, a vida do administrador. A única limitação desta ferramenta é o número máximo de duas conexões simultâneas, por servidor.

## Utilizando o Terminal Services no modo de Compartilhamento de Aplicações:

Para utilizar o Terminal Services no modo de compartilhamento de aplicações, você deve instalar o serviço Terminal Services (Serviços de Terminal). Após a instalação você deve instalar as aplicações que serão compartilhadas e configurar o número de licenças de acordo com o número de usuários que irão acessar o Terminal Services no modo de compartilhamento de aplicações. A seguir você aprenderá a executar estas tarefas.

### Instalando o serviço Terminal Services.

Instalando o Terminal Services: Para instalar o Terminal Services siga os passos indicados a seguir:

1. Faça o logon como administrador ou com uma conta com permissão de administrador.
2. Abra o Painel de Controle: Iniciar -> Painel de Controle.
3. Dê um clique duplo na opção Adicionar ou remover programas.
4. Será exibida a janela Adicionar ou remover programas. Nas opções do lado esquerdo da janela, dê um clique na opção Adicionar/remover componentes do Windows
5. Será aberto o assistente de componentes do Windows.
6. O Terminal Services é um dos componentes do Windows Server 2003. Para que os clientes possam se conectar com o Terminal Services você também deve adicionar o Terminal Server Licensing, que é o componente que permitirá que o administrador adicione mais licenças, habilitando mais usuários a fazer a conexão via Terminal Services. Localize estas duas opções Terminal server e Licenciamento do Terminal server e dê um clique para marcá-las, conforme indicado na Figura 9.10:

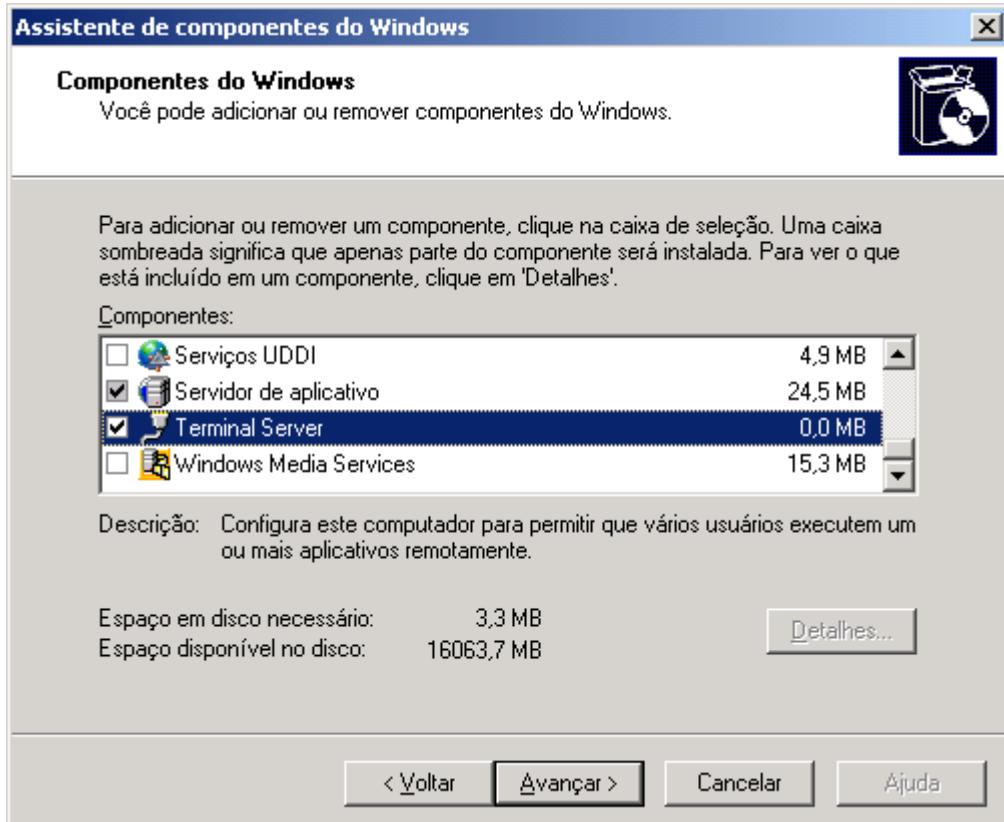


Figura 9.10 Selezionando o Terminal Services para instalação.

7. Clique em Avançar, para seguir para a próxima etapa do assistente.

Será exibida uma mensagem de aviso, indicada na Figura 9.11, com diversas informações relevantes.

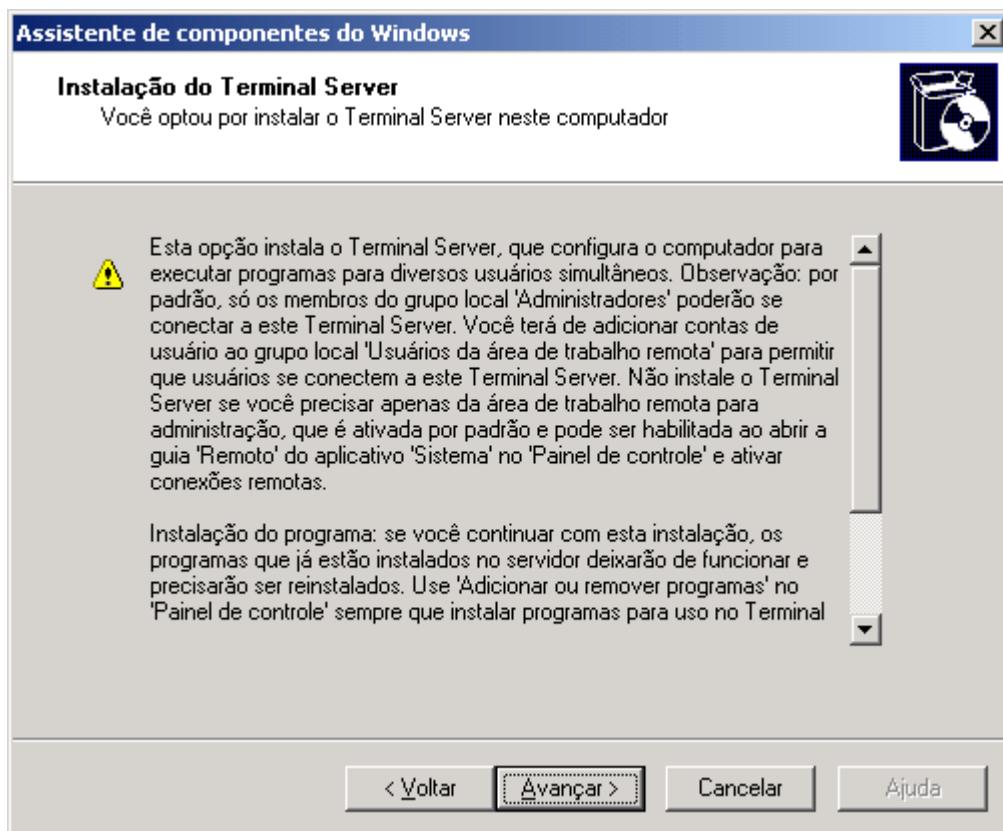


Figura 9.11 A tela com avisos importantes.

A primeira informação relevante é que, por padrão, somente os membros do grupo Administrators (Administradores) tem permissão para conectar-se remotamente ao Terminal Services no modo de compartilhamento de aplicação. Para permitir que outros usuários possam fazer essa conexão remotamente, você deve adicionar as contas dos usuários que farão a conexão, ao grupo Remote Desktop Users (Usuários da área de trabalho remota), grupo este já descrito anteriormente..

Também é emitido um aviso que as aplicações atualmente instaladas não estarão habilitadas para o modo de compartilhamento de aplicação, ou seja, para que elas possam ser acessadas por múltiplos usuários, elas deverão ser reinstaladas no servidor. Você deve ter cuidado, pois esta mensagem está bastante confusa e leva a interpretações incorretas. Da maneira como a mensagem foi redigida, dá a impressão que depois da instalação do Terminal Services, todas as aplicações deixarão de funcionar, mesmo localmente, no servidor. Isso não é verdade. O que a mensagem “queria ter dito” é que as aplicações atualmente instaladas, não estarão automaticamente habilitadas para serem usadas no modo de compartilhamento de aplicações, via acesso remoto. Mas continuarão funcionando, localmente, sem problema nenhum.

É importante salientar que nem todas as aplicações do mercado são compatíveis com o modo de compartilhamento de aplicação. Não significa que se a aplicação rodar isoladamente no servidor, irá também funcionar no modo de compartilhamento de aplicação, para que vários usuários possam acessá-la simultaneamente. Evidentemente que a grande maioria das aplicações é compatível com o modo de compartilhamento. Todas as aplicações que foram testadas

e certificadas para o uso com o Windows Server 2003, irão rodar, sem problemas, no modo de compartilhamento de aplicações.

8. Clique em Avançar, para seguir para a próxima etapa do assistente.
9. Nesta etapa você deve selecionar o modo de segurança que será utilizado. O modo Segurança máxima é bem mais seguro, e disponibiliza os novos recursos do Windows Server 2003 em relação à segurança, porém pode ser incompatível com algumas aplicações mais antigas. Você pode selecionar este modo durante a instalação e se houver aplicações críticas que não são compatíveis com este modo, você pode alternar para o modo Segurança reduzida, a qualquer momento, utilizando o console de configuração do Terminal Services, o qual será visto mais adiante.
10. Selecione o modo Segurança máxima e clique em Avançar, para seguir para a próxima etapa do assistente.
11. Nesta etapa você deve definir se o Terminal Server Licensing que está sendo instalado irá gerenciar o licenciamento do Terminal Services em toda a empresa ou apenas no domínio onde ele está sendo instalado. Selecione a opção desejada e clique em Avançar, para seguir para a próxima etapa do assistente.
12. O Windows Server 2003 inicia o processo de instalação e emite mensagens sobre o andamento da instalação. Durante a etapa de cópia dos arquivos você pode ser solicitado a inserir o CD de instalação do Windows Server 2003 no drive. Se isso acontecer, insira o CD de instalação do Windows Server 2003 no drive.
13. O assistente detecta que o CD foi inserido no drive e continua o processo de instalação.
14. A tela final do assistente é exibida com uma mensagem informando que o assistente foi concluído com sucesso. Clique em Concluir para fechar o assistente.
15. É exibida uma mensagem de que o servidor deve ser reinicializado. Clique em Sim para reiniciá-lo.

Pronto, o Terminal Server e o Licenciamento do Terminal Server foram instalados e estão prontos para serem utilizados. Agora você aprenderá sobre como instalar programas para rodar no modo de compartilhamento de aplicação e como configurar o licenciamento do Terminal Server.

O servidor será inicializado e, no primeiro logon, após a instalação do Terminal Services, o sistema de Ajuda do Terminal Services será automaticamente carregado e exibido, conforme indicado na Figura 9.12:

---

**DICA:** No site [www.veritest.com](http://www.veritest.com), você encontra uma lista das aplicações certificadas para o Windows Server 2003.

---

**IMPORTANTE:** Nesta tela também é emitido um aviso de que o terminal services funcionará por 120 dias. Durante este período você deve adquirir as licenças necessárias junto à Microsoft e configurá-las utilizando o Terminal Server Licensing. Não esqueça deste detalhe para os exames de Certificação do MCSE 2003. Seria uma boa questão.

---

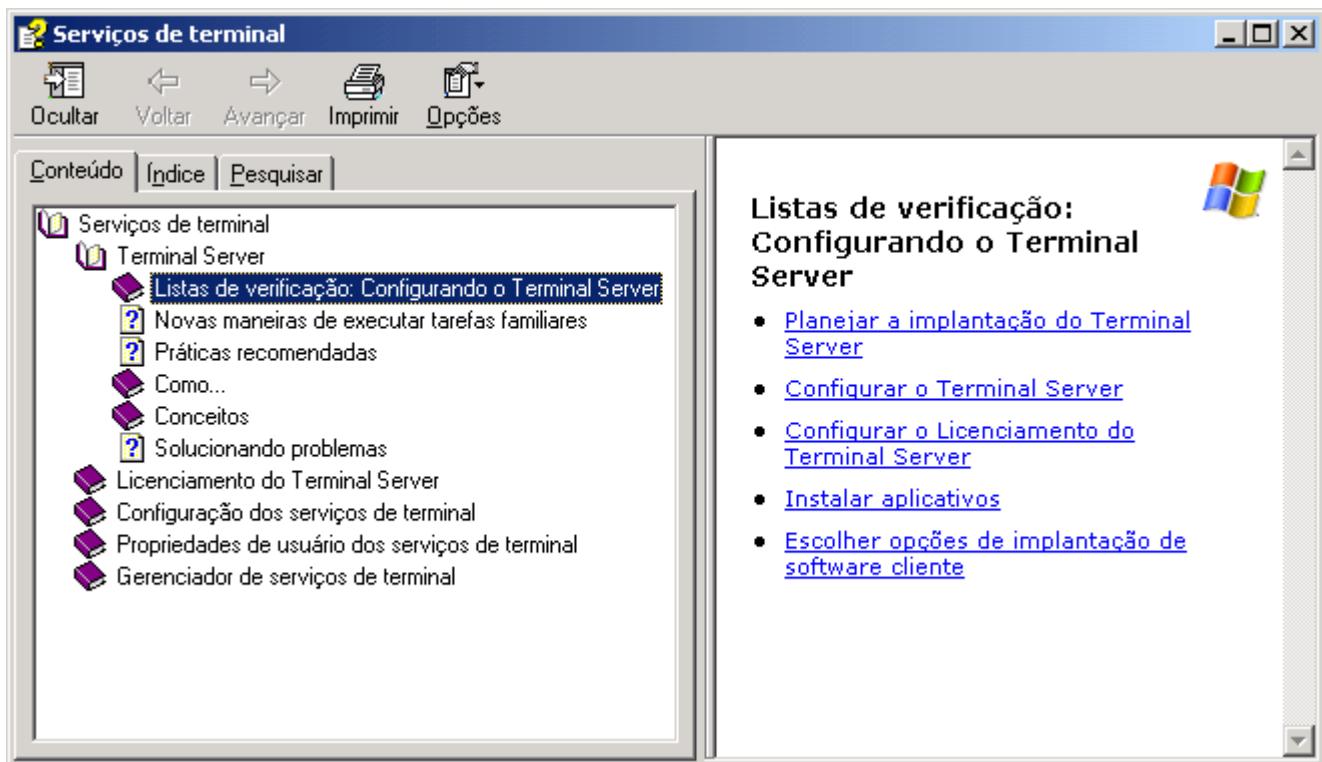


Figura 9.12 O sistema de Ajuda do Terminal Services.

### Configurando o licenciamento para o Terminal Services.

O Terminal Server requer licenças para que os clientes possam fazer o logon. Qualquer cliente que tente fazer o logon no Terminal Services, deve ser capaz de receber uma licença de acesso válida, a qual é disponibilizada pelo Licenciamento do Terminal Server. Sem receber a licença, não será permitido o logon do cliente.

O licenciamento do terminal services é “separado” do licenciamento do Windows Server 2003. Conforme comentado no Capítulo 1, sobre instalação do Windows Server 2003, devem ser adquiridas as chamadas CAL – Cliente Access License, para que clientes da rede possam se conectar aos servidores com o Windows Server 2003. Já para o Terminal Server é outro tipo de licença, ou seja, o fato de ter licenças para conectar com o Windows Server 2003, não implica que estas licenças também sejam válidas para o Terminal Server no modo de compartilhamento de aplicações. Licenças específicas, para acessar o Terminal Server no modo de compartilhamento de aplicações, devem ser ativadas.

Após ter comprado as licenças de acesso via Terminal Server, junto à Microsoft, você deve utilizar o console Licenciamento do Terminal Server para configura-las. As informações sobre o número total de licenças disponíveis, o número de licenças em uso e o número de licenças ainda livres para serem utilizadas por novas conexões, são armazenadas no Licenciamento do Terminal Server. Quando um cliente tenta fazer uma conexão com o Terminal Server, este entra em contato com o Licenciamento do Terminal Server, para verificar se existem licenças disponíveis, ou melhor, se existe, pelo menos, uma licença disponível para o novo cliente que está tentando se conectar.

Um único Servidor de licenciamento do Terminal Server, pode ser utilizado por vários servidores com o Terminal Server em modo de compartilhamento de aplicação.

**IMPORTANTE:** Conforme descrito anteriormente, você deve instalar e configurar o Licenciamento do Terminal server, para que os clientes possam acessar o Terminal Services no modo de compartilhamento de aplicações. Se não for configurado o licenciamento, o Terminal Services deixará de funcionar após 120 dias.

Após ter instalado o Licenciamento do Terminal Server você deve ativá-lo e instalar as licenças de acesso que foram adquiridas junto à Microsoft. Isso é feito através do uso do Assistente para ativação das licenças do Terminal Server

Para ativar o licenciamento você precisará de uma conexão com a Internet. Também é possível fazer a ativação por telefone. A seguir mostro os passos para a ativação via Internet.

Para ativar o licenciamento automaticamente, siga os passos indicados a seguir:

1. Faça o logon como administrador ou com uma conta com permissão de administrador.
2. Certifique-se de que você tem uma conexão com a Internet.
3. Abra o console de Licenciamento do Terminal Server: Iniciar -> Ferramentas administrativas -> Licenciamento do Terminal Server.
4. Clique com o botão direito do mouse no nome do servidor para o qual será ativado o licenciamento.
5. No menu de opções que é exibido clique em Ativar Servidor.
6. Será aberto o assistente para ativação das licenças.
7. Clique em Avançar para seguir para a próxima etapa do assistente.
8. Será exibida a tela para que você selecione o método de conexão. Por padrão vem selecionada a opção Conexão automática que é o método recomendado. Aceite este método e clique em Avançar para seguir para a próxima etapa do assistente.
9. O assistente demora alguns instantes, tentando localizar o servidor da Microsoft responsável pelo licenciamento e exibe uma tela para que você preencha os dados da sua empresa, conforme indicado na Figura 9.13:

**NOTA:** Após a instalação do Terminal Server no modo de compartilhamento de aplicações, será possível utilizá-lo, sem a compra das licenças de acesso, durante um período de 120 dias. Terminado este período, os clientes não conseguirão mais se conectar, enquanto não forem ativadas e configuradas as licenças de acesso. Estou repetindo este tópico, várias vezes, propositadamente.

**NOTA:** Dependendo das configurações que você estiver utilizando no Internet Explorer, pode ser necessária a adição do site de ativação da Microsoft, na lista de sites confiáveis.

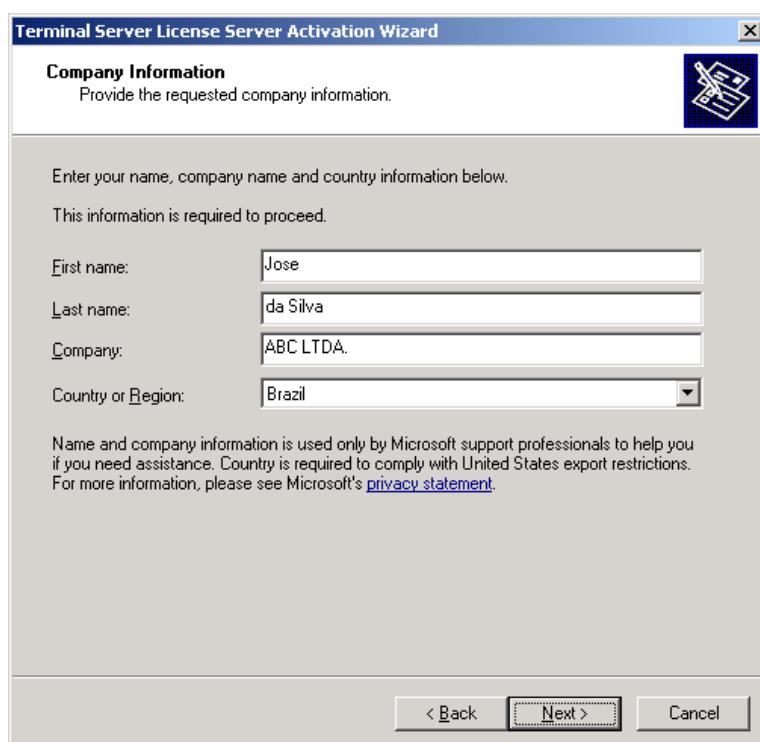


Figura 9.13 Informações sobre a empresa.

10. Clique em Avançar para seguir para a próxima etapa do assistente.
11. É exibida uma tela onde você pode preencher informações tais como email, nome da empresa ou filial, Endereço, Cidade, Estado e CEP. Estas informações são opcionais.
12. Clique em Avançar para seguir para a próxima etapa do assistente.
13. O assistente tenta entrar em contato com um servidor de ativação da Microsoft, conforme indicado na Figura 9.14:



Figura 9.14 Localizando um servidor de ativação.

14. Será exibida a tela final do assistente, informando que o servidor de licenciamento foi ativado com sucesso. A próxima etapa é instalar as licenças no Terminal Server. Certifique-se de que a opção Iniciar o Assistente de Ativação... esteja marcada. Com esta opção marcada, o Windows Server 2003 já abre o assistente para instalação das licenças de cliente.
15. Clique em Avançar para abrir o assistente de instalação das licenças.
16. Será aberto o assistente para instalação das CAL (Cliente Access License) do Terminal Server. A primeira etapa do assistente é apenas informativa. Clique em Avançar para seguir para a próxima etapa do assistente.
17. Novamente o assistente tenta se conectar com o servidor de ativação da Microsoft.
18. Em seguida é exibida a tela para que você informe o tipo de contrato de licenciamento utilizado pela sua empresa. (entre os vários programas de licenciamento disponibilizados pela Microsoft). Selecione o tipo de contrato e clique em Avançar para seguir para a próxima etapa do assistente.
19. Nesta etapa, você tem que informar o código de habilitação para cada licença. Este código é fornecido pela Microsoft, quando você compra as licenças de acesso. Informe o código para cada licença e depois clique no botão Adicionar.
20. Depois é só seguir as etapas restantes do assistente e pronto, o Terminal Services estará pronto para ser utilizado no modo de compartilhamento de aplicações. Que dizer, quase pronto, pois ainda resta você aprender como instalar as aplicações para que possam ser acessadas no modo compartilhado. Conforme descrito anteriormente, as aplicações que já estavam instaladas, antes da instalação do Terminal Services, não estarão habilitadas para o uso compartilhado. Para tal elas terão que ser reinstaladas. No próximo tópico você aprenderá como instalar aplicações para uso compartilhado, via Terminal Services no modo de compartilhamento de aplicações.

## Instalando aplicações para uso no modo compartilhado.

Se você estiver utilizando o Terminal Server no modo de administração (apenas habilitando o recurso de Desktop Remoto), não serão precisos cuidados adicionais para instalar as aplicações. Ou seja, o processo de instalação é o mesmo de instalar um aplicativo no Windows Server 2003, nada de diferente. Isso porque neste modo, o número máximo de conexões simultâneas é dois e este modo é utilizado, pelo administrador, para acessar os consoles

administrativos do Windows Server 2003 (DNS, WINS, DHCP, Usuários e Computadores do Active Directory e assim por diante).

Já no modo de Compartilhamento de Aplicações existem alguns pontos que devem ser observados. Primeiro é importante salientar que neste modo, as aplicações poderão ser utilizadas por vários usuários conectados simultaneamente. O Windows Server 2003 terá que tratar destes acessos simultâneos, sendo capaz de manter uma ambiente personalizado para cada usuário. Aplicações que obtiveram o logotipo “Certified for Windows”, irão funcionar, sem problemas, com o Terminal Server no modo de Compartilhamento de Aplicações. Conforme citado anteriormente, no site [www.veritest.com](http://www.veritest.com), você encontra uma relação das aplicações que possuem o logotipo “Certified for Windows”.

Para aplicações que não tem o logo “Certified for Windows” podem ser necessários passos adicionais para que ela possam ser executadas no modo de Compartilhamento de Aplicações. Algumas destas aplicações poderão ser fornecidas com scripts de adaptação, os quais deverão ser executados para que a aplicação possa ser executada no modo de Compartilhamento de Aplicações. Outras poderão, simplesmente, não funcionar neste modo.

Quando você instala o Terminal Services em modo da Compartilhamento de Aplicações, o Windows Server 2003 pode ser colocado em dois modos de operação distintos:

- ◆ Install Mode (Modo de Instalação)
- ◆ Execute Mode (Modo de Execução).

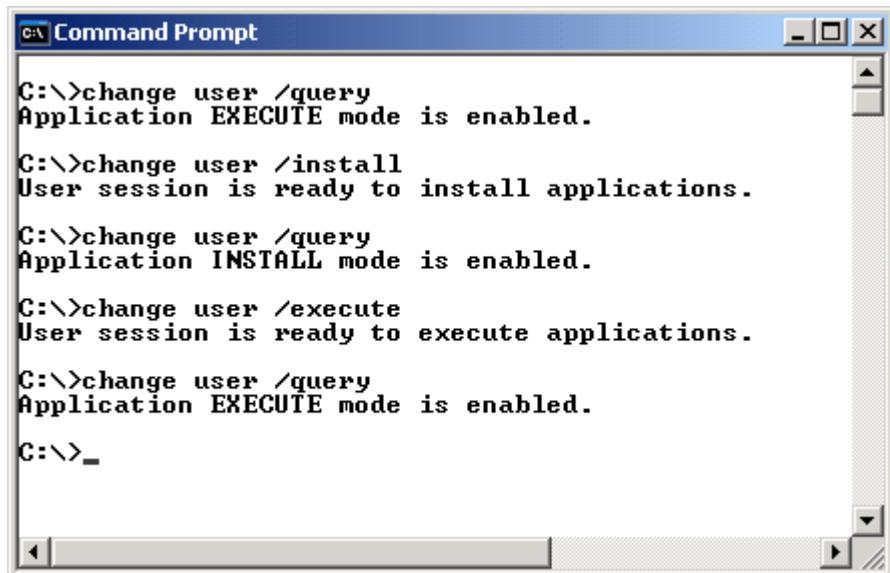
O modo de execução é o modo normal de operação, no qual deve estar o Windows Server 2003, para que os usuários possam acessar o Terminal Services e as aplicações disponíveis. Para aplicações que não tem o logotipo “Certified for Windows”, você deve alternar para o modo de instalação (Install Mode) para instalar a aplicação, caso contrário esta aplicação não irá funcionar corretamente. Após ter feito a instalação, você deve alternar de volta para o modo de execução (Execute Mode), para que a aplicação possa ser acessada pelos usuários, via Terminal Services.

Quando você inicia o processo de instalação de uma aplicação, o Windows Server 2003 é capaz de detectar a necessidade de alternar para o modo de instalação e faz esta alteração sem problemas. Quando você usa a opção Adicionar ou remover programas) do Painel de controle, o Windows Server 2003 também alterna para o modo de instalação. Uma terceira opção para alternar entre os modos de execução e instalação e vice-versa é o comando change, o qual será descrito logo a seguir.

O comando change tem diferentes opções e diferentes parâmetros de linha de comando, conforme descrito a seguir:

- ◆ change user /query -> Informa em que modo está o Windows Server 2003 (EXECUTE ou INSTALL)
- ◆ change user /install -> Habilita o modo de instalação
- ◆ change user /execute -> Retorna ao modo de execução.

Na Figura 9.15 é exibido um exemplo de execução do comando change user com as três opções descritas anteriormente.



```
C:\>change user /query
Application EXECUTE mode is enabled.

C:\>change user /install
User session is ready to install applications.

C:\>change user /query
Application INSTALL mode is enabled.

C:\>change user /execute
User session is ready to execute applications.

C:\>change user /query
Application EXECUTE mode is enabled.

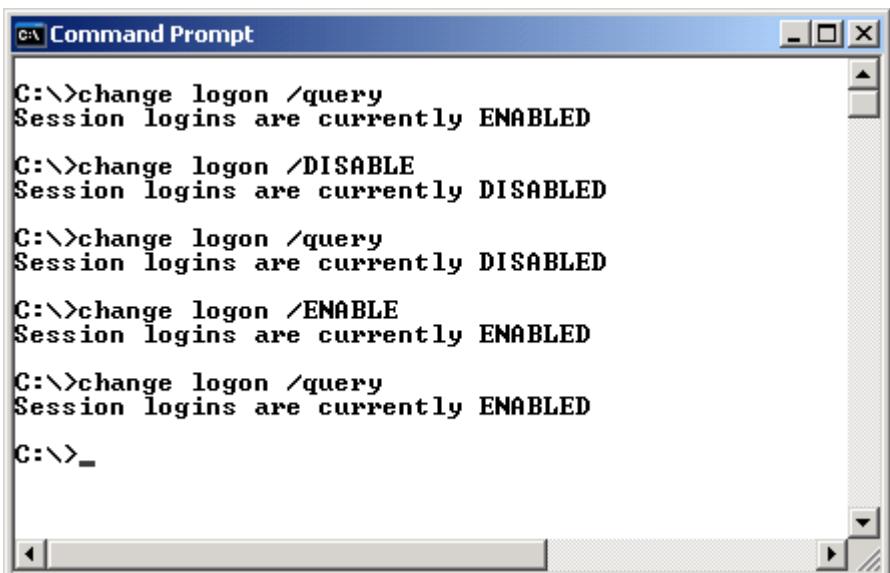
C:\>_
```

Figura 9.15 O comando change user.

Você também pode utilizar o comando change com a opção logon, conforme descrito a seguir. Esta opção é utilizada para habilitar ou desabilitar o logon de usuários via Terminal Services.

- ◆ change logon /query -> Informa em se o logon está habilitado ou desabilitado (ENABLED ou DISABLED)
- ◆ change logon /disable -> Desabilita o logon de novos usuários. As conexões dos usuários atualmente logados, serão mantidas.
- ◆ change user /enable -> Habilita novamente o logon dos usuários, via Terminal Services.

Na Figura 9.16 é exibido um exemplo de execução do comando change logon com as três opções descritas anteriormente.



```
C:\>change logon /query
Session logins are currently ENABLED

C:\>change logon /DISABLE
Session logins are currently DISABLED

C:\>change logon /query
Session logins are currently DISABLED

C:\>change logon /ENABLE
Session logins are currently ENABLED

C:\>change logon /query
Session logins are currently ENABLED

C:\>_
```

Figura 9.16 O comando change logon.

## Instalando o Office 2000 para uso através do Terminal Services.

O Microsoft Office 2000 é um excelente exemplo de aplicação que precisa de algumas configurações especiais para que possa rodar via Terminal Services. O Office 2000 foi projetado para ser utilizado por um único usuário por vez. Para que ele possa funcionar no Windows Server 2003, com o Terminal Services no modo de Compartilhamento de Aplicações, algumas modificações devem ser efetuadas.

O primeiro passo é fazer o download de algumas ferramentas do Resource Kit do Office 2000, a partir do seguinte endereço:

<http://download.microsoft.com/download/6/b/3/6b34f4c7-44e6-4d85-91d9-1acf9479da7d/orktools.exe>

Este arquivo contém ferramentas que darão suporte a instalação do Office 2000 para uso via Terminal Services, no modo de Compartilhamento de Aplicações.

Após ter feito o download do arquivo orktools.exe e de tê-lo instalado, siga os passos indicados a seguir, para instalar o Office 2000:

1. Faça o logon no servidor como administrador ou com uma conta com permissão de administrador.
2. Use a opção Adicionar ou remover Programas do Painel de controle, para iniciar a instalação do Office 2000 a partir do drive de CD.
3. Na linha de comando do arquivo de instalação, acrescente o seguinte texto na parte final, após o arquivo de instalação (.exe):

**TRANSFORMS="Caminho\termsrvr.mst"**

Onde CAMINHO é o caminho completo para a pasta onde foram instaladas as ferramentas do Resource Kit do Office 2000, descritas anteriormente. Normalmente estas ferramentas são instaladas no seguinte caminho:

**C:\Arquivos de programas\ORKTools\ToolBox\Tools\Terminal Server Tools\Termsrvr.mst**

Observe que o arquivo que fará as modificações necessárias é passado como um parâmetro para o arquivo de instalação. O arquivo de instalação do Office 2000 irá acessar as informações do arquivo Termsrvr.mst e irá utilizá-las para criar uma instalação do Office 2000, adaptada a utilização via Terminal Server no modo de Compartilhamento de aplicações.

4. Siga os passos do assistente de instalação para completar a instalação do Office 2000. Pronto, agora o Office 2000 está instalado e habilitado para ser utilizado via Terminal Server, no modo de Compartilhamento de aplicações. Agora os usuários poderão se conectar ao Terminal Server e utilizar os aplicativos do Office 2000 (Word, Excel, Access e PowerPoint) remotamente.

## Administração do Terminal Services.

Uma vez que você instalou e colocou o Terminal Services para funcionar, é hora de conhecer as ferramentas de administração e as opções de configuração disponíveis. Existem, basicamente, três consoles para administração do Terminal Services:

- ◆ **Gerenciador dos serviços de terminal:** Esta ferramenta é utilizada para monitorar e controlar as conexões com o Terminal Services. Com esta ferramenta você pode exibir todas as conexões estabelecidas com o Terminal Services.
- ◆ **Configuração dos serviços de terminal:** Esta ferramenta é executada no servidor onde o Terminal Server está instalado. É utilizada para configurar uma série de propriedades do Terminal Server, conforme você aprenderá logo em seguida.

---

**NOTA:** Caso o endereço anterior não funcione corretamente, acesse a seguinte página: <http://www.microsoft.com/office/ork/2000/appndx/toolbox.htm> e procure pela opção: "Office Resource Kit core tool set"

---

- ◆ **Licenciamento do Terminal Server:** Esta ferramenta, já utilizada anteriormente, é utilizada para ativar o Terminal Server e para configurar o número de licenças de acesso disponíveis.

A seguir você aprenderá a utilizar o console Gerenciador dos serviços de terminal e o console Configuração dos serviços de terminal.

## Gerenciando as conexões com o Gerenciador dos serviços de terminal.

Neste item mostrarei, através de um exemplo prático, como utilizar a ferramenta Gerenciador dos serviços de terminal, para executar uma série de tarefas, tais como: procurar servidores com o Terminal Server instalado, criar novas conexões, cancelar sessões e assim por diante.

Para utilizar o Gerenciador dos serviços de terminal, para executar uma série de tarefas administrativas, siga os passos indicados a seguir:

1. Faça o logon como administrador ou com uma conta com permissão de administrador, no servidor onde está instalado o Terminal Services.
2. Abra o Gerenciador dos serviços de terminal: Iniciar -> Ferramentas administrativas -> Gerenciador de serviços de terminal.
3. A primeira vez que você abre o Gerenciador dos serviços de terminal é exibida uma mensagem, indicada na Figura 9.17, avisando que algumas funcionalidades, tais como o Controle Remoto, somente estão disponíveis quando o Gerenciador dos serviços de terminal é utilizado através de uma sessão do Terminal Server, como por exemplo, quando o administrador se conecta ao servidor usando o recurso de Área de Trabalho Remota e depois de conectado, abre o Gerenciador dos serviços de terminal.

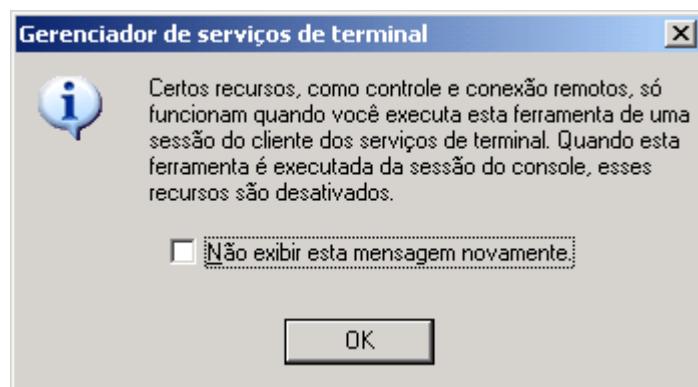
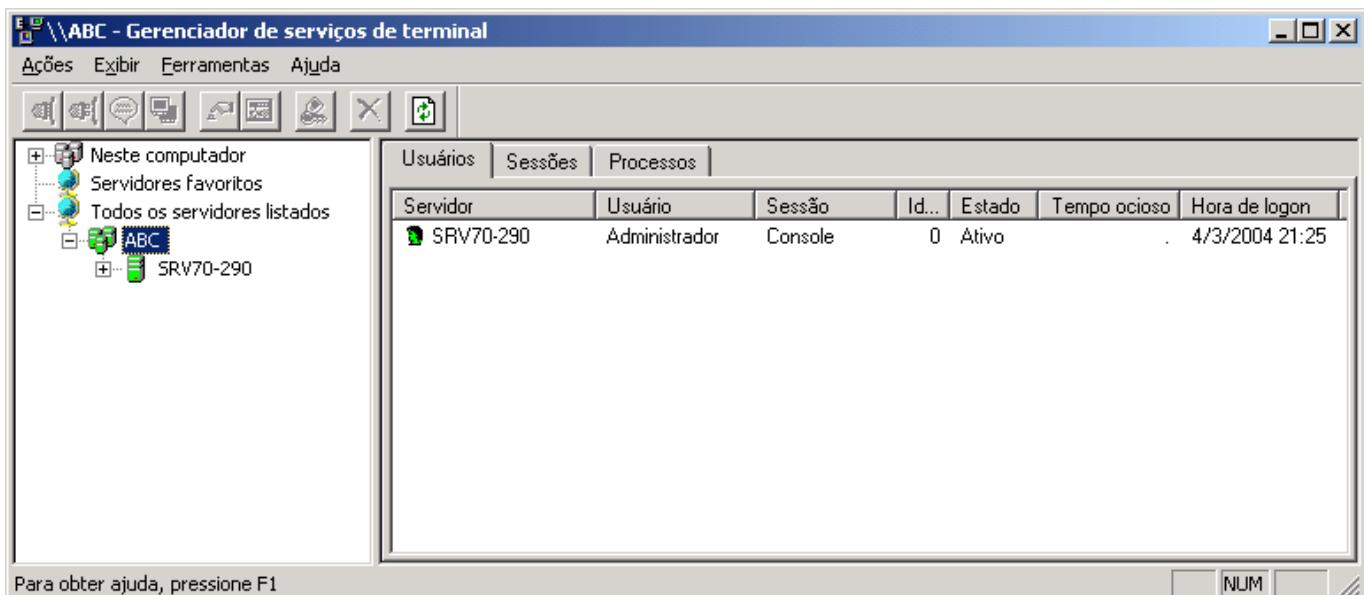


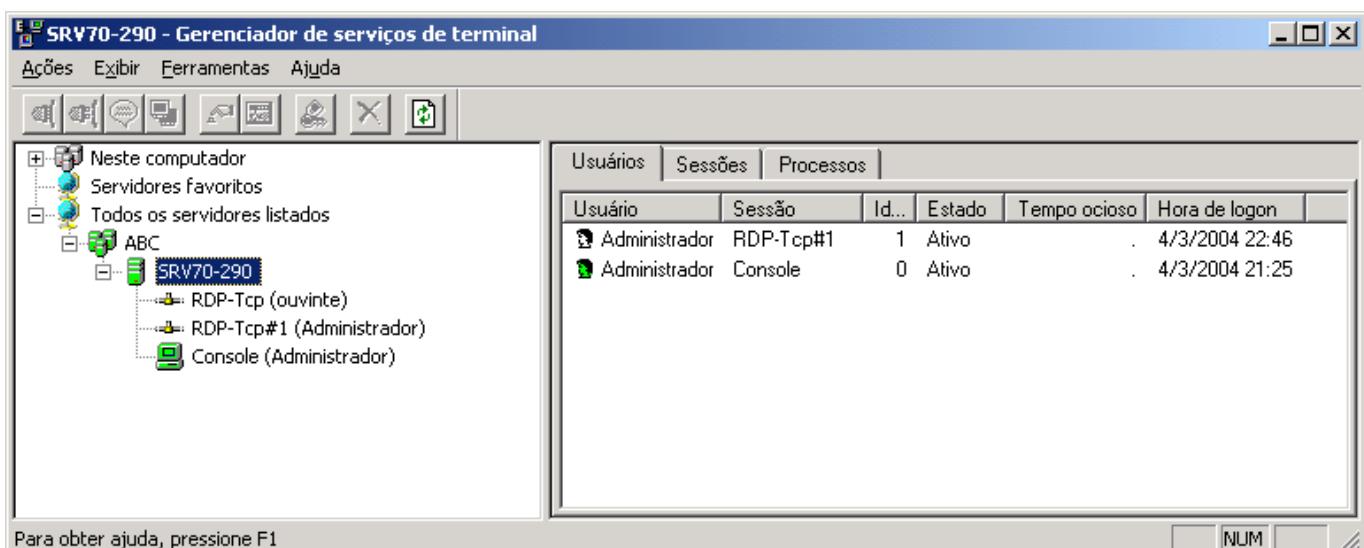
Figura 9.17 Mensagem de aviso ao abrir o Gerenciador dos serviços de terminal.

4. Marque a opção Não exibir esta mensagem novamente e clique em OK para fechar a mensagem de aviso.
5. Será exibido o console de administração do Terminal Server. Por padrão todos os servidores do domínio, que estão com o Terminal Server instalados, são adicionados a este console, conforme exemplo da Figura 9.18 (onde é exibido o único servidor do domínio, com o Terminal Server instalado):



**Figura 9.18 O console de administração do Terminal Server.**

6. Você pode fazer com que sejam exibidos todos os servidores disponíveis com o Terminal Server instalado. Para pesquisar todos os servidores com Terminal Server, na sua rede, independentemente do domínio, clique com o botão direito do mouse na opção Todos os servidores listados e, no menu de opções que é exibido, clique em Atualizar servidores em todos os domínios.
7. Para gerenciar as conexões de um servidor você deve conectar-se ao referido servidor. Para isso basta dar um clique duplo no nome do servidor, conforme exemplo da Figura 8.19, onde foi feita uma conexão com o servidor SRV70-290. A cor azul do ícone, ao lado do nome do servidor, indica que a conexão foi efetuada com sucesso. Observe que, no painel da direita, são exibidas as conexões atualmente ativas e abaixo do nome do servidor são exibidas mais opções, as quais serão descritas neste exemplo.



**Figura 9.19 Conectando-se com o servidor SRV70-290.**

8. No painel da direita estão disponíveis três guias: Usuários, Sessões e Processos. Por padrão a guia Usuários vem selecionada. No Exemplo da Figura 9.19, é exibida a lista dos usuários conectados. Observe que o usuário Administrator tem duas sessões abertas neste servidor. Uma é o logon local que ele fez, diretamente no servidor. Esta sessão é indicada pelo valor Console, na coluna Sessão. Console indica o logon local, diretamente no servidor. A outra sessão foi feita a partir de um computador com o Windows 2000 Server instalado, utilizando o Cliente de serviços de terminal e o logon também foi feito usando a conta Administrator. Esta sessão é identificada pelo valor RDP-Tcp#1, na coluna Sessão. O RDP é abreviatura de Remote Desktop Protocol, que é o protocolo utilizado para comunicação do cliente com o Terminal Server. TCP indica que este protocolo utiliza o TCP como protocolo de transporte e #1 indica que foi a primeira conexão. Ao clicar com o botão direito do mouse, em uma das sessões remotas que estão sendo exibida (do tipo RDP), serão disponibilizadas diversas opções relacionadas com a sessão, tais como: Conectar, Desconectar, Enviar uma mensagem, Redefinir, Status e Fazer logoff. Quando você desconecta uma sessão, todos os programas que estavam abertos nesta sessão continuam sendo executados, mas as entradas e saídas desta sessão não são mais transmitidos para a sessão do cliente, conectado remotamente. Se o usuário fizer a conexão novamente, receberá o mesmo ambiente que havia anteriormente, sem perda de dados. Ao desconectar uma sessão não serão liberados recursos no servidor (tais como memória e processador) e a sessão, mesmo desconectada, continuará a contar como uma licença de acesso que está sendo utilizada. O usuário somente pode desconectar suas próprias sessões e o administrador pode desconectar as sessões de qualquer usuário. Para desconectar uma sessão basta clicar com o botão direito do mouse na sessão a ser desconectada e clicar na opção Desconectar. Será exibida uma mensagem pedindo confirmação, conforme indicado na Figura 9.20:

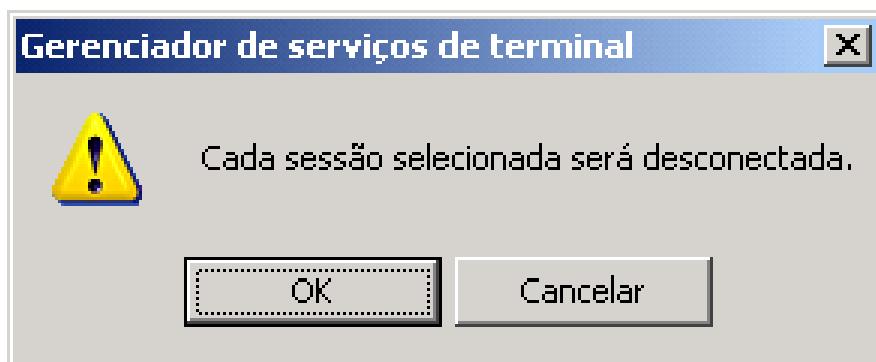


Figura 9.20 Confirmação para desconectar uma sessão.

9. Clique em OK e pronto, a sessão será desconectada. O usuário que criou a sessão também receberá, no computador onde a sessão foi inicializada, uma mensagem de que a sessão foi desconectada pelo administrador. Uma das situações práticas onde pode ser útil o recurso de desconectar sessões, é para usuários móveis. Por exemplo, um vendedor que trabalha com um notebook e quando chega em um cliente, conecta-se a rede da empresa usando o Terminal Services. Ao invés de enderrar a sessão, ele pode simplesmente desconectá-la. Ao chegar no próximo cliente, ele conecta a sessão novamente e terá exatamente o mesmo ambiente anterior, com os mesmos programas abertos e prontos para o uso. A desvantagem desta abordagem, conforme descrito anteriormente, é que as sessões desconectadas continuam ocupando recursos de hardware no servidor, uma vez que os programas de uma sessão desconectada, continuam rodando normalmente. O administrador pode desconectar várias sessões ao mesmo tempo. Para isso basta selecionar as sessões a serem desconectadas (usando as teclas Ctrl ou Shift, em combinação com o mouse, para selecionar as várias seções) e depois clicar com o botão direito do mouse em uma das sessões selecionadas e, no menu de opções que é exibido, clicar em Desconectar.

10. Você também pode exibir o status de uma sessão. Clique com o botão direito do mouse na sessão e, no menu de opções que é exibido, clique em Status. Será aberta a janela de status da sessão, onde são exibidas informações tais como: bytes recebidos, bytes enviados, frames com erro, % frames com erro e assim por diante, conforme indicado na Figura 9.21. Para fechar a janela de status basta clicar em Fechar.

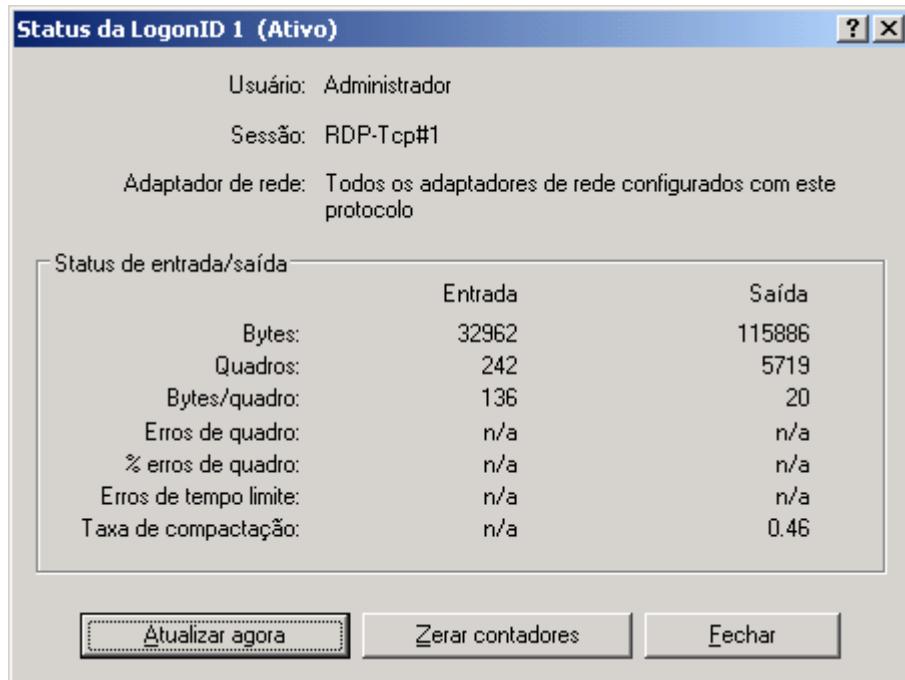
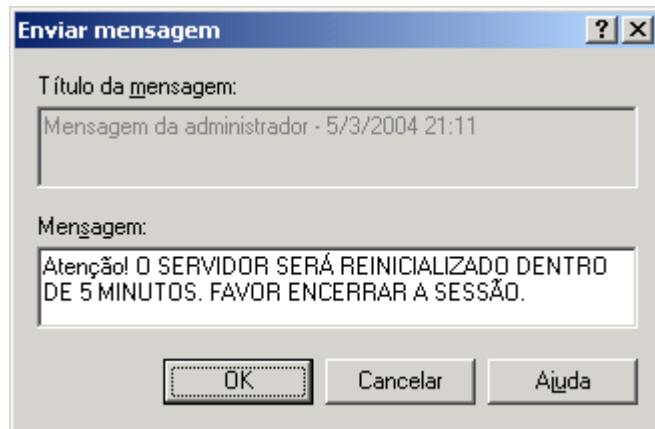


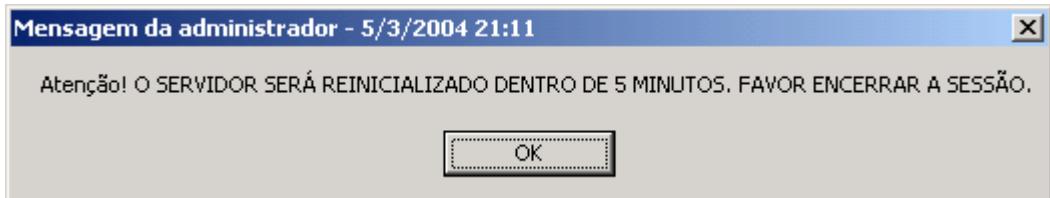
Figura 9.21 Status sobre a sessão.

11. Você também pode redefinir (resetar seria um termo mais adequado, mas acho que ainda não existe no idioma Português) uma sessão. Para isso clique com o botão direito do mouse na sessão e no menu de opções que é exibido clique em Redefinir. Ao redefinir uma sessão, pode haver perda de dados, pois todos os programas serão encerrados, o que irá liberar recursos no servidor. Será exibida uma mensagem pedindo confirmação. Clique em OK para fechar a mensagem e redefinir a sessão. O administrador pode redefinir várias sessões ao mesmo tempo. Para isso basta selecionar as sessões a serem redefinidas (usando as teclas Ctrl ou Shift, em combinação com o mouse) e depois clicar com o botão direito do mouse em uma das sessões selecionadas e, no menu de opções que é exibido, clicar em Redefinir.
12. Você pode enviar uma mensagem para os usuários que estão conectados via Terminal Services. A mensagem pode ser enviada para o usuário de uma única sessão ou para vários usuários. Para enviar a mensagem para mais de um usuário, basta selecionar as respectivas sessões. Após ter selecionado as sessões para as quais serão enviadas mensagens, clique com o botão direito do mouse em uma das seções selecionadas e, no menu de opções que é exibido, clique em Enviar mensagem. Será aberta a janela Enviar mensagem. Digite a mensagem a ser enviada, conforme exemplo da Figura 9.22:



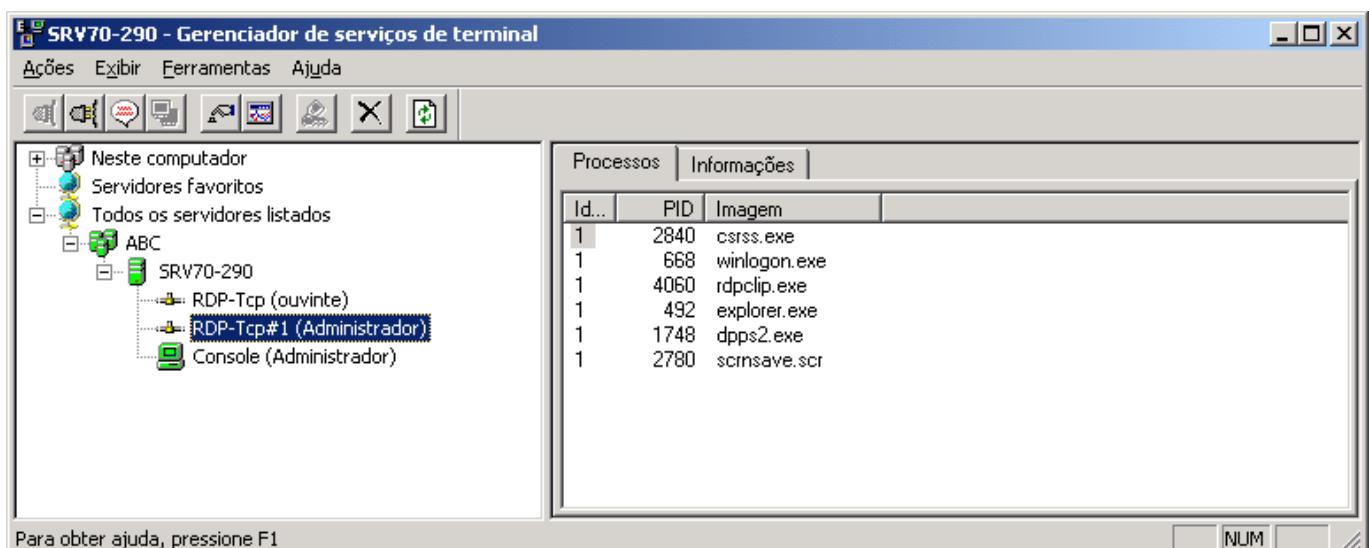
**Figura 9.22 Enviando uma mensagem**

13. Clique em OK e pronto, os usuários das sessões selecionadas, receberão a mensagem, conforme exemplo da Figura 9.23:



**Figura 9.23 Mensagem recebida pelo usuário.**

14. Você também pode exibir informações sobre os processos que estão em execução por uma determinada sessão. Para isso basta dar um clique no sinal de +, ao lado do nome do servidor. Abaixo do servidor será exibida a lista das sessões do servidor. Clique na seção para a qual você deseja exibir os processos. No painel da direita serão exibidas as guias Processos e Informação. A guia Processos já vem selecionada por padrão e exiba a listagem de processos em execução pela respectiva sessão, conforme exemplo da Figura 9.24:



**Figura 9.24 Processos em execução por uma determinada sessão.**

15. Estas informações também podem ser exibidas a nível de servidor ou de todos os servidores do domínio. Por exemplo, se você clicar no nome de um servidor, no painel da direita serão exibidas as guias Usuários, Sessões e Processos. A guia Usuários exibirá a lista de todos os usuários com sessões abertas com o servidor selecionado no painel da esquerda. A guia Sessões exibirá a lista de todas as sessões do servidor e a guia Processos exibirá a lista de todos os processos de todas as sessões do servidor. Se você clicar no nome do domínio, serão exibidas as mesmas guias: Usuários, Sessões e Processos, porém em cada guia, serão exibidas informações sobre todo o domínio. Por exemplo, quando um domínio está selecionado e você clica na guia Sessões, será exibida a listagem de todas as sessões em todos os servidores Terminal Server do domínio.
16. Feche o console de Administração do Terminal Server.

## Configurações do Terminal Server.

Neste item mostrarei, através de um exemplo prático, como utilizar a ferramenta Configuração dos serviços de terminal. Com esta ferramenta você pode definir uma série de configurações para o Terminal Server.

Para configurar o Terminal Server, utilizando o console Configuração dos serviços de terminal, siga os passos indicados a seguir:

1. Faça o logon como administrador ou com uma conta com permissão de administrador.
2. Abra o console Configuração dos serviços de terminal: Iniciar -> Ferramentas administrativas -> Configuração dos serviços de terminal.
3. Será aberto o console de configuração do Terminal Server, com as opções Conexões e Configurações do servidor disponíveis, conforme indicado na Figura 9.25.:

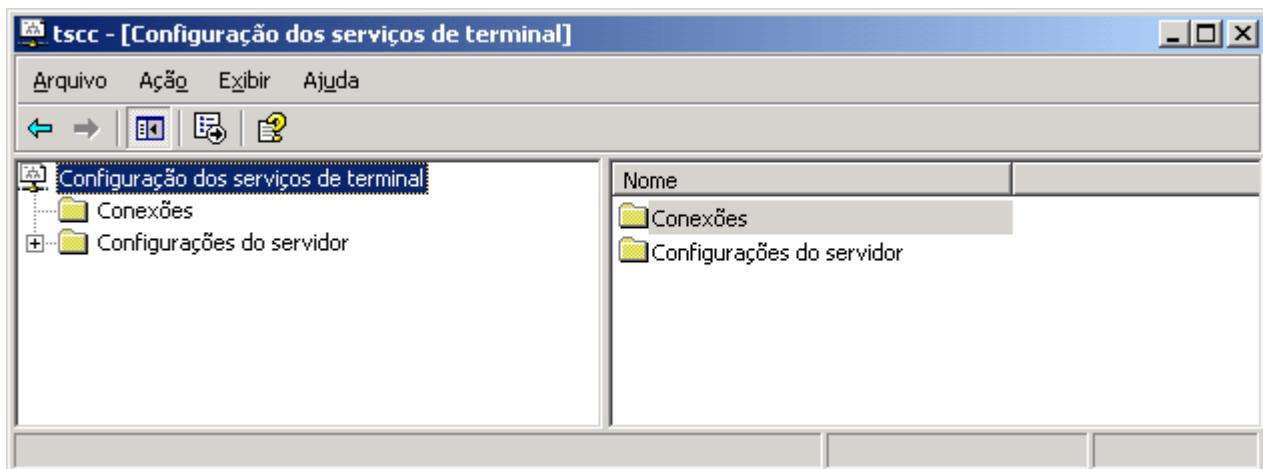


Figura 9.25 O console de configuração do Terminal Server.

4. A maioria das configurações disponíveis são feitas através da opção Conexões. Clique na opção Conexões. No painel da direita será exibida a opção RDP-Tcp. Clique com o botão direito do mouse nesta opção. No menu de opções que é exibido, clique em Propriedades. Será aberta a janela de propriedades, na qual você pode definir uma série de propriedades que serão aplicadas às conexões do Terminal Server. Por padrão, a guia Geral vem selecionada, conforme indicado na Figura 9.26:

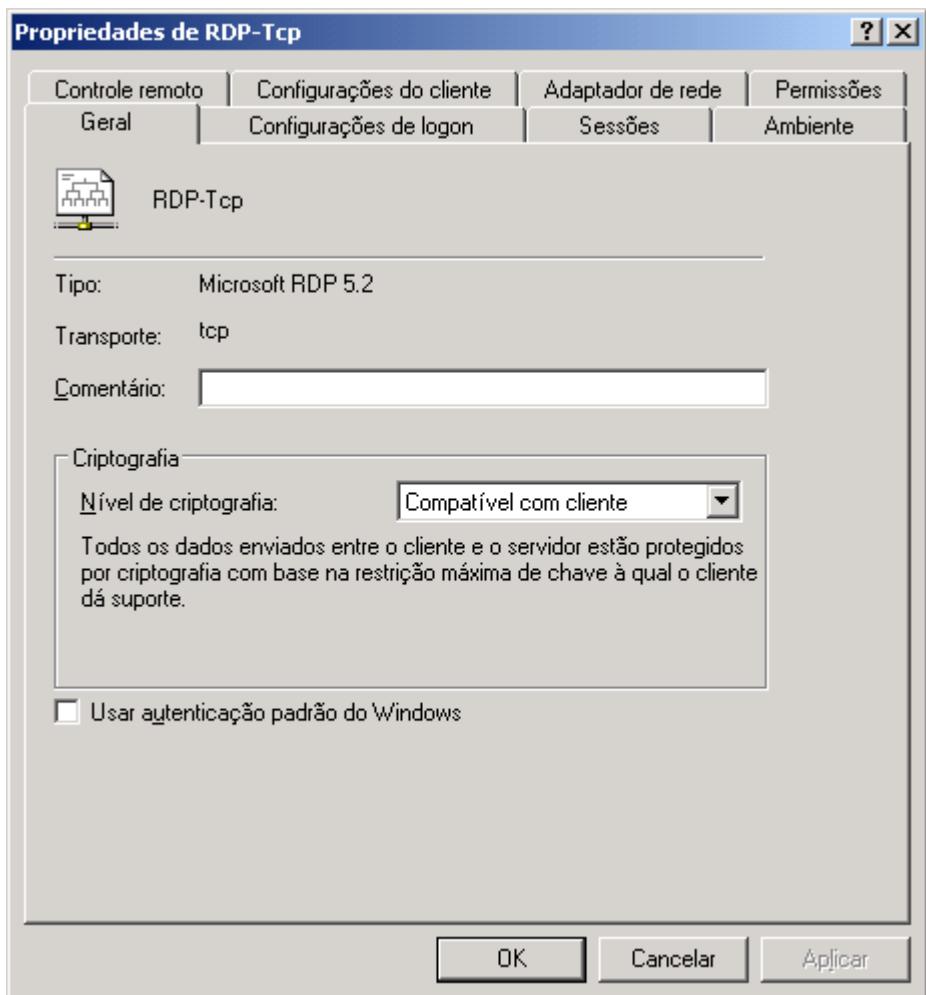


Figura 9.26 A guia Geral de Propriedades.

Nesta guia estão disponíveis as seguintes opções de configuração:

- ◆ **Comentário:** Fornece um espaço para que você insira informações sobre as conexões, como por exemplo: Conexões no domínio ABC.
- ◆ **Nível de criptografia:** Lista os níveis disponíveis de criptografia usados para proteger os dados enviados entre o cliente e o servidor. Todos os níveis utilizam a criptografia RSA RC4. O nível Client Compatible (Compatível com o cliente), faz a criptografia dos dados trocados entre o cliente e o servidor, usando o tamanho máximo de chave suportado pelo cliente. Este nível é aconselhável para ambientes que tem uma variedade diferente de clientes se conectando com o Terminal Services, tais como diferentes versões do Windows, Linux, Macintosh e assim por diante. O nível Baixo criptografa dados enviados do cliente para o servidor usando uma chave de 40 bits ou de 56 bits. O Terminal Server usa uma chave de 56 bits quando os clientes do Windows 2000 ou XP se conectam e uma chave de 40 bits quando a conexão é efetuada com versões anteriores do cliente. Essa criptografia baseada em entrada é usada para proteger dados confidenciais como, por exemplo, a senha de um usuário. O nível Médio criptografa dados enviados do cliente para o servidor e do servidor

**IMPORTANTE:** Para o exame, você deve conhecer bem as opções de configuração da opção RDP-Tcp.

para o cliente usando uma chave de 40 bits ou de 56 bits. O Terminal Services usa uma chave de 56 bits quando os clientes do Windows 2000 ou XP se conectam e uma chave de 40 bits quando a conexão é efetuada com versões anteriores do cliente. Use a criptografia média para assegurar os dados confidenciais quando eles forem transportados pela rede para exibição em clientes remotos. Se você estiver nos Estados Unidos ou Canadá, poderá selecionar o nível Alto, que criptografa dados enviados do cliente para o servidor e do servidor para o cliente usando a criptografia de 128 bits de alta segurança.

- ◆ **Usar autenticação padrão do Windows:** Especifica se o padrão da conexão será a autenticação padrão do Windows quando um outro pacote de autenticação estiver instalado no servidor.

5. Defina as opções desejadas e dê um clique na guia Configurações de logon. Serão exibidas as opções indicadas na Figura 9.27:

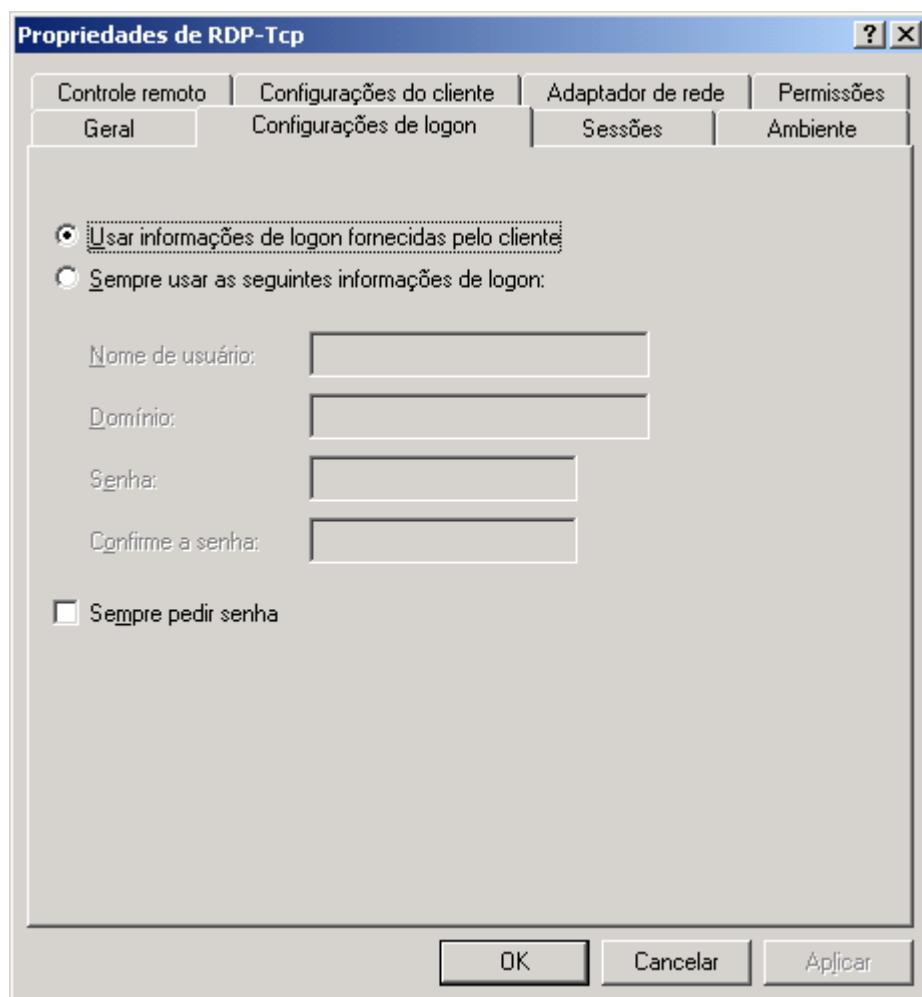


Figura 9.27 A guia de configurações de logon, das Propriedades da sessão.

Nesta guia estão disponíveis as seguintes opções de configuração:

- ◆ **Usar informações de logon fornecidas pelo cliente:** Esta é a opção marcada por padrão. Especifica que as configurações de logon são recuperadas do cliente. As configurações do cliente são definidas no Gerenciador de conexões de cliente.

- ◆ **Sempre usar as seguintes informações de logon:** Ao marcar esta opção você poderá definir as informações de logon a serem utilizadas. Ao marcar esta opção, serão habilitados os campos para que você digite o nome de uma conta, domínio e a respectiva senha (duas vezes). As informações fornecidas serão utilizadas para efetuar o logon em todas as sessões.
  - ◆ **Sempre pedir senha:** Especifica se o usuário sempre será solicitado a fornecer uma senha antes de efetuar logon no servidor.
6. Defina as opções desejadas e dê um clique na guia Sessões. Serão exibidas as opções indicadas na Figura 9.28:

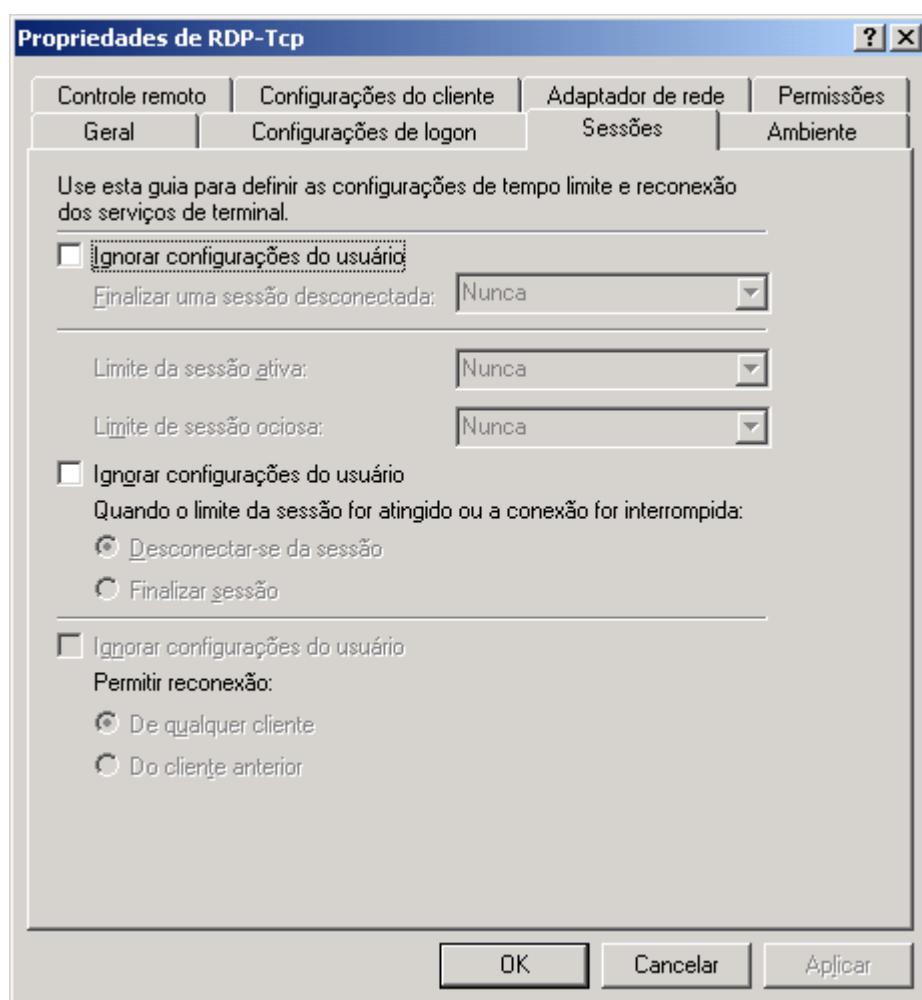


Figura 9.28 A guia Sessões.

Nesta guia estão disponíveis as seguintes opções de configuração:

- ◆ **Primeira opção - Ignorar configurações do usuário:** Especifica se serão substituídas as configurações definidas por padrão na conta do usuário (Guia Terminal Services). Ao marcar esta opção, serão habilitadas as listas: Finalizar uma sessão desconectada, Limite de sessão ativa e Limite de sessão ociosa.

---

**IMPORTANTE:** Saiba que é possível sobreescrivar as configurações definidas nas propriedades da conta do usuário, em relação ao Terminal Server. Também é importante que você conheça bem, as opções da guia Sessões. Estes são tópicos importantes para o Exame 70-290.

---

Na lista Finalizar uma seção desconectada, você pode digitar ou selecionar o tempo máximo que uma sessão desconectada permanecerá no servidor. Quando o tempo limite é alcançado, a sessão desconectada será encerrada. Quando uma sessão é encerrada, ela é excluída permanentemente do servidor. Selecione Nunca para permitir que as sessões desconectadas permaneçam no servidor indefinidamente. Você pode selecionar o espaço de tempo ou digitar o número de minutos, horas ou dias na caixa. Especifique as unidades de tempo usando m para minutos, h para horas e d para dias. O tempo máximo que pode ser especificado é de 49 dias e 17 horas. Não é uma boa prática permitir que sessões desconectadas permaneçam por muito tempo no servidor, antes de serem finalizadas, pois isso faz com que sejam ocupados recursos (memória e processador), do servidor. Pode haver situações onde o tempo de resposta do servidor fica extremamente elevado, devido a um grande número de sessões desconectadas, que continuam ocupando recursos do servidor. Nestas situações, a solução indicada é diminuir o tempo para que uma seção desconectada seja finalizada.

Na lista Limite de sessão ativa, você pode digitar ou selecionar o tempo máximo que uma sessão de usuário pode permanecer ativa no servidor. Quando o tempo limite for alcançado, o usuário será desconectado da sessão ou a sessão será encerrada. Quando uma sessão é encerrada, ela é excluída permanentemente do servidor. Selecione Nunca para permitir que a sessão continue indefinidamente. Você pode selecionar o espaço de tempo ou digitar o número de minutos, horas ou dias na caixa. Especifique as unidades de tempo usando m para minutos, h para horas e d para dias. O tempo máximo que pode ser especificado é de 49 dias e 17 horas.

Na lista Limite de sessão ociosa, você pode digitar ou selecionar o tempo máximo que uma sessão ociosa (sessão sem atividade do cliente) permanece no servidor. Quando o tempo limite é alcançado, o usuário é desconectado da sessão ou a sessão é encerrada. Quando uma sessão é encerrada, ela é excluída permanentemente do servidor. Selecione Nunca para permitir que as sessões desconectadas permaneçam no servidor indefinidamente. Você pode selecionar o espaço de tempo ou digitar o número de minutos, horas ou dias na caixa. Especifique as unidades de tempo usando m para minutos, h para horas e d para dias. O tempo máximo que pode ser especificado é de 49 dias e 17 horas.

- ◆ **Segunda opção - Ignorar configurações do usuário:** Ao selecionar esta opção, serão habilitadas opções para você definir qual deve ser o comportamento do Terminal Server quando o limite de tempo da sessão for atingido ou a conexão for interrompida, sobrescrevendo as opções definidas nas propriedades da conta do usuário, no domínio. Ao marcar esta opção, serão habilitadas as opções a seguir:
  - ◆ **Desconectar-se da seção:** Esta opção especifica que o usuário será desconectado da sessão quando o limite da sessão for alcançado ou quando a conexão for interrompida.
  - ◆ **Encerrar a sessão:** Esta opção especifica que uma sessão será encerrada quando seu tempo limite for alcançado ou a conexão for interrompida. Quando uma sessão é encerrada, ela é excluída permanentemente do servidor.
  - ◆ **Terceira opção – Ignorar configurações do usuário - Permitir reconexão:** Ao selecionar esta opção, serão habilitadas opções para você definir qual deve ser o comportamento do Terminal Server em relação à reconexões, sobrescrevendo as opções definidas nas propriedades da conta do usuário, no domínio. Ao marcar esta opção, serão habilitadas as opções a seguir
  - ◆ **De qualquer cliente:** Esta opção especifica que os usuários têm permissão para reconectar-se com uma sessão desconectada a partir de qualquer computador. Por padrão, Serviços de terminal permite a reconexão com uma sessão desconectada em qualquer computador.
  - ◆ **Do cliente anterior:** Esta opção especifica que os usuários têm permissão para reconectar-se com uma sessão desconectada apenas a partir do computador no qual a sessão teve origem. Essa opção somente oferece suporte a clientes Citrix ICA que fornecem um número de série ao conectar-se.

7. Defina as opções desejadas e dê um clique na guia Ambiente. Serão exibidas as opções indicadas na Figura 9.29:

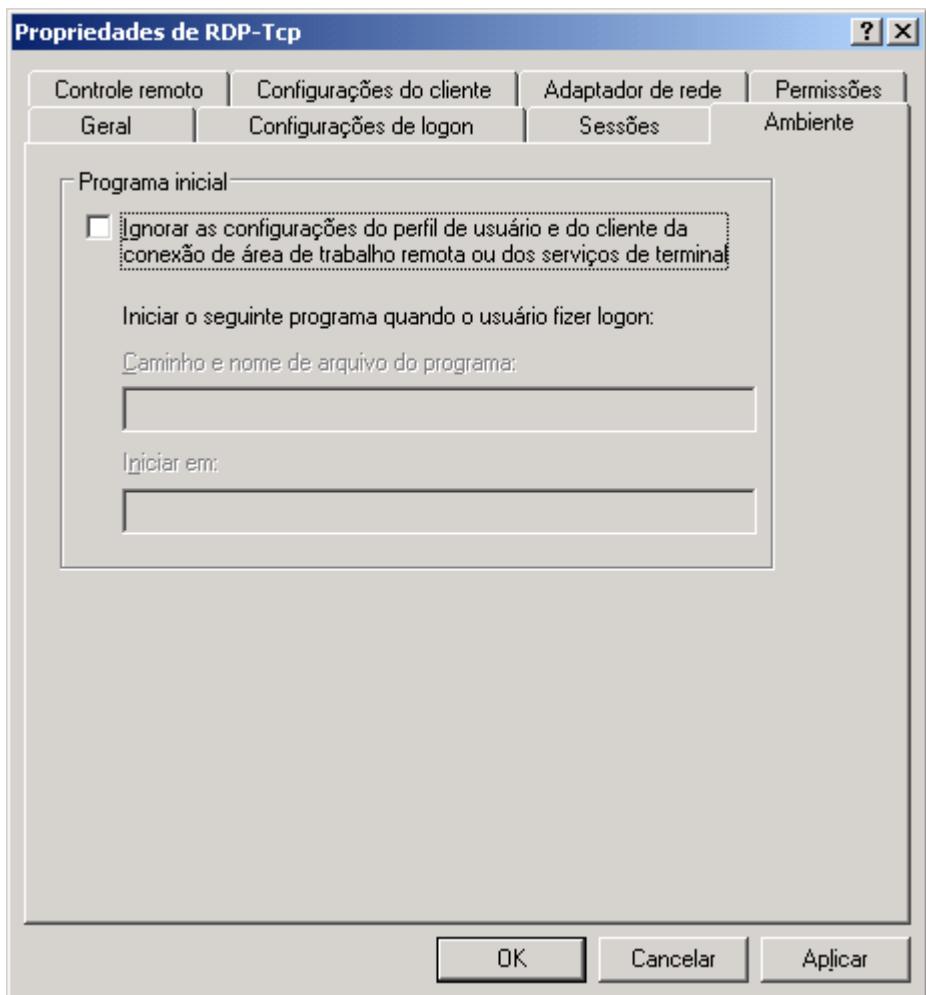


Figura 9.29 A guia de Ambiente.

Nesta guia estão disponíveis as seguintes opções de configuração:

- ◆ Ignorar configurações do perfil do usuário e do cliente da conexão da área de trabalho remota ou dos serviços de terminal: Define que devem ser ignoradas as configurações do ambiente, definidas no cliente, como por exemplo as configurações definidas na guia Ambiente, da janela de propriedades da conta do usuário. Ao marcar esta opção serão habilitados dois campos, um para que você digite o nome de um programa a ser executado quando a sessão é iniciada e outro para informar a pasta onde está o referido programa.
8. Defina as opções desejadas e dê um clique na guia Controle Remoto. Serão exibidas as opções indicadas na Figura 9.30:

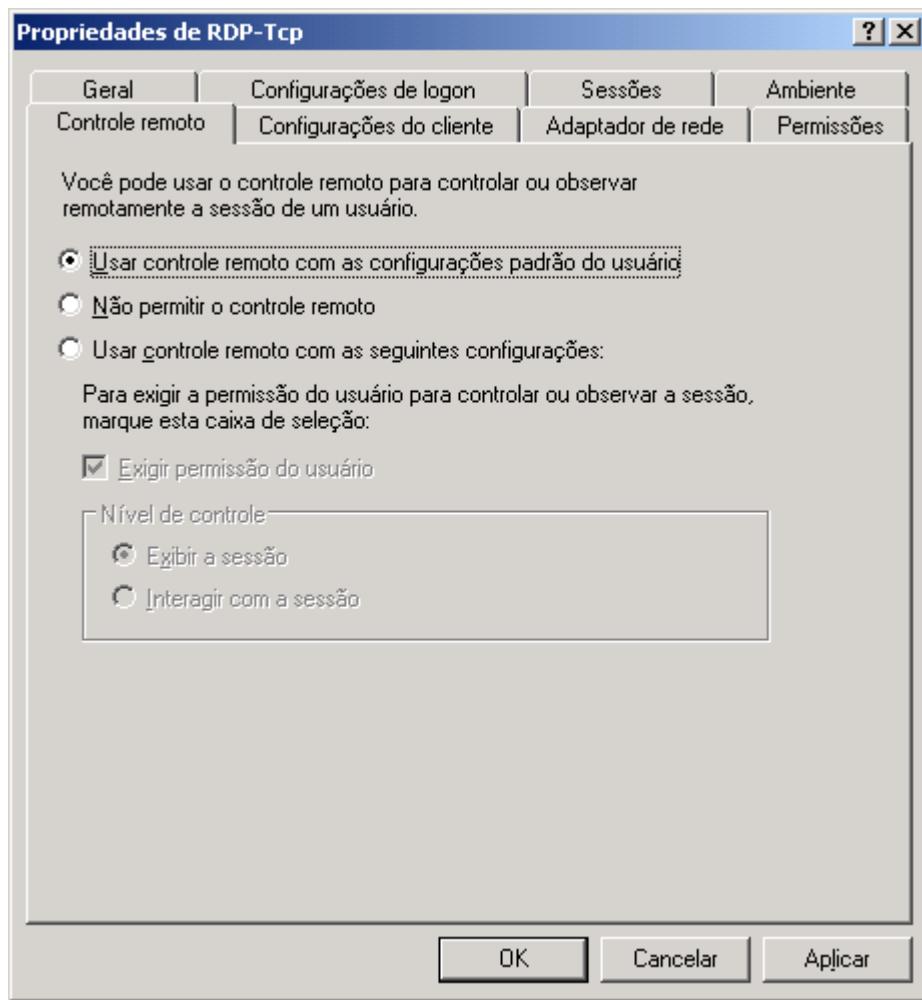
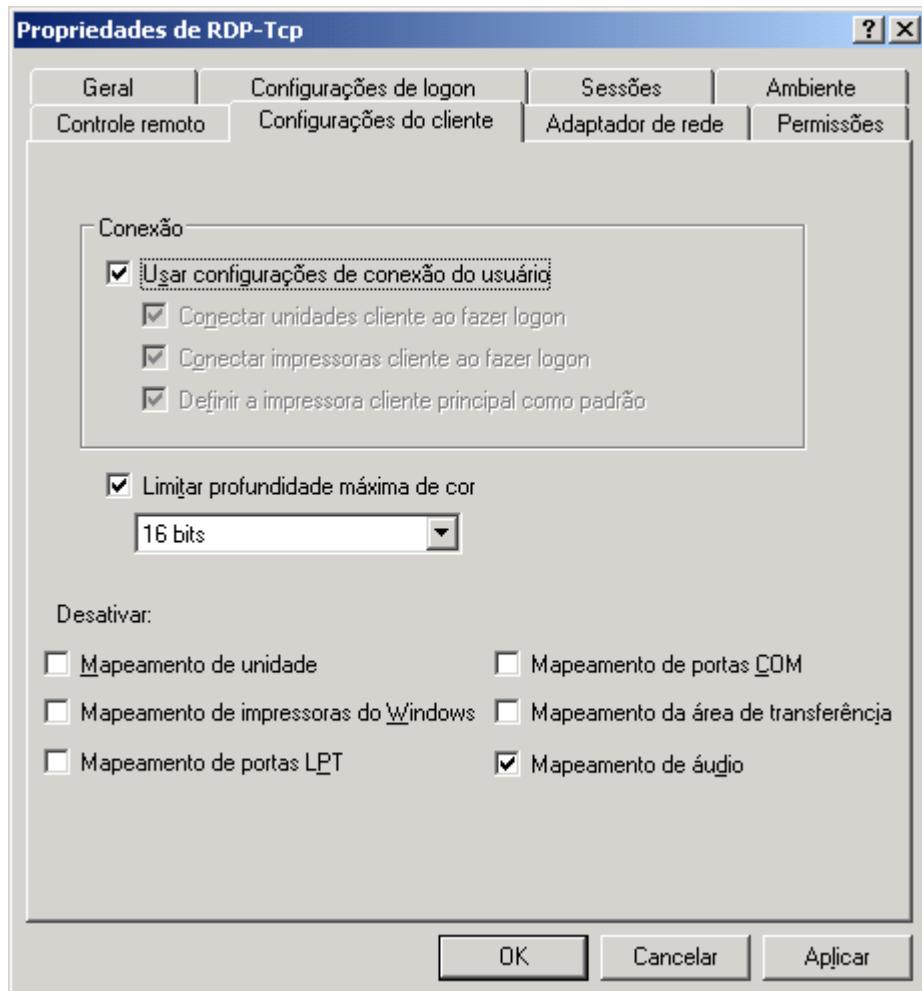


Figura 9.30 A guia Controle remoto.

O controle remoto é um recurso que permite ao administrador tomar o controle de uma sessão do usuário e ter acesso ao mesmo console que está sendo exibido ao usuário. Ao fazer o controle remoto, o administrador também terá o controle do mouse e do teclado do usuário. Na prática é como se o administrador estivesse sentado em frente ao computador no qual o usuário iniciou a sessão. O controle remoto é uma excelente ferramenta para suporte remoto. Pode ser habilitado ou desabilitado a nível de usuário, na guia Remoto da janela de propriedades da conta do usuário. Nesta guia estão disponíveis as seguintes opções de configuração:

- ◆ **Usar o controle remoto com as configurações padrão do usuário:** Esta opção especifica que as configurações de controle remoto serão recuperadas das configurações definidas nas propriedades da conta do usuário.
- ◆ **Não permitir o controle remoto:** Desabilita a funcionalidade de controle remoto.
- ◆ **Usar o controle remoto com as seguintes configurações:** Especifica que o controle remoto será permitido na conexão e permitirá a definição de configurações de acesso remoto. A configuração do controle remoto em cada conexão afetará todas as sessões que utilizam a conexão. Ao marcar esta opção, serão habilitadas as seguintes configurações adicionais:
- ◆ **Exigir permissão do usuário:** Especifica se será exigida a permissão de usuário para controlar a sessão remotamente. Quando esta opção for marcada, uma mensagem será exibida para o cliente, solicitando permissão para que o administrador possa visualizar ou participar da sessão, controlando-a remotamente.
- ◆ **Nível de controle – Exibir a sessão:** Especifica que a sessão do usuário apenas poderá ser visualizada.

- ◆ **Nível de controle – Interagir com a sessão:** Especifica que a sessão do usuário poderá ser controlada ativamente com o teclado e o mouse, pelo administrador.
9. Defina as opções desejadas e dê um clique na guia Configurações do cliente. Serão exibidas as opções indicadas na Figura 9.31:



**Figura 9.31 A guia Configurações do cliente.**

Com as opções desta guia você define uma série de configurações relacionadas ao cliente que está criando a sessão. Nesta guia estão disponíveis as seguintes opções de configuração:

- ◆ **Usar configurações de conexão do usuário:** Esta opção define se as configurações de conexão, definidas nas propriedades da conta do usuário serão utilizadas. Ao desmarcar esta opção, serão habilitadas as seguintes configurações adicionais:
- ◆ **Conectar unidades cliente ao efetuar o logon:** Essa opção define se todos os drives de rede, mapeados pelo usuário, devem ser reconectados automaticamente durante o logon.
- ◆ **Conectar impressoras cliente ao efetuar o logon:** Essa opção define que as impressoras de rede, do cliente, devem ser reconectadas automaticamente, durante o logon.
- ◆ **Definir a impressora cliente principal como padrão:** Define a impressora padrão do cliente como sendo também a impressora padrão para a sessão. Ou seja, se dentro da sessão, o usuário enviar alguma impressão, esta será

enviada para a impressora definida como padrão, no computador a partir do qual o usuário se conectou ao Terminal Server.

- ◆ **LIMITAR PROFUNDIDADE MÁXIMA DE COR:** Define o número máximo de cores, para configuração da tela, que pode ser utilizada através de uma sessão com o Terminal Services.
- ◆ **Desativar o seguinte:** Neste grupo estão disponíveis uma série de opções para desabilitar recursos específicos, tais como:
  - ◆ **Mapeamento de unidade:** Marque esta opção para desabilitar o mapeamento de drivers do cliente.
  - ◆ **Mapeamento de impressoras do Windows:** Especifica se o mapeamento da impressora cliente do Windows será desativado. Por padrão, esse recurso está desmarcado (ativado). Quando ativado (desmarcado), os clientes podem mapear as impressoras do Windows e todas as filas da impressora cliente serão reconectadas automaticamente quando for efetuado logon. No entanto, quando os mapeamentos de porta LPT e COM forem desativados (marcados), não será possível criar as impressoras manualmente. Quando desativado (marcado), os clientes não poderão mapear as impressoras do Windows e as filas da impressora cliente não serão reconectadas quando for efetuado logon. Entretanto, será possível reconectar impressoras manualmente se o mapeamento de porta LPT ou COM estiver ativado (desmarcado).
  - ◆ **Mapeamento de portas LPT:** Especifica se o mapeamento de porta LPT de cliente será desativado. Por padrão, esse recurso está desmarcado (ativado). Quando ativado (desmarcado), as portas LPT do cliente serão mapeadas automaticamente para impressão e estarão disponíveis na lista de portas do Assistente para adicionar impressora. Será preciso criar manualmente a impressora para a porta LPT usando o Assistente para adicionar impressora. Quando desativado (marcado), as portas LPT do cliente não serão mapeadas automaticamente. Você não poderá criar manualmente impressoras usando portas LPT.
  - ◆ **Mapeamento de portas COM:** Especifica se o mapeamento de porta COM de cliente será desativado. Por padrão, este recurso está desmarcado (ativado). Quando ativado (desmarcado), as portas COM de cliente serão mapeadas automaticamente para impressão e estarão disponíveis na lista de portas do Assistente para adicionar impressora. Será preciso criar manualmente a impressora para a porta COM usando o Assistente para adicionar impressora. Quando desativado (marcado), as portas COM de cliente não serão mapeadas automaticamente. Você não poderá criar manualmente impressoras para portas COM.
  - ◆ **Mapeamento da área de transferência:** Especifica se o mapeamento da área de transferência do cliente será desativado. Por padrão, este recurso está desmarcado (ativado).
  - ◆ **Mapeamento de áudio:** Define se o mapeamento de áudio do cliente deve ou não ser desabilitado.

10. Defina as opções desejadas e dê um clique na guia Adaptador de rede. Serão exibidas as opções indicadas na Figura 9.32.

Nesta guia você define se para efetuar conexões via Terminal Services, estarão disponíveis todos os adaptadores de rede do servidor ou somente um adaptador específico (lista Adaptador de rede). Você também pode definir que o servidor aceita um número ilimitado de conexões (Conexões ilimitadas) ou pode limitar o número de conexões, clicando na opção Nº Máximo de conexões e definindo o número de conexões no campo ao lado desta opção.

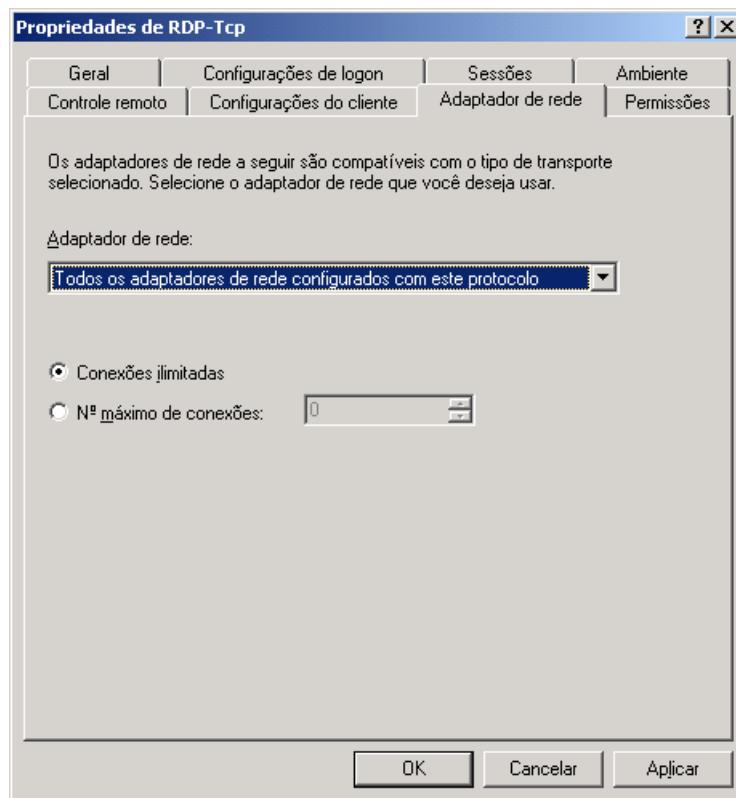


Figura 9.32 A guia Adaptador de rede.

11. Defina as opções desejadas e dê um clique na guia Permissões. Serão exibidas as opções indicadas na Figura 9.33:

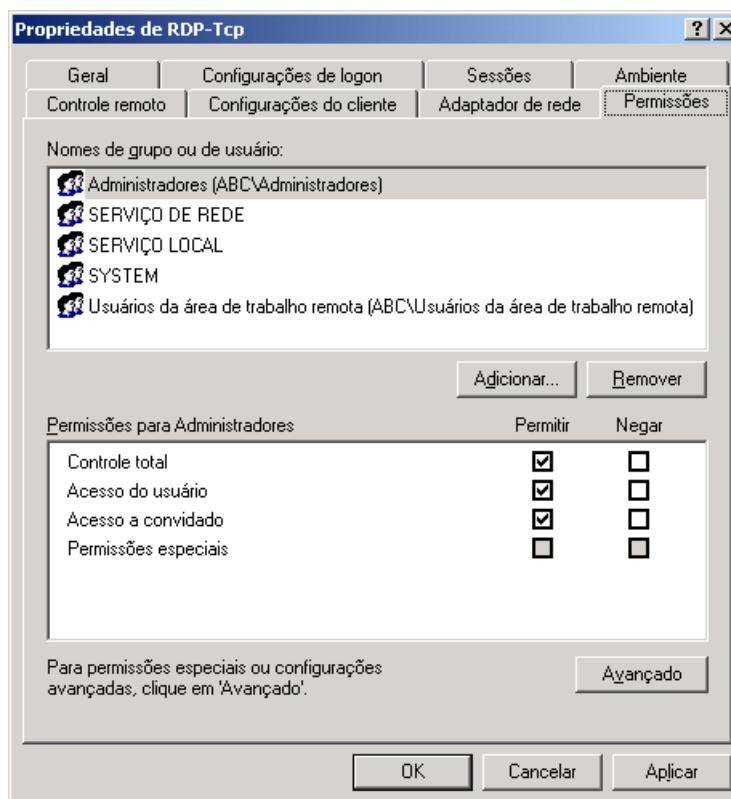


Figura 9.33 A guia Permissões.

Esta guia apresenta uma lista de controle de acesso (ACL – Access Control List), semelhante a lista que é apresentada, para controle das permissões de acesso em pastas e arquivos de um volume formatado com NTFS. Nesta guia você define quais usuários e grupos terão permissões de acesso as sessões do Terminal Services e qual o nível de acesso dos usuários e grupos que tem permissão de acesso.

12. Defina as opções desejadas e dê um clique em OK para aplicar as configurações efetuadas.
13. No painel da esquerda, clique na opção Configurações do servidor). Serão exibidas as opções indicadas na Figura 9.34 e descritas logo a seguir.

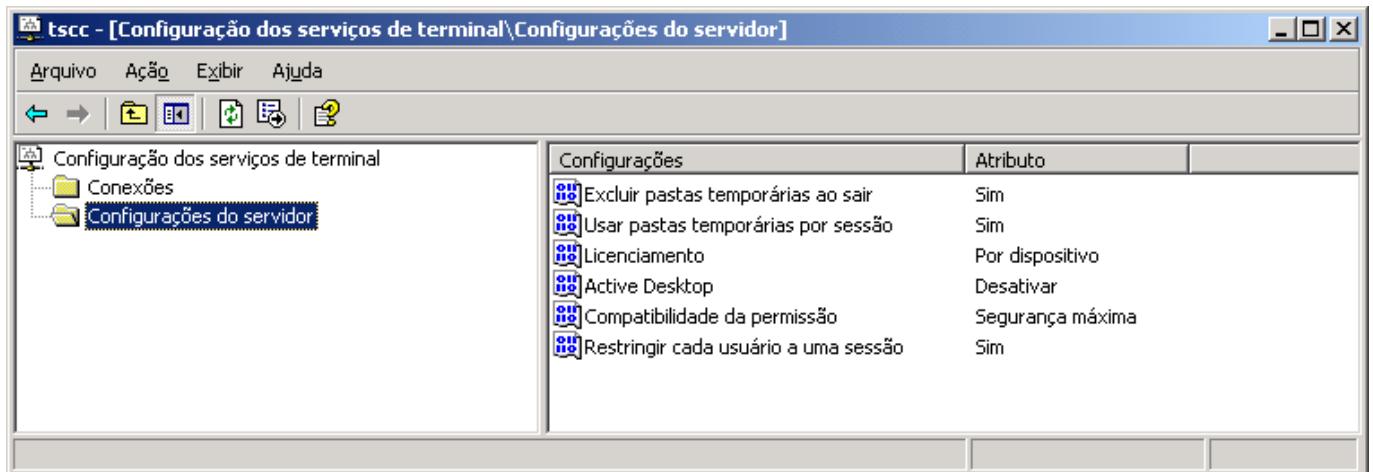


Figura 9.34 Opções de Configurações do servidor.

Estão disponíveis as seguintes opções de configurações do servidor:

- ◆ **Excluir pastas temporárias ao sair:** Define se as pastas temporárias devem ou não ser excluídas ao encerrar a sessão. O padrão é Sim. Para alterar esta configuração basta dar um clique duplo sobre ela. Será exibida a janela com os valores que podem ser definidos para esta opção (no caso Sim ou Não), conforme exemplo da Figura 9.35. Clique no valor desejado e depois em OK. Este procedimento é utilizado para configurar o valor de qualquer uma das opções de configuração do servidor, ou seja, clique duplo para abrir a janela de opções. Depois clique no valor desejado para marcá-lo e clique em OK para aplicá-lo.

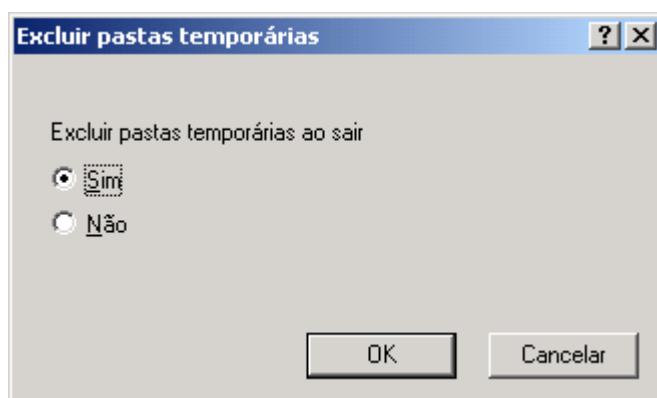


Figura 9.35 Definindo valores para a opção.

- ◆ **Usar pastas temporárias por sessão:** Por padrão está habilitada (Sim). Quando habilitada faz com que seja criada uma pasta temporária separada para cada sessão com o terminal services.

- ◆ **Licenciamento:** Esta opção permite que você defina o modo de licenciamento: Per device ou Per user. Para maiores detalhes sobre as diferenças entre estes dois tipos de licenciamento, consulte o Capítulo 1.
- ◆ **Active Desktop:** Esta opção está desabilitada (Desativar), por padrão. Quando esta opção for habilitada, os usuários poderão utilizar os recursos do Active Desktop ao se conectar ao Terminal Services. Desabilite esta opção para reduzir o tráfego de rede nas sessões do Terminal Services.
- ◆ **Compatibilidade de permissão:** Esta opção permite que você escolha entre Segurança máxima e Segurança reduzida. Somente use Segurança reduzida, se você utiliza aplicações antigas, que dependem de acesso completo a Registry do sistema. Embora o mais indicado é que estas aplicações sejam substituídas.
- ◆ **Restringir cada usuário a uma única sessão:** Quando esta opção está habilitada (que é o padrão), cada usuário poderá criar uma única sessão, ao mesmo tempo, com o Terminal Services.

14. Defina as configurações de servidor desejadas e feche o console de configuração do Terminal Services.

Bem, sobre Terminal Services era isso. A seguir você aprenderá alguns tópicos sobre a Assistência Remota, tópicos estes relevantes para o Exame 70-280.

## O Recurso de Assistência Remota.

Neste tópico apresentarei uma breve descrição do recurso de Assistência Remota, focando nos tópicos mais importantes para o Exame 70-290.

A assistência remota permite que uma pessoa de confiança (um amigo, uma pessoa do suporte ou um administrador do setor de informática) auxilie de forma remota e ativa uma outra pessoa com problema no computador. O assistente (também chamado de especialista) poderá ver a tela do usuário que está solicitando assistência e dar algum conselho. Com a permissão do usuário, o assistente poderá inclusive assumir o controle do computador do usuário e executar tarefas remotamente.

Por exemplo, imagine que você tem em uma das filiais da empresa, um servidor com o Windows 2003 Server instalado e que este servidor não faz parte do domínio. Vamos supor que o Administrador local está enfrentando problemas e gostaria de ter a ajuda do Administrador da matriz da empresa. Como o servidor da filial não faz parte do domínio, não será possível para o Administrador da filial, logar remotamente (a não ser que ele conheça a senha de Administrador local, do servidor da filial). Nesta situação, o Administrador da filial pode enviar um convite para o Administrador da matriz, solicitando uma assistência remota. O Administrador da filial, define o nível de acesso que o administrador da Matriz irá ter. Os níveis possíveis são somente ter acesso a tela do servidor remoto ou poder assumir o controle, tendo acesso ao controle do teclado e do mouse do servidor remoto.

Porém o uso mais comum do recurso de Assistência Remota é para fornecer suporte aos usuários da rede. Você pode utilizar este recurso, para que os usuários (de estações baseadas no Windows XP, uma vez que este recurso não está disponível no Windows 2000) solicitem assistência remota para um técnico da equipe de suporte. O técnico poderá ter acesso a tela do usuário ou, dependendo das políticas de segurança da empresa e da permissão do usuário, o técnico poderá inclusive assumir o controle do mouse e do teclado. Como o recurso de assistência remota gera pouco tráfego de rede, este recurso pode, inclusive, ser utilizado para fornecer suporte técnico a distância, onde os técnicos da filial da empresa, prestam assistência técnica remota, para uma ou mais filiais. É um recurso realmente importante e que, certamente, economiza dinheiro com viagens, diárias e, principalmente, com o tempo para solução dos problemas. Com o uso da Assistência Remota, problemas que talvez demorassem dias para ser resolvidos (até que um técnico viajasse para a filial da empresa), poderão ser resolvidos em minutos.

A assistência remota normalmente inicia com uma solicitação de ajuda do usuário, através de email, do Windows Messenger ou de um convite salvo como um arquivo. Entretanto, um assistente também poderá oferecer ajuda sem que tenha recebido primeiro uma solicitação de um usuário.

A assistência remota exige que os dois computadores estejam executando o Windows XP ou um produto da família Windows Server 2003.

## Tipos de conexões de assistência remota

A assistência remota pode ser usada nas seguintes situações:

- ◆ Em uma rede local (LAN).
- ◆ Na Internet.
- ◆ Entre um indivíduo na Internet e um indivíduo atrás de um firewall. As conexões através de um firewall requerem que a porta TCP 3389 esteja aberta.

## Questões de segurança

Se um usuário permitir e tiver permissão da diretiva de grupo, ou através das configurações de Sistema no Painel de controle, um assistente poderá controlar o computador do usuário e executar qualquer tarefa que poderia ser executada pelo usuário, incluindo acesso à rede. As configurações a seguir estão disponíveis para resolver problemas de segurança em sua organização:

- ◆ **No firewall:** Para determinar se uma pessoa dentro de sua organização pode solicitar ajuda fora da organização, proíba ou permita o tráfego de entrada e saída através da porta 3389 no firewall.
- ◆ **Diretiva de grupo, via GPOs.** Você pode definir a diretiva de grupo para permitir ou proibir que os usuários solicitem ajuda usando a assistência remota. Você também pode determinar se os usuários poderão permitir que alguma pessoa controle remotamente seus computadores ou apenas o vejam.  
Além disso, você pode definir a diretiva de grupo para permitir ou proibir que um assistente remoto ofereça assistência remota ao computador local.
- ◆ **Computador individual.** O administrador de um computador individual poderá desativar as solicitações de assistência remota nesse computador, o que impedirá que qualquer pessoa que esteja utilizando o computador envie um convite de assistência remota.

## Habilitando o recurso de Assistência Remota

Por padrão, o recurso de Assistência Remota está desabilitado. Para que possa ser utilizado, o recurso de Assistência Remota deve ser habilitado. Este recurso pode ser habilitado manualmente em cada computador ou através das configurações das Políticas de Segurança do Domínio. A seguir descrevo como habilitar, manualmente, o recurso de Assistência Remota, em um computador.

Para habilitar o recurso de assistência remota, siga os passos indicados a seguir:

1. Faço o logon com uma conta com permissão de Administrador.
2. Abra o Painel de Controle.
3. Dentro do Painel de controle, dê um clique duplo na opção Sistema.

4. Será aberta a janela Propriedades do sistema, com a guia Geral selecionada por padrão. Dê um clique na guia Remoto. Serão exibidas as opções indicadas na Figura 9.36:

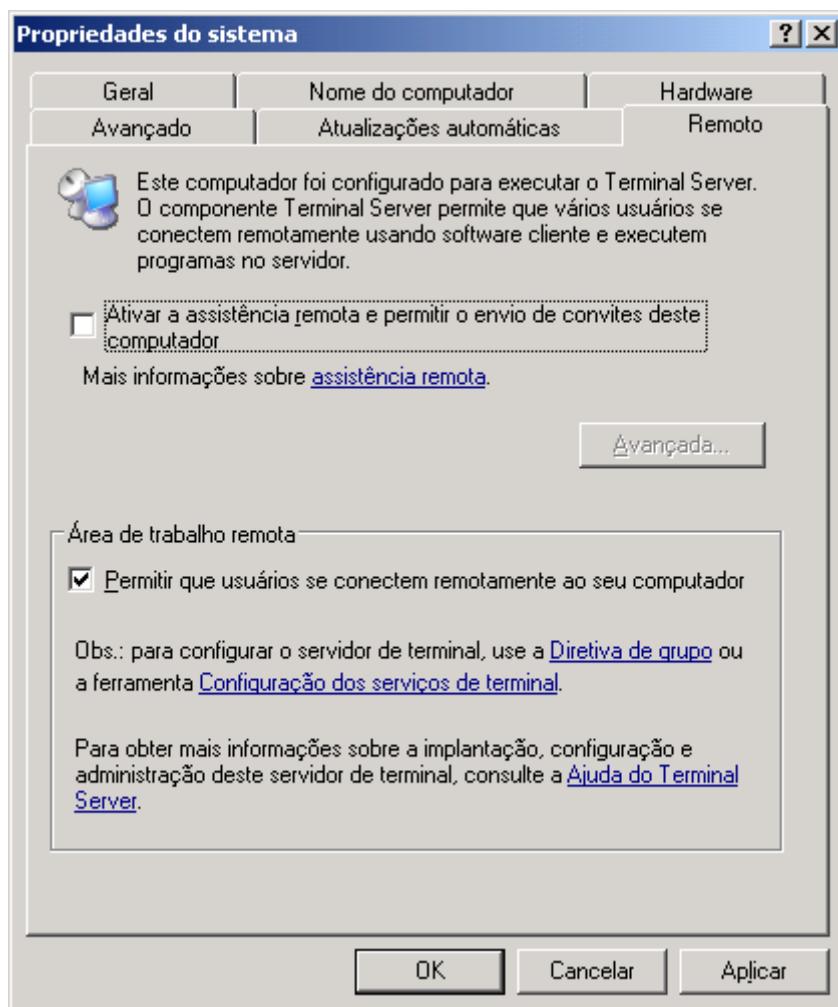


Figura 9.36 A guia Remoto.

5. Observe que, por padrão, a opção “Ativar a assistência remota e permitir o envio de convites deste computador”, vem desmarcada. Para habilitar que seja enviado um convite para assistência remota, a partir deste computador, você deve marcar esta opção.  
6. Marque esta opção.  
7. O botão Avançada... será ativado. Através deste botão, você tem acesso as configurações da Assistência remota.  
8. Dê um clique no botão Avançada...  
9. Será exibida a janela Configurações da assistência remota, indicada na Figura 9.37:

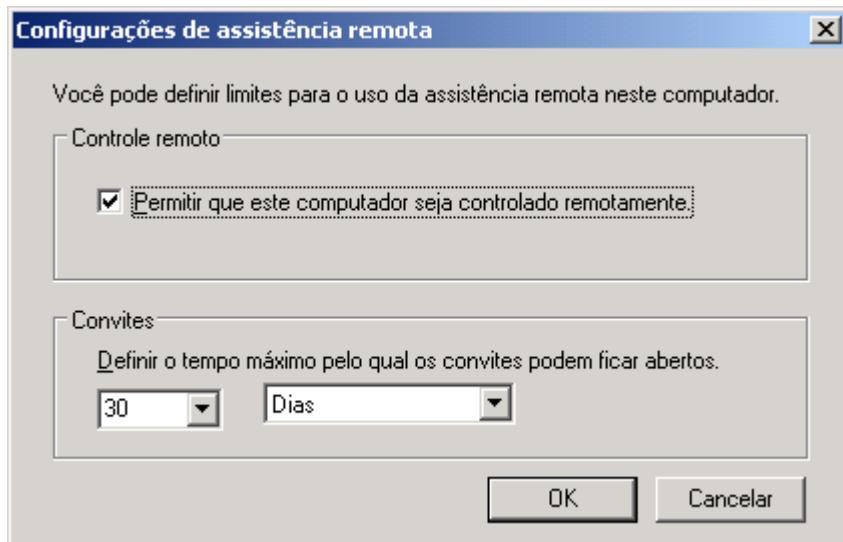


Figura 9.37 Configurações avançadas.

10. Nesta janela você tem as seguintes opções de configuração:

- ◆ **Permitir que este computador seja controlado remotamente:** Marque esta opção para permitir o controle remoto. Ou seja, ao marcar esta opção, quando o técnico aceitar o convite de assistência remota que você enviou, ele também terá acesso ao teclado e ao mouse, ou seja, embora remotamente, é como se ele estivesse “sentado” na frente do seu computador. Este recurso deve ser utilizado com cuidado, obviamente por questões de segurança.
- ◆ **Convites:** Nesta lista você define o tempo máximo pelo qual os convites são válidos. Ou seja, o usuário envia um convite, qual seria o tempo máximo dentro do qual este convite pode ser utilizado, antes que perca a validade. Se um técnico tentar utilizar um convite que perdeu a validade, não será possível estabelecer o controle remoto.

11. Defina as configurações desejadas e clique em OK.

12. Você estará de volta à guia Remoto. Clique em OK para fechar a janela de Propriedades do Sistema.

## Enviando um convite de assistência remota

Uma coisa que o amigo leitor deve estar se perguntando é como o usuário faz, para enviar um convite de assistência remota, para um técnico do suporte técnico ou para um outro usuário qualquer. Bem, é exatamente deste tópico, que tratarei agora.

Algumas vezes, a melhor maneira de corrigir um problema é ter alguém que aponte como fazê-lo. A assistência remota é uma opção conveniente que permite que outra pessoa (denominada assistente ou especialista) se conecte ao seu computador e o oriente passo a passo para solucionar o problema.

Seguindo as etapas da Assistência remota, o usuário pode usar o Windows Messenger ou uma mensagem de email para convidar um assistente a se conectar ao seu computador. O usuário também pode salvar o convite em um arquivo. Depois que o assistente estiver conectado, ele poderá ver a tela de seu computador e conversar com você sobre o que ambos estão vendo. Com sua permissão, o assistente poderá usar o próprio mouse e teclado para controlar seu computador.

Para solicitar a assistência remota, siga os passos indicados a seguir:

1. Clique no botão Iniciar e, em seguida, clique em Ajuda e suporte.

2. No painel da direita, clique na opção Assistência remota.
3. Nas opções que são exibidas, clique em Convide alguém para ajudá-lo.
4. Será aberto um assistente, passo-a-passo, para que você crie e envie um convite de assistência remota. Siga as outras instruções para criar e enviar um convite.
5. A pessoa recebe o convite, ou por email ou via Windows Messenger, com um link na qual o técnico cria, para iniciar a sessão de assistência remota com o computador do cliente.

Alguns detalhes importantes sobre a Assistência remota:

- ◆ A assistência remota exige que os dois computadores estejam executando o Windows XP ou um produto da família Windows Server 2003.
- ◆ Se você solicitar assistência usando o Windows Messenger, seu assistente também deverá estar inscrito no Windows Messenger.
- ◆ Vocês dois precisarão estar conectados à Internet ou à mesma rede local (LAN) quando usarem a assistência remota.
- ◆ Se houver vários usuários em um computador, o administrador só poderá ver suas próprias permissões. Ele não poderá ver as permissões da assistência remota criadas pelos outros usuários do computador.
- ◆ Os firewalls provavelmente impedirão de usar a assistência remota para solicitar ajuda de uma outra pessoa fora do firewall. Nesse caso, consulte o administrador da rede. A assistência remota usa o protocolo de área de trabalho remota (RDP) para estabelecer uma conexão entre um usuário que está solicitando ajuda e um assistente que está oferecendo ajuda. O RDP usa a porta TCP 3389 para essa conexão. Para permitir que os usuários de uma organização solicitem ajuda fora da organização usando a assistência remota, a porta 3389 deverá estar aberta no firewall. Para proibir os usuários de solicitarem ajuda fora da organização, essa porta deverá estar fechada no firewall. Se o administrador fechar a porta 3389, serão bloqueados todos os serviços de terminal e de área de trabalho remota. Para liberar esses serviços, mas limitar as solicitações de assistência remota, você deve habilitar a porta 3389 e usar as GPOs para desabilitar a Assistência remota. Se a porta estiver aberta somente para tráfego de saída, um usuário poderá solicitar assistência remota usando o Windows Messenger.

## O novo recurso de Shadow Copies.

O recurso de shadow copies é uma das novidades do Windows Server 2003. Este recurso pode ser habilitado individualmente, em cada volume de um servidor com o Windows Server 2003. Uma vez habilitado este recurso, todas as pastas compartilhadas no volume passarão a utilizar o recurso de shadow copies.

O recurso de shadow copies permite que o Windows Server 2003 mantenha cópias de várias versões de um mesmo arquivo e permite que o usuário, tenha acesso as diferentes versões disponíveis (na prática, havendo espaço disponível, um histórico de até 64 versões do mesmo arquivo, pode ser mantido).

Por exemplo, vamos supor que você crie um arquivo do Word e salve ele em um volume com o recurso de shadow copies habilitado. Daqui a uma semana você abre este mesmo arquivo, faz algumas alterações e salva o arquivo novamente. Com o recurso de shadow copies, será mantida uma cópia da versão anterior, cópia esta que poderá inclusive ser acessada, se for necessário. Podem ser mantidas

**IMPORTANTE: O firewall de conexão com a Internet (ICF) da Microsoft permite tráfego de entrada e saída de assistência remota, contanto que a solicitação inicial de assistência tenha sido feita no computador em que o firewall está ativado. O ICF foi projetado para ser usado somente com computadores autônomos ou pertencentes a um grupo de trabalho.**

várias versões do mesmo arquivo. O número de versões que é mantida pelo recurso de shadow copies depende do tamanho do próprio arquivo e do espaço em disco reservado para este recurso.

Este recurso funciona como se fosse uma “lixeira” da rede, porém uma lixeira modificada, onde são mantidas várias versões do mesmo arquivo, podendo estas versões serem acessadas pelo cliente. Este recurso funciona também como um backup alternativo. Rapidamente o usuário pode recuperar uma versão mais recente do arquivo (provavelmente mais recente do que a versão que está na fita de backup), sem ter que esperar uma hora ou mais até que o arquivo seja restaurado a partir de uma fita de backup.

O recurso de shadow copies traz muitos benefícios, dentre os quais gostaria de destacar os seguintes:

- ◆ Recuperação rápida e fácil de arquivos que foram excluídos acidentalmente. Se você excluir, por engano, um arquivo, poderá abrir uma versão anterior e copiá-la para um local seguro.
- ◆ Recuperação rápida e fácil de arquivos que foram sobreescritos por engano.
- ◆ Comparação de versões dos arquivos. Você pode utilizar uma versão anterior para identificar as mudanças que foram efetuadas em um determinado arquivo.

É fundamental lembrar que o recurso de shadow copies não é um recurso que irá substituir o backup. Principalmente porque as diferentes versões do mesmo arquivo são gravadas no mesmo disco. Ou seja, se o disco for danificado você perderá a última versão e também todas as versões mantidas no recurso de shadow copies. Nesta situação a única maneira de recuperar as informações é restaurando a partir do backup. Existe a possibilidade de configurar o recurso de Shadow Copies, para que as cópias sejam armazenadas em um volume diferente do volume original. Esta pode ser uma boa estratégia em termos de desempenho, porém nem nesta situação, o recurso de Shadow Copies deve ser considerado um substituto para o Backup.

Quando o espaço reservado para a manutenção de versões anteriores dos arquivos for preenchido, os arquivos mais antigos serão descartados, para que novos possam ser gravados. Você aprenderá a configurar o espaço reservado para o recurso de shadow copies mais adiante, nos exemplos práticos.

## Mais algumas observações sobre o recurso de shadow copies.

A quantidade mínima de espaço que pode ser reservada para este recurso é de 100 MB. O valor padrão é 10% do tamanho do volume onde o recurso de shadow copies será habilitado. As versões antigas, mantidas pelo recurso de shadow copies poderão ser gravadas em um volume diferente do volume original.

O volume a ser reservado para este recurso depende da forma como os arquivos são utilizados. Se você tem arquivos que são alterados diariamente, será necessário

---

**NOTA:** Permitam que eu me queixe, mais uma vez, das traduções que são feitas. Já vi algumas traduções de shadow copies como sendo “sombras de cópia”, mas, sinceramente, me recuso a utilizar esta tradução. Por isso, neste tópico, vou utilizar o termo original: shadow copies.

---

**NOTA:** O recurso de shadow copies é configurado através da janela de propriedades do volume (C;D: e assim por diante), na guia Shadow Copies, conforme mostrarei na parte prática mais adiante.

---

**IMPORTANTE:** Para que os clientes possam utilizar o recurso de shadow copies, deve ser instalado o software cliente de shadow copies em cada estação de trabalho que irá utilizar este recurso. Na parte prática mostrarei como fazer esta instalação. Em resumo, para o exame, não se esqueça que para habilitar o recurso de Shadow Copies, são necessários dois passos. O primeiro é habilitar este recurso no volume onde está a pasta compartilhada, que será acessada através da rede. O segundo passo é instalar o cliente de Shadow Copies, em todas as estações de trabalho que deverão ter acesso a este recurso. Lembre-se bem destes dois passos, para o exame.

---

uma boa quantidade de espaço para este recurso. Se você tem arquivos que raramente são alterados, a quantidade de 10% do volume pode ser mais do que suficiente.

## O agendamento do recursos de shadow copies.

Quando você habilita o recurso de shadow copies, o Windows Server 2003 cria um agendamento padrão e define um intervalo. A cópia dos arquivos é feita de acordo com este agendamento.

Este agendamento pode ser alterado e deve ser adaptado de acordo com as características de uso do volume. Na parte prática você aprenderá a alterar este agendamento.

## Habilitando o recurso de shadow copies em um volume:

Neste item mostrarei como habilitar o recurso de shadow copies em um volume. Você verá que as configurações são extremamente simples.

Exemplo: Para habilitar o recurso de shadow copies em um volume, siga os passos indicados a seguir:

1. Faça o logon como administrador ou com uma conta com permissão de administrador.
2. Abra o Meu computador ou o Windows Explorer.
3. Clique com o botão direito do mouse no volume onde será habilitado o recurso de shadow copies. No menu de opções que é exibido clique em Propriedades.

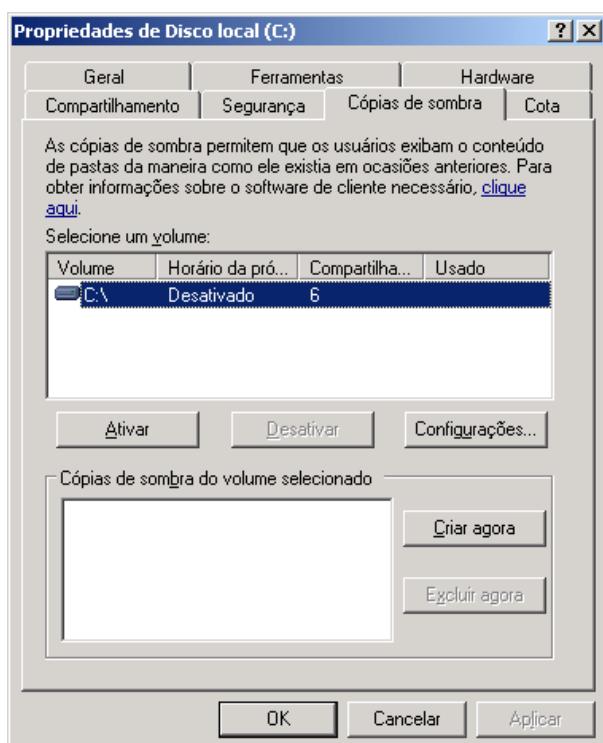


Figura 9.38 A guia Cópias de sombra.

**IMPORTANTE:** As versões anteriores dos arquivos, mantidas pelo recurso shadow copies são somente leitura, ou seja, você não poderá fazer alterações diretamente nestas cópias. Você poderá abrir estas cópias e salvar em uma nova pasta e fazer alterações, mas não diretamente nas cópias mantidas pelo recurso de shadow copies. Por exemplo, se você abrir uma planilha do Excel ou um documento do Word, a partir de uma cópia mantida pelo recurso de Shadow Copies, esta cópia será somente leitura. Se você fizer alterações e tentar salvar, será emitida uma mensagem informando que a cópia é somente leitura. Você pode usar o comando Arquivo -> Salvar como, para salvar a cópia em um local alternativo. A cópia salva no local alternativo, usando o comando Arquivo -> Salvar como, poderá ser alterada.

**NOTA:** Se você tiver que alterar o volume onde são gravadas as cópias, todas as cópias existentes serão excluídas e um novo histórico começará a ser criado no novo volume. Por isso é importante planejar com cuidado o espaço necessário, antes de habilitar o recurso de shadow copies em um volume. Este é mais um dos motivos pelos quais o recurso de Shadow Copies não pode ser utilizado em substituição ao Backup.

4. Será exibida a janela de propriedades do volume. Clique na guia Shadow Copies (Cópias de sombra). Será exibida a figura indicada na Figura 9.38.
5. Observe que, por padrão, o recurso de shadow copies está desabilitado.
6. Para habilitar o recurso de shadow copies clique no botão Ativar.
7. Será exibida uma janela com uma mensagem de aviso, informando sobre o agendamento padrão que será criado para o recurso de shadow copies. Clique em Sim para fechar esta janela e habilitar o recurso de shadow copies.
8. O recurso será habilitado. Você estará de volta a guia Cópias de sombra. Nesta mesma janela você já pode configurar as opções deste recurso. Clique no botão Configurações...
9. Será aberta a janela na qual você pode definir o espaço máximo em disco a ser utilizado pelo recurso de shadow copies No exemplo da Figura 9.39, estou definindo um tamanho máximo de 4GB (4096 MB) para este recurso.



**Figura 9.39 Definindo o espaço a ser utilizado pelo recurso de shadow copies.**

10. Nesta janela você também tem acesso ao botão Agendar... Este botão permite que você defina o agendamento para que sejam feitas as cópias dos arquivos pelo recurso de shadow copies. Clique no botão Agendar...
11. Será aberta a janela para você configurar o agendamento. Esta é a mesma janela que você utilizou para definir o agendamento de uma tarefa agendada e das rotinas de backup, que você aprendeu a utilizar no Capítulo 8. No exemplo da Figura 9.40 estou definindo um agendamento diário, para realizar a cópia às 7:00 horas da manhã. Para que a cópia seja efetuada mais do que uma vez por dia, você pode definir múltiplos agendamentos, clicando no botão Novo, conforme descrito no Capítulo 8.

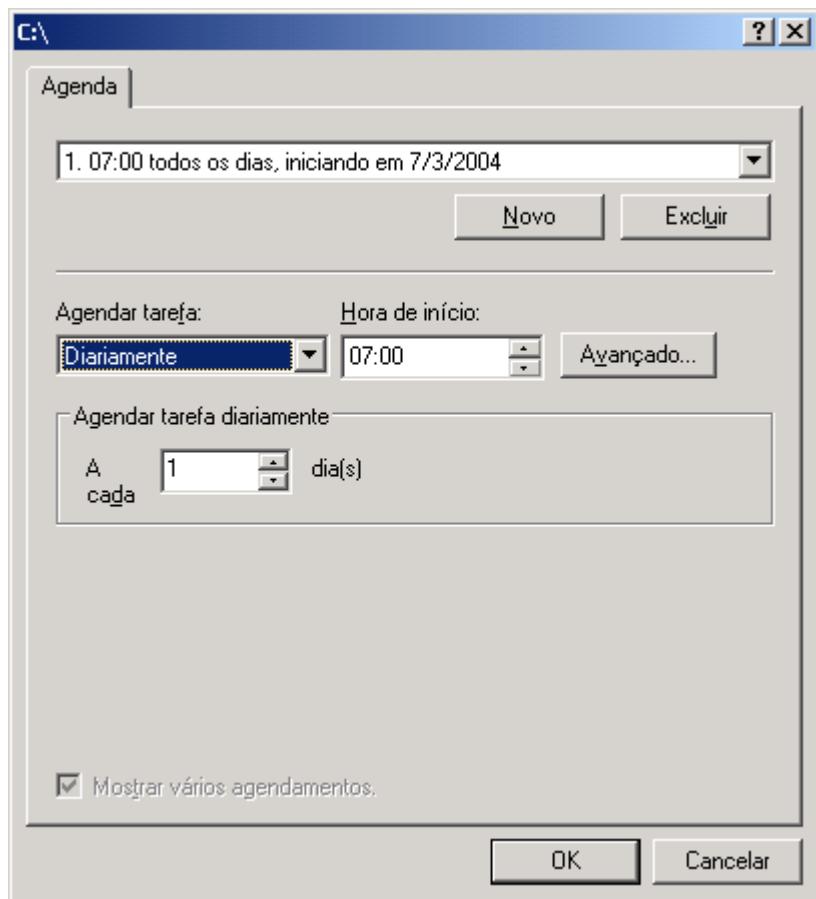


Figura 9.40 Agendamento diário para as 7:00 hs.

12. Defina o agendamento desejado e clique em OK.
13. Você estará de volta à janela de configurações. Dê um clique em OK para fechá-la.
14. Você estará de volta à janela de propriedades do volume. Nesta janela você pode utilizar o botão Criar agora, para fazer com que o Windows Server 2003 faça uma cópia dos arquivos que foram alterados, imediatamente, sem esperar pelo próximo agendamento.
15. Ao lado deste botão é exibida uma listagem com o histórico das cópias efetuadas.
16. Clique em OK para fechar a janela de propriedades.

Pronto, o recurso de shadow copies está habilitado no volume. O próximo passo é instalar o software que permite aos clientes utilizar o recurso de shadow copies. Este software tem que ser instalado na estação de trabalho dos clientes que irão utilizar este recurso. Este software é chamado de “Previous Versions Client”. Antes de mostrar como instalar o cliente do shadow copies, apresento mais uma recomendação importante:

- ◆ Não utilize o recurso de shadow copies em servidores que estão configurados para dual-boot com outras versões do Windows. Nestes casos pode acontecer de os arquivos de shadow copies serem corrompidos.

## Instalando o cliente de shadow copies.

Para que um usuário acessando uma pasta compartilhada no servidor (pasta esta que está em um volume para o qual o recurso de shadow copies foi habilitado) possa utilizar o recurso de shadow copies, é necessário que o cliente de

shadow copies seja instalado na estação de trabalho do usuário. Os arquivos de instalação do cliente shadow copies estão disponíveis na seguinte pasta, de qualquer servidor com o Windows Server 2003 instalado:

**%systemroot%\system32\clients\twclient\x86\twcli32.msi**

Onde %systemroot% é a pasta onde o Windows Server 2003 foi instalado.

O arquivo twcli32.msi é um arquivo de instalação, no padrão do Microsoft Installer. Este arquivo pode ser instalado em todas as estações de trabalho da rede, usando o recurso de distribuição de software via GPO ou pode ser disponibilizado em um drive de rede para que os usuários instalem em suas estações de trabalho. Este arquivo tem apenas 287 KB. A seguir mostro como fazer a instalação do cliente de shadow copies.

Exemplo: Para instalar o cliente de shadow copies manualmente, siga os passos indicados a seguir:

1. Faça o logon como administrador ou com uma conta com permissão de administrador.
2. Abra o Windows Explorer e localize o arquivo twcli32.msi.
3. Dê um clique duplo neste arquivo para iniciar a instalação do cliente de shadow copies.
4. A instalação é rapidamente efetuada e uma mensagem de que a instalação foi efetuada com sucesso é exibida. Clique em Concluir, para fechar esta mensagem.

Pronto, o cliente de shadow copies foi instalado. Agora você aprenderá a utilizá-lo.

## Acessando as shadow copies:

1. Abra o Windows Explorer ou o Meu computador.
2. Clique com o botão direito do mouse no drive de rede para o qual você deseja acessar as shadow copies.
3. No menu de opções que é exibido clique em Propriedades.
4. Será exibida a janela de propriedades do drive de rede. Clique na guia Versões Anteriores. Será exibida a janela indicada na Figura 9.41:

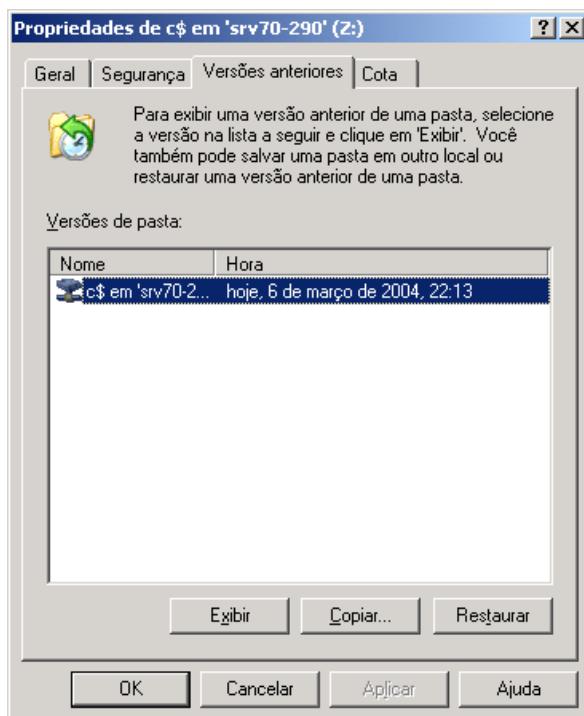


Figura 9.41 A janela de versões anteriores.

5. Observe que é exibida a lista de cópias disponíveis. No exemplo da Figura 9.41 esta disponível uma única cópia de versão anterior.
6. Clique em uma das cópias e depois clique em Copiar. Será exibida uma janela para que você selecione uma pasta de destino para onde será copiada a versão anterior com todo o conteúdo do drive de rede. Observe que sempre é copiado todo o conteúdo e não apenas os arquivos que mudaram entre uma cópia e outra. Selecione a pasta de destino e clique em OK. A cópia será iniciada. Uma vez finalizada a cópia você terá acesso a uma versão da pasta compartilhada e de todo o seu conteúdo, no momento em que a cópia foi realizada pelo recurso de shadow copies.
7. Você pode marcar uma das cópias e clicar no botão Exibir. Será aberta uma janela com todo o conteúdo do drive de rede.
8. O conteúdo da cópia é somente leitura, conforme comentado anteriormente. Você pode navegar pelas pastas e arquivos da cópia e usar o recurso de copiar e colar para copiar um ou mais arquivos. Com esta opção você pode recuperar um único arquivo ou uma única pasta, ao invés de ter que copiar todo o conteúdo do drive.
9. Feche a janela que exibe uma cópia dos arquivos.
10. Você estará de volta à guia Versões anteriores. Você pode marcar uma versão e clicar no botão Restaurar, para restaurar a versão que está marcada. Use esta opção com cuidado, pois ao usar esta opção, os arquivos que estão atualmente em uso na pasta compartilhada, serão substituídos pelos arquivos da cópia que está sendo restaurada. Com esta operação todo o conteúdo é restaurado, você não terá a opção de selecionar os arquivos a serem restaurados.
11. Clique em OK para fechar a janela de propriedades.

**IMPORTANTE:** Se você usar a opção restaurar, a versão anterior, será restaurada "em cima" da versão atual, ou seja, a versão anterior irá sobrepor a versão atual. Se você quer ter uma acesso a versão anterior de um arquivo, porém sem sobrepor a versão atual, você deve usar a opção Copiar, ao invés da opção Restaurar.

## Desabilitando o recurso de shadow copies em um volume:

Neste item mostrarei como desabilitar o recurso de shadow copies em um volume.

Exemplo: Para desabilitar o recurso de shadow copies em um volume, siga os passos indicados a seguir:

1. Faça o logon como administrador ou com uma conta com permissão de administrador.
2. Abra o Meu computador ou o Windows Explorer.
3. Clique com o botão direito do mouse no volume onde será desabilitado o recurso de shadow copies. No menu de opções que é exibido clique em Propriedades.
4. Será exibida a janela de propriedades do volume. Clique na guia Cópias de sombra.
5. Clique no botão Desativar. Será exibida uma mensagem solicitando confirmação para que seja desabilitado o recurso de shadow copies. Clique em Sim para confirmar que o recurso será desabilitado no volume que está sendo configurado.
6. Você estará de volta à guia Cópias de sombra. Observe que já aparece o status Desativado, ao lado da letra do volume.
7. Clique em OK para fechar a janela de propriedades.

Pronto, o recurso de Shadow Copies foi desabilitado no volume.

## Gerenciando shadow copies com o comando vssadmin.

Você pode gerenciar o recurso de shadow copies com o comando vssadmin. Este comando tem várias opções. A seguir comento as principais opções deste comando. Na Ajuda do Windows Server 2003 você encontra uma referência completa, com todas as opções do comando vssadmin. É só abrir a ajuda do Windows Server 2003 e pesquisar usando a palavra vssadmin.

Utilizações do comando vssadmin:

```
vssadmin list shadows
```

Este comando exibe uma lista completa de todas as cópias armazenadas no volume, conforme exemplo a seguir:

```
C:\>vssadmin list shadows

vssadmin 1.1 - Volume Shadow Copy Service administrative command-line tool

(C) Copyright 2001 Microsoft Corp.

Contents of shadow copy set ID: {b9fef05a-98da-4d44-b1bf-0625ffed3ca9}

Contained 1 shadow copies at creation time: 6/26/2003 11:29:59 PM

Shadow Copy ID: {93df4e9-1355-4116-bd1d-b7bd126e961a}

Original Volume: (C:)\\?\Volume{3ca6c0d3-75cf-11d7-b6a1-806e6f6e6963}\

Shadow Copy Volume: \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy4

Originating Machine: srv-win2003.abc.com

Service Machine: srv-win2003.abc.com

Provider: 'Microsoft Software Shadow Copy provider 1.0'

Type: ClientAccessible

Attributes: Persistent, Client-accessible, No auto release, No writers,

Differential

Contents of shadow copy set ID: {02ca95b2-e231-496f-915e-cd0f59221bb8}

Contained 1 shadow copies at creation time: 6/26/2003 11:33:10 PM

Shadow Copy ID: {edc13c66-fc15-486c-adca-28fdf6521c49}

Original Volume: (C:)\\?\Volume{3ca6c0d3-75cf-11d7-b6a1-806e6f6e6963}\

Shadow Copy Volume: \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy5

Originating Machine: srv-win2003.abc.com

Service Machine: srv-win2003.abc.com

Provider: 'Microsoft Software Shadow Copy provider 1.0'

Type: ClientAccessible

Attributes: Persistent, Client-accessible, No auto release, No writers,

Differential

vssadmin create shadow /for=C:
```

Este comando é utilizado para criar uma cópia manualmente para o volume C: É equivalente ao botão Create Now da guia Shadow Copies.

```
vssadmin Delete Shadows
```

É utilizada para eliminar shadow copies de um volume. Existem algumas opções que podem ser utilizados com este comando, como por exemplo a opção /Oldest, conforme exemplo a seguir:

```
vssadmin Delete Shadows /For=C: /Oldest
```

Este comando irá eliminar a shadow copies mais antiga do volume.

A seguir, acrescentaremos o próximo “ingrediente” na nossa salada de frutas. Apresentarei os tópicos sobre GPO, que você precisa conhecer, para o Exame 70-290

## Group Police Objects – GPOs.

### Introdução

O recurso de GPOs não faz parte diretamente do programa oficial para o Exame 70-290. Porém existem uma série de configurações, de itens que fazem parte do programa oficial, as quais são feitas usando-se GPOs. Por isso é importante que o candidato tenha uma noção básica sobre o recurso de GPOs, pois certamente aparecerão questões que abordam o entendimento básico de GPOs.

O recurso de Group Policy Objects (GPO) é de “enorme” utilidade para o administrador. Com o uso de GPO o administrador pode definir as configurações de vários elementos da estação de trabalho do usuário, como por exemplo os programas que estarão disponíveis, os atalhos do menu Iniciar que estarão disponíveis, configurações de Internet, de rede e assim por diante. Por exemplo, o administrador pode configurar, via GPO, quais grupos de usuários deverão ter acesso ao menu Executar e quais não terão, pode configurar a página inicial do Internet Explorer para um grupo de usuários ou para toda a empresa, pode fazer configurações de Proxy e por aí vai. São milhares (literalmente “milhares”) de opções de configurações que estão disponíveis via GPO.

As configurações feitas via GPO são aplicadas para usuários, computadores, member servers e DCs, mas somente para computadores executando Windows 2000 (Server ou Professional), Windows XP Professional (uma vez que um computador com o Windows XP Home não pode ser configurado para fazer parte de um domínio) ou Windows Server 2003. Para versões mais antigas do Windows, tais como Windows 95/98/Me e NT 4.0, o recurso de GPO não é aplicado.

Vou iniciar este tópico com a fundamentação teórica necessária para que você entenda exatamente o que é o recurso de GPO, como ele se aplica em um domínio, em que níveis ele pode ser configurado e quais as opções que o administrador tem para garantir que as configurações definidas via GPO, sejam aplicadas nas estações de trabalho dos usuários.

Em seguida passarei as ações práticas relacionadas com GPO. Desde a alteração da GPO padrão do domínio, passando pela criação de novas políticas de segurança e aplicações destas políticas em diferentes níveis, dentro do domínio.

Também falarei sobre as configurações de segurança e definição de permissões, relacionadas com GPO. Com a configuração das permissões de acesso a uma determinada GPO, o administrador pode fazer com que um conjunto de políticas de segurança sejam aplicadas apenas a um determinado grupo de usuários ou computadores (é importante lembrar que no Windows Server 2003, é possível adicionar as contas de computadores como membros de um grupo). Apresentarei o conceito de herança de GPO, conceito importante quando se aplicam diferentes políticas em diferentes níveis dentro do domínio.

## Group Policy Objects – Fundamentação Teórica

Quem já trabalhou na administração de uma rede baseada no Windows sabe o quanto é trabalhoso (e com um custo elevado), manter a configuração de milhares de estações de trabalho rodando diversas versões do Windows. Existem diversas questões/problemas que tem que ser enfrentados:

- ◆ Como definir configurações de maneira centralizada, para que seja possível padronizar as configurações das estações de trabalho?
- ◆ Como impedir que os usuários possa alterar as configurações do Windows (diversas versões), muitas vezes inclusive causando problemas no Windows, o que faz com que seja necessário um chamado à equipe de suporte, para colocar a estação de trabalho novamente em funcionamento?
- ◆ Como aplicar configurações de segurança e bloquear opções que não devam estar disponíveis para os usuários de uma maneira centralizada, sem ter que fazer estas configurações em cada estação de trabalho. Quando houver alterações, eu gostaria de poder fazê-las em um único local e ter estas alterações aplicadas em toda a rede ou em partes específicas da rede.
- ◆ Como fazer a instalação e distribuição de software de uma maneira centralizada, sem ter que fazer a instalação em cada estação de trabalho da rede.
- ◆ Como definir um conjunto de aplicações diferente, para diferentes grupos de usuários, de acordo com as necessidades específicas de cada grupo.
- ◆ Como aplicar diferentes configurações aos computadores de diferentes grupos de usuários, de acordo com as necessidades específicas de cada grupo.

A primeira tentativa de “responder” a estas necessidades, recorrentemente levantadas pelos administradores de redes baseadas no Windows foi a introdução das chamadas Polices e do Police Editor, juntamente com o Windows NT 4.0. Com o uso das Polices era possível definir uma série de configurações, as quais eram aplicadas à registry da estação de trabalho do usuário quando ele fizesse o logon no domínio. Por exemplo, era possível utilizar as Polices para impedir que um usuário do Windows 95/98/Me pressionasse a tecla ESC para cancelar a tela de logon e ter acesso ao Windows sem fazer o logon no domínio. Eu digo “uma primeira tentativa”, porque o uso de Polices não passou muito disso, uma tentativa, uma vez que muitas das demandas não foram atendidas por este recurso.

Já com o lançamento do Windows 2000 Server e com a introdução do recurso de GPOs, o administrador tem um recurso realmente poderoso, capaz de atender todas as demandas descritas anteriormente. É importante salientar que as GPOs somente são aplicadas a computadores com o Windows 2000, Windows XP ou Windows Server 2003. Estações de trabalho que ainda estejam com versões mais antigas do Windows, tais como Windows 95, Windows 98, Windows Me ou Windows NT 4.0, terão como único recurso de configuração o uso de Polices e do Police Editor. O recurso de GPOs não é aplicado a estas versões mais antigas.

Então em uma rede, onde você tem estações de trabalho com as novas versões do Windows (2000, XP e 2003) e estações de trabalho com versões mais antigas (95, 98, Me e NT 4.0), você terá que utilizar os dois recursos. Polices para as versões mais antigas do Windows, sempre levando em consideração as limitações deste recurso, em comparação com o uso de GPOs e usar GPOs para as estações de trabalho com versões mais novas do Windows.

As GPOs incluem configurações que são aplicadas a nível de usuário (ou seja, em qualquer estação de trabalho que o usuário faça o logon, as políticas associadas a sua conta de usuário serão aplicadas) e a nível de computador (ou seja, qualquer usuário que faça o logon no computador terá as políticas de computador aplicadas). Por exemplo, se o administrador definiu uma política de usuário para o grupo do usuário jsilva, de tal maneira que o menu Executar não deva estar disponível para este grupo. Em qualquer estação de trabalho que o jsilva fizer o logon, o menu Executar não estará disponível.

Agora imagine que o administrador configurou uma política de computador, para o grupo de computadores da seção de contabilidade, definindo que o menu Executar não deve estar disponível nestes computadores. Qualquer usuário que faça o logon em qualquer um dos computadores da seção de contabilidade, não terá disponível o menu Executar, independentemente dos grupos aos quais pertença a conta do usuário, uma vez que a política está sendo aplicada ao computador (independentemente do usuário que esteja utilizando-o).

Mas enfim, o que as GPOs podem fazer:

- ◆ **Gerenciar centralizadamente, configurações definidas na registry do Windows, com base em templates de administração (Administrative Templates).** As GPOs criam arquivos com definições da registry. Estes arquivos são carregados e aplicados na estação de trabalho do usuário, nas partes referentes a configuração de Usuários e configuração de Computador da registry. As configurações de usuário são carregadas na opção HKEY\_CURRENT\_USER (HKCU), da registry (No Capítulo 12 falarei um pouco mais sobre a Registry do Windows Server 2003). As configurações de computador são carregadas na opção HKEY\_LOCAL\_MACHINE (HKLM), da registry. A idéia é relativamente simples. Ao invés de ter que configurar estas opções em cada estação de trabalho, o administrador cria elas centralizadamente, usando GPOs. Durante o logon, o Windows aplica as configurações definidas na GPO.
- ◆ **Atribuição de scripts:** Com o uso de GPOs o administrador pode configurar um script para ser executando na inicialização e também no desligamento do Windows. Também podem ser definidos scripts de log on e log off.
- ◆ **Redireção de pastas:** O administrador pode configurar uma GPO para que pastas tais como Meus documentos e Minhas imagens sejam redirecionadas para uma pasta compartilhada em um servidor. Com isso os dados do usuário passam a estar disponíveis no servidor e poderão ser acessados de qualquer estação de trabalho da rede, na qual o usuário faça o logon. Além disso, com os dados no servidor, é possível criar e implementar uma política de backup centralizada.
- ◆ **Gerenciamento de software:** Com o uso de GPO o administrador pode fazer a instalação de aplicações de uma maneira centralizada. É possível associar uma aplicação com um grupo de usuários. Quando o usuário fizer o logon, o ícone da aplicação já é exibido no menu Iniciar. Quando ele clicar neste ícone a aplicação será instalada a partir de um servidor da rede, cujo caminho foi configurado vai GPO. Também é possível publicar aplicações. Neste caso, ao fazer o logon, o usuário tem que acessar a opção Adicionar ou remover programas, do Painel de controle e solicitar que a aplicação seja instalada.
- ◆ **Definir configurações de segurança:** Para computadores executando o Windows 2000, Windows XP Profissional ou Windows Server 2003, existe uma GPO localmente nestes computadores. Esta GPO pode ser utilizada para configurar uma série de opções do ambiente de trabalho do usuário. As configurações definidas na GPO local somente se aplicam ao computador onde as configurações estão sendo definidas. Algumas funcionalidades tais como distribuição de software e redireção de pastas não estão disponíveis na GPO local, somente em GPOs aplicadas no Active Directory, conforme descrito logo a seguir. A GPO local somente deve ser utilizada quando houver necessidade de uma configuração específica em um determinado computador. As configurações que se aplicam a grupos de computadores e usuários devem ser configuradas via GPOs aplicadas no Active Directory, já que isso facilita a configuração e atualização das configurações de uma maneira centralizada.

---

**NOTA: A GPO local é gravada, por padrão, na seguinte pasta: systemroot%\System32\GroupPolicy.**

---

Além da GPO local, podem ser aplicadas GPOs definidas no Active Directory, para aplicação nos computadores que fazem parte do domínio. Pode inclusive acontecer de haver “conflitos” de configurações entre a GPO local e uma ou

mais GPOs do domínio. Neste caso existem configurações (que você aprenderá mais adiante), que definem, em caso de conflito, se deve ser aplicada a definição da GPO local ou a definição da GPO do domínio.

Existe uma GPO padrão para o domínio. Configurações feitas nesta GPO serão aplicadas a todos os usuários e computadores do domínio. Configurações gerais, que devam ser aplicadas a todos os objetos do domínio, devem ser definidas nesta GPO.

## Políticas de usuários e políticas de computador:

As políticas de usuários, isto é, políticas associadas a conta do usuário ou a um grupo ao qual o usuário pertence, são configuradas na opção Configuração de usuário, do console de administração de GPOs (o qual você aprenderá a utilizar mais adiante, neste capítulo) e são aplicadas quando o usuário faz o logon. Políticas de computador são configuradas através da opção Configurações de computador, do console de administração das GPOs e são aplicadas quando o computador é inicializado. Existe também um intervalo de atualização, dentro do qual as políticas são reaplicados e quaisquer mudanças que tenham sido feitas pelo administrador, serão aplicadas aos usuários e computadores.

As políticas definidas no Active Directory são aplicadas somente a objetos do tipo usuário e computador. Por questões de desempenho, as políticas não podem ser configuradas para objetos do tipo Grupos. Porém é possível utilizar o mecanismo de permissões de acesso das GPOs, para limitar a aplicação de uma GPO somente a um ou mais grupos de usuários e computadores.

É possível criar objetos do tipo GPO e associá-los a diferentes elementos do Active Directory. Um objeto do tipo GPO pode ser criado e associado com o domínio, com uma unidade organizacional ou com um site. Além da GPO que pode ser criada localmente em cada computador com o Windows 2000, Windows XP Professional ou Windows Server 2003, conforme descrito anteriormente.

As GPOs são aplicadas em uma ordem específica, caso esteja definida mais de uma GPO para o usuário que estiver fazendo o logon ou para o computador que está sendo reinicializado. Por exemplo, quando o usuário faz o logon, são aplicadas a GPO do domínio e mais (se houver), a GPO da unidade organizacional a qual pertence a sua conta e a GPO local da estação de trabalho que ele está utilizando. A ordem de aplicação das GPOs é a seguinte:

- ◆ A GPO local.
- ◆ GPO definida para o site ao qual pertence o computador.
- ◆ GPOs do domínio
- ◆ GPOs definidas a nível de unidade organizacional, da OU pai para a OU filho. Por exemplo, se foi criada uma OU “Divisão Sul” e, dentro desta OU as divisões: Finanças, Contabilidade e Vendas e a conta do usuário jsivla está na OU Vendas. Primeiro será aplicada a GPO da OU “Divisão Sul” e depois a GPO da OU Vendas.

Por padrão, as políticas aplicadas por último, tem precedência sobre as políticas aplicadas anteriormente. Por exemplo, a GPO de domínio é aplicada. Em seguida

**IMPORTANTE:** Outra GPO que existe por padrão é uma GPO associada com a OU Domain Controllers (Controladores de domínio). Esta GPO é aplicado somente aos DCs do domínio. Embora seja possível mover a conta de um DC para outra unidade organizacional, este não é um procedimento recomendado. Ao mover a conta de um DC da unidade organizacional Domain Controllers para outra unidade organizacional, a GPO padrão para os DCs deixará de ser aplicado ao DC que foi movido, pois esta GPO está ligada a unidade organizacional Domain Controllers. Por exemplo, se você precisa habilitar a auditoria das tentativas de logon com e sem sucesso, mais indicado é que você habilite a diretiva na GPO associado a OU Domain Controllers, pois todo evento de autenticação é gerado em um DC do domínio.

**IMPORTANTE:** No Windows 2000 havia o comando Secedit, o qual era utilizado para forçar uma atualização de políticas, com a reaplicação das GPOs em uma estação de trabalho. Este comando não existe mais no Windows Server 2003. No Windows Server 2003, o comando para atualização das políticas é o comando Gpupdate.

vem a GPO definida na Unidade Organizacional. Se houver um conflito entre a GPO de domínio e a GPO da unidade organizacional, irá prevalecer a configuração definida na GPO da unidade organizacional (aplicada por último). O administrador pode configurar a GPO de domínio (ou outras GPOs em qualquer nível), para que suas configurações não possam ser sobreescritas (substituídas) pelas configurações de GPOs de nível mais baixo, em caso de conflito. Por exemplo, o administrador pode definir na GPO de domínio, que nenhum usuário terá acesso ao menu Executar e marcar a GPO onde está esta configuração com a opção No override (Não sobreescrivê-lo). Com isso, mesmo que exista um GPO em uma unidade organizacional, permitindo o uso do comando Executar, esta configuração não será aplicada, uma vez que a GPO do domínio não permite que sejam alteradas suas configurações em caso de conflito. Este mecanismo é uma maneira que o administrador tem, de garantir que determinadas configurações sejam aplicadas em todo o domínio, independentemente das configurações que são efetuadas em nível de unidade organizacional.

## Novidades no Windows Server 2003.

O Windows Server 2003 aprimorou o mecanismo de GPOs do Windows 2000 Server e introduziu novas funcionalidades, que facilitam ainda mais o trabalho do administrador.

A seguir apresento uma lista das novidades introduzidas pelo Windows Server 2003, em relação ao recurso de Group Policy Objects:

- ◆ **Templates de administração (Administrative templates):** Foram introduzidas 220 novas opções de configuração via GPO, em relação as configurações existentes. Também foram criados arquivos de Ajuda com a descrição completa de todas as configurações disponíveis em cada um dos templates. Na Figura 9.42, é exibido o arquivo de ajuda, no qual estão descritas todas as opções de configuração do template Ineteres.adm, o qual contém as opções de configuração do Internet Explorer. O arquivo de ajuda apresenta uma descrição detalhada de todas as opções de configuração disponíveis.

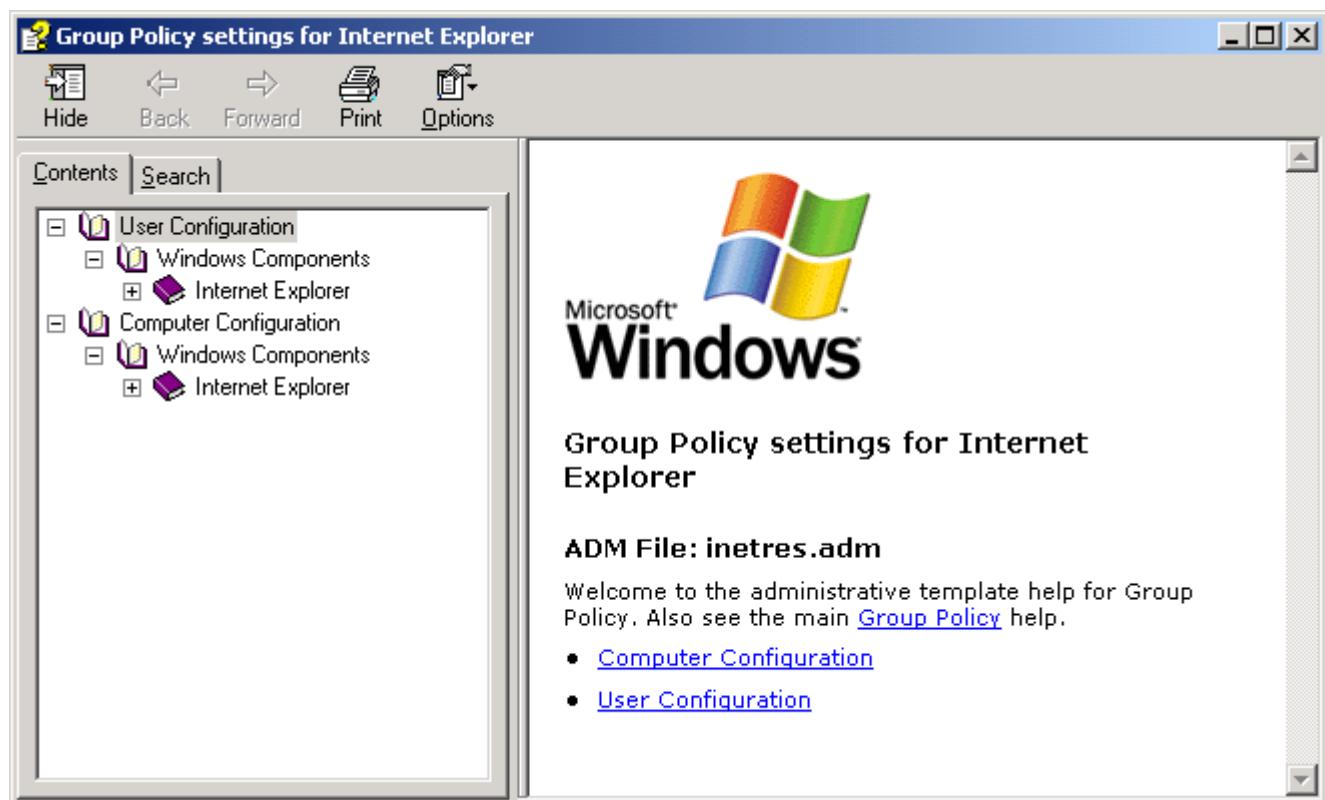


Figura 9.42 O arquivo de ajuda do template de configuração do Internet Explorer via GPO.

- ◆ **Novos comandos:** O comando gpupdate é utilizado para atualizar as polices aplicadas ao computador ou ao usuário logado e substitui o comando secedit /refreshpolicy, utilizado no Windows 2000 Server. O comando gprestart (disponibilizado no Resource Kit do Windows 2000 Server) foi aprimorado e agora está disponível com o Windows XP Professional, Windows XP edição de 64 bits e em todas as edições do Windows Server 2003.
- ◆ **Redireção de pastas:** Ficou mais fácil fazer a redireção de pastas, usando GPOs. Agora o administrador não precisa mais utilizar variáveis de ambiente tais como %username%, como parte do caminho de redireção. Existe uma nova opção para redirecionar a pasta Meus documentos para o diretório home do usuário (para detalhes sobre o diretório home, consulte o tópico sobre User profile, no Capítulo 4). Esta opção é para uso em ambientes onde o mecanismo de roaming profiles e diretório home já está implementado.
- ◆ **Instalação de software:** Existem novas opções que permitem que sejam habilitada ou desabilitada a disponibilidade de aplicações de 32 bits, em computadores rodando versões de 64 bits do Windows (Windows XP edição de 64 bits ou Windows Server 2003 edição de 64 bits). Também existe uma nova opção para habilitar/desabilitar a publicação de informações sobre as classes OLE de um pacote de software. Mas a novidade que eu achei mais interessante, mais útil para o administrador é a opção para forçar que uma aplicação que foi associada com o usuário, seja automaticamente instalada, antes mesmo de o usuário ter clicado no ícone da aplicação. Ou seja, quando o usuário clicar no ícone da aplicação ele já terá sido instalada e não será necessária a instalação através da rede.
- ◆ **Resultant Set of Policy (Conjunto resultante de políticas) - RSoP:** E de todas as novidades, sem dúvidas, esta é a mais útil. Esta é uma nova ferramenta, a qual facilita a resolução de problemas relacionados às políticas de segurança. Com esta ferramenta o administrador pode ter uma descrição detalhada do conjunto efetivo de políticas que está sendo aplicado a um usuário e poderá corrigir erros existentes.
- ◆ **Suporte entre florestas:** Com o Windows Server 2003 é possível gerenciar e aplicar políticas para objetos e usuários localizados em florestas remotas, as quais mantenham relações de confiança com a floresta na qual você trabalha. Esta novidade é consequência do mecanismo de relação de confiança entre florestas, o qual também é uma novidade do Windows Server 2003. Com este mecanismo também é possível usar a ferramenta RsoP em florestas remotas.

## Entendendo como é feito o processamento e aplicação das GPOs.

Este é um item que eu considero de fundamental importância para o administrador. Configurar as GPOs, conforme você verá mais adiante, é relativamente simples, com o uso do console de administração das GPOs.

Porém, mais do que saber configurar as GPOs, o administrador precisa entender exatamente como as GPOs são processadas e aplicadas às estações de trabalho e aos usuários. Com este entendimento, o administrador tem condições de planejar as políticas a serem implementadas e também de resolver problemas relacionados a aplicação das GPOs. Por isso é fundamental que o administrador entenda, exatamente, como é feito o processamento e aplicação das GPOs.

No NT Server 4.0 as configurações de Polices são armazenadas em um arquivo com a extensão .pol, arquivo este que é gravado no compartilhamento NETLOGON do PDC e de todos os BDCs do domínio. Para clientes Windows 9x/Me o arquivo deve ter o nome config.pol e para clientes com o NT 4.0, o arquivo deve ter o nome ntconfig.pol. As configurações definidas neste arquivo são carregadas durante o logon e aplicadas à registry da estação de trabalho do usuário. As configurações de usuário são carregadas na opção HKEY\_CURRENT\_USER (HKCU), da registry. As configurações de computador são carregadas na opção HKEY\_LOCAL\_MACHINE (HKLM), da registry.

Já no Windows Server 2003 o processamento das GPOs segue caminhos bem diferentes, os quais serão descritos neste item.

No NT Server 4.0 um único conjunto de políticas é aplicado ao usuário/computador, conjunto este que é definido no arquivo .POL, carregado quando o computador é inicializado e o usuário faz o logon. Já no Windows Server 2003 (e também no Windows 2000 Server), mais de um conjunto de políticas pode ser aplicado ao mesmo usuário/computador. Por exemplo, imagine o usuário jsilva, do domínio abc.com, cuja conta está na OU Vendas, dentro da OU RegiãoSul. Para este usuário, será aplicada a GPO local, mais a GPO do domínio (uma ou mais GPOs que estiverem definidas no domínio abc.com), mais o conjunto de GPOs definidas para a OU RegiãoSul e mais o conjunto de GPOs definidas para a OU Vendas.

As configurações das GPOs são armazenadas em uma estrutura de pastas e arquivos dos DCs do domínio. Estas informações são gravadas na pasta SYSVOL e são replicadas para todos os DCs do domínio. Na Figura 9.43 apresento uma visão geral da pasta onde ficam gravadas as informações sobre as GPOs do domínio abc.com (C:\WINDOWS\SYSVOL\sysvol\abc.com\Policies), onde o Windows Server 2003 está instalado na pasta Windows, no drive C:

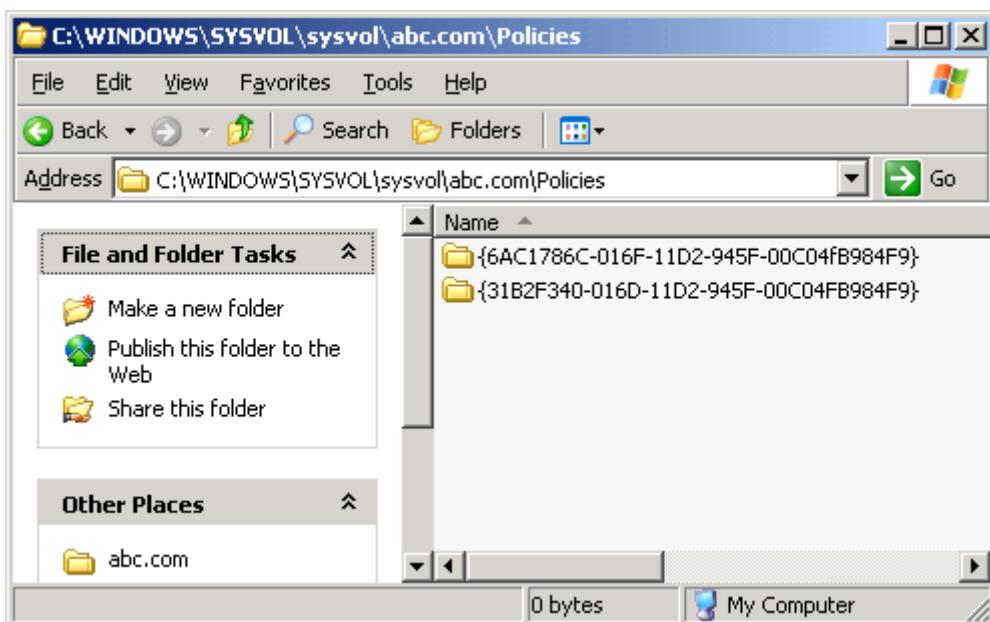


Figura 9.43 A pasta com informações das GPOs.

Cada pasta representa uma determinada GPO. Ao abrir uma destas pastas, será exibido o seguinte conteúdo:

- ◆ **Pasta Adm:** Contém os arquivos com os templates administrativos.]
- ◆ **Pasta Scripts:** Se houver scripts definidos neste template, esta pasta conterá os scripts e arquivos relacionados.
- ◆ **Pasta MACHINE:** Contém as configurações que se aplicam a computadores. Esta pasta contém um arquivo chamado Registry.pol, o qual contém as configurações de registry que serão aplicadas ao computador durante a inicialização (veja os passos de aplicação das polices durante a inicialização do computador, mais adiante). Quando o computador é inicializado, é feito o download do arquivo Registry.pol e são aplicadas as configurações definidas neste arquivo. As configurações são aplicadas na opção HKEY\_LOCAL\_MACHINE, da registry.
- ◆ **Pasta USER:** Contém as configuração que se aplicam a usuários. Esta pasta contém um arquivo chamado Registry.pol, o qual contém as configurações de registry que serão aplicadas ao usuário quando este fizer o logon (veja os passos de aplicação das polices durante a inicialização do computador, mais adiante). Quando o computador é inicializado, é feito o download do arquivo Registry.pol e são aplicadas as configurações definidas neste arquivo. As configurações são aplicadas na opção HKEY\_CURRENT\_USER, da registry
- ◆ **Arquivo GPT.INI:** Informações sobre a versão da GPO. Utilizada pelo serviço de replicação.

Abra uma destas pastas, por exemplo a pasta Adm. Serão exibidos os templates administrativos disponíveis, conforme exemplo da Figura 9.44:

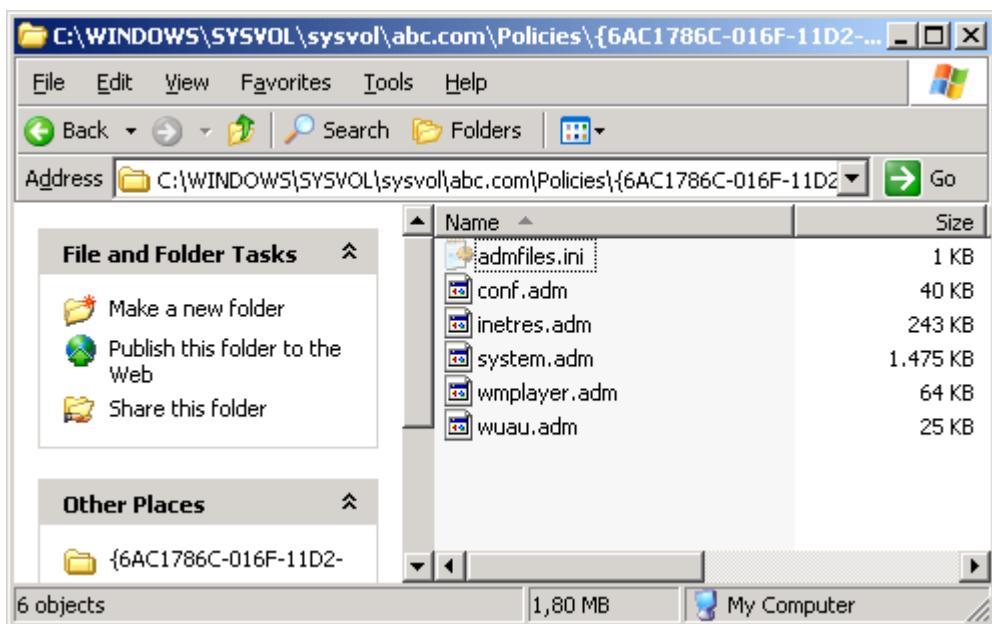


Figura 9.44 Templates administrativos.

Em resumo: As informações sobre as GPOs são gravadas em uma estrutura de pastas e arquivos, dentro da pasta SYSVOL. Esta estrutura é replicada para todos os DCs do domínio. As informações gravadas na pasta SYSVOL são os chamados modelos de GPOs, oficialmente conhecidos como Group Policy Template (GPT). O template é que define quais opções de configuração estarão disponíveis, para serem configuradas via GPO. Por exemplo, o template de GPO para usuários define quais opções de usuários poderão ser configuradas via GPO. Quando uma nova GPO é criada, o Windows Server 2003 cria a GPO com base nos templates da pasta Sysvol. A nova GPO que é criada e as configurações nela definidas são armazenadas no Active Directory. Esta GPO é conhecida como GPC – Group Policy Container. Ou seja, uma GPO é criada com base em um modelo (GPT, armazenado na pasta SYSVOL). O modelo define quais opções de configuração estarão disponíveis. Após criada e configurada, a GPO é salva na base de dados do Active Directory, quando é conhecida como GPC – Group Policy Container. Estas definições muitas vezes se confundem. Nos exemplos práticos, quando você aprenderá a criar e a configurar as políticas, usarei sempre o termo genérico GPO.

Toda GPO é dividida em duas partes também conhecidas como seções:

- ◆ Seção do usuário.
- ◆ Seção do computador.

Conforme o próprio nome sugere, estas seções contém as configurações específicas aplicadas a usuários ou computadores especificamente. Quando um computador com o Windows 2000, Windows XP Professional ou Windows Server 2003, pertencente ao domínio é inicializado, o Windows verifica se existem novas GPOs ou alterações nas GPOs existentes e aplica as configurações definidas na seção do computador (independentemente de algum usuário ter feito o logon ou não). Quando o usuário faz o logon no domínio (em qualquer computador da rede com uma das versões do Windows descritas no início do parágrafo), o Windows verifica se existem GPOs a serem aplicadas a este usuário ou alterações nas GPOs já aplicadas e aplica as configurações definidas na seção de usuário destas GPOs. Estas informações, ficam gravadas no Active Directory. Conforme descrito anteriormente (estou insistindo

neste ponto porque ele é muito importante), uma GPO é criada com base nos modelos armazenados na pasta Sysvol (GPT- Group Policy Templates). Uma vez criada e configurada, a GPO é salva no Active Directory (tornando-se uma GPC – Group Policy Container). Quando um usuário faz o logon o Windows Server 2003 verifica no Active Directory se existem GPCs a serem aplicadas para o usuário. Quando um computador é inicializado, o Windows Server 2003 verifica no Active Directory, se existem GPCs a serem aplicadas ao computador. É isso.

## Detalhando a ordem de processamento das GPOs.

As GPOs são processadas na seguinte seqüência:

1. GPO Local: Cada computador com o Windows 2000, Windows XP Professional ou Windows Server 2003, possui uma GPO local, a qual é aplicada em primeiro lugar, antes das demais GPOs que possam estar disponíveis.
2. GPO associada ao site do qual faz parte o computador que está sendo inicializado. Lembre, que um site é definido por uma ou mais sub-redes. O Windows Server 2003 identifica a qual site pertence um computador, pelas identificação de rede do computador (propriedades do Protocolo TCP/IP).
3. GPOs associadas ao domínio: Em seguida são processadas as GPOs associadas ao domínio, conforme a ordem de execução definida pelo administrador.
4. GPOs associadas a todas as OUs do caminho. Por exemplo, se um computador pertence a OU Vendas, que está dentro da OU RegiãoSul, primeiro serão aplicadas as GPOs da OU RegiãoSul, para depois serem aplicadas as GPOs associadas a OU Vendas. Quando houver mais de uma GPO associada a mesma OU, as GPOs serão aplicadas na seqüência que foi definida pelo administrador.

Com esta seqüência, as GPOs aplicadas por último tem preferência em relação as que são aplicadas anteriormente. Por exemplo, se na GPO do domínio está que o usuário não deve ter acesso ao comando Iniciar -> Executar, porém na GPO da OU do usuário este comando está habilitado, valerá a configuração da GPO da OU, ou seja, comando habilitado, uma vez que esta GPO será aplicada por último. O administrador tem meios para fazer com que uma GPO de nível mais alto, como por exemplo a GPO de domínio, não tenha suas configurações sobreescritas por GPOs de nível mais baixo, aplicadas por último, como uma GPO associada a uma unidade organizacional. Para implementar esta configuração, o administrador marca a opção “No Override” (Não sobrecrever), conforme você aprenderá na parte prática.

Algumas exceções na ordem de aplicação das GPOs:

- ◆ Qualquer GPO que estiver associada a um site, domínio ou unidade organizacional (a única exceção é a GPO local), poderá ser configurada com a opção “No Override”, de tal maneira que suas configurações não possam ser sobreescritas pelas GPOs que serão aplicadas depois. Caso duas GPOs, no mesmo caminho, tenham esta opção marcada, valerá a configuração da GPO que estiver mais acima na hierarquia de objetos. Por exemplo, se uma GPO de domínio está marcada com a opção No Override e uma GPO de uma unidade organizacional também está marcada com a opção No Override, em caso de conflito nas configurações destas duas GPOs, valerá a configuração da GPO de domínio, que é a que está mais acima na hierarquia de objetos do Active Directory.

---

**IMPORTANTE:** Deve ser observado que a propriedade No Override é uma propriedade da ligação da GPO com o domínio, site ou unidade organizacional. Esta não é uma propriedade da GPO propriamente dita. Uma GPO poderá ser associada em diferentes locais no Active Directory. Por exemplo posso associar uma determinada GPO com o domínio e também com uma ou mais unidades organizacionais do domínio. Em uma das associações posso habilitar a opção No Override, em outras não e assim por diante. Lembre (principalmente para os exames de certificação do MCSE 2003): A propriedade No Override é uma propriedade da ligação (objeto do tipo link) entre uma GPO e um domínio, site ou unidade organizacional e não uma propriedade da GPO propriamente dita.

---

## O recurso de loopback.

Existe um recurso avançado das polices, o qual é conhecido como Loopback. Este recurso é especialmente recomendado para computadores que estão conectados à rede da empresa mas com acesso ao público externo, como por exemplo em quiosques de informação ao público, terminais de auto-atendimento e computadores de salas de treinamentos.

O recurso de Loopback permite que você defina uma ordem alternativa para aplicação das GPOs. Lembrando que a ordem padrão é: local, site, domínio e unidade organizacional. O recurso de Loopback pode ser configurado com os valores Not configured (Não configurado), Enabled (Habilitado) ou Disabled (Desabilitado). Se este recurso for habilitado, ele poderá ser configurado com as opções Merge ou Replace, conforme descrito a seguir:

**IMPORTANTE:** Computadores que não fazem parte do domínio, como por exemplo computadores configurados para fazer parte de um Workgroup, irão processar e aplicar apenas a GPO local, uma vez que todas as demais GPOs são carregadas a partir do Active Directory. Como o computador não faz parte do domínio, ele não tem acesso ao Active Directory.

- ◆ **Loopback configurado com a opção Replace:** Com este método, a lista de execução padrão (que define a seqüência de aplicação das GPOs) será substituída pela lista definida no próprio computador.
- ◆ **Loopback configurado com a opção Merge:** Com este método, a lista de execução padrão (que define a seqüência de aplicação das GPOs) será concatenada com lista definida no próprio computador. As GPOs obtidas a partir da lista definida no próprio computador serão aplicadas por último, o que fará com que estas GPOs tenham precedência em relação as GPOs definidas pela lista padrão, obtida a partir do Active Directory.

## Ordem de eventos quando o computador é inicializado e o usuário faz o logon:

Neste item descrevo a ordem de eventos que ocorrem quando um computador é inicializado e quando o usuário faz o logon.. Considerando um computador que pertence ao domínio e possui o Windows 2000, Windows XP Professional ou Windows Server 2003, instalado,

1. O computador é ligado, o Windows é inicializado e os serviços de rede são carregados.
2. Uma lista ordenada de objetos do tipo GPO é obtida pelo computador. A maneira como esta lista é obtida, depende dos seguintes fatores:
  - 2.1. O computador deve fazer parte do domínio e obter esta lista a partir das informações do Active Directory. Se o computador não fizer parte do domínio, apenas a GPO local será aplicada.
  - 2.2. A lista depende de onde está contida a conta do computador, no Active Directory. Por exemplo, a unidade organizacional onde encontra-se a conta, definirá quais GPOs serão aplicadas, as configurações de rede definem a qual site pertence o computador e quais GPOs de site (se houver alguma), serão aplicadas e assim por diante.
  - 2.3. De a lista de GPOs ter sido alterada desde a última inicialização. Se a lista de GPOs não foi alterada, nenhum processamento será feito.
3. As configurações relativas ao computador serão aplicadas, a partir da lista de GPOs obtidas. As GPOs são aplicadas na ordem descrita anteriormente: local, site, domínio e unidade organizacional.
4. Se houver um script de inicialização configurado ele será executado. Pode haver mais de um script de inicialização configurado. Neste caso eles serão executados na ordem em que foram definidos e de maneira síncrona, ou seja, um script é executado e somente que ele concluir a sua execução, o próximo será executado e assim por diante. Existem também um tempo máximo de execução para cada script, que por padrão é de 600 segundos. Se o script não terminar a sua execução neste tempo, ele será encerrado e o próximo script (se houver) será inicializado.
5. Após terem sido feitos estes processamentos, a tela de logon é exibida. O usuário pressiona CTRL-ALT-DEL para fazer o logon.

6. O usuário digita as suas informações de logon e é validado por um dos DCs da rede. Após a validação do usuário, a sua profile é carregada.
7. Uma lista ordenada de objetos do tipo GPO é obtida pela usuário. A maneira como esta lista é obtida, depende dos seguintes fatores:
  - 7.1. Se o usuário está fazendo o logon no domínio e, portanto, recebendo a lista de GPOs a serem aplicadas a partir do Active Directory.
  - 7.2. Se o recurso de Loopback está habilitado e, estando habilitado, qual opção está definida (Merge ou Replace).
  - 7.3. A lista depende de onde está contida a conta do usuário, no Active Directory. Por exemplo, a unidade organizacional onde encontra-se a conta, definirá quais GPOs serão aplicadas.
  - 7.4. De a lista de GPOs ter sido alterada desde a última inicialização. Se a lista de GPOs não foi alterada, nenhum processamento será feito. Este comportamento pode ser alterado.
8. As configurações relativas ao usuário serão aplicadas, a partir da lista de GPOs obtidas. As GPOs são aplicadas na ordem descrita anteriormente: local, site, domínio e unidade organizacional.
9. O script de logon definidos nas GPOs serão executados. Estes scripts são executados sem que seja exibida uma tela de execução dos scripts e de maneira síncrona, ou seja, um após o outro, conforme descrito para a execução de scripts de inicialização. O script de logon, definido nas propriedades da conta do usuário, no Active Directory, será executado após a execução dos scripts definidos via GPOs. Este script é executado e uma janela do prompt de comando é exibida. Observe que podem ser executados vários scripts de logon, em seqüência, sendo que estes scripts são definidos nas GPOs que se aplicam ao usuário e o último script a ser executado é o script de logon definido nas propriedades da conta do usuário, no Active Directory.
10. A área de trabalho do usuário é carregada e o Windows está pronto para ser utilizado.

Alguns casos especiais em relação a execução das polices:

- ◆ Pode acontecer uma situação em que o usuário está fazendo o logon em um computador que pertence a um domínio do NT Server 4.0, porém fazendo o logon em um domínio baseado no Windows Server 2003 (sendo que existem relações de confiança entre os domínios). Neste caso, para as configurações de computador serão aplicadas as configurações definidas no sistema de Polices do NT 4.0 e para o usuário, será aplicada a parte relativa as configurações de usuário, das GPOs definidas no domínio de origem do usuário. Pode ocorrer o contrário, ou seja, a conta de computador ser de um domínio do Windows Server 2003 e a conta do usuário de um domínio do NT Server 4.0. Neste caso serão aplicadas as configurações de computador, obtidas via GPO e as configurações de polices definidas para o usuário, no domínio de origem da conta.
- ◆ Se for um computador com o Windows XP Professional ou Windows Server 2003, porém pertencente a um domínio baseado no NT Server 4.0, somente serão aplicadas as polices do NT Server 4.0, já que em um domínio baseado no NT Server 4.0 não existe o conceito de GPO.

## **Entendendo como funciona o mecanismo de herança – Policy inheritance**

Por padrão, as GPOs são aplicadas a partir do objeto pai (a raiz do domínio), passando pelos objetos filho, até a unidade organizacional onde está a conta do usuário ou do computador. É importante salientar este funcionamento é dentro de um mesmo domínio, não existe uma herança de GPOs entre domínios. Por exemplo, as GPOs aplicadas em um domínio raiz abc.com, não serão herdadas e aplicadas nos domínios filho, tais como vendas.abc.com e rh.abc.com.

Porém dentro do domínio, o funcionamento é o padrão descrito nos itens anteriores. Se você associar uma GPO com um determinado elemento do Active Directory (um domínio ou uma unidade organizacional), as configurações desta GPO também serão aplicadas a todos os objetos contidos nos elementos filho. Por exemplo, se você aplicar uma GPO

no domínio, todos os objetos do domínio receberão as configurações desta GPO. Se você aplicar uma GPO a uma unidade organizacional, todos os objetos (inclusive objetos contidos em unidades organizacionais dentro da unidade organizacional que está sendo configurada) contidos nesta unidade organizacional receberão estas configurações. Porém é importante lembrar que, ao associar uma GPO com um objeto filho (por exemplo uma unidade organizacional), as configurações desta GPO irão sobrescrever as configurações do objeto Pai (por exemplo o domínio), pois são executadas por último, a não ser que o mecanismo de No Override tenha sido habilitado na GPO do objeto Pai.

Para entender os conceitos apresentados a seguir, vamos considerar o exemplo de um domínio chamado abc.com, no qual foi criada uma unidade organizacional chamada Sul. Dentro desta unidade organizacional foi criada uma outra unidade organizacional chamada Vendas. Para a discussão que apresentarei a seguir, Sul é referenciada como OU pai (em Inglês é usado o termo Parent) e Vendas é referenciada como OU filho (em Inglês é usado o termo child).

Se nas configurações de GPO da OU pai, houver itens que estão marcados como Não configurados, a OU filho não irá herdar estes itens “não configurados”. Lembrando que a maioria das opções pode ser marcada como Enabled (Habilitada), Disabled (Desabilitada) ou Not defined (Não definida). As opções que tiverem o valor padrão como desabilitado, também serão definidas como desabilitado na OU filho. As opções que estiverem configuradas na OU pai, habilitadas ou desabilitadas (não confundir com aquelas que tem o valor padrão como desabilitada) e as respectivas opções não estiverem configuradas na OU filho, serão herdadas pela OU filho, com o mesmo valor definido na OU pai (habilitada ou desabilitada). Se uma determinada opção estiver configurada na OU filho, valerá o que está configurado na OU filho, a não ser que a opção No Override tenha sido definida na GPO da OU pai.

Se as configurações definidas na OU pai e as políticas definidas em uma OU filho são compatíveis, isso é, se não houver conflito, a OU filho irá herdar as definições da OU pai e irá aplicá-las normalmente na OU filho.

Se houver configurações definidas na OU pai, as quais são incompatíveis com as configurações definidas na OU filho (por exemplo, uma determinada police está habilitada na GPO da OU pai e desabilitada na police da OU filho), estas configurações não serão herdadas pela OU filho. Será aplicada a configuração definida na OU filho.

#### Como bloquear a herança (Blocking inheritance):

A herança pode ser bloqueada tanto em nível de domínio quanto em nível de unidade organizacional. Esta opção é configurada nas propriedades do domínio ou da OU respectivamente, conforme você aprenderá na parte prática, mais adiante.

#### Forçando a herança (Enforcing inheritance):

Para forçar a herança, ou seja, para fazer com que os objetos filho, obrigatoriamente, tenham que aplicar as configurações definidas no objeto pai, você utiliza a opção No Override (Não substituir), já descrita anteriormente e que será exemplificada na parte prática. Ao marcar esta opção, você força todos os objetos filho a herdarem as configurações definidas no objeto Pai, mesmo que existam conflitos de configuração e mesmo que a opção Blocking inheritance tenha sido habilitada no objeto filho.

#### Algumas observações importantes:

- ◆ Polices que foram configuradas com a opção No Override (Não substituir) serão aplicadas, independentemente das configurações existentes nos objetos filho.
- ◆ As opções No Override (Não substituir) e Blocking inheritance (Bloquear herança de diretiva) devem ser utilizadas com cautela, pois o uso muito intensivo destes recursos, torna difícil o trabalho de identificar e resolver problemas de configuração, quando não se está obtendo o resultado desejado.

## **Exemplos práticos de uso das opções “No Override (Não substituir)” e “Block Policy inheritance (Bloquear herança de diretiva)”:**

Neste tópico vou descrever algumas situações práticas, onde o uso das configurações “No Override” e “Block Policy inheritance” se aplica.

### **Situação 01:**

Como administrador do domínio abc.com você gostaria de implementar um conjunto de configurações usando GPO. Este conjunto deve ser aplicado a todos os computadores e usuários dos domínios. Essas configurações não devem ser sobreescritas por GPOs ligadas a objetos filhos, tais como GPOs ligadas a OUs do domínio. Qual a solução para a situação descrita?

Esta é uma situação de solução bastante simples e ao mesmo tempo muito comum. Neste caso, como as configurações devem ser aplicadas a todos os usuários e computadores do domínio, elas devem ser feitas na GPO padrão do domínio, com a qual você aprenderá a trabalhar mais adiante. Para que estas configurações não possam ser sobreescritas por configurações definidas nas GPOs dos objetos filho, você deve marcar a opção No Override (Não sobreescrivir), na guia Diretiva de grupo (botão Opções...) da janela de propriedades do domínio. Este é um exemplo típico (talvez o mais típico que possa ser imaginado) de onde é necessário a utilização da propriedade No Override (Não sobreescrivir).

### **Situação 02:**

Como administrador do domínio abc.com você gostaria de implementar um conjunto de configurações usando GPO. Este conjunto deve ser aplicado a todos os computadores e usuários dos domínios. Existe uma única OU do domínio, na qual devem ser aplicadas configurações especiais e não devem ser aplicadas as configurações definidas na GPO padrão do domínio. Nesta OU estão as contas de usuários e computadores do setor de pesquisa, e uma série de configurações especiais de segurança devem ser aplicadas via GPO. Qual a solução para a situação descrita?

Nesta situação o administrador deve configurar a GPO padrão do domínio, com as configurações que serão utilizadas pela maioria dos usuários e computadores, com exceção dos usuários e computadores da OU Pesquisa. Na OU pesquisa, crie e configure uma GPO com as configurações exigidas pelos usuários e computadores desta OU. Marque a opção Block Policy inheritance (Bloquear herança de diretiva), na guia Diretiva de grupo da janela de propriedades da OU pesquisa. Com esta configuração a OU pesquisa não irá herdar as definições de GPOs aplicadas ao domínio e somente será aplicadas as GPOs definidas na própria OU Pesquisa, que é exatamente o que deve ser feito para solucionar a questão proposta.

Bem, sobre a teoria inicial de GPOs era isso. Agora você aprenderá uma série de ações práticas sobre GPOs. Após as ações práticas falarei sobre uma outra funcionalidade muito importante das GPOs que é a distribuição de software. Durante os exemplos práticos serão apresentados diversos conceitos relacionados com o tópico que está sendo exemplificado.

## **Implementação e Administração de GPOs.**

Neste tópico apresentarei uma série de itens relacionados a implementação, configuração e administração das GPOs. A medida que forem sendo apresentados os exemplos, também apresentarei a teoria associada. Você aprenderá desde como abrir o console para administração das GPOs, como fazer as configurações básicas e passará por tópicos mais avançados, tais como a descrição detalhada de como as informações sobre GPOs são armazenadas no Active Directory e como utilizar o recurso de distribuição de software via GPOs.

## O console de administração das GPOs.

Existe um console especialmente criado para a criação, configuração e administração das GPOs. Este console pode ser aberto de várias maneiras. Uma das mais utilizadas é através da janela de propriedades do domínio ou da janela de propriedades de uma OU do domínio. Nestas janelas está disponível uma guia chamada Group Policy, na qual são listadas as GPOs que estão sendo aplicadas. Você também pode criar um console personalizado e adicionar somente o Snap-in para administração das GPOs.

Eu, particularmente, prefiro acessar o console através das propriedades do domínio ou das propriedades de uma OU, pois com este método tenho uma visão geral da hierarquia de objetos do Active Directory e posso, rapidamente, acessar administrar as GPOs de cada objeto. Neste item mostrarei os passos necessários para acessar o console de administração das GPOs, usando o console Usuários e computadores do Active Directory.

Exemplo: Utilizar o console Usuários e Computadores do Active Directory para acessar, rapidamente, as GPOs configuradas no domínio:

1. Faça o logon como administrador ou com uma conta com permissão de administrador.
2. Abra o console Usuários e computadores do Active Directory: Iniciar -> Ferramentas administrativas -> Usuários e computadores do Active Directory.
3. Para abrir a GPO padrão do domínio, dê um clique com o botão direito do mouse no domínio desejado e, no menu de opções que é exibido, clique em Propriedades. Será exibida a janela de propriedades do domínio.
4. Clique na guia Diretiva de grupo. Será exibida a lista de GPOs definidas para o domínio, conforme indicado na Figura 9.45. Observe que, por padrão, está associada uma única GPO, chamada Default Domain Policy.

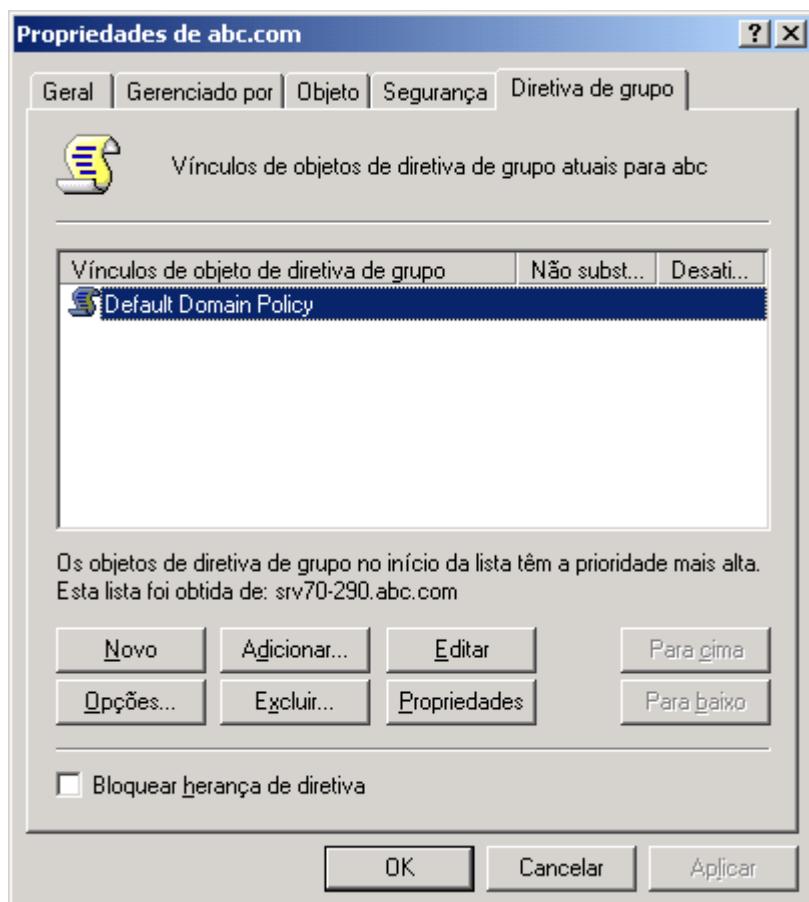


Figura 9.45 Lista de GPOs para o domínio abc.com.

5. Clique na GPO Default Domain Policy para selecioná-la e em seguida clique no botão Editar. Será aberto o console Editor de objeto de diretiva de grupo, com a GPO Default Domain Policy carregada.
6. Feche este console.
7. Clique com o botão direito do mouse em uma das unidades organizacionais criadas pelo administrador desejado e, no menu de opções que é exibido, clique em Propriedades. Será exibida a janela de propriedades da respectiva OU.
8. Clique na guia Diretiva de grupo. Observe que, por padrão, nenhuma GPO é definida a nível de unidade organizacional.
9. Feche o console Usuários e computadores do Active Directory.

Agora que você já sabe como acessar o console de administração de uma determinada GPO, é hora de entender as opções disponíveis e aprender a trabalhar com elas.

## Usando o console de configuração das GPOs.

Neste tópico mostrarei como “navegar” pelas opções disponíveis em um console de administração de uma GPO e como alterar as configurações das opções disponíveis.

Alterando configurações de uma GPO: Para alterar as configurações de uma GPO, o primeiro passo é carregar a GPO a ser alterada no console Group Policy Editor. No item anterior você aprendeu duas diferentes maneiras para carregar uma GPO no console Group Policy Editor.

Exemplo: Para acessar a GPO padrão do domínio e fazer alterações, siga os passos indicados a seguir:

1. Faça o logon como administrador ou com uma conta com permissão de administrador.
2. Abra a GPO Default Domain Policy, usando os passos descritos anteriormente.
3. A interface de administração de uma GPO é muito semelhante a interface de administração de pastas e subpastas do Windows Explorer. Observe que, por padrão, são exibidas duas opções no painel da esquerda, conforme indicado na Figura 9.46:

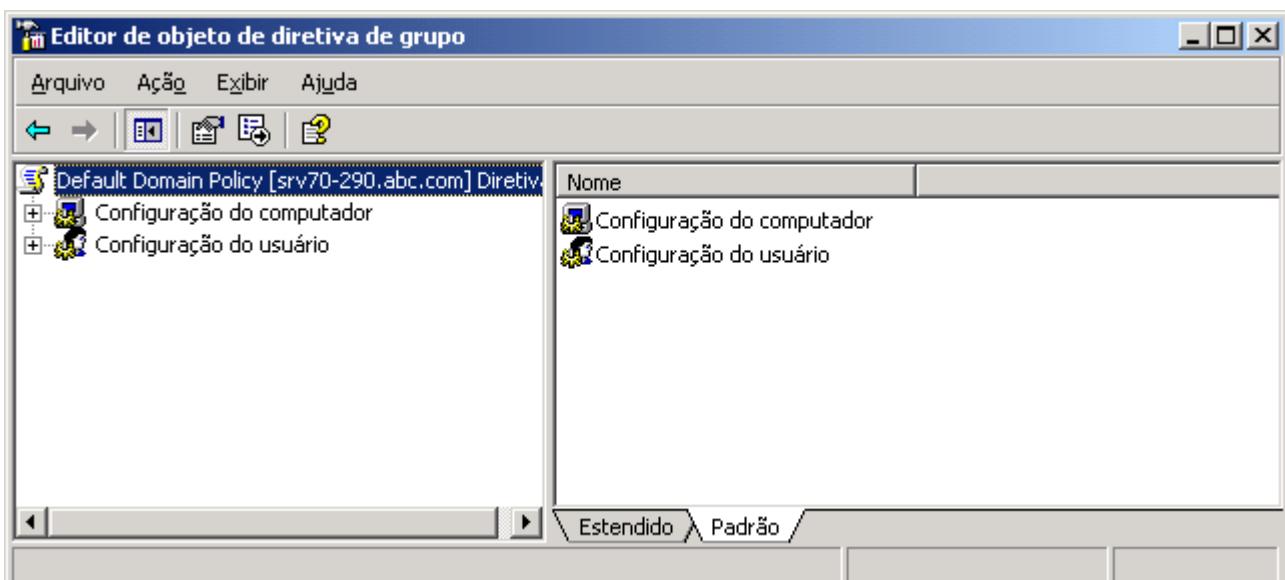


Figura 9.46 Opções da GPO Default Domain Policy.

**DICA:** Você pode abrir o console para edição da GPO local usando o console gpedit.msc, o qual já é instalado durante a instalação do Windows Server 2003. Para abrir este console, basta utilizar o comando Iniciar -> Executar. Digite gpedit.msc no campo Abrir e clique em OK.

Configuração do computador: Contém as opções de configuração que são aplicadas ao computador, durante o processo de inicialização, conforme detalhado anteriormente.

Configuração do usuário: Contém as opções de configuração que são aplicadas ao usuário, quando este faz o logon, conforme detalhado anteriormente.

4. Na parte de baixo do painel da direita, existem duas guias: Estendido e Padrão. Por padrão é selecionada a guia Estendido. Este é um novo modo de visualização que foi introduzido no Windows XP e que está presente no Windows Server 2003. No modo de visualização Estendido, quando você clica em uma determinada opção no painel da direita, é exibido um texto explicativo sobre a opção. Ao clicar na guia Padrão será exibido o modo padrão de visualização, sem a explicação relativa ao item selecionado.
5. Clique no sinal de + ao lado da opção Configuração do computador, no painel da esquerda. Será exibidos três grupos de polices que podem ser configuradas:

Configurações de software

Configurações do Windows

Modelos administrativos



Figura 9.47 Grupos de Polices disponíveis.

6. Agora você aprenderá a alterar as configurações de uma police. Aliás, você já parou para pensar porque o nome é GPO – Group Policy Objects. Group Policy significa um grupo de políticas ou um grupo de diretivas. Isto é em uma GPO estão disponíveis centenas de opções de configuração. Cada opção é uma police, uma política de segurança. As opções que estão disponíveis dependem dos templates (modelos) de polices, chamados de GPT – Group Policy Templates, os quais são gravados na pasta SYSVOL, conforme descrito anteriormente. E Objects, porque todos os componentes do Active Directory são denominados de objetos. Então uma GPO nada mais é do que um objeto do Active Directory, o qual representa um grupo de políticas, um grupo de polices um Group Policy. É isso.
7. Apenas a título de exemplo, vamos supor que você queira configurar a police que oculta o comando Executar do menu iniciar. Nos próximos passos vou mostrar como configurar esta police, apenas para ilustrar como é feita a configuração de uma police.

**NOTA:** As configurações de computador são aplicadas quando o computador é inicializado, conforme descrito anteriormente. Porém existem algumas configurações de segurança, que são reaplicadas periodicamente, normalmente a cada quinze minutos. Estas opções são reaplicadas, para garantir que os computadores estão com as configurações de segurança corretas e para evitar problemas com segurança.

**NOTA:** Clique no sinal de + ao lado da opção Configurações do usuários. Observe que são exibidos os mesmos grupos de polices da opção Configurações do computador, conforme indicado na Figura 9.47.

8. Esta police está disponível no seguinte caminho: Configuração do usuário -> Modelos administrativos -> Menu Iniciar e Barra de tarefas. Para acessar esta opção basta ir navegando no painel da esquerda, da mesma maneira que você navega pelas pastas e subpastas de um volume, usando o Windows Explorer. Por exemplo, clique no sinal de + ao lado da opção Configuração do usuário, para exibir os grupos de opções disponíveis. Clique no sinal de + ao lado da opção Modelos administrativos, para exibir as opções disponíveis. Das opções que são exibidas, clique em Menu ‘Iniciar’ e barra de tarefas, para selecioná-la. No painel da direita será exibida a lista de polices que podem ser configuradas para esta opção, conforme indicado na Figura 9.48:

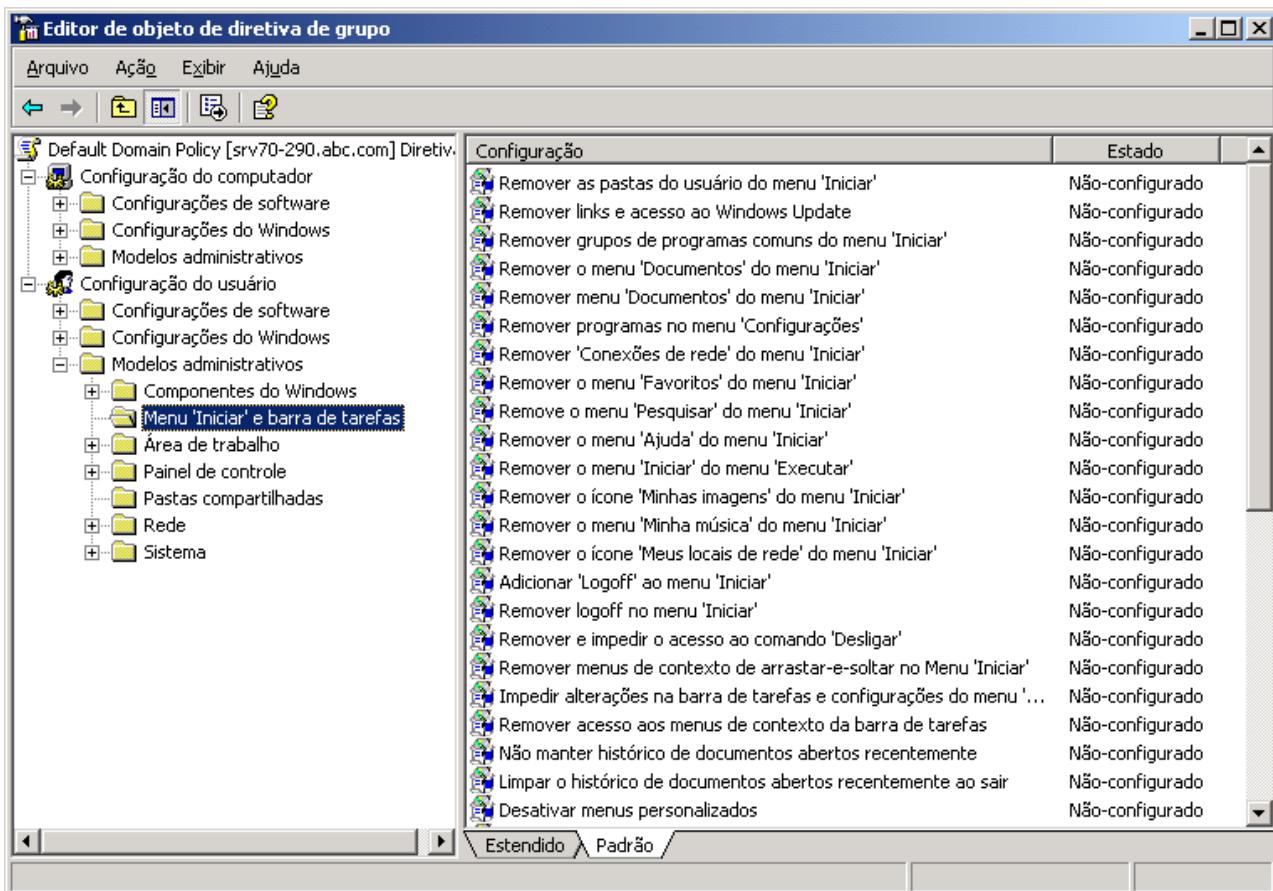


Figura 9.48 Polices disponíveis para a opção Menu ‘Iniciar’ e barra de tarefas.

9. Observe que somente para este item estão disponíveis dezenas de polices que podem ser configuradas. A maioria das polices está com o status Não-configurado, que na prática significa: não está sendo aplicada. Para configurar uma police basta dar um clique duplo nela, para abrir a janela com as opções de configuração. Na listagem de polices localize a opção Remover o menu ‘Iniciar’ do menu ‘Executar’ (mais um exemplo da má qualidade da tradução que é feita no Windows. O correto seria: Remover o comando Executar do menu Iniciar.) e clique nesta opção para selecioná-la. Para configurar a police dê um clique duplo nela, para abrir a janela com as opções de configuração.
10. Será aberta a janela com as propriedades de configuração da police. Para habilitar esta police e com isto fazer com que o menu Executar não seja exibido, marque a opção Ativado (ou seja, você está habilitando a política que faz com que o menu Executar seja retirado do menu Iniciar), conforme indicado na Figura 9.49:

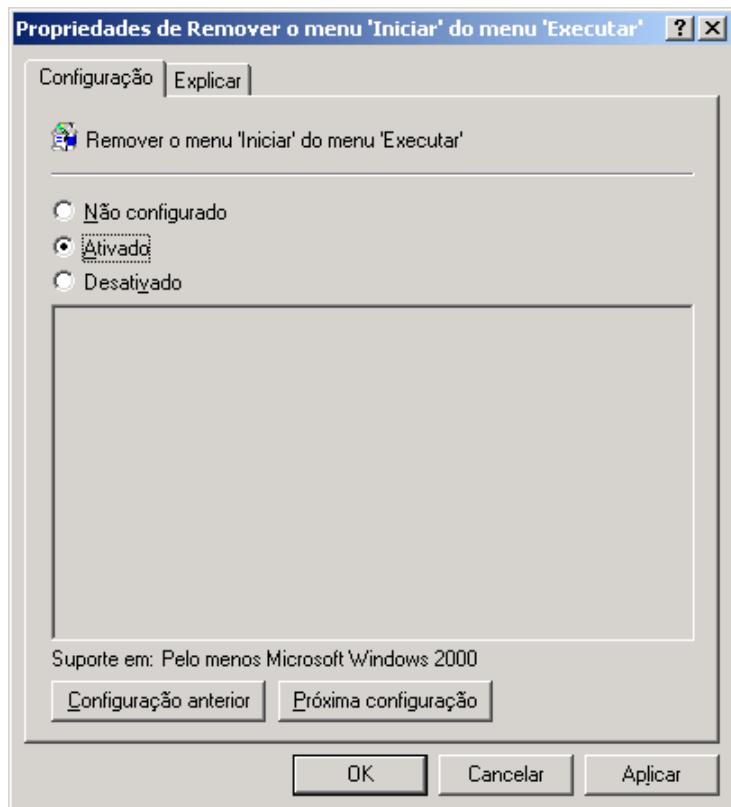


Figura 9.49 Habilitando a police que remove o comando Executar.

11. Clique na guia Explicar. Será exibido um texto com uma explicação detalhada sobre a aplicação da police, quais as consequências da sua habilitação e todos os demais detalhes sobre a police que está sendo configurada. Para configurar a police clique em OK. Pronto, na próxima vez que os usuários do domínio fizerem o logon (qualquer usuário, uma vez que estou fazendo a configuração na GPO padrão do domínio, a qual será aplicada a todos os usuários do domínio), a police será aplicada e o comando Iniciar -> Executar não estará mais disponível.
12. A maioria das polices apresenta as opções Não-configurado, Ativado e Desativado. Porém existem polices que exigem informações adicionais, como o exemplo da police Limitar tamanho do perfil, a qual encontra-se no caminho: Configuração do usuário -> Modelos administrativos -> Sistema -> Perfis de usuário. Ao habilitar esta police, você também deve informar o tamanho máximo que será configurado para o profile dos usuários, bem como outras opções de configurações, conforme indicado na Figura 9.50:
13. Como você deve ter observado, configurar as polices é extremamente simples. É uma questão de localizar a police a ser configurada, dar um clique duplo para abrir a janela de propriedades da police e configurá-la. Mas no “localizar a police a ser configurada” é que reside, talvez, a grande dificuldade. Isso porque eu são milhares de opções disponíveis e localizar exatamente o que você está precisando, pode não ser uma tarefa das mais simples. Com o lançamento do Resource Kit do Windows Server 2003, previsto para outubro próximo, é provável que a Microsoft disponibilize um arquivo de help com a descrição de todas as polices disponíveis. Pelo menos no Windows 2000 Server este arquivo é disponibilizado com o Resource Kit do Windows 2000 Server. Já está disponível para download, uma planilha com a descrição de todas as polices disponíveis na opção Administrative Templates (que é a opção com o maior número de polices). Esta referência está no formato de planilha do Excel e descreve as polices que se aplicam ao Windows 2000, Windows XP Professional e Windows Server 2003. Você pode fazer o Download desta planilha no seguinte endereço:

<http://download.microsoft.com/download/a/a/3/aa32239c-3a23-46ef-ba8b-da786e167e5e/PolicySettings.xls>

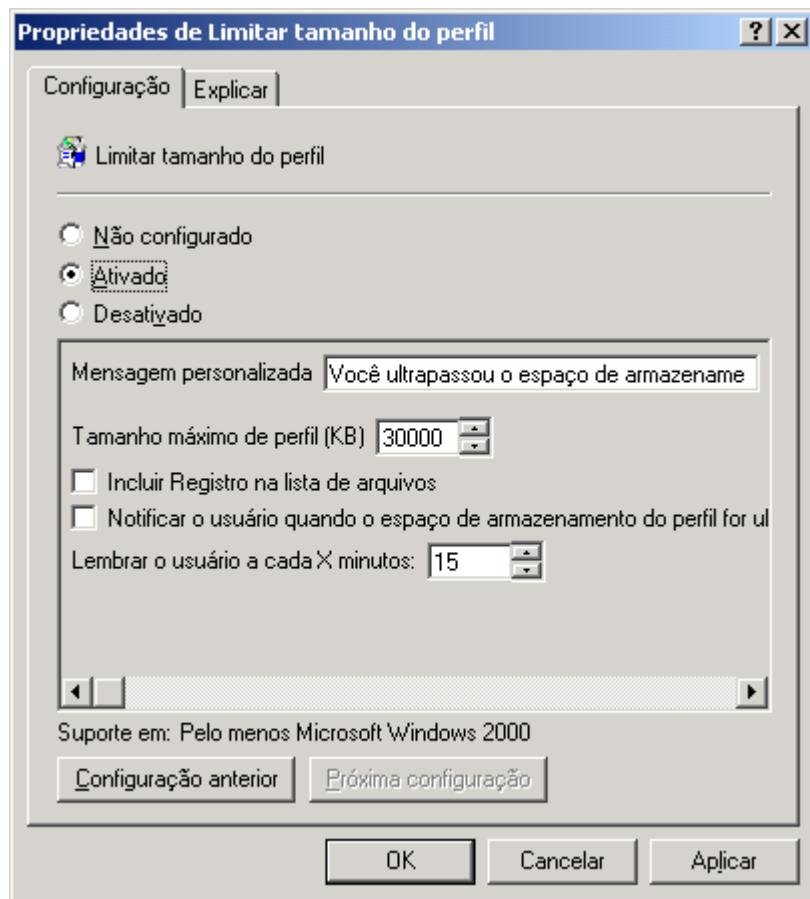


Figura 9.50 Um exemplo de police que precisa de configurações adicionais.

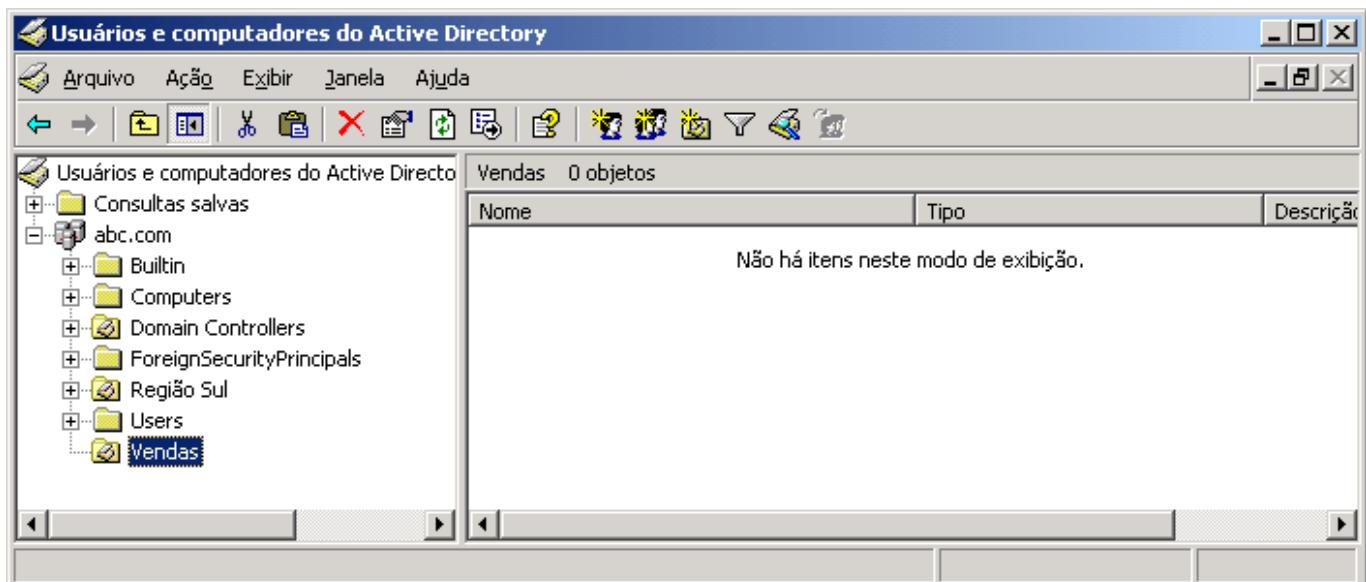
A seguir mais alguns links úteis em relação ao recurso de GPOs no Windows Server 2003:

- ◆ <http://www.microsoft.com/grouppolicy>
- ◆ <http://www.microsoft.com/windowsserver2003/technologies/management/grouppolicy/default.mspx>
- ◆ <http://www.microsoft.com/windowsserver2003/gpmc/default.mspx>
- ◆ <http://www.microsoft.com/windowsserver2003/techinfo/overview/gpintro.mspx>
- ◆ <http://www.microsoft.com/windowsserver2003/techinfo/overview/gpintro.mspx>

14. É importante salientar que quando você está configurando uma GPO não existe o conceito de salvar as alterações que foram efetuadas. Quando você abre a janela de propriedades de uma police, faz alterações e clica em OK, estas alterações já serão salvas no Active Directory. Não é preciso executar nenhum comando para salvar as alterações, antes de fechar o console de administração da GPO.
15. Feche o console de administração da GPO

## Criando uma nova GPO e associando-a com uma unidade organizacional:

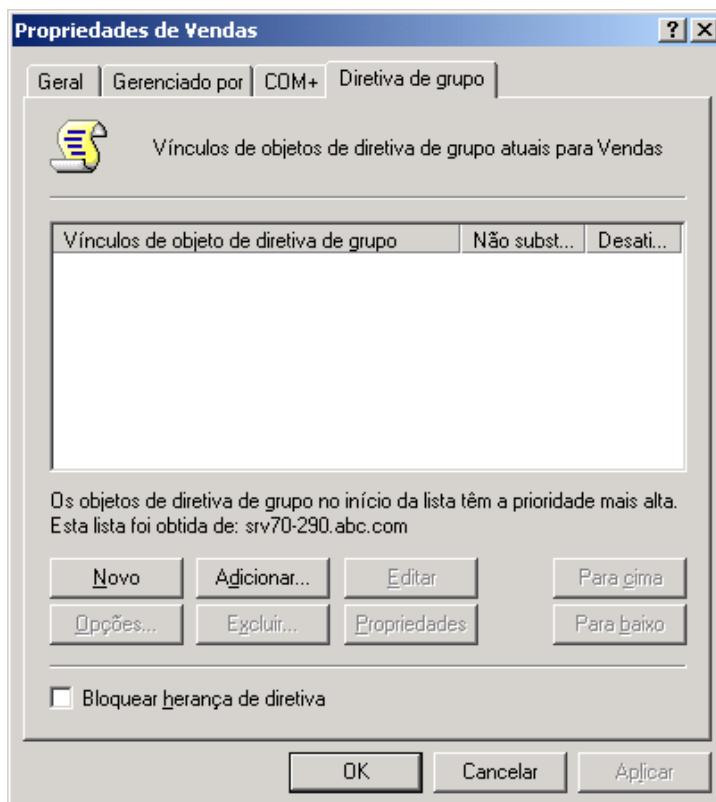
Neste tópico você aprenderá a criar uma novo GPO, associada a uma unidade organizacional e a configurar as propriedades da GPO e da ligação da GPO associada com a unidade organizacional. Para o exemplo deste item, criarei uma GPO chamada Configurações da seção de vendas, a qual será associada com a Unidade organizacional Vendas, do domínio abc.com, conforme ilustrado na Figura 9.51:



**Figura 9.51** A unidade organizacional **Vendas**, utilizada neste exemplo.

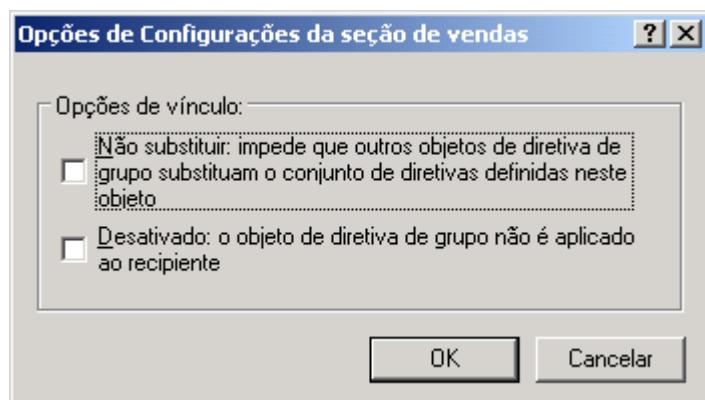
Exemplo: Para criar uma GPO associada a uma unidade organizacional e configurá-la, siga os passos indicados a seguir:

1. Faça o logon como administrador ou com uma conta com permissão de administrador.
2. Abra o console Usuários e computadores do Active Directory.
3. Localize a unidade organizacional para a qual você quer criar uma nova GPO. Clique com o botão direito do mouse nesta unidade organizacional e, no menu de opções que é exibido, clique na opção Propriedades.
4. Será exibida a janela de propriedades da unidade organizacional. Clique na guia Diretiva de grupo. Serão exibidas as opções da guia Diretiva de grupo, conforme indicado na Figura 9.52:



**Figura 9.52** A guia **Diretiva de grupo..**

5. Por padrão, quando uma unidade organizacional é criada, nenhuma GPO é associada com a unidade organizacional. Nesta situação, a unidade organizacional herda as configurações das GPOs definidas no domínio. Para criar uma nova GPO dê um clique no botão Novo.
6. Será criada uma nova GPO com o nome de Novo objeto de diretiva de grupo. Neste momento você deve digitar um nome para a GPO que está sendo criada. Digite Configurações da seção de vendas e clique no espaço em branco, fora do nome.
7. A GPO Configurações da seção de vendas será criada e já é exibida na lista de GPOs associadas a unidade organizacional. O próximo passo é configurar as polices que serão aplicadas pela GPO Configurações da seção de vendas.
8. Para configurar as polices que serão aplicadas, basta clicar na GPO Configurações da seção de vendas e depois clicar no botão Editar. A GPO Configurações da seção de vendas será carregada no console Group Policy Editor. Neste momento você pode configurar as polices que serão aplicadas pela GPO Configurações da seção de vendas. Para uma descrição resumida das opções disponíveis. Após ter feito as configurações desejadas, basta fechar o console Group Policy Editor, não é preciso salvar as alterações, uma vez que estas vão sendo salvas automaticamente, a medida que você define as configurações de cada police.
9. Ao fechar o console Group Policy Editor você estará de volta à guia Diretiva de grupo, da janela de propriedades da unidade organizacional que está sendo configurada. Observe que nesta janela está disponível a opção Bloquear herança de diretiva, já comentada anteriormente. O administrador pode marcar esta opção, para impedir que as configurações definidas nos objetos Pai, sejam propagadas para a unidade organizacional que está sendo configurada. Esta opção não terá efeito, se a opção Não sobrescrever tiver sido habilitada nas GPOs dos objetos pai.
10. Para configurar as opções da GPO, clique na GPO Configurações da seção de vendas para selecioná-la. Em seguida clique no botão Opções. Será exibida a janela de opções da GPO Configurações da seção de vendas, conforme indicado na Figura 9.53:



**Figura 9.53 A janela de opções da GPO.**

Nesta janela estão disponíveis as opções descritas a seguir:

- ◆ **Não sobrescrever:** Esta opção é utilizada para impedir que a aplicação da GPO seja bloqueada nos objetos filho, através do uso da opção Bloquear herança de diretiva, já descrita anteriormente.
- ◆ **Desativado:** Ao marcar esta opção, a GPO deixará de ser aplicada a unidade organizacional.

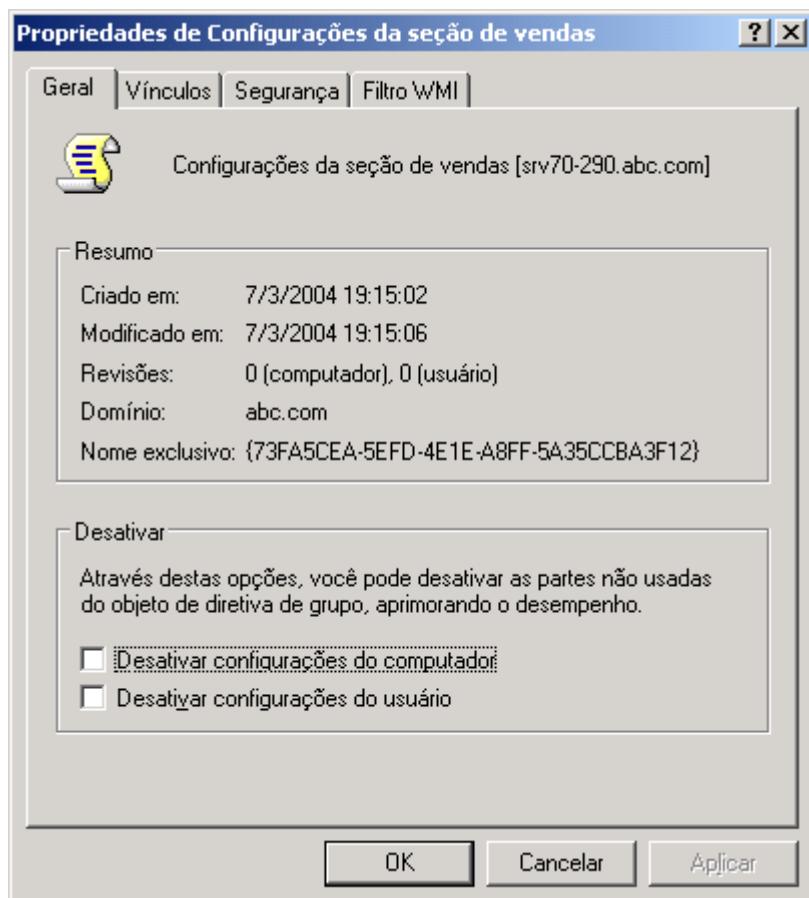
11. Defina as configurações desejadas e clique em OK.
12. Feitas as configurações desejadas é só clicar no botão Fechar. A GPO foi criada, configurada.

## Configurando as Propriedades de uma GPO.

Neste tópico você aprenderá a configurar as propriedades de uma GPO. Conforme mostrarei existem uma série de opções que podem ser configurada e que afetam a maneira como a GPO será aplicada.

Exemplo: Para configurar as propriedades de uma GPO, siga os passos indicados a seguir:

1. Faça o logon como administrador ou com uma conta com permissão de administrador.
2. Abra o console Usuários e computadores do Active Directory.
3. Localize o container (domínio ou unidade organizacional) onde está a GPO a ser configurada. Clique com o botão direito do mouse neste container e, no menu de opções que é exibido, clique na opção Propriedades.
4. Será exibida a janela de propriedades do container. Clique na guia Diretiva de grupo. Serão exibidas as opções de configuração da guia Diretiva de grupo.
5. Clique na GPO a ser configurada para selecioná-la e em seguida clique no botão Propriedades.
6. Será exibida a janela de propriedades da GPO, com a guia Geral selecionada, conforme indicado na Figura 9.54:



**Figura 9.54 A guia de opções gerais das propriedades da GPO.**

7. Nesta guia são exibidas informações gerais sobre a GPO, tais como a data de criação e data da última modificação. Também estão disponíveis as opções para desabilitar toda a árvore de configurações de computador (Desativar

configurações do computador) e uma opção para desabilitar toda a árvore de configurações de usuário (Desativar configurações do usuário). Estas opções são especialmente úteis, em situações onde você está enfrentando problemas com a aplicação das polices. Por exemplo, se você já identificou que o problema é com as polices aplicadas ao computador, pode marcar a opção Desativar configurações do computador, para desabilitar estas opções, até que você possa fazer uma análise detalhada e identificar onde estão os problemas.

8. Defina as configurações desejadas e dê um clique na guia Vínculos. Nesta guia você pode pesquisar em todo o domínio (em um ou mais domínios), para listar onde a GPO está sendo aplicada. Por exemplo, para listar em quais unidades organizacionais a GPO está sendo listada. Esta opção é especialmente útil para a resolução de problemas e conflitos na aplicação das GPOs. Ao clicar no botão Localizar agora, será feita uma pesquisa em todo o domínio selecionado no campo Domínio. No exemplo da Figura 9.55, foi feita uma pesquisa no domínio abc.com, e como resultado a GPO está sendo aplicada em duas OUs: abc.com/Contabilidade e abc.com/Vendas.

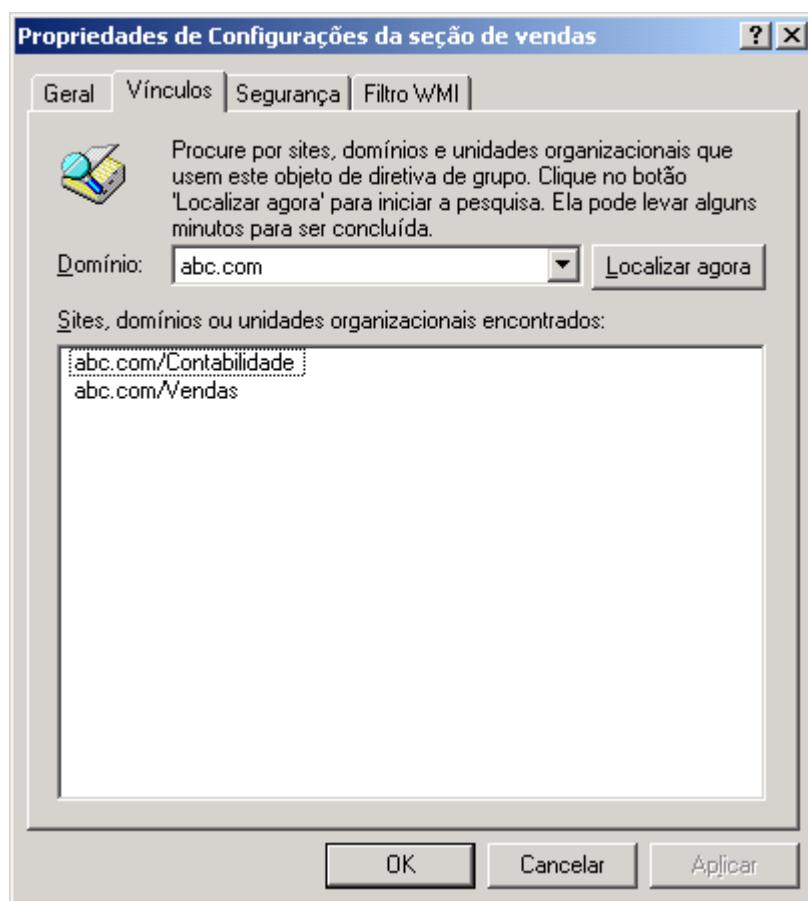


Figura 9.55 A lista de containers onde a GPO está sendo aplicada.

9. Clique na guia Segurança. Esta guia é muito semelhante a guia Segurança, da janela de propriedades de uma pasta ou arquivo, em um volume formatado com NTFS. Ou seja, é uma ACL – Access Control List (Lista de Controle de Acesso). Ou seja, associada a GPO, existe uma lista de controle de acesso. Com esta lista podem ser implementadas muitas soluções práticas, que surgem no dia-a-dia do uso das GPOs. Por exemplo, suponha que o administrador queira que as configurações de uma GPO sejam aplicadas apenas para um determinado grupo de usuários e não para todos os usuários de uma unidade organizacional. Neste caso, basta definir permissões de acesso apenas para o grupo para o qual devem ser aplicadas as configurações da GPO. Outra situação que pode acontecer é a seguinte: Imagine que determinadas restrições devam ser aplicadas para todos os usuários, com

exceção de um determinado grupo, como por exemplo o grupo Administradores. Neste caso, basta colocar permissão de acesso negada ao grupo Administradores e permissão de acesso para o grupo Todos. Neste caso as configurações serão aplicadas para todos os usuários, com exceção dos usuários do grupo Administradores, o qual teve acesso a GPO negado. Na Figura 9.56 é exibido o exemplo onde foi negada a permissão Aplicar diretiva de grupo (Apply Group Policy) para o grupo Administradores. A permissão Aplicar diretiva de grupo é necessária para os grupos que deverão ter as configurações aplicadas a seus membros. A permissão Gravação é necessária para os usuários que devam ter permissão de alterar a GPO.

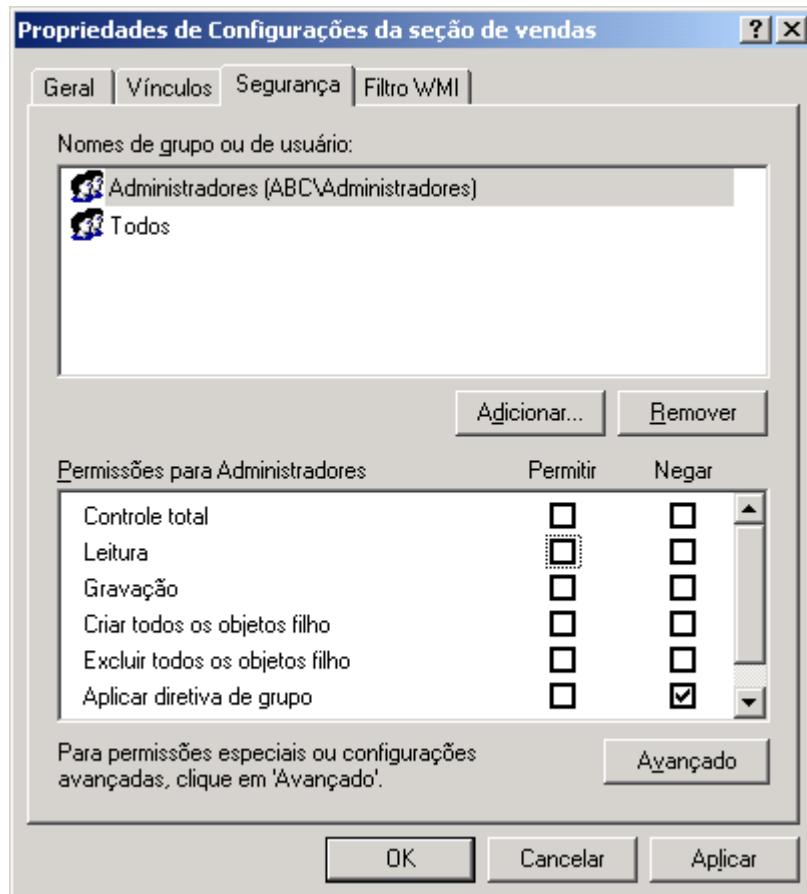


Figura 9.56 A lista de permissões para a GPO.

10. Defina as configurações de segurança desejadas e clique na guia Filtro WMI. WMI é uma tecnologia para monitoração e gerenciamento do ambiente de hardware e software dos computadores. É possível criar filtros WMI (como se fossem consultas em um banco de dados), para selecionar apenas computadores que atendam um ou mais critérios. Por exemplo, é possível aplicar um filtro WMI para selecionar apenas os computadores que tem 128 MB ou mais de memória RAM. Este filtro WMI pode ser salvo e utilizado para definir em quais computadores será aplicado uma GPO. Por exemplo, se você está fazendo uma distribuição do Office XP, usando a distribuição de software via GPO. O administrador pode criar um filtro WMI para selecionar apenas os computadores que atendam as necessidades de hardware do Office XP. Depois o administrador aplica o filtro WMI para que a GPO seja aplicada apenas aos computadores que atendam os requisitos de instalação do Office XP. O administrador usa a guia WMI, para indicar o filtro a ser utilizado.
11. Defina as configurações desejadas e dê um clique em OK para aplicá-las.

Muito bem, sobre GPO, para o Exame 70-290 é isso. Você precisa conhecer algumas diretivas específicas, as quais serão abordadas nos capítulos onde forem tratados os tópicos relacionados com as diretivas. Só a título de exemplo, vamos citar duas diretivas, as quais controlam o recurso de Assistência remota, descrito anteriormente neste capítulo. Estas diretivas são acessadas através do seguinte caminho: Configurações do computador -> Modelos administrativos -> Sistema -> Assistência remota. A seguir descrevo as duas diretivas disponíveis, nesta opção:

- ◆ **Assistência remota solicitada:** Esta diretiva Especifica se os usuários podem solicitar a assistência de outro usuário por meio da assistência remota. Se o status for definido como ‘Ativado’, um usuário pode criar um convite de assistência remota que uma pessoa (“especialista”) pode usar em outro computador para se conectar ao computador do usuário. Se for concedida permissão, o especialista pode ver a atividade da tela, do mouse e do teclado do usuário em tempo real.

A configuração ‘Permitir controle remoto deste computador’ especifica se um usuário pode controlar este computador de um computador diferente. Se o usuário convidar um especialista para se conectar ao computador e lhe der permissão, o especialista pode assumir o controle do computador. O especialista só pode fazer pedidos para assumir o controle durante a sessão de assistência remota. O usuário pode interromper o controle remoto a qualquer momento.

A configuração ‘Tempo máximo da permissão’ define um limite para o tempo pelo qual o convite de assistência remota pode permanecer aberto.

A configuração ‘Selecionar o método para enviar convites por email’ especifica o padrão de email a ser usado para enviar convites de assistência remota. Dependendo do seu programa de email, você pode usar o padrão Mailto (o destinatário do convite se conecta por meio de um link da Internet) ou o padrão SMAPI (Simple MAPI) (o convite é anexado ao email).

Observação: o programa de email deve dar suporte para o padrão de email selecionado.

Se o status for definido como ‘Desativado’, os usuários não poderão pedir assistência remota e o computador não poderá ser controlado de outro computador.

Observação: um especialista pode se conectar a este computador apenas com a permissão explícita do usuário. Se a assistência remota for desativada nesta configuração ou for definida como ‘Não configurada’ e desativada no ‘Painel de controle’, a configuração ‘Oferecer assistência remota’ também será desativada.

Se o status for definido como ‘Não configurado’, os próprios usuários poderão ativar ou desativar e configurar a assistência remota em ‘Propriedades do sistema’ no ‘Painel de controle’. Se o status for definido como ‘Não configurado’, o tempo máximo padrão pelo qual o convite de assistência remota pode permanecer aberto será determinado pela configuração do ‘Painel de controle’.

- ◆ **Oferecer assistência remota:** Use essa configuração para determinar se uma pessoa de suporte ou administrador de informática (conhecida como “especialista”) pode ou não oferecer assistência remota a este computador, sem a solicitação explícita do usuário por meio de um canal, de email ou do Instant Messenger. Usando esta configuração, um especialista poderá oferecer assistência remota ao computador.

Observação: o especialista não poderá se conectar ao computador sem se anunciar nem o controlar sem a permissão do usuário. Quando o especialista tentar se conectar, o usuário ainda terá a oportunidade de aceitar ou negar a conexão (concedendo ao especialista privilégios somente para exibição na sua área de trabalho) e, desse momento em diante, o usuário deverá clicar explicitamente em um botão para permitir que o especialista controle remotamente a área de trabalho, se o controle remoto estiver ativado.

Se você ativar esta configuração, poderá oferecer assistência remota. Ao definir esta configuração, você tem duas opções: selecionar ‘Permitir que auxiliares somente vejam o PC’ ou ‘Permitir que auxiliares controlem remotamente o computador’. Além de fazer essa seleção, ao definir esta configuração você também especifica a lista de usuários ou grupos de usuários que terão permissão para usar a assistência remota. Eles são conhecidos como “auxiliares”.

Para configurar a lista de auxiliares, clique em ‘Mostrar’. Será aberta uma nova janela, em que você poderá digitar os nomes dos auxiliares. Adicione cada usuário ou grupo separadamente. Ao digitar o nome do usuário ou grupo de usuários auxiliares, use o seguinte formato:

<Nome de domínio>\<Nome de usuário> ou  
<Nome de domínio>\<Nome de grupo>

Se você desativar esta configuração de diretiva ou não a definir, os usuários ou grupos não poderão oferecer assistência remota não solicitada ao computador.

## Gerenciamento de Hardware e de Drivers.

Para finalizar a nossa “salada de frutas”, falarei um pouco sobre o gerenciamento de hardware e de drivers no Windows Server 2003. Sempre manterei o foco apenas nos tópicos relevantes para o Exame 70-290 ou nos tópicos que são necessários, para o entendimento de tópicos relevantes para o exame.

### Adicionando, removendo e gerenciando o Hardware do computador.

Hardware é qualquer equipamento ou placa que faz parte do seu computador. Por exemplo, uma placa de som, um Modem para acessar a Internet via linha telefônica, uma placa para captura de Vídeo, etc.

Todo hardware fabricado atualmente, segue um padrão chamado “Plug and Play”. Este padrão torna extremamente simples, a instalação de novos componentes de hardware. Basta instalá-los fisicamente, e ao ligar o computador, o Windows Server 2003 reconhece a presença do novo dispositivo de hardware e instala o driver necessário para que este funcione. O Padrão Plug and Play está presente a partir do Windows 95, e também existe no Windows 98 e Windows 2000 Professional, além do Windows 2000 Server.

Porém podem existir situações em que você tenha que instalar um Hardware mais antigo, o qual não está dentro do padrão Plug and Play, ou também pode acontecer de um dispositivo Plug and Play não ser reconhecido automaticamente. Nestas situações você deve utilizar a opção “Adicionar hardware” no Painel de controle. Com esta opção é possível fazer com que o Windows Server 2003 detecte o novo hardware instalado, ou caso não seja detectado, você pode fazer com que o driver necessário seja carregado a partir de um disquete ou CD-ROM.

Além disso, caso um dispositivo de hardware tenha sido retirado do computador, porém o respectivo Driver não tenha sido corretamente desinstalado, você pode remover o driver que não é mais necessário utilizando a opção “Adicionar hardware”.

Nunca é demais ressaltar que a instalação e configuração de novos dispositivos de hardware, envolve conhecimentos técnicos de hardware, por isso é recomendado que sempre que você precisar instalar um novo dispositivo, caso você não conheça bem hardware, é recomendado que você entre em contato com um técnico especializado. A instalação de maneira incorreta de drivers ou dispositivos de hardware, pode fazer com que o Windows Server 2003 deixe de funcionar corretamente, sendo que em situações mais graves, pode ser necessária a reinstalação do sistema.

Todo dispositivo de hardware precisa de um ou mais programas o qual permite que o Windows Server 2003 comunique-se com o dispositivo e vice-versa. O Programa ou conjunto de programas que faz a comunicação do Sistema Operacional com um dispositivo de hardware, é conhecido como Driver do dispositivo. Por exemplo, ao conectar uma nova impressora no seu computador, você precisa instalar o driver da impressora, antes que os seus programas possam imprimir corretamente, ao instalar uma nova placa de rede, você precisa instalar o Driver da placa de rede e assim por diante. O CD de instalação do Windows Server 2003 já vem com o Driver para milhares (é isto mesmo: milhares) de dispositivos diferentes. Quando você instala um dispositivo de hardware, para o qual o Driver está no CD de instalação do Windows Server 2003, o processo é bastante simples. Você desliga o computador e instala o dispositivo de Hardware. Ao ligar o computador o Windows Server 2003 reconhece o dispositivo e já carrega o driver adequado, a partir do CD de instalação do Windows Server 2003. A única coisa de diferente que você vê, logo após ter feito o logon, é uma janelinha com uma mensagem de que um novo Hardware foi encontrado e o respectivo driver está sendo instalado. Pode acontecer de ser aberta uma janela solicitando que você coloque o CD de instalação do Windows Server 2003 no drive de CD, para que possam ser copiados os arquivos necessários. Também pode-se ter situações em que o driver para o hardware que está sendo instalado, não esteja no CD de instalação do Windows Server 2003. Porém, todo o dispositivo de Hardware vem com um disquete ou CD-ROM, no qual estão disponíveis os drivers do dispositivo, para as várias versões do Windows. Nestas situações, após ter reconhecido o dispositivo de Hardware, o Windows Server 2003 solicita que seja fornecido o caminho onde estão os arquivos de instalação do driver do dispositivo. Agora é só informar se os arquivos estão no disquete ou no CD-ROM. Uma terceira opção que você tem é o Windows Update. O Windows Update é um site da Microsoft, no qual são disponibilizadas todas as atualizações, correções e Service Packs para o Windows. Pode acontecer de o driver não estar no CD de instalação do Windows Server 2003, mas estar disponível no site do Windows Update.

Exemplo: Neste exemplo vou abrir a opção “Adicionar hardware”, porém não irei instalar nenhum novo dispositivo de hardware; apenas irei descrever algumas das opções disponíveis.

1. Abra o Painel de controle: Iniciar -> Painel de controle.
2. Certifique-se de que o modo de exibição tradicional esteja sendo utilizado e não o modo de exibição por categorias.
3. Dê um clique duplo na opção Adicionar hardware. Irá surgir a tela inicial do assistente de hardware, conforme indicado na Figura 9.57:

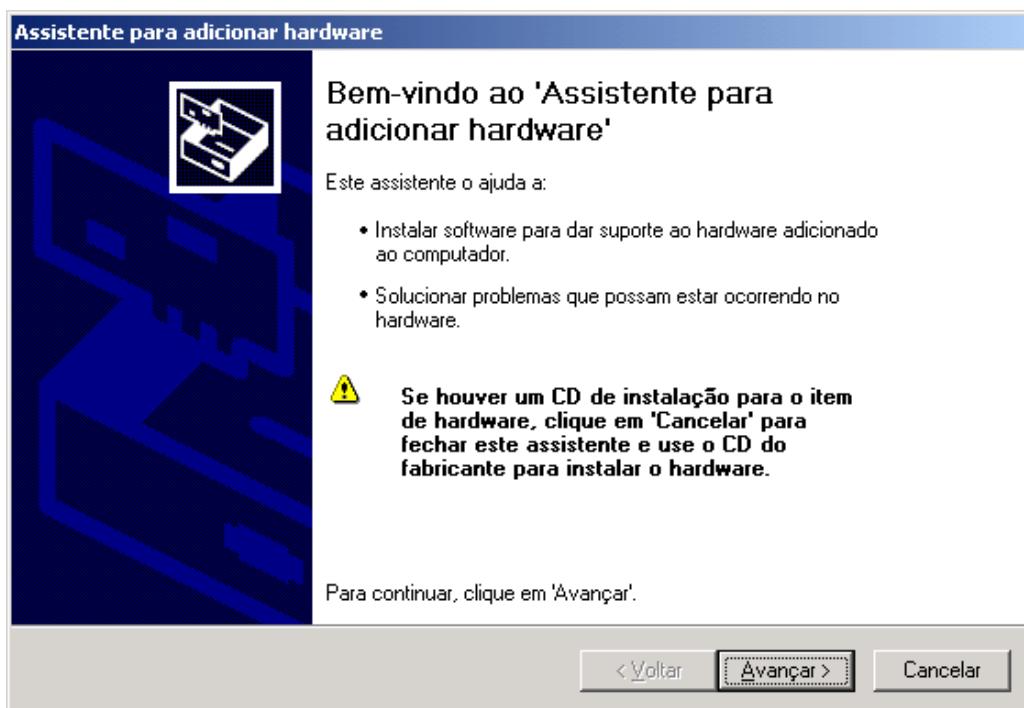
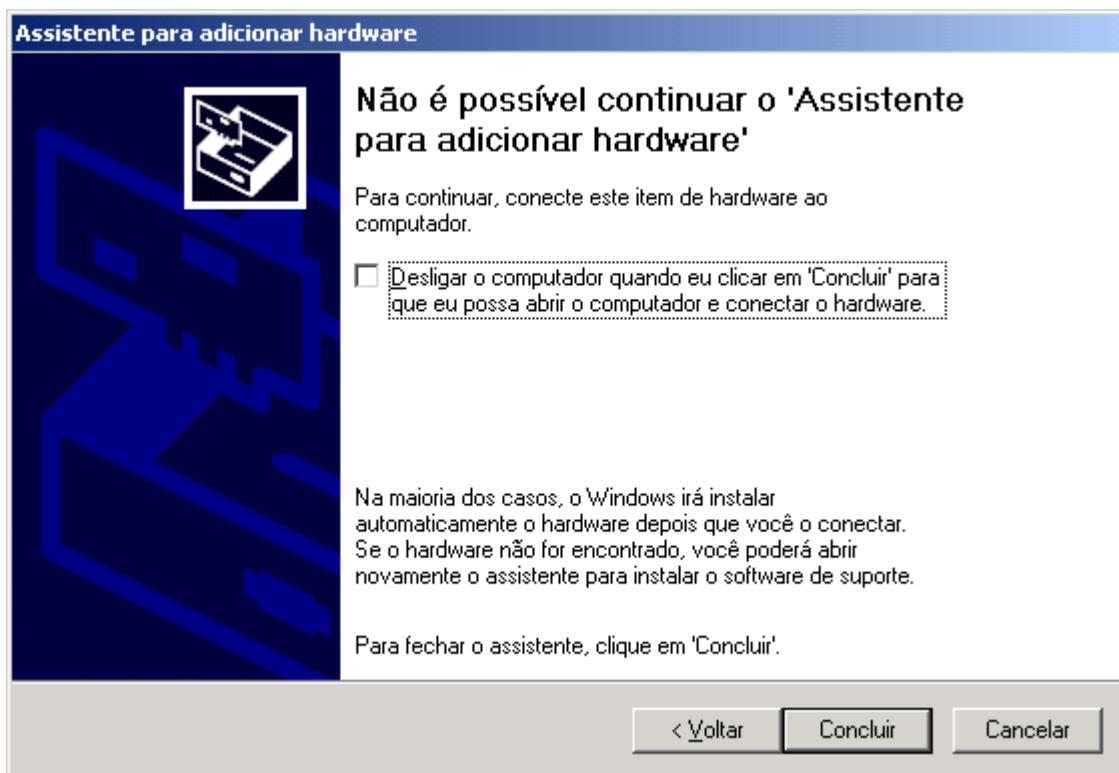


Figura 9.57 A tela inicial do assistente de hardware.

4. Dê um clique no botão Avançar, para ir para a próxima etapa. O Windows Server 2003 pode demorar algum tempo, pois nesta etapa ele irá procurar por novos dispositivos de Hardware que tenham sido instalados porém ainda não foram configurados.
5. Surge uma tela com duas opções.

Sim, já conectei um item de Hardware: Utilize esta opção se o dispositivo de Hardware já está instalado fisicamente no computador, porém não foi detectado automaticamente pelo Windows Server 2003. Se você marcar esta opção, ao clicar no botão Avançar, será exibida uma lista com todos os dispositivos de hardware instalados no computador. Você pode marcar um dos dispositivos e clicar no botão Avançar para tentar solucionar problemas com dispositivos que não estão funcionando.

- ◆ Não, ainda não adicionei o item de hardware: Se você marcar nesta opção e clicar no botão Avançar, o Windows Server 2003 informa que não é possível continuar com o assistente de Hardware, que você deve desligar o computador, instalar o item de hardware e ligar novamente o computador, conforme indicado na Figura 9.58.



**Figura 9.58** O assistente de Hardware informa que você precisa desligar o computador, instalar o novo dispositivo e ligar o computador novamente.

6. Como você não irá instalar nenhum novo dispositivo neste momento, clique no botão Cancelar, para fechar o Assistente de hardware.

## O Gerenciador de Dispositivos

O Gerenciador de dispositivos fornece um modo de exibição gráfica de todo o hardware instalado no computador. Você pode usar o Gerenciador de dispositivos para atualizar os drivers (ou software) de dispositivos de hardware, modificar configurações de hardware e solucionar problemas.

Você pode usar o Gerenciador de dispositivos para:

- Determinar se o hardware do seu computador está funcionando corretamente.
- Alterar as definições da configuração de hardware.
- Identificar os drivers de dispositivos que estão carregados para cada dispositivo e obter informações sobre cada driver.
- Alterar configurações avançadas e propriedades dos dispositivos.
- Instalar drivers de dispositivo atualizados.
- Desativar, ativar e desinstalar dispositivos.
- Retornar à versão anterior de um driver.
- Imprimir um resumo dos dispositivos instalados no computador.

O Gerenciador de dispositivos é geralmente utilizado para verificar o status do hardware e atualizar drivers de dispositivo no computador. Os usuários avançados com amplo conhecimento sobre hardware de computador podem também usar os recursos de diagnóstico do Gerenciador de dispositivos para solucionar conflitos entre dispositivos e alterar configurações de recursos, mas isso deve ser feito com extrema cautela.

Normalmente, não será necessário usar o Gerenciador de dispositivos para alterar configurações de recursos, pois estes são alocados automaticamente pelo sistema durante a configuração do hardware.

Você pode usar o Gerenciador de dispositivos para gerenciar dispositivos apenas em um computador local. O Gerenciador de dispositivos funcionará apenas no modo somente leitura em um computador remoto.

A seguir faremos um pequeno exemplo prático, onde mostrarei como executar algumas operações disponíveis no Gerenciador de dispositivos.

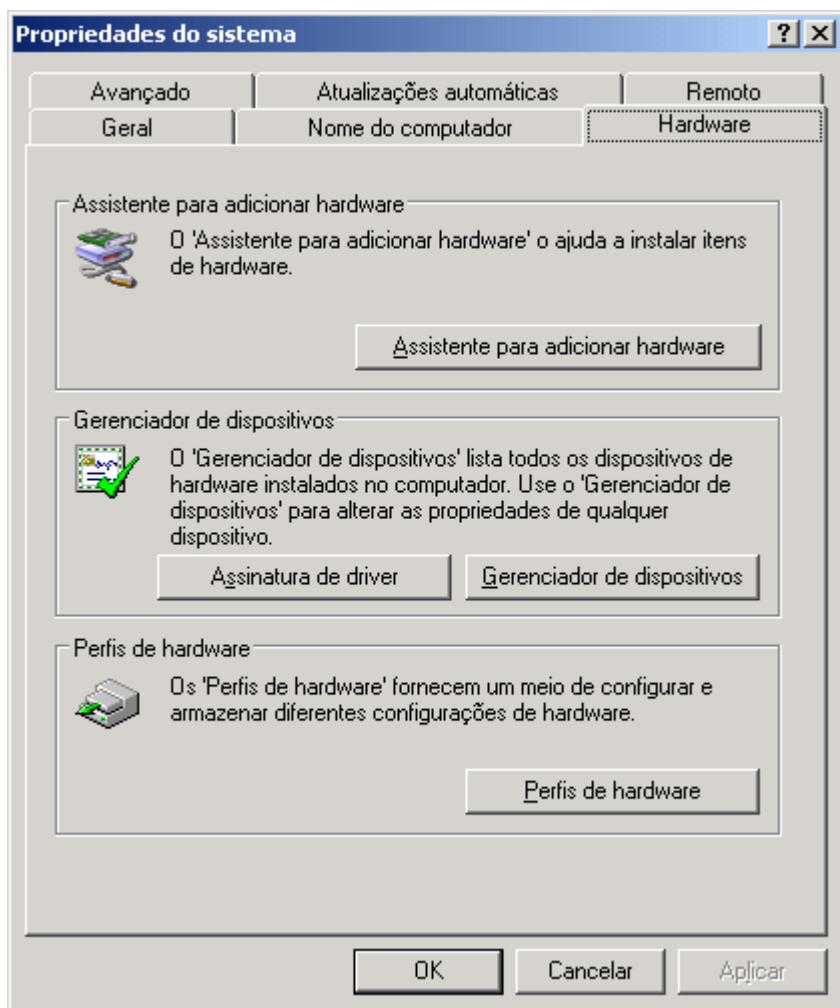
Exemplo: Para acessar o Gerenciador de Dispositivos, siga os passos indicados a seguir:

1. Faça o logon com uma conta com permissão de administrador.
2. Abra o Painel de controle.
3. Dê um clique duplo no ícone Sistema, do Painel de controle
4. Será aberta a opção Propriedades do sistema. Dê um clique na guia Hardware. Serão exibidas as opções indicadas na Figura 9.59:

**IMPORTANTE:** A opção de voltar à versão anterior de um driver é um recurso bastante útil, mais conhecido como Roll back driver. Por exemplo, imagine que você instalou uma nova versão para o drive da placa de rede de um servidor. O servidor foi reinicializado, você fez o logon normalmente, porém o desempenho está "sofrível". Você verifica que o processador está com uma taxa constante de ocupação, próximo aos 100%. A causa provável do problema é a nova versão do driver da placa de rede. Você pode usar o recurso de Roll back, para retornar a versão anterior e solucionar o problema de desempenho. Lembre-se deste recurso para o exame.

**IMPORTANTE:** A alteração incorreta de configurações de recursos pode desativar o hardware e fazer com que o computador não funcione direito ou fique inoperante. Apenas os usuários que têm experiência em hardware e em configurações de hardware devem alterar configurações de recursos.

**IMPORTANTE:** Somente contas com perfil de Administrador, terão permissão para gerenciar drivers de dispositivos de hardware.



**IMPORTANTE:** Se você não puder acessar o Gerenciador de dispositivos a partir dos snap-ins de extensão do Gerenciamento do computador em um computador remoto, certifique-se de que o serviço Registro remoto tenha sido iniciado no computador remoto. O serviço de Registro remoto deve ter sido inicializado, para que você possa usar os consoles de gerenciamento remoto. Você precisa dispor das permissões apropriadas no computador remoto para iniciar o serviço. Você também poderá receber essa mensagem de erro se o computador remoto estiver executando o Microsoft®Windows 95. O Gerenciamento do computador não oferece suporte a acesso remoto para computadores que estejam executando o Windows 95.

Figura 9.59 A guia Hardware.

5. Dê um clique no botão Gerenciador de dispositivos. Será aberto o Gerenciador dispositivos, onde é exibida uma árvore, onde são listados todos os dispositivos de hardware instalados no computador, conforme indicado na Figura 9.60:

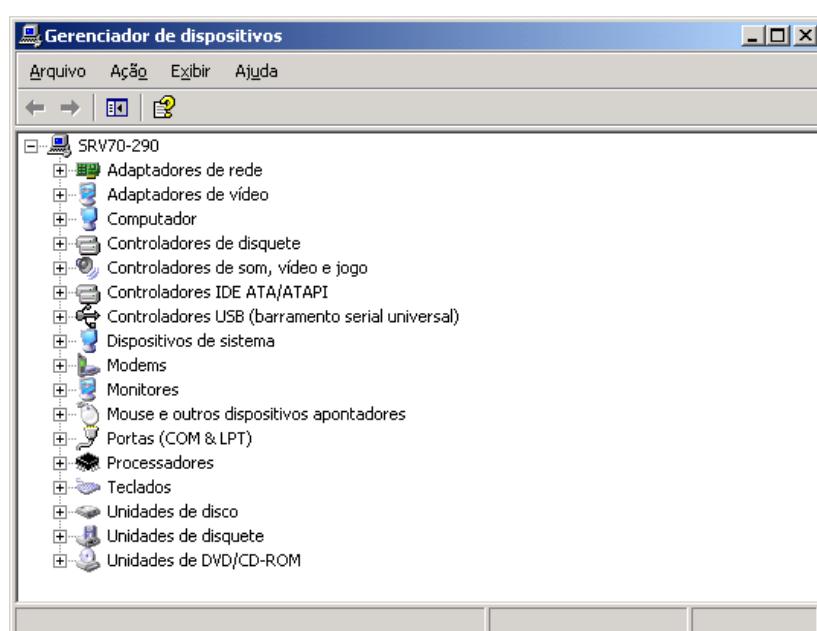


Figura 9.60 A guia Hardware.

6. Vamos acessar as propriedades de um driver instalado. No meu exemplo, vou clicar no sinal de +, ao lado da categoria Adaptadores de rede. Será exibida uma lista de todos os adaptadores de rede instalados. Dê um clique duplo em um deles, para exibir as propriedades do respectivo driver, conforme exemplo da Figura 9.61:

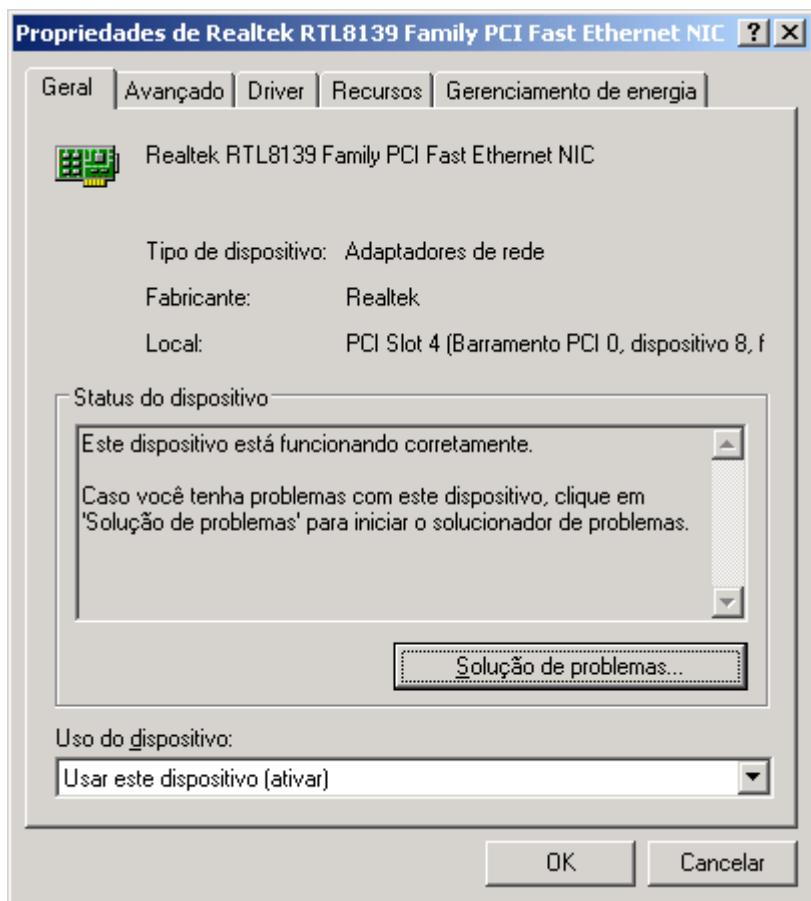
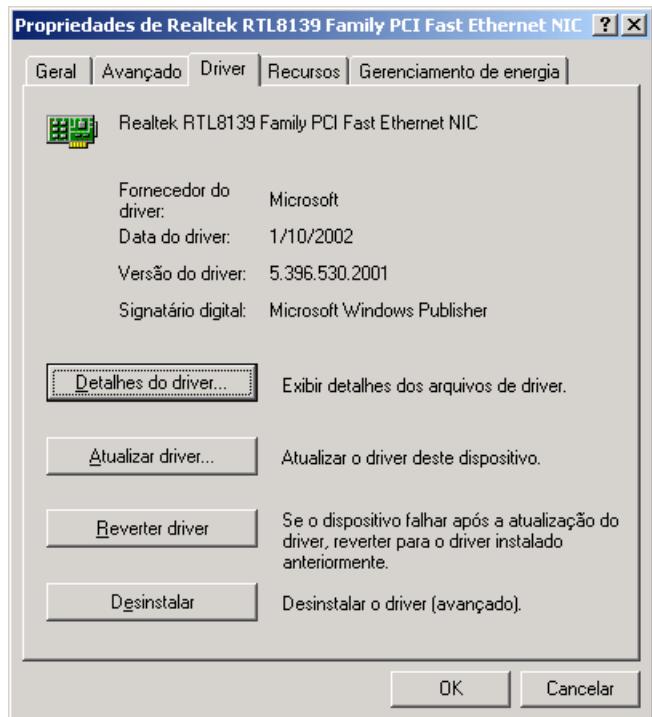


Figura 9.61 Acessando as propriedades de um driver.

7. Dê um clique na guia Driver. Serão exibidas as opções indicadas na Figura 9.62, as quais serão detalhadas logo a seguir.

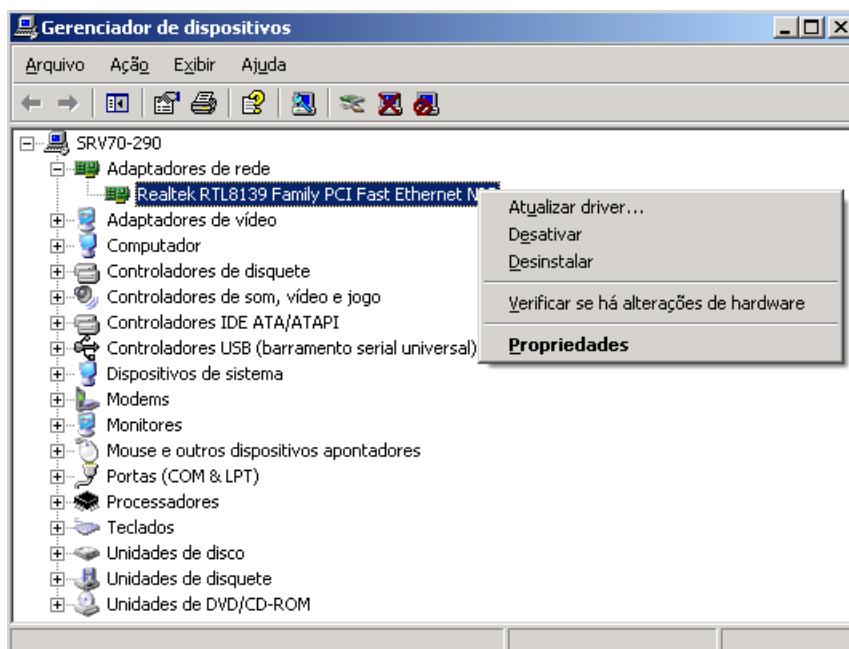
Nesta guia, cabe destacar a função dos seguintes botões:

- ◆ **Detalhes de driver:** Ao clicar neste botão, será aberta uma janela com informações detalhadas sobre o driver.
- ◆ **Atualizar driver:** Clique para alterar ou atualizar o driver de dispositivo selecionado. Isso inicia o Assistente para atualização de hardware.
- ◆ **Reverter driver:** Este é o famoso Roll back, ou seja, desinstalar a versão atual e voltar a versão anterior do driver. Conforme descrito anteriormente, esta função é útil em situações onde após a instalação de uma nova versão de um driver, o sistema começa a apresentar problemas de estabilidade ou de desempenho. Se você conseguir fazer o logon no modo normal ou no modo de segurança, será possível usar esta função, para voltar a versão anterior do driver e solucionar os problemas causados pela nova versão. Lembre-se bem desta função para o exame.
- ◆ **Desinstalar:** Esta opção pode ser utilizada para desinstalar o driver de um dispositivo.



**Figura 9.62 A guia Driver, das propriedades do driver.**

8. Dê um clique na guia Recursos. Nesta guia são exibidos os recursos de hardware utilizados pelo driver, tais como IRQ, Intervalo de memória e assim por diante. Nesta guia será informado se o dispositivo está em conflito com algum outro driver instalado no sistema. Por exemplo, se dois drivers tentarem utilizar a mesma IRQ, haverá um conflito de IRQs.
9. Clique em OK para fechar a janela de propriedades do driver. Você estará de volta ao Gerenciador de dispositivos.
10. Ao clicar com o botão direito do mouse em um driver, você tem uma série de opções, conforme indicado na Figura 9.63:



**Figura 9.63 Opções ao clicar com o botão direito do mouse.**

11. Feche o Gerenciador de dispositivos.

## Assinatura de drivers

Os arquivos de drivers de dispositivo de hardware e do sistema operacional incluídos no Windows têm uma assinatura digital da Microsoft. Uma assinatura digital indica que um driver ou arquivo em particular atendeu a um determinado nível de teste e que não foi alterado ou substituído por outro processo de instalação do programa. Os drivers de dispositivo para produtos de hardware que têm o logotipo Desenvolvido para Microsoft Windows XP ou Desenvolvido para Microsoft Windows Server 2003 têm uma assinatura digital da Microsoft, que indica que a compatibilidade do produto com o Windows foi testada e que esse produto não foi alterado após os testes.

Dependendo de como o administrador configurou o computador, o Windows irá ignorar os drivers de dispositivo que não estiverem assinados digitalmente, exibir um aviso quando detectar os drivers de dispositivo que não estiverem assinados digitalmente (o comportamento padrão) ou impedir que você instale drivers de dispositivo sem assinaturas digitais.

O Windows inclui os seguintes recursos para garantir que os drivers de dispositivo e arquivos do sistema permaneçam no seu estado original, ou seja, digitalmente assinados.

- ◆ Proteção de arquivo do Windows
- ◆ Verificador de arquivos do sistema
- ◆ Verificação de assinatura de arquivo

No exemplo prático a seguir, mostro como definir o comportamento do Windows em relação a assinatura de drivers e quais as opções disponíveis.

Exemplo: Para definir opções de verificação de assinatura de arquivo, siga os passos indicados a seguir:

1. Faça o logon com uma conta com permissão de administrador.
2. Abra o Painel de controle. Dentro do Painel de controle, dê um clique duplo na opção Sistema.
3. Clique na guia Hardware. Na guia Hardware, clique no botão Assinatura de driver.
4. Será aberta a janela Opções de assinatura de driver, indicada na Figura 9.64



Figura 9.64 Opções de assinatura de driver.

5. Estão disponíveis as seguintes opções:
  - ◆ **Ignorar...**: Selecione esta opção para permitir que todos os drivers de dispositivo sejam instalados no computador, independentemente de terem ou não uma assinatura digital. Essa opção não estará disponível, a menos que você tenha efetuado logon como um administrador ou um membro do grupo Administradores. Tenha cuidado ao utilizar esta opção, a qual pode representar um problema de segurança, ao permitir que drivers não assinados sejam instalados.
  - ◆ **Avisar...**: Selecione esta opção para exibir uma mensagem de aviso sempre que um programa de instalação ou o Windows tentar instalar um driver de dispositivo sem uma assinatura digital. Esse é o comportamento padrão do Windows. Ao tentar instalar um driver não assinado, será exibida uma mensagem de advertência, na qual você pode escolher entre cancelar a instalação ou instalar o driver, mesmo este não estando assinado digitalmente.
  - ◆ **Bloquear...**: Selecione esta opção para impedir que um programa de instalação ou o Windows instale drivers de dispositivo sem uma assinatura digital.
6. Selecione a opção desejada e clique em OK para aplicá-la.
7. Você estará de volta a guia Hardware.
8. Clique em OK para fechar a janela de Propriedades do sistema.

## Conclusão.

Este foi um capítulo no estilo “salada de frutas”, ou seja, de tudo um pouco. Abordei uma série de tópicos importantes para o Exame 70-290. Neste capítulo foram abordados os seguintes tópicos:

- ◆ O uso do Terminal Services
- ◆ O Recurso de Desktop Remoto
- ◆ O Recurso de Shadow Copies
- ◆ Noções Básicas sobre GPO – Group Policy Objects
- ◆ Gerenciamento de Hardware e de Drives
- ◆ Resolução de Problemas de Hardware e Drives.

**DICA:** Se você fez logon como um administrador ou como um membro do grupo Administradores, em Opção do administrador, marque a opção Tornar esta ação o padrão do sistema para aplicar a configuração selecionada como padrão para todos os usuários que efetuaram logon no computador.

**IMPORTANTE:** Além do que eu apresenta em cada capítulo é sempre importante que você procure complementar os seus estudos, usando a Ajuda do Windows e a Internet. Quanto mais materiais você utilizar, para se preparar para o exame, maiores serão as suas chances de obter aprovação.

# Introdução

Neste capítulo tratarei de assuntos relacionados com Auditoria de eventos no Windows Server 2003 e com as configurações dos direitos de usuários e grupos. Sempre focarei os pontos relacionados ao Exame 70-290.

Vou iniciar o Capítulo explorando mais algumas opções do console Computer Management (Gerenciamento do computador). Você já utilizou este console em outros capítulos. Com a opção Ferramentas do sistema, do console Gerenciamento do computador, o administrador tem acesso a uma série de funções, tais como:

- ◆ **Visualizar eventos:** Esta opção será detalhada durante este capítulo, quando tratarei sobre os Logs de Auditoria do Windows Server 2003.
- ◆ **Pastas compartilhadas:** Utilizada para o gerenciamento e criação de pastas compartilhadas no computador local e em outros computadores da rede. Esta opção foi detalhada no Capítulo 6.
- ◆ **Usuários e grupos locais:** Utilizada para a criação de contas de usuários e grupos locais em servidores configurados como Member servers ou Standalone server. Em DCs esta opção não estará disponível.
- ◆ **Logs e alertas de desempenho:** Esta opção dá suporte ao monitoramento detalhado da utilização de recursos do sistema operacional. Será vista no Capítulo 11.
- ◆ **Gerenciador de dispositivos:** Você pode usar o Gerenciador de dispositivos para atualizar os drivers (ou software) de dispositivos de hardware, modificar configurações de hardware e solucionar problemas. Tratei sobre o Gerenciador de dispositivos no Capítulo 9.

Na seqüência você aprenderá sobre os logs de auditoria do Windows Server 2003 (opção Visualizar Eventos). Mostrarei o conceito e a implementação prática de uma política de uso para os logs de auditoria. Tratarei, dentre outros, dos seguintes tópicos:

- ◆ Visualizando e configurando eventos de auditoria.
- ◆ Habilitando e desabilitando eventos de auditoria.
- ◆ Filtragem e pesquisa nos logs de auditoria.
- ◆ Configurações das propriedades do log.
- ◆ Exportação dos logs para outros formatos.

O próximo passo é entender o conceito de Diretivas de Segurança relacionadas com as configurações de auditoria. Mostrarei uma série de diretivas que podem ser configuradas e que afetam a maneira como a auditoria é realizada nos servidores do domínio.

Na parte final do Capítulo mostrarei como habilitar a auditoria em alguns recursos, nos quais a auditoria por padrão não é habilitada, como por exemplo: auditoria no acesso a pastas e arquivos e auditoria no acesso a impressoras. Você aprenderá a habilitar a auditoria nestes objetos e a consultar o log de auditoria, para localizar os eventos relacionados.

# Log de Eventos e de Auditoria – Conceito.

Quando você trabalha com o Windows Server 2003, o qual é utilizado como sistema operacional para servidores da rede, a segurança é uma preocupação constante. Não poderia ser diferente. O sistema operacional deve ser capaz de disponibilizar alguns serviços básicos em relação a segurança: identificação (através do mecanismo de contas de usuários, logon e do protocolo Kerberos), restrição de acesso aos recursos (com base no mecanismo de permissões de acesso, através do uso de uma ACL – Access Control List, Lista de Controle de Acesso a cada recurso da rede) e também deve ser capaz de registrar as ações que estão sendo executadas nos recursos da rede, juntamente com informações sobre o horário da ação, quem foi o usuário que executou a ação e outras informações relevantes. O registro do que é feito na rede é gravado no Log do Sistema. O sistema de log do Windows Server 2003 permite o registro de um grande número de eventos, conforme mostrarei neste capítulo. A ação de pesquisar/consultar o log de eventos, em busca de informações é conhecido como auditoria.

Auditoria é um processo de acompanhamento das ações que são executadas nos servidores do domínio, através da rede, tanto ações do próprio Sistema operacional, como por exemplo a inicialização de um serviço, mas principalmente ações do usuário, como um logon ou um acesso aos arquivos de uma pasta compartilhada. Por exemplo, toda vez que o Windows Server 2003 é inicializado uma série de serviços são iniciados automaticamente, como o serviço spooler que controla a impressão, o serviço Workstation que controla a interface gráfica do Windows Server 2003 e assim por diante. Cada um destes serviços é capaz de escrever eventos nos logs de auditoria do Windows Server 2003. Um evento é uma mensagem que pode ser informativa, pode ser um aviso e pode ser uma mensagem de erro. Um outro exemplo, quando um usuário tenta fazer o logon e informa uma senha errada, um evento é gravado no log de segurança, neste caso é gravado uma mensagem (evento) de falha de logon.

A auditoria de segurança monitora vários eventos relativos à segurança. O monitoramento de eventos do sistema é necessário para detectar invasores e tentativas de comprometer os dados do sistema. Uma tentativa de logon sem êxito é um exemplo de um evento que pode ser submetido à auditoria.

Os tipos mais comuns de eventos a serem submetidos à auditoria são:

- ◆ **Acesso a objetos, como arquivos e pastas:** Por exemplo, repetidas tentativas de acessar determinados arquivos, por um usuário que não tem permissão de acesso, podem caracterizar uma tentativa de quebra de segurança.
- ◆ **Gerenciamento de contas de usuários e grupos:** ficam registradas informações sobre quem fez alterações nas contas de usuários e grupos.
- ◆ **Quando os usuários fazem logon e logoff no sistema:** Por exemplo, logons efetuados fora do horário normal de trabalho, merecem uma atenção especial do administrador.

Além da auditoria de eventos relacionados à segurança, um log de segurança é gerado, oferecendo um meio para que você visualize os eventos de segurança registrados no log. O log de segurança pode ser exibido com o console Visualizar eventos, o qual você aprenderá a utilizar neste capítulo.

Uma mensagem no log do sistema, possui informações tais como o usuário que executou a ação, a ação executada e se esta foi executada com sucesso ou não.

O log de eventos do Windows Server 2003 pode ser configurado, de tal maneira que o administrador escolha quais eventos devem ser gravados no log, como por exemplo: tentativas de logon com sucesso, tentativas de logon sem sucesso ou ambas . Por exemplo, o administrador pode definir que seja registrado um evento no log de segurança, toda vez que um usuário tentar acessar um determinado arquivo, sem ter a devida permissão (tentativa de acesso sem sucesso).

Também é possível definir se o acesso a arquivos, pastas e impressoras devem ser monitorados ou não (por padrão este monitoramento está desabilitado. Na parte final do capítulo mostrarei como habilitar este monitoramento). Além

disso, você pode definir se devem ser monitorados somente acessos bem sucedidos ou acessos negados (sem sucesso), tais como um usuário com permissão somente de leitura que tenta alterar um determinado arquivo, em uma pasta compartilhada.

Os logs do sistema são acessados utilizando a opção Event Viewer (Visualizar eventos) do console Gerenciamento do computador. Também é possível utilizar o console Visualizar eventos que é acessado através da opção Iniciar -> Ferramentas Administrativas -> Visualizar eventos. O console Visualizar eventos é configurado para carregar apenas o Snap-in para trabalhar com eventos, diferente do console Gerenciamento do Computador, o qual é configurado para carregar uma série de Snap-ins, dentre eles, o Snap-in Visualizar eventos.

Por padrão, são criados três logs no sistema de log do Windows:

- ◆ **Application (Log do aplicativo):** Contém erros, avisos e mensagens informativas de diversos programas que rodam no Windows Server 2003. Por exemplo, o Microsoft SQL Server 2000 (banco de dados da Microsoft), grava uma série de eventos no log Aplicativo. O log do aplicativo contém eventos registrados por aplicativos ou programas. Por exemplo, um programa de banco de dados pode registrar um erro de arquivo no log do aplicativo. Os desenvolvedores de software decidem quais eventos monitorar, isto é, ao desenvolver um programa, é possível definir quais eventos o programa irá gravar no log de eventos do Windows Server 2003. Linguagens como o Delphi, VB.NET, Visual Basic 6 e C#, fornecem comandos para que um programa possa gravar eventos no log do Windows Server 2003.
- ◆ **Security (Log de segurança):** Contém informações sobre o sucesso ou não de eventos de auditoria, de acordo com definições da política de auditoria. Conforme mostrarei mais adiante, a política de auditoria define quais eventos de segurança serão monitorados. O log de segurança registra eventos como tentativas de logon válidas e inválidas, assim como eventos relacionados ao uso de recursos, como criar, abrir ou excluir arquivos ou outros objetos. Um administrador pode especificar os eventos que serão registrados no log de segurança. Por exemplo, se você ativou a auditoria de logon, as tentativas de logon no sistema serão registradas no log de segurança. Por padrão somente usuários com permissão de administrador podem acessar o log de segurança.
- ◆ **System (Log do sistema):** Contém erros, avisos e informações geradas pelo próprio Windows Server 2003. O Windows Server 2003 define quais os eventos serão gerados. O log do sistema contém eventos registrados pelos componentes de sistema do Windows Server 2003. Por exemplo, a falha de um driver ou de outro componente do sistema ao ser carregado durante a inicialização é registrada no log do sistema. Os tipos de evento registrados no log pelos componentes do sistema são determinados previamente pelo Windows Server 2003.

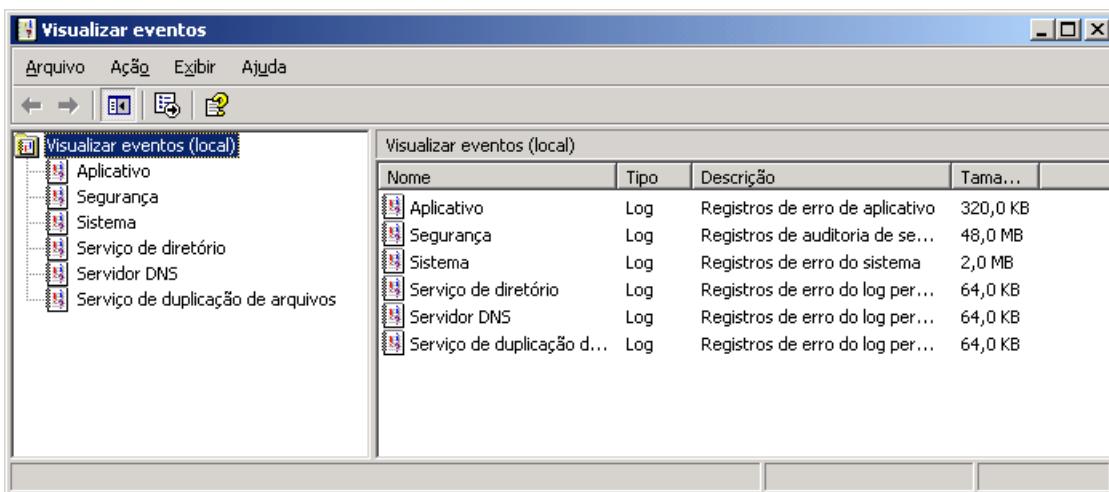


Figura 10.1 Opções de log em um DC com o Windows Server 2003.

Cabe aqui salientar que o principal objetivo da existência de um sistema de Auditoria/Log, é manter um acompanhamento de tudo o que está acontecendo no sistema. Quando algum problema acontece, como por exemplo, um serviço que deixa de funcionar, o primeiro lugar que o administrador vai em busca de informação é no log do sistema. Informações importantes sobre segurança podem ser encontrados no log de Segurança.

No visualizador de eventos, podem existir cinco tipos diferentes de eventos, conforme descritos abaixo:

- ◆ **Error (Erro):** Representado por um círculo vermelho com um x branco. Indica um problema sério tal como perda de dados ou de alguma funcionalidade de um serviço ou dispositivo que não está operando corretamente.. Por exemplo, se um serviço falhar durante a inicialização, um evento de erro será logado.
- ◆ **Warning (Aviso):** Representado por um triângulo amarelo com um ponto de exclamação. Um evento que não é necessariamente um erro, mas pode representar um problema futuro. Por exemplo, quando o espaço em disco está ficando pequeno, uma aviso será logado.
- ◆ **Information (Informações):** Representado por um balão branco, com um ponto de exclamação azul dentro. Descreve uma operação de sucesso de uma aplicação, driver ou serviço. Por exemplo, quando um driver de rede é carregado com sucesso, um evento de informação é logado. Na Figura 10.2, é mostrada uma tela onde aparecem os três tipos de eventos descritos anteriormente.

**NOTA: A medida que novos serviços vão sendo instalados, novas opções vão sendo adicionadas ao console Visualizar eventos. Por exemplo, ao instalar o DNS em um servidor Windows Server 2003, uma opção DNS é adicionada ao Visualizador de eventos, entrada essa que trata de eventos relacionados com o serviço de DNS. Outro exemplo, em um servidor configurado como DC, uma nova categoria de eventos é criada: Directory Service (Serviço de Diretório), conforme exemplo da Figura 10.1, onde são exibidas as opções de log disponíveis em um DC com o Windows Server 2003 instalado.**

The screenshot shows the Windows Event Viewer window titled "Visualizar eventos". The left pane displays a tree view of event logs: "Visualizar eventos (local)" with branches for "Aplicativo", "Segurança", "Sistema", "Serviço de diretório", "Servidor DNS", and "Serviço de duplicação de arquivos". The right pane shows a table of events with columns: Tipo, Data, Hora, Fonte, Categoria, Evento, and Usuário. The table contains 9,672 entries. The first few rows are as follows:

| Tipo        | Data     | Hora     | Fonte                   | Categoria  | Evento | Usuário |
|-------------|----------|----------|-------------------------|------------|--------|---------|
| Aviso       | 9/3/2004 | 21:27:46 | LsaSrv                  | SPNEGO ... | 40961  | N/A     |
| Informações | 9/3/2004 | 20:56:54 | Service Control Manager | Nenhuma    | 7036   | N/A     |
| Informações | 9/3/2004 | 20:56:54 | Service Control Manager | Nenhuma    | 7035   | Adminin |
| Aviso       | 9/3/2004 | 20:27:41 | LsaSrv                  | SPNEGO ... | 40961  | N/A     |
| Aviso       | 9/3/2004 | 19:27:40 | LsaSrv                  | SPNEGO ... | 40961  | N/A     |
| Aviso       | 9/3/2004 | 18:27:40 | LsaSrv                  | SPNEGO ... | 40961  | N/A     |
| Aviso       | 9/3/2004 | 17:27:39 | LsaSrv                  | SPNEGO ... | 40961  | N/A     |
| Aviso       | 9/3/2004 | 16:27:37 | LsaSrv                  | SPNEGO ... | 40961  | N/A     |
| Erro        | 9/3/2004 | 16:06:20 | Netlogon                | Nenhuma    | 5774   | N/A     |

Figura 10.2 Os eventos de Erro, Aviso e Informações.

- ◆ **Success Audit (Auditoria com êxito):** Representado por uma chave amarela. Evento gravado no log Segurança. Indica o evento de um acesso com sucesso. Por exemplo, se for habilitada a auditoria de tentativas de logon com sucesso, esse evento pode indicar um usuário que fez o logon com sucesso.

- ◆ **Failure Audit (Auditoria sem êxito):** Representado por um cadeado amarelo. Evento gravado no log Segurança. Indica o evento de um acesso sem sucesso. Por exemplo, se for habilitada a auditoria de tentativas de logon sem sucesso, esse evento pode indicar um usuário que não conseguiu efetuar o logon. Na figura 10.3, é mostrado um exemplo dos dois tipos de eventos de segurança: Auditoria com êxito e Auditoria sem êxito.

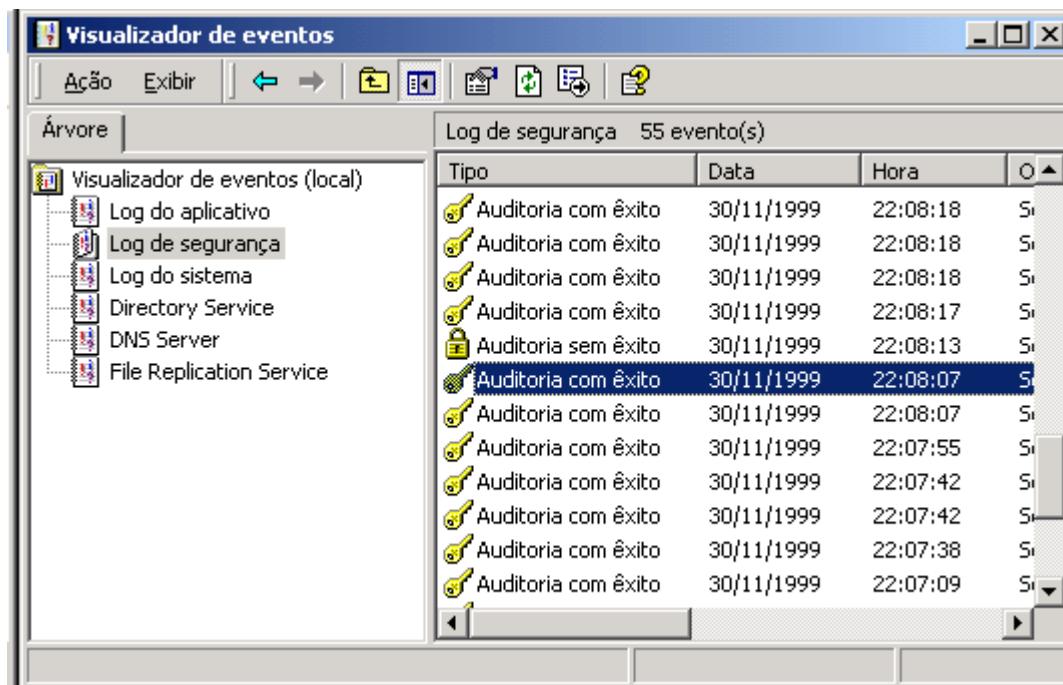


Figura 10.3 Os eventos de Auditoria com êxito e Auditoria sem êxito.

Agora que você já conhece os tipos de log que existem e os diferentes tipos de eventos que cada log pode apresentar, é hora de aprender a administrar e a consultar os logs do Windows Server 2003.

## Trabalhando com o Log de Eventos.

Neste tópico você aprenderá a executar uma série de ações práticas relacionadas com os logs de auditoria do Windows Server 2003. Desde simplesmente abrir o console Visualizar eventos e acessar os logs, passando pelas configurações e propriedades de cada log individualmente, até operações de exportar as informações dos logs para formatos que possam ser lidos em ferramentas como o Excel e o Access. Vou iniciar com um exemplo básico de utilização do console Visualizar de eventos.

### Exemplo: Visualizando eventos e detalhes dos eventos.

1. Faça o logon como Administrador ou com uma conta com permissão de administrador.
2. Abra o console Visualizar eventos: Iniciar -> Ferramentas Administrativas -> Visualizar eventos.
3. Será exibida a janela Visualizar eventos, indicada na Figura 10.4:

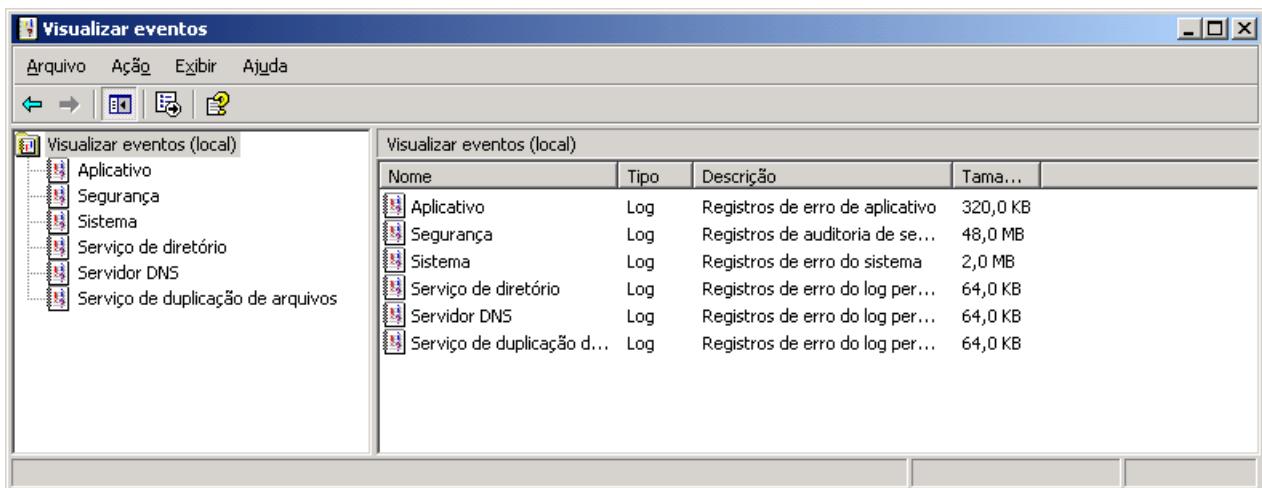


Figura 10.4 O console Visualizar eventos.

4. Dê um clique no log Aplicativo. Será exibida uma listagem com os diversos eventos gerados pelos aplicativos instalados no Windows Server 2003.
5. Dê um clique no log Segurança. Será exibida uma listagem com os diversos eventos gerados pelas diversas opções de auditoria de segurança que estão habilitadas no servidor (mais adiante você aprenderá a configurar estas diretrivas de segurança). Por padrão o Windows Server 2003 já habilita uma série de auditorias relacionadas com segurança (diferente do que acontece, por exemplo, no Windows XP Professional, onde, por padrão, nenhum evento de segurança está habilitado para ser auditado, isto é, para ter eventos gravados no log de segurança).
6. Dê um clique no log Sistema. Será exibida uma listagem com os diversos eventos gerados pelo próprio Windows Server 2003, conforme exemplo da Figura 10.5:

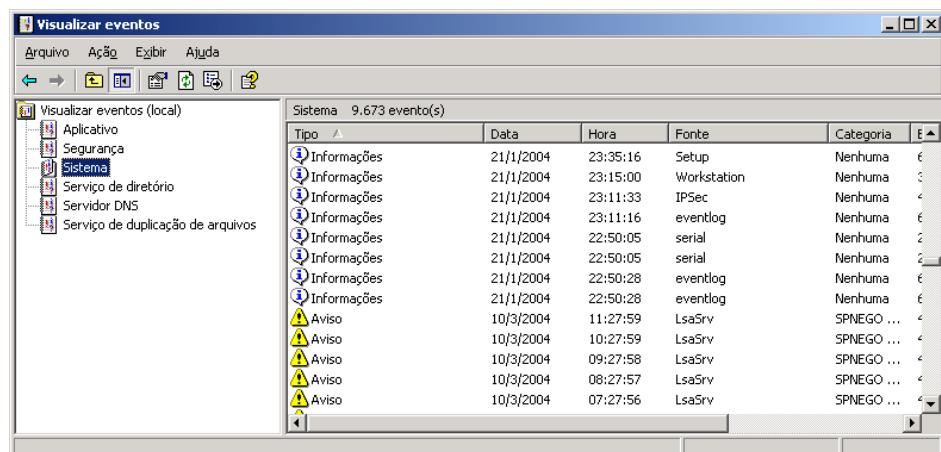


Figura 10.5 Eventos gerados pelo Windows Server 2003.

7. A listagem de eventos pode ser facilmente classificada de acordo com vários critérios, conforme exemplificarei mais adiante.

**NOTA:** Observe que além dos log padrão: Application (Aplicativo), Security (Segurança) e System (Sistema), também existem logs para o DNS, Directory Service (Serviços de Diretório) e para o serviço de replicação de arquivos, que a equipe de tradução insiste em traduzir como Serviço de duplicação de arquivos. O servidor que estou utilizando no exemplo é um DC, por isso os logs do DNS (que está instalado no próprio DC) e do serviço de diretório. O logo do serviço de replicação de arquivos foi instalado quando utilizei o DFS para criar réplicas de algumas pastas compartilhadas. O DFS utiliza o serviço de replicação de arquivos do Windows Server 2003, para manter as diversas réplicas sincronizadas, isto é, quando alterações são feitas em arquivos de uma réplica, é o serviço de replicação de arquivos que repassa estas alterações para as demais réplicas. Observe que cada log ocupa um determinado espaço em disco. No exemplo da

Observe que existem diversas colunas de informação para cada evento. Da esquerda para a direita, temos, por padrão, as seguintes colunas: Tipo, Data, Hora , Fonte, Categoria, Evento, Usuário e Computador.

Descrição das colunas padrão, dos logs do Windows Server 2003:

- ◆ **Tipo:** Uma classificação da gravidade do evento. Pode ser um dos seguintes tipos: Erro, Informações ou Aviso nos logs do sistema ou do aplicativo, Auditoria com êxito ou Auditoria sem êxito no log de segurança. No modo de exibição de lista normal de Visualizar eventos, cada um destes tipos é representado por um ícone diferente, conforme já descrito anteriormente.
  - ◆ **Data:** A data na qual o evento ocorreu, conforme a configuração de data/hora do sistema.
  - ◆ **Hora:** A hora local na qual o evento ocorreu, conforme a configuração de data/hora do sistema..
  - ◆ **Fonte:** O software que registrou o evento, que pode ser um nome de programa, como o “SQL Server,” ou um componente do sistema ou de um grande programa, como um nome de driver.
  - ◆ **Categoria:** Uma classificação do evento definida pela fonte do evento. Essa informação é usada principalmente no log de segurança. Por exemplo, para auditorias de segurança, isso corresponde a um dos tipos de eventos que podem ser gravados para o log de segurança: Com sucesso ou Sem sucesso.
  - ◆ **Evento:** Um número que identifica o tipo de evento específico. A primeira linha da descrição normalmente contém o nome do tipo de evento. Por exemplo, 6005 é a identificação do evento que ocorre quando o serviço Log de eventos é iniciado. A primeira linha da descrição de um evento é O serviço Log de eventos foi iniciado. A identificação do evento e a fonte podem ser usadas pela equipe de suporte para solucionar problemas do sistema.. No site <http://support.microsoft.com> você pode pesquisar maiores detalhes sobre um determinado número de evento.
  - ◆ **Usuário:** O nome de usuário em nome do qual o evento ocorreu. Este nome é a identificação de cliente se o evento foi realmente causado por um processo do servidor ou a identificação primária se a representação não estiver ocorrendo. Quando aplicável, uma entrada de log de segurança conterá as identificações primárias e de representação, ou seja, o nome de logon do usuário. A representação ocorre quando o Windows Server 2003 permite que um processo assuma os atributos de segurança de outro. Por exemplo, se você estiver fazendo uma auditoria, para descobrir todos os eventos de tentativa de logon no domínio, com sucesso ou com falha, de um determinado usuário, digamos jsilva. Neste caso, você terá que acessar o log de Segurança de todos os DCs do domínio (já que não existe um sistema centralizado de logs, dentro do domínio) e aplicar um filtro, para que sejam exibidos apenas os eventos cuja campo Usuário seja jsilva. Em seguida você pode exportar os resultados obtidos em cada DC para um arquivo de texto e importar todos os arquivos de texto no Excel ou no Access, para consolidar todos os eventos para o usuário jsilva e poder fazer pesquisas nestes dados.
  - ◆ **Computador:** O nome do computador onde o evento foi gerado. O nome do computador é normalmente seu próprio nome, a menos que você esteja visualizando um log de eventos em outro computador da rede.
8. Se você clicar no cabeçalho da coluna Tipo, por exemplo, a listagem de eventos será classificada pelo tipo de evento, isto é, todos os eventos de erro juntos, todos os eventos de informação juntos e todos os eventos de aviso juntos e assim por diante. Além disso surge uma setinha ao lado da palavra Tipo, indicando que a listagem está classificada pela coluna Tipo, conforme indicado pela Figura 10.6. Você pode classificar a listagem, por qualquer uma das colunas, bastando para isso clicar no título da respectiva coluna.

**Figura 10.4 o log de segurança é o que ocupa o maior espaço (48,0 MB). Mostrarei mais adiante, que o administrador pode configurar o espaço máximo que cada log pode ocupar e o que fazer com os eventos mais antigos, quando o espaço máximo é atingido.**

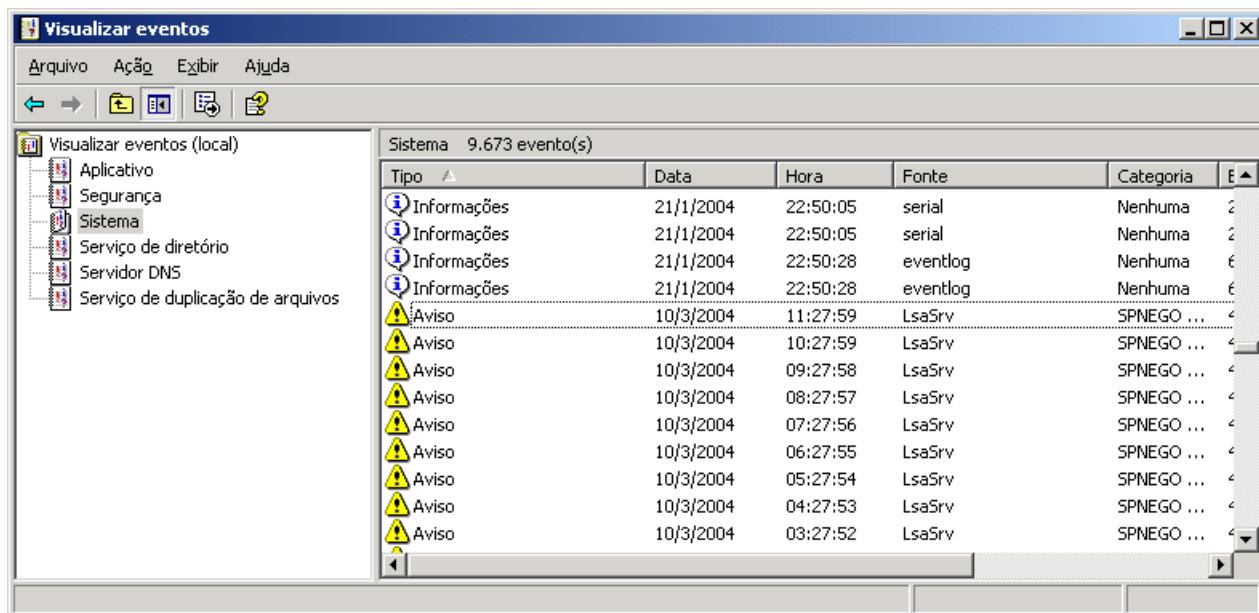


Figura 10.6 Eventos classificados pelo tipo.

9. Para exibir os detalhes de um evento, basta dar um clique duplo no respectivo evento. O Windows Server 2003 abre uma janela com informações detalhadas sobre o evento, qual a sua origem, causa e qual o usuário relacionado. Observe na Figura 10.7, onde são exibidos os detalhes sobre um evento de segurança do tipo Auditoria sem êxito, devido a uma falha de logon do usuário Administrador. Conforme o próprio evento informa, a causa mais provável foi uma senha digitada incorretamente.

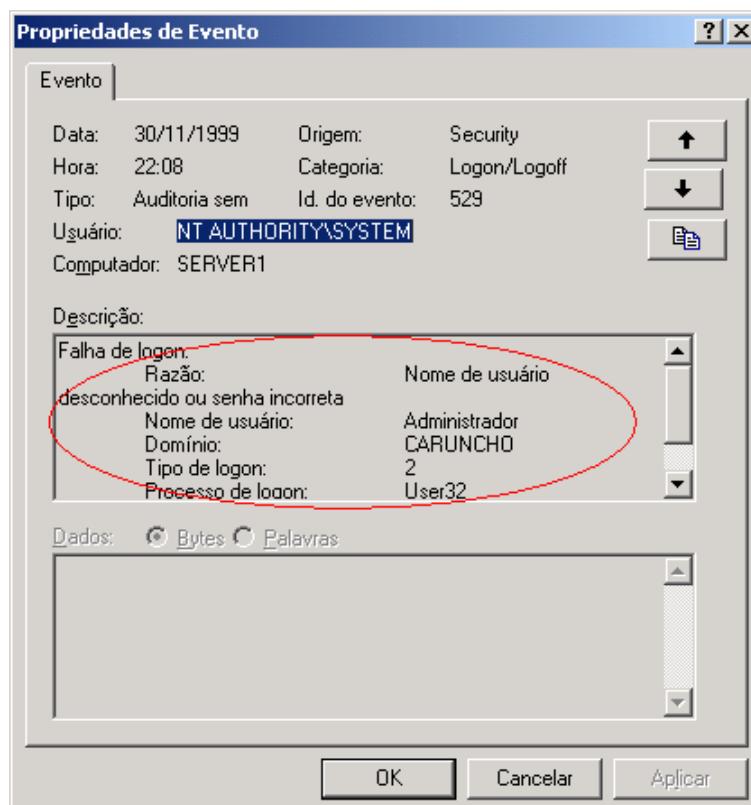


Figura 10.7 Detalhes sobre um evento de segurança do tipo Auditoria sem êxito.

10. Você pode configurar quais colunas de informação são exibidas para cada evento. Selecione o comando Exibir -> Adicionar/Remover Colunas... Será exibida a janela indicada na Figura 10.8, onde, por padrão, são exibidas todas as colunas.

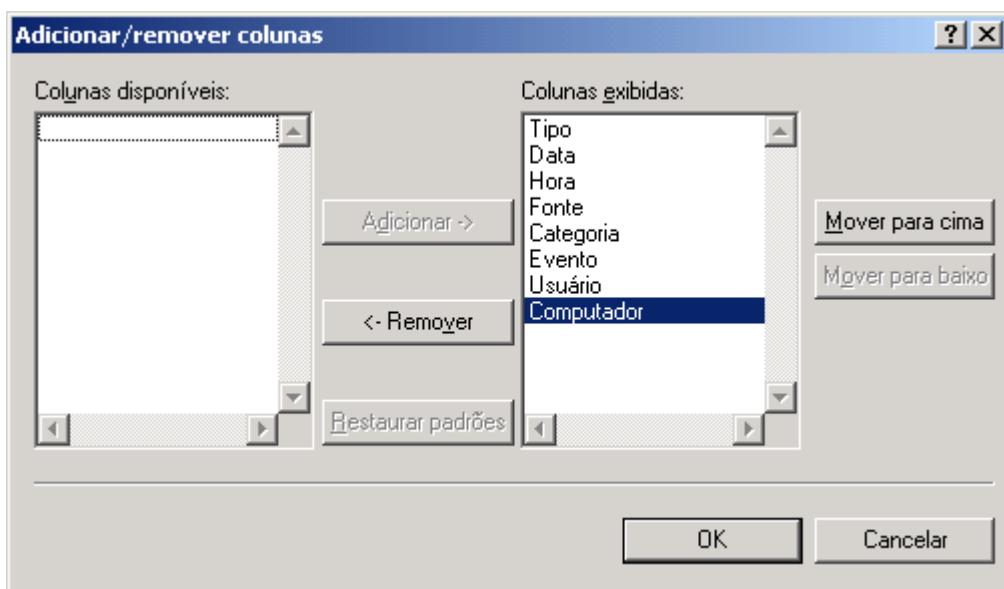


Figura 10.8 A janela para configurar as colunas a serem exibidas.

Para remover uma coluna, marque-a na lista Colunas exibidas e clique no botão Remover. Para adicionar uma coluna, marque-a na lista Colunas disponíveis e clique em Adicionar. Você pode alterar a posição das colunas, marcando a coluna na lista Colunas exibidas e utilizando os botões Mover para cima e Mover para baixo.

11. Faça as configurações desejadas e clique em OK.
12. Feche o console para visualização dos eventos.

Exercício: Abra novamente o Visualizador de eventos e navegue pelos diferentes Logs: Aplicativo, Segurança e Sistema. Dê um clique duplo sobre alguns eventos e verifique os detalhes sobre o evento. Vá para a opção Aplicativo e classifique a listagem pelo Tipo, depois pela Data.

## Habilitando/configurando os eventos do log de segurança.

Conforme foi descrito no item anterior, o Windows Server 2003 permite que o administrador configure quais eventos de segurança devem e quais não devem ser auditados. Para que sejam auditadas determinadas ações ligadas com a segurança - tais como tentativas de logon e acesso a arquivos e pastas – algumas diretivas tem que ser habilitadas. As opções de segurança, são habilitadas através de diretivas de segurança, configuradas via GPO.

Em um computador com o Windows Server 2003, configurado como member server ou como standalone server, deve ser utilizado o console Local Security Policy (Diretiva de segurança local), acessada através da opção Ferramentas administrativas.

No exemplo deste item utilizarei o console Domain Security Policy (Diretivas de Segurança do Domínio). Com isso estou configurando opções que serão válidas para todos os computadores (clientes e servidores do domínio). Depois farei uma tentativa de logon com uma senha errada e você observará se foi gerado um evento no log de segurança. Então mãos a obra.

Neste exemplo mostrarei como habilitar algumas opções de auditoria, as quais não estão habilitadas por padrão. Por exemplo, a auditoria do acesso à arquivos e pastas não é habilitado por padrão. Para que o administrador possa auditar o acesso a pastas e arquivos (isto é, fazer com que sejam gravados eventos no log de eventos, quando os usuários acessam uma determinada pasta e seus arquivos), primeiro o administrador tem que habilitar uma diretiva de auditoria, para que o Windows Server 2003 passe a auditar o acesso a pastas e arquivos. Outro exemplo seria a auditoria do uso de impressoras, a qual por padrão também é desabilitada. Neste exemplo, mostrarei quais os passos para que o administrador possa habilitar as diretivas de auditoria e apresentarei uma descrição das diretivas disponíveis.

Exemplo: Para habilitar a auditoria de eventos de segurança, siga os seguintes passos:

1. Faça o logon com uma conta com permissão de administrador.
2. Abra o console Diretivas de segurança de domínio: Iniciar -> Ferramentas Administrativas -> Políticas de Segurança do Domínio.
3. Será aberta a janela Configurações de segurança padrão de Domínio, conforme indicado na Figura 10.9:

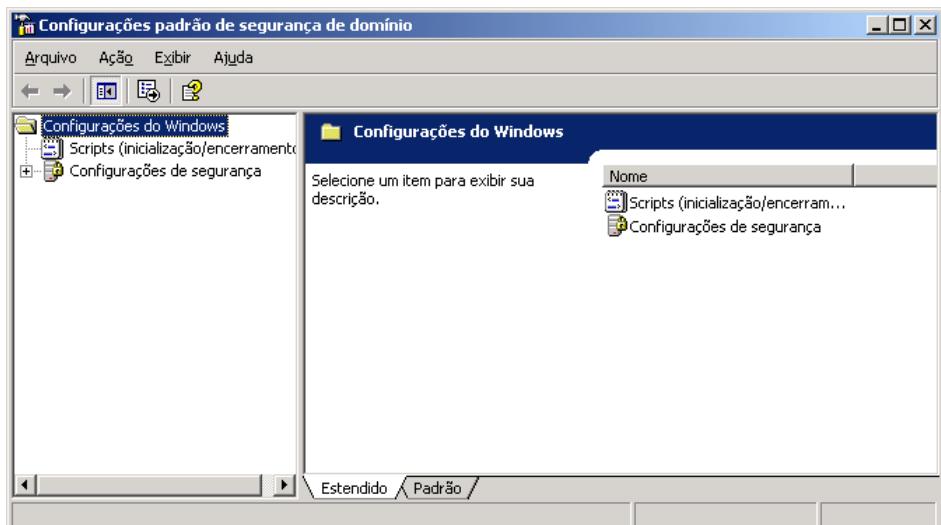


Figura 10.9 O console para configurações das diretivas de segurança do domínio.

4. Clique no sinal de + ao lado da opção Configurações de segurança, para exibir as opções disponíveis. Clique no sinal de + ao lado da opção Diretivas locais, para exibir as opções disponíveis.
5. Nas opções que surgem, dê um clique na opção Diretivas de auditoria . No painel da direita são exibidas as várias diretivas de auditoria disponíveis, as quais são indicadas na Figura 10.10 e explicadas logo a seguir. Observe ao lado do nome de cada diretiva, o status Não-definido, indicando que não existe definição para esta diretiva, isto é, esta diretiva estivesse desabilitada.

**NOTA:** Se você estiver em um Controlador de Domínio, com o Windows 2000 Server ou como Windows Server 2003 instalado, você tem duas opções. Pode ser utilizada a opção Domain Controller Security Policy (Diretivas de segurança de controlador de domínio), do menu Administrative Tools (Ferramentas Administrativas). Com esta opção você está configurando diretivas válidas somente para o controlador de domínio no qual você está logado. Também pode ser utilizada a opção Domain Security Policy (Diretivas de Segurança de Domínio), do menu Administrative Tools (Ferramentas administrativas). Com esta opção você está configurando diretivas válidas para todo o domínio.

**IMPORTANTE:** Porém não basta habilitar as diretivas. Por exemplo, não basta habilitar a diretiva que orienta o Windows Server 2003 a monitorar o acesso a pastas e arquivos. Depois de habilitada a auditoria, o administrador tem que definir quais pastas e arquivos devem ser monitoradas (por padrão nenhuma pasta é monitorada, mesmo após a respectiva diretiva de segurança ter sido habilitada) e para quais usuários e grupos deve ser feito o monitoramento. Esta segunda etapa na configuração de auditoria de acesso a pastas, arquivos e impressoras será descrita em exemplos mais adiante, neste capítulo.

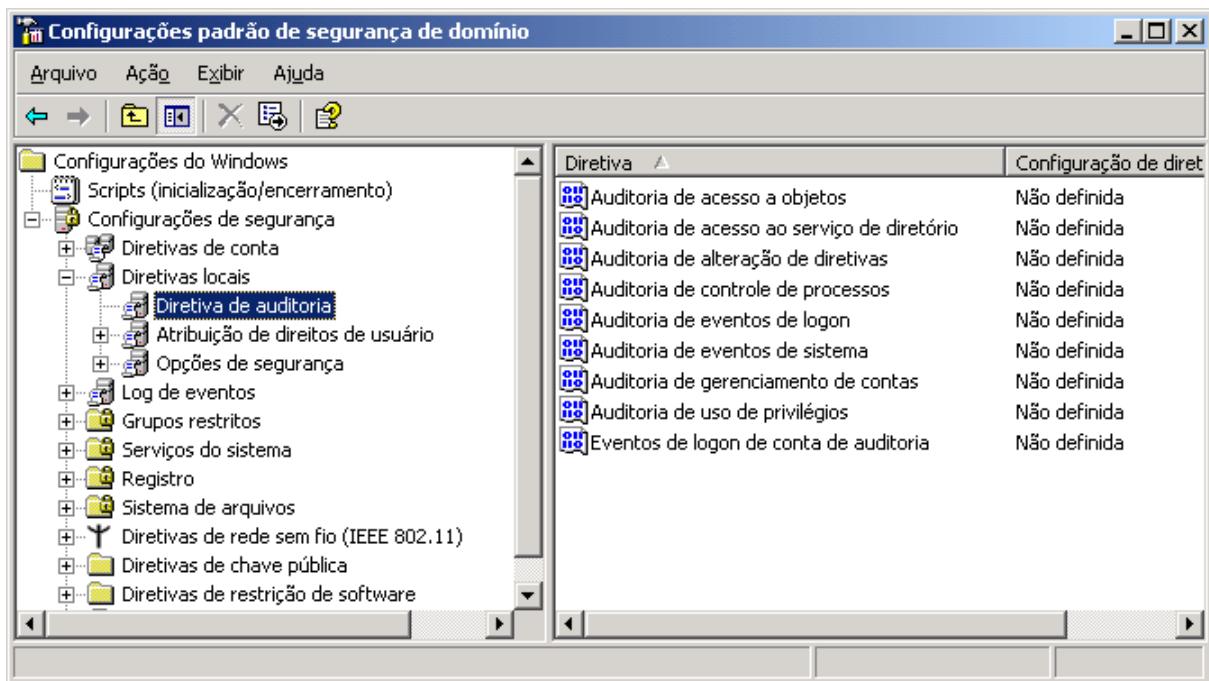


Figura 10.10 Opções para configuração das Diretivas de auditoria.

A seguir apresento uma descrição das diretrivas de auditoria disponíveis:

◆ **Audit account logon events (Auditoria de eventos de logon de conta):**

Com esta opção você pode configurar se os eventos de logon devem ou não ser auditados. São considerados eventos de logon, qualquer logon feito em uma estação de trabalho da rede, que pertença ao domínio e com uma conta do domínio.

Conforme descrito anteriormente, a validação do logon é feita nos DCs, onde está instalado o Active Directory. Neste caso se o usuário jsivla fizer o logon com a sua conta de domínio, na sua estação de trabalho, um evento de logon será gerado para este usuário. Além disso você define se devem ser auditados os eventos com sucesso (quando o usuário faz o logon normalmente) ou com falha (quando o usuário não consegue fazer o logon, por exemplo, por ter digitado uma senha incorreta). Para configurar esta auditoria, basta dar um clique duplo nela. Será aberta a janela Propriedades de Eventos de logon de conta de auditoria (a confusão no nome é por conta da equipe de tradução). Para habilitar esta diretiva você deve marcar a opção Definir as configurações dessas diretrivas (o plural também é por conta da equipe de tradução). Ao marcar esta opção, serão habilitadas as opções Éxito e Falha. Para passar a registrar os eventos de logon com sucesso, marque a opção Éxito. Com isso sempre que um usuário fizer um logon no domínio, com sucesso, será registrado um evento no log de eventos do DC que autenticou o usuário. Para passar a registrar os eventos de falha de logon, marque a opção Falha. Com isso, sempre que um usuário fizer uma tentativa de logon sem sucesso, será registrado um evento no log de eventos do DC onde a tentativa de logon foi feita. Na Figura 10.11 é exibida a janela de propriedades desta diretiva e as opções que podem

**NOTA:** Estas opções de auditoria também poderiam ser configuradas através da GPO (Group Policy Object) padrão do domínio. No Capítulo 9 você teve uma introdução ao assunto GPO, focando nos pontos cobrados no Exame 70-290. Para um estudo completo sobre GPOs, consulte o Capítulo 18 do meu livro: Windows Server 2003 – Curso Completo, 1568 páginas.

**IMPORTANTE:** O nome correto desta auditoria é Auditoria de eventos de logon de conta, porém no console Configurações padrão de segurança do domínio, esta diretiva aparece, incorretamente, com o seguinte nome: Eventos de logon de conta de auditoria. Esta é mais uma pérola da tradução, que contribui para tornar confuso um recurso que é fácil de utilizar.

ser configuradas para esta auditoria. Após ter definido as configurações desejadas, basta clicar em OK. O mais comum para este diretiva é habilitar tanto os eventos de sucesso, quanto os eventos de falha, para que fique registrado no log do servidor, todos os eventos de logon, que seja com sucesso, quer seja com falha.

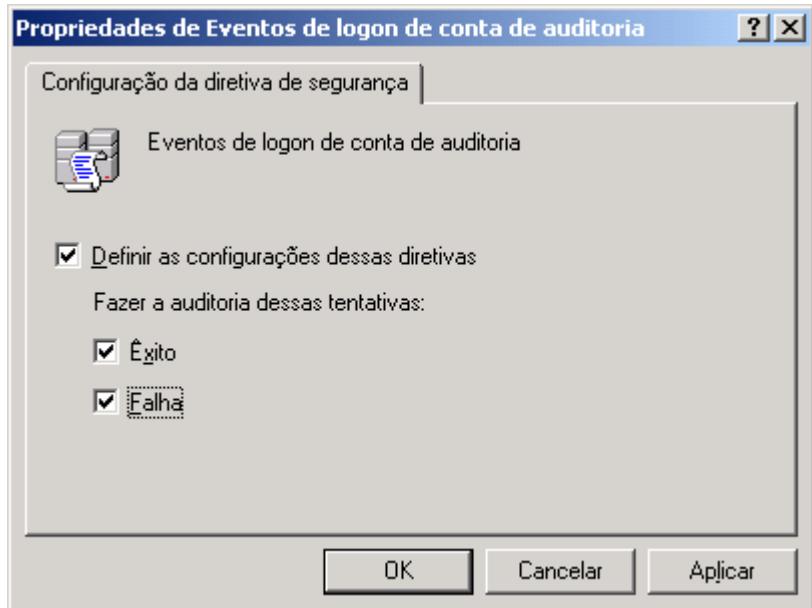


Figura 10.11 Opções para a diretiva de auditoria de eventos de logon.

- ◆ Audit account management (Auditoria de gerenciamento de contas): Esta diretiva determina se deve ser feita a auditoria de cada evento de gerenciamento de conta de um usuário, grupo ou computador do domínio. Os exemplos de eventos de gerenciamento de conta incluem: criação ou alteração de uma conta, renomeação de uma conta, ativação/desativação da conta, incluir um usuário em um grupo ou retirar o usuário de um grupo, o administrador definir a senha de uma conta e assim por diante.

As configurações padrão para esta diretiva são as seguintes:

- ◆ Sucesso em controladores de domínio.
- ◆ Sem auditoria nos Member Servers

Para configurar esta auditoria, basta dar um clique duplo nela. Será aberta a janela de propriedades da auditoria. Para habilitar esta diretiva você deve marcar a opção Definir as configurações dessas diretrivas. Ao marcar esta opção, serão habilitadas as opções Êxito e Falha. Para passar a registrar os eventos de gerenciamento de contas com sucesso, marque a opção Sucesso. Com isso sempre que o administrador ou outro usuário com as devidas permissões, fizer alterações em uma conta, um evento será gravado no log de eventos. Para passar a registrar os eventos de falha de gerenciamento de contas, marque a opção Failure. Com isso, sempre que o administrador ou um usuário sem as devidas permissões, fizer uma tentativa alterar uma conta, será registrado um evento no log de eventos. Na Figura 10.12 é exibida a janela de propriedades desta auditoria e as opções que podem ser configuradas para esta auditoria. Após ter definido as configurações desejadas, basta clicar em OK. O mais comum para esta diretiva é habilitar apenas o log dos eventos sem sucesso, ou seja, de tentativas que um usuário faz de alterar contas do domínio, sem ter as devidas permissões para isso. Esta situação pode acontecer quando, por exemplo, um usuário está tentando alterar a senha de outro usuário para fazer um logon com a conta deste segundo usuário.

**IMPORTANTE:** É muito importante que você conheça este ponto, ou seja, para fazer a auditoria de eventos de logon de contas do domínio, a diretiva a ser habilitada é a diretiva Auditoria de eventos de logon de conta. Existe uma outra auditoria, com um nome semelhante – Auditoria de eventos de logon, porém esta segunda é usada para fazer a auditoria de eventos de logon usando contas locais dos computadores e não as contas do domínio. Certifique-se de que você entendeu bem a diferença entre estas duas diretivas, pois este é um ponto importante para o exame.

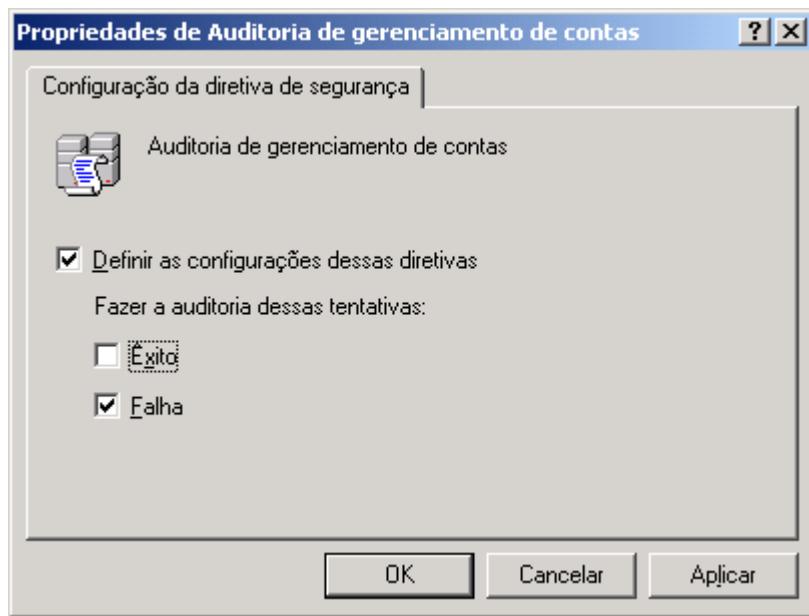


Figura 10.12 Opções para a diretiva de auditoria de eventos de gerenciamento de contas.

- ◆ **Auditoria de acesso ao serviço de diretório:** Define se serão auditadas tentativas de acesso com sucesso, com falha ou ambas, a objetos do Active Directory, para os quais tenha sido habilitada a auditoria dos acessos. O Active Directory, conforme explicado no Capítulo 02, é a base de dados na qual ficam armazenados uma série de objetos, como por exemplo: contas de usuários, grupos de usuários, Unidades organizacionais, domínios, sites, etc. Por exemplo, podemos implementar uma política para detectar tentativas de alteração sem sucesso, nas contas que fazem parte do grupo Administradores. Por padrão esta política está desabilitada para controladores de domínio e indefinida para os demais computadores. Um cuidado que deve ser tomado é o de habilitar somente as auditorias realmente necessárias, de acordo com a política de segurança da empresa, pois se forem habilitadas auditoria em um grande número de objetos, pode haver uma queda de desempenho, além de um crescimento exagerado no tamanho do log de segurança. Por padrão esta auditoria está desabilitada.
- ◆ **Audit logon events (Auditoria de eventos de logon):** Esta diretiva determina se deve ser feita a auditoria de cada instância de logon ou logoff de usuário, bem como de qualquer conexão de rede com o computador local, ou no caso com o DC que eu estou utilizando. Se você estiver registrando no log os eventos da Auditoria de eventos de logon de conta com êxito em um controlador de domínio, as tentativas de logon de um usuário, a partir da sua estação de trabalho não gerarão auditorias de logon (as quais serão geradas se a diretiva Auditoria de eventos de logon de conta, descrita anteriormente, estiver habilitada). Somente tentativas de logon de rede e interativas no próprio controlador de domínio gerarão eventos de logon. Resumindo, Auditoria de eventos de logon de conta são gerados no local onde reside a conta; ou seja, no DC. Eventos de logon são gerados no local onde ocorre a tentativa de logon. Se for um logon interativo no DC, no próprio DC, se for um logon interativo em um member server, no log de auditoria local do member server. Você pode configurar para que sejam auditadas tentativas de logon com sucesso, com falha ou ambas. No caso de um computador com o Windows Server 2003, as tentativas de logon são consideradas as tentativas locais ou tentativas feitas via Terminal Service Client.

- ◆ **Audit object access (Auditoria de acesso a objetos):** Determina se deve ser feita a auditoria do acesso de um usuário a um objeto — por exemplo, um arquivo, uma pasta, uma chave da Registry, uma impressora etc. São considerados objetos, todos aqueles elementos que possuem uma ACL – Access Control List (Lista de Controle de Acesso). Por exemplo, uma pasta em uma partição NTFS, onde são definidas permissões de acesso (além de habilitar esta diretiva, posteriormente a pasta deve ser configurada para registrar eventos de acesso no log de auditoria, conforme exemplo mais adiante). Se você definir esta configuração de diretiva, poderá especificar se haverá auditoria de acessos com êxito, acessos sem êxito ou se não ocorrerá auditoria desse tipo de evento. As auditorias com êxito geram uma entrada de auditoria quando um usuário acessa com êxito um objeto. Por exemplo, o usuário tem permissão de leitura em um arquivo e ele acessa o arquivo para leitura. Este é um evento com sucesso. As auditorias sem êxito geram uma entrada de auditoria quando um usuário tenta acessar sem êxito um objeto, como por exemplo, tentar imprimir em uma impressora na qual ele não tem permissão ou tentar alterar um arquivo para o qual ele tenha apenas permissão de leitura. É interessante observar que a definição de Auditoria de acesso a objetos ocorre em duas etapas. Primeiro o administrador deve habilitar esta diretiva, para acessos com sucesso, com falha ou ambos. Em seguida, em cada objeto (pasta, impressora, arquivo, etc) a ser auditado, o administrador deve configurar a auditoria e especificar quais usuários ou grupos devem ser monitorados. Apenas habilitar a diretiva não fará com que o acesso aos objetos sejam auditados. Por padrão esta diretiva está desabilitada.
- ◆ **Audit policy change (Auditoria de alteração de diretivas):** Determina se deve ser feita a auditoria das alterações efetuadas nas diretivas de segurança. O normal é habilitar a auditoria de eventos sem sucesso, para tentar identificar tentativas de alteração das diretivas, por usuários não autorizados. Alterar as diretivas é uma das maneiras de criar brechas na segurança do sistema, por isso somente usuários autorizados devem ter este nível de permissão.
- ◆ **Audit process tracking (Auditoria de controle de processos):** Determina se deve ser feita a auditoria de informações de controle de eventos detalhadas, como ativação de programas, término de processo, duplicação de identificador e acesso indireto a objeto. Esta diretiva é utilizada para fazer uma auditoria dos programas que estão rodando no computador, na tentativa de detectar usuários que estão tentando utilizar programas para os quais eles não tem permissão ou tentando instalar processos que possam abrir o servidor para ataques de segurança.
- ◆ **Audit system events (Auditoria de eventos de sistema):** Determina se deve ser feita a auditoria quando um usuário reiniciar ou desligar o computador, ou quando ocorrer um evento que afete a segurança do sistema ou o log de segurança.
- ◆ **Audit privilege use (Auditoria de uso de privilégios):** Determina se deve ser feita a auditoria de cada instância do uso de um direito do usuário. Direitos (rights) são permissões especiais, como por exemplo incluir um computador como membro de um domínio, fazer o logon interativamente nos controladores de domínio, alterar a hora dos servidores e assim por diante. Estes direitos podem ser configuradas pelo Administrador, o qual pode “dar” estes direitos para determinados usuários ou grupos.

**IMPORTANTE:** Vou insistir neste ponto. Lembre-se que a diretiva Auditoria de eventos de logon de conta é utilizada para fazer auditoria de logon de contas do domínio, já a diretiva Auditoria de eventos de logon, é utilizada para a auditoria de eventos de logon de contas locais.

Feita a descrição das várias diretivas, vamos continuar o nosso exemplo.

6. No painel da direita, localize uma diretiva chamada Eventos de logon de conta de auditoria (uma “maravilhosa” tradução) e dê um clique duplo para abri-la. Será exibida a janela com as configurações atuais para esta diretiva.
7. Marque as opções conforme indicado na Figura 10.13 e dê um clique em OK para habilitar a auditoria de eventos de logon de contas do domínio. Observe que está sendo habilitada a auditoria tanto para os eventos com sucesso quanto para a falha no logon.

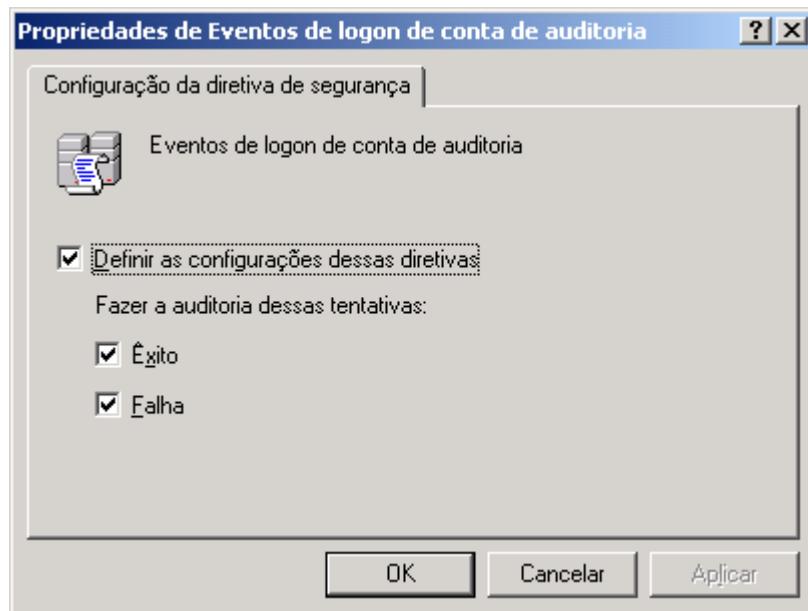


Figura 10.13 Habilitando a auditoria de eventos de logon.

8. Você deve ter voltado para o console Configurações locais de segurança. Observe que ao lado da diretiva, o status agora aparece como sendo Êxito, Falha, diferente do status anterior que era Não-Definido. Isso indica que esta auditoria está habilitada tanto para eventos de sucesso quanto falha de logon.
9. Feche o console para configuração das diretivas de segurança do domínio.

Agora é hora de testar se o Windows Server 2003 está fazendo a auditoria de eventos de logon. Farei o logon como usuário user02 (utilize um usuário qualquer da sua rede, com permissão de logon no DC) e vou informar uma senha incorreta, para simular uma falha na tentativa de logon. O Windows Server 2003 vai dizer que não pode efetuar o logon. Depois vou fazer o logon como Administrador e verificar no log de segurança se existe um evento para a tentativa de logon sem sucesso.

Exemplo: Para gerar um evento de falha de logon e verificar se o evento foi gravado no log de Segurança do Windows Server 2003.

1. Se estiver logado como Administrador faça o logoff.
2. Tente fazer o logon como usuário user02 (utilize um usuário cadastrado na sua rede), mas digite uma senha incorreta.
3. O Windows Server 2003 informa que o logon não pode ser feito.
4. Agora faça o logon como Administrador (desta vez digite a senha correta).
5. Abra o console Visualizar eventos: Iniciar -> Ferramentas Administrativas -> Visualizar eventos.

6. Dê um clique na opção Segurança.
7. Na listagem de eventos, procure o primeiro evento do tipo Auditoria sem êxito. Dê um clique duplo sobre o evento para exibir os seus detalhes.
8. Este evento descreve a tentativa de logon, sem sucesso, do usuário user02, conforme pode ser visto na Figura 10.14.

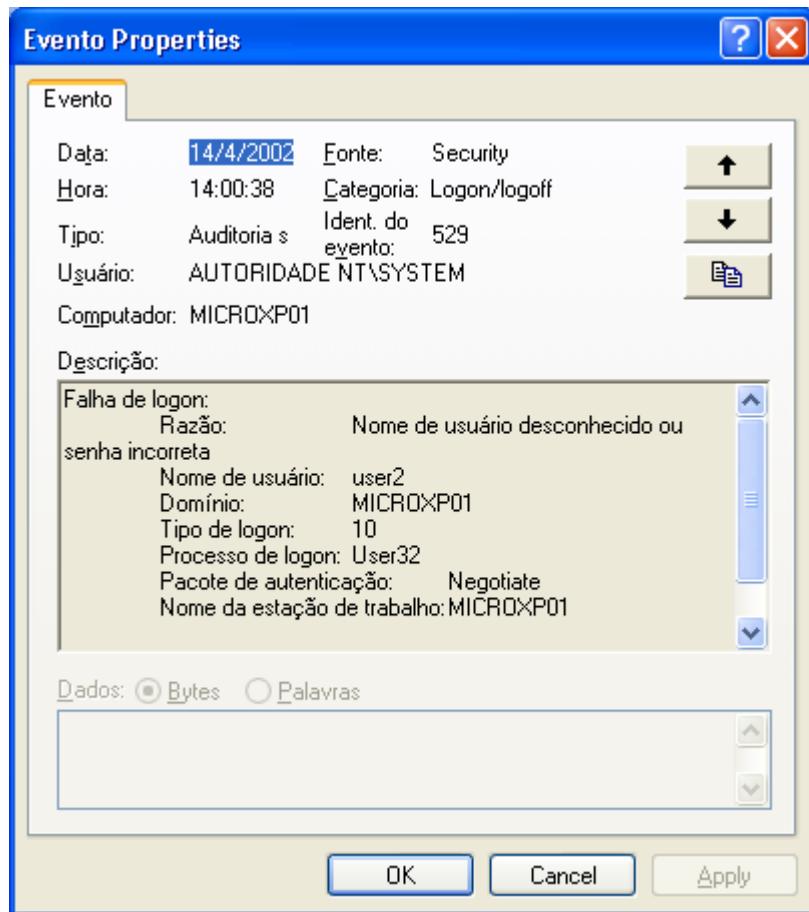


Figura 10.14 Falha na tentativa de logon do usuário user2.

9. Para ver uma descrição completa do evento, você pode copiar o texto do evento para a área de transferência do Windows Server 2003. Para isso clique no botão Copiar (botão com o desenho de duas folhas sobrepostas, logo abaixo do botão com uma seta para baixo). Depois abra o Bloco de notas e selecione o comando Editar -> Colar. Para o nosso exemplo, obteremos o texto indicado a seguir:

```

Tipo de evento: Auditoria sem êxito
Fonte de evento: Security
Categoria do evento: Logon/logoff
Id. do evento: 529
Data: 14/4/2002
Hora: 14:00:38
Usuário: AUTORIDADE NT\SYSTEM
Computador: MICROXP01
Descrição:
Falha de logon:
  Razão: Nome de usuário desconhecido ou senha incorreta
  Nome de usuário: user2
  Domínio: MICROXP01
  Tipo de logon: 10
  
```

**Processo de logon:** User32  
**Pacote de autenticação:** Negotiate  
**Nome da estação de trabalho:** MICROXP01

Para obter mais informações, visite o Centro de ajuda e suporte em <http://go.microsoft.com/fwlink/events.asp>.

Observe o seguinte trecho do texto:

Razão: Nome de usuário desconhecido ou senha incorreta

Este trecho indica, com precisão, o motivo que gerou o evento: uma falha de logon devido a um nome de usuário desconhecido ou senha incorreta. No nosso exemplo o problema foi devido a uma senha digitada incorretamente.

10. Dê um clique em OK para fechar a janela com os detalhes do evento.
11. Feche o Visualizador de eventos.

## Recomendações da Microsoft, para configurações de auditoria.

Na documentação oficial do Windows Server 2003, você encontra algumas recomendações sobre as opções de auditoria que devem ser habilitadas. A seguir coloco estas recomendações.

Recomendações da documentação Oficial do Windows Server 2003, sobre auditoria de eventos:

Para minimizar o risco de ameaças à segurança, há diversas medidas de auditoria que podem ser tomadas. A seguir é exibida uma lista dos vários eventos para os quais é aconselhado que seja feita uma auditoria, bem como a ameaça específica à segurança que o evento de auditoria monitora. Na verdade não é a auditoria que irá reduzir os riscos. As informações obtidas a partir da auditoria de segurança, permitem que o administrador tome as medidas necessárias para reduzir os riscos de segurança e bloquear ataques contra a segurança.

---

**NOTA:** Por padrão somente usuários com permissão de administrador, tem permissão para acessar os eventos do log Segurança. Os demais logs: Aplicativo e Sistema, podem ser acessados por qualquer usuário.

---

- ◆ **Auditoria de falha ao fazer logon/logoff:** Serve como prevenção para uma violação por senha aleatória, isto é, para programas que tentam várias senhas, na tentativa de “adivinhar” a senha do usuário. A melhor maneira de se prevenir deste tipo de ataque é configurando as políticas de senha, para que a senha seja bloqueada após três ou quatro tentativas de logon sem sucesso, conforme descrito em detalhes no Capítulo 4.
- ◆ **Auditoria de êxito ao fazer logon/logoff:** Serve com uma proteção para o caso de violação por senha roubada, ou seja, para detectar quando um usuário conseguiu descobrir a senha de outro(s) usuário(s). Também serve como um registro das atividades de logon no domínio, de tal maneira que seja possível identificar usuários que estão fazendo o logon fora do horário normal de trabalho. Por exemplo, um usuário que está chegando duas horas antes do expediente ou está vindo à noite na empresa, merece um acompanhamento mais cuidadosa.
- ◆ **Auditoria em caso de êxito em eventos de uso de privilégios, gerenciamento de usuários e grupos, diretivas de alteração de segurança, reinicialização, desligamento e sistema:** Utilizada para detectar o uso incorreto dos privilégios, ou a tentativa de utilizar estes privilégios, por usuários não autorizados. Por exemplo, para detectar se um usuário que não tem permissão para instalar novos programas, está tentando instalar programas ou para detectar se um usuário que não tem permissão para alterar senhas está tentando alterar a senha das contas de outros usuários.
- ◆ **Auditoria em caso de êxito ou falha para eventos de acesso a arquivos e objetos. Auditoria em caso de êxito ou falha do Gerenciador de arquivos no acesso de leitura/gravação a arquivos confidenciais por usuários ou grupos suspeitos:** Utilizada para monitorar o acesso indevido a arquivos confidenciais, como por exemplo o

banco de dados com informações sobre salários, finanças ou com os dados da contabilidade da empresa. Por exemplo, você pode definir que sejam auditados os acessos a uma pasta que contém documentos de pesquisas e desenvolvimentos de novos produtos da empresa, para detectar se alguém está tentando acessar estas informações sem ter permissão de acesso para tal. Isso pode indicar uma tentativa de espionagem.

- ◆ Auditoria em caso de êxito ou falha para eventos de acesso a objetos e impressoras com acesso a arquivos.  
**Auditoria em caso de êxito ou falha do Gerenciador de impressão no acesso a impressoras por usuários ou grupos suspeitos:** Utilizada para detectar o acesso impróprio a impressoras, como por exemplo um usuário tentando imprimir um grande número de cópias após o expediente, o que normalmente caracteriza o uso da impressora da empresa para impressão de trabalhos pessoais.
- ◆ Auditoria em caso de êxito ou falha no acesso à gravação de arquivos de programa (extensões .exe e .dll).  
**Auditoria em caso de êxito ou falha no controle de processos:** Execução de programas suspeitos; análise do log de segurança para verificar se há tentativas inesperadas de modificar arquivos de programa ou criar processos inesperados. Execução apenas quando o log do sistema estiver sendo monitorado ativamente: Utilizada para detectar quaisquer tentativas de modificar arquivos fundamentais para o funcionamento do Windows Server 2003, o que pode acontecer, por exemplo, no caso de uma infecção por vírus.

Estas são apenas recomendações gerais. A política de segurança da empresa é que irá definir, dentro das necessidades de cada empresa, quais eventos serão auditados e qual a forma de análise destes eventos.

## Filtrando eventos nos logs de auditoria.

A medida que eventos vão sendo gravados nos diferentes logs, a lista de eventos vai ficando bastante extensa, e com isso fica mais difícil para localizar um determinado evento. Podem existir situações em que o administrador está interessado em um único tipo de evento, ou eventos relacionados com um determinado serviço ou programa, ou ainda somente eventos gerados por um determinado usuário ou computador. Por exemplo, pode ser que o administrador precise visualizar apenas os eventos sobre tentativas de logon sem êxito, ou eventos relacionados ao SQL Server 2000, ou ainda todos os eventos de logon para a conta jsilva e assim por diante.

No Visualizador de eventos, é possível filtrar os eventos de acordo com determinados critérios, de tal forma que somente sejam exibidos os eventos que estão de acordo com os critérios especificados. Muitas vezes quando o administrador está tentando solucionar um determinado problema, pode ser útil fazer que sejam exibidos apenas os eventos de erro, ou mais especificamente, os eventos de erro relacionados com o serviço e/ou programa que está apresentando problemas. O administrador também pode filtrar os eventos de segurança por tipo, como por exemplo: somente com sucesso ou somente com falha e assim por diante. Existem diversas opções de filtragem, conforme mostrarei nos exemplos práticos, logo a seguir.

## Exemplo - Para filtrar os eventos do log do sistema, pelo tipo de evento, siga os passos indicados a seguir:

1. Faça o logon com uma conta com permissão de administrador.
2. Abra o console Visualizar eventos: Iniciar -> Ferramentas Administrativas -> Visualizar eventos.
3. Dê um clique na opção Sistema.
4. Observe que estão sendo exibidos eventos de três diferentes tipos: Erro, Informação e Aviso, conforme indicado pela Figura 10.15:

Figura 10.15 Listagem exibindo eventos de Erro, Informação e Aviso.

5. Vou fazer com que sejam exibidos somente os eventos do tipo Erro.
6. Selecione o comando Exibir -> Filtro...
7. Será exibida a janela Propriedades do Sistema, com a guia Filtro selecionada, conforme indicado na Figura 10.16.

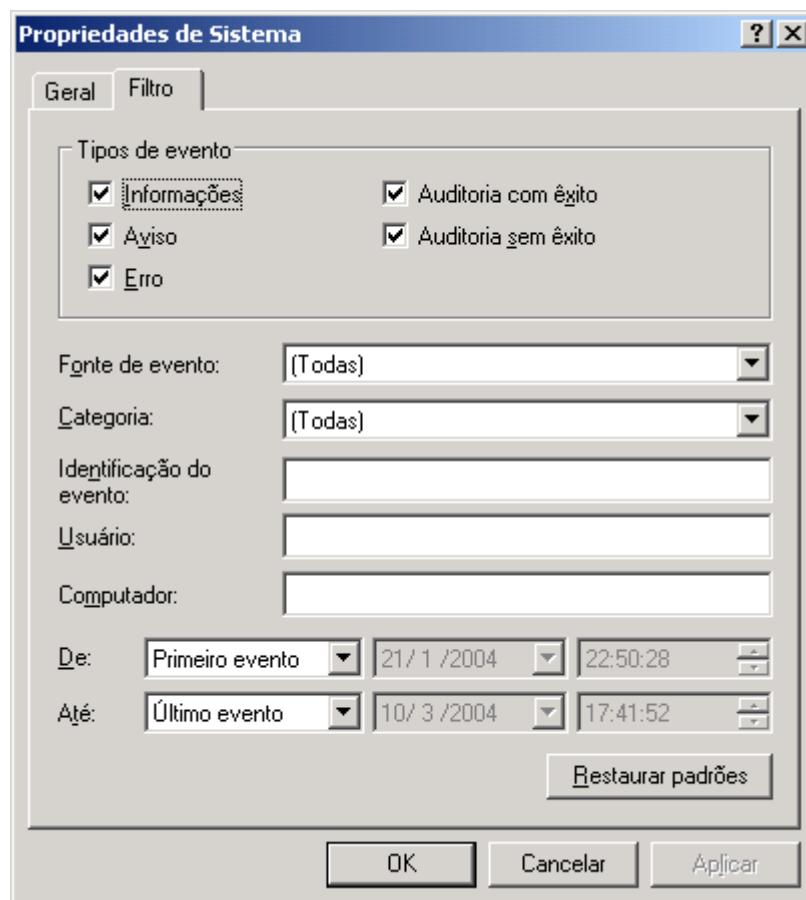


Figura 10.16 Janela para definir critérios de filtragem.

8. Na parte de cima da janela, onde é exibido o grupo de opções Tipos de eventos, desmarque todas as opções, com exceção da opção Erro. Neste grupo estão as opções para definir quais tipos de eventos serão exibidos. Como quero exibir apenas os eventos do tipo Erro, estou deixando marcada apenas a opção Erro.

A lista Fonte do evento permite identificar o software ou serviço que registrou o evento em log. Este software pode ser um aplicativo ou um componente do sistema, como um driver de Hardware, por exemplo. Por padrão, todas as fontes são registradas em log. Para identificar o software que registrou um evento em log, clique com o botão direito do mouse no evento e, em seguida, clique em Propriedades. Se você selecionar uma opção nesta lista, serão exibidos apenas os eventos para a opção selecionada. Por exemplo, se você deseja exibir apenas eventos de Erro associados com o CD-ROM, você marcaria a opção Erro e na lista Fonte de evento, selecionaria CD-ROM.

A lista Categoria lista a categoria do evento, conforme definido pela fonte. Por padrão, todas as categorias são registradas em log. Para identificar a categoria de um evento, clique com o botão direito do mouse no evento e, em seguida, clique em Propriedades.

O Campo Identificação do evento especifica o número do evento de um evento específico. O número do evento ajuda a equipe de suporte técnico a rastrear os eventos no sistema. Para conhecer a Id. do evento, clique com o botão direito do mouse no evento e, em seguida, clique em Propriedades. Para uma descrição associada com o Id do evento, consulte os manuais do programa (ou do Hardware) ao qual o evento se refere. Para pesquisar pelo ID dos eventos gerados pelo Windows Server 2003 ou por um dos produtos da Microsoft (SQL Server, Exchange Server, etc.), consulte o site <http://support.microsoft.com>.

O campo Usuário fornece um espaço para você digitar um texto que corresponde exatamente ao texto no campo Nome de usuário, isto é, o nome de logon do usuário. Este campo não diferencia maiúsculas de minúsculas. Para identificar o usuário de um evento, clique com o botão direito do mouse no evento e, em seguida, clique em Propriedades. Por exemplo, você pode fazer com que sejam exibidos, apenas os eventos relacionados a um determinado usuário que está sob investigação, por sucessivas tentativas de acessar arquivos para os quais ele não tem autorização.

O campo Computador permite que você especifique o nome exato do computador em que ocorreu o evento registrado. Este campo não diferencia maiúsculas de minúsculas. Para identificar o computador em que ocorreu um evento, clique com o botão direito do mouse no evento e, em seguida, clique em Propriedades.

Nos campos De e Até, você pode limitar o período para o qual você quer que os logs sejam exibidos. O botão Restaurar Padrões é utilizado para restaurar as configurações originais de filtragem para o Windows Server 2003.

9. Clique no botão OK para aplicar o filtro.

Você terá voltado para o Visualizador de eventos. Observe que somente os eventos do tipo Erro são exibidos, conforme indicado pela Figura 10.17:

The screenshot shows the Windows Event Viewer window titled 'Visualizar eventos'. The left pane displays a tree view of event sources: 'Visualizar eventos (local)', 'Aplicativo', 'Segurança', 'Sistema', 'Serviço de diretório', 'Servidor DNS', and 'Serviço de duplicação de arquivos'. The right pane is a grid table titled 'Exibição filtrada mostrando 4.497 de 9.707 evento(s)'. The columns are 'Tipo', 'Data', 'Hora', 'Fonte', 'Categoria', and 'E'. All rows in the table show an 'Erro' type event from 'Netlogon' on '10/3/2004' at various times between 16:06:24 and 16:06:28, with 'Nenhuma' category. A vertical scroll bar is visible on the right side of the table.

Figura 10.17 Somente os eventos do tipo Erro sendo exibidos.

10. Repita as passos de 6 até 9, só que ao invés de deixar marcada a opção Erro, deixe marcada a opção Informações.
11. Ao dar um clique em no botão OK, será exibida uma listagem do log do sistema, apenas com os eventos do tipo Informação.
12. Para voltar a exibir todas os eventos, dê um clique com o botão direito do mouse na opção Sistema e, no menu que surge aponte para Exibir, e no menu Exibir dê um clique na opção Todos os Registros.
13. Feche o visualizador de eventos.

Outro critério importante que pode ser utilizada para a filtragem dos eventos é a Origem do evento (Event Source). Por exemplo, todos os eventos relacionados com impressoras tem como origem Print. Eventos relacionados com discos rígidos tem como origem disk e assim por diante. O fato de ser possível filtrar os eventos de acordo com a sua origem, facilita o trabalho de detecção de problemas, pois permite que sejam exibidos somente os eventos relacionados ao item que está apresentando problema.

Exemplo: Para filtrar os eventos do log do sistema pelo origem do evento, siga os passos indicados a seguir:

1. Faça o logon com uma conta com permissão de administrador.
2. Abra o console Visualizar eventos: Iniciar -> Ferramentas Administrativas -> Visualizar eventos.
3. Farei com que sejam exibidos somente os eventos cuja origem é ntfs, isto é, eventos ligados com o sistema de arquivos NTFS.
4. Selecione o comando Exibir -> Filtro...
5. Será exibida a janela Propriedades do Sistema, com a guia Filtro selecionada
7. Na lista Fonte do evento, selecione ntfs, conforme indicado na Figura 10.18:

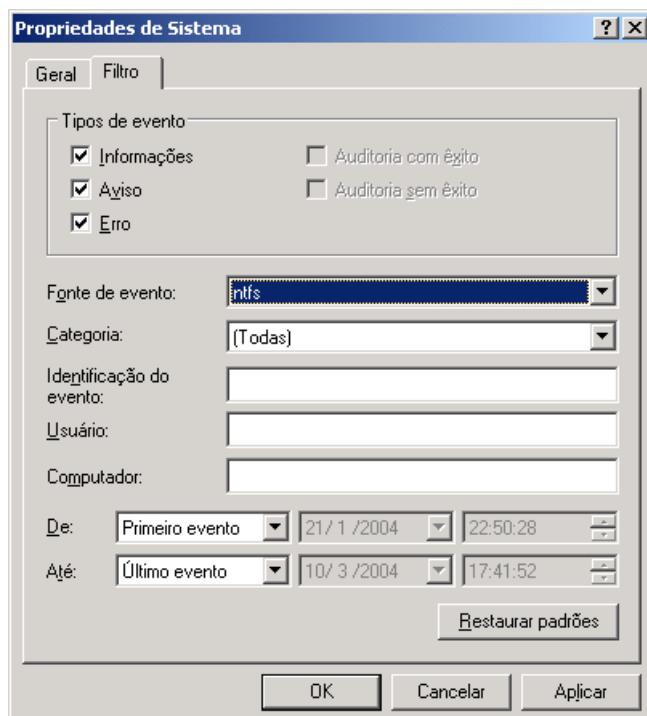


Figura 10.18 Selecionando eventos cuja origem é ntfs.

---

**NOTA: Se você fechar o Visualizador de eventos, todos os filtros serão eliminados. Com isso, na próxima vez que o Visualizador de eventos for aberto, todos os eventos estarão sendo exibidos, sem a aplicação de filtros.**

---

8. Dê um clique no botão OK para aplicar o filtro.
9. Na listagem que surge, observe que somente são exibidos eventos cuja origem é ntfs. isso pode ser confirmado observando-se a coluna Origem.
10. Dê um clique duplo sobre qualquer um dos eventos, para abrir a janela com detalhes sobre o evento.
11. Observe na mensagem para ver se o evento realmente tem a ver com o sistema de arquivos ntfs.
12. Na janela da Figura 10.19, coloquei um exemplo de um evento que foi gerado, onde a origem é o sistema de arquivos NTFS (observe o campo Fonte, onde o valor é ntfs).

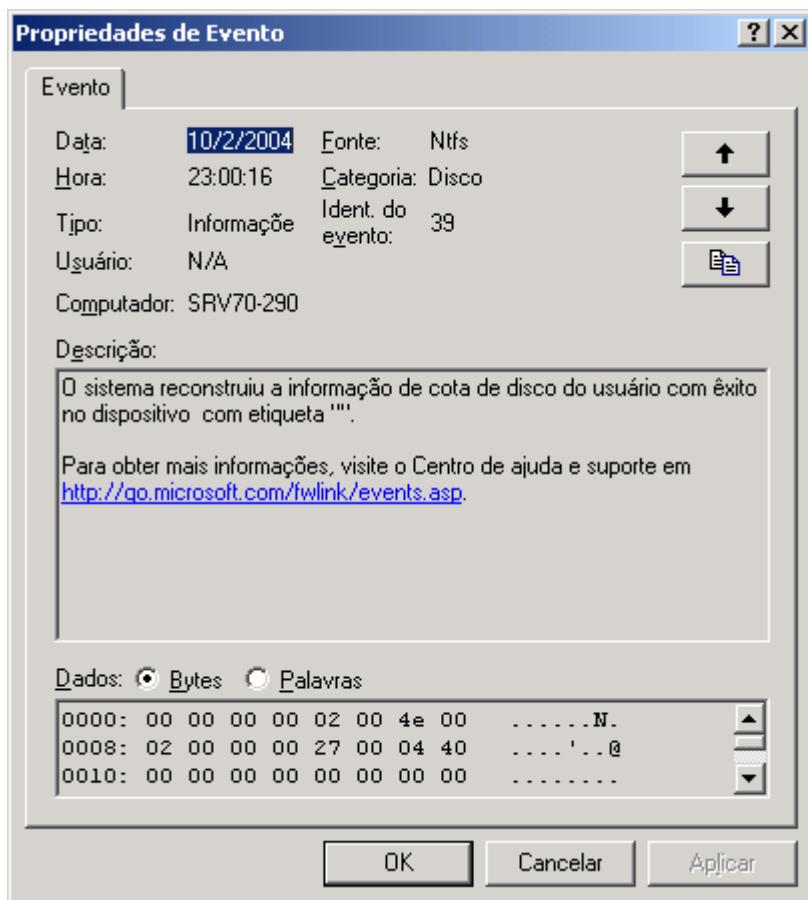


Figura 10.19 Evento em que a origem é o sistema de arquivos NTFS.

13. Feche o visualizador de eventos.

## Configurando as propriedades do log.

Existem algumas propriedades importantes dos logs que podem ser configuradas. A medida que novos eventos vão sendo gravados no log, o tamanho do log vai aumentando. O log consome espaço no disco rígido. Se nos permitíssemos que o log crescesse indefinidamente, poderíamos chegar a uma situação em que o espaço em disco iria se esgotar.

Para evitar que isso aconteça o administrador pode definir um tamanho máximo para cada log e definir qual o comportamento do log, quando este tamanho máximo for atingido. Por exemplo, o administrador define o tamanho máximo que cada

**IMPORTANTES:** A aplicação de filtros funciona de maneira independente entre os diferentes logs. Por exemplo, se você aplicar um filtro para o log Sistema, o filtro não tem efeito sobre o log Aplicativo ou sobre o log Segurança.

log pode ocupar, uma vez atingido o tamanho máximo o que fazer – continuar gravando e sobrescrever os eventos mais antigos ou parar de gravar e descartar novos eventos ou até mesmo fazer com que o Windows Server 2003 “pare”, até que seja liberado espaço no log.

Essas configurações também são independentes para cada tipo de log. Por exemplo o Log de sistema pode ter um tamanho máximo diferente dos demais logs.

Agora é hora de praticar um pouco para aprender a configurar essas propriedades dos logs.

## Exemplo - Para definir o tamanho máximo e o local onde o Log é gravado, siga os passos indicados a seguir:

1. Faça o logon com uma conta com permissão de administrador.
2. Abra o console Visualizar eventos: Iniciar -> Ferramentas Administrativas -> Visualizar eventos.
3. Agora vou definir um tamanho máximo para o log Sistema.
4. Dê um clique com o botão direito do mouse no log Sistema. No menu que surge dê um clique em Propriedades. Ira surgir a janela de propriedades do log Sistema, indicada na Figura 10.20:

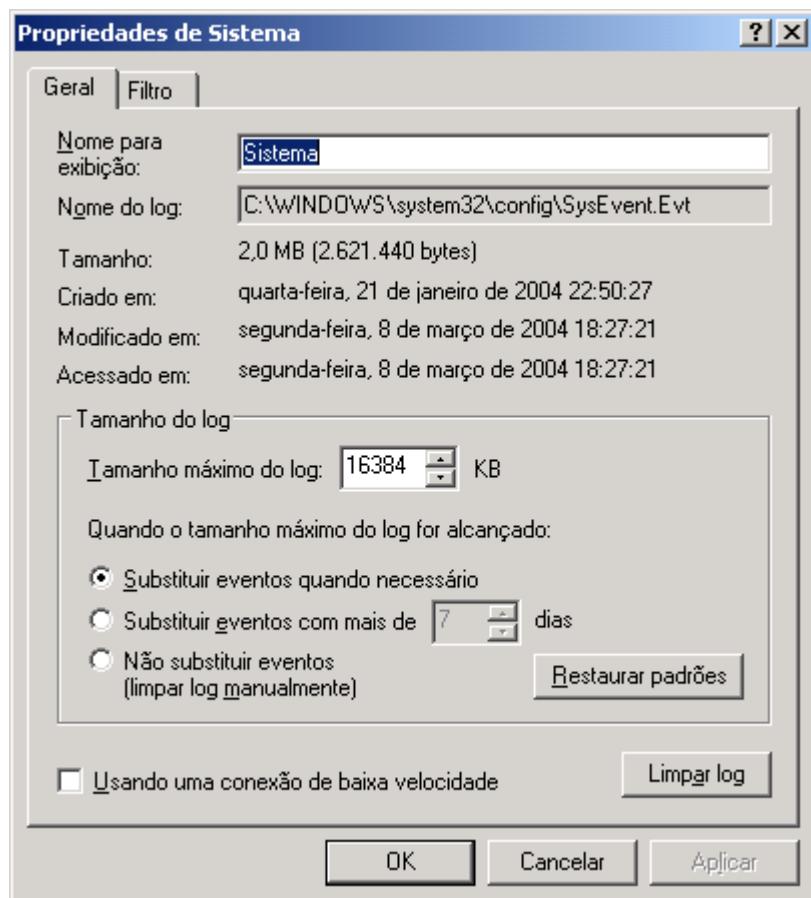


Figura 10.20 Propriedades para o log Sistema.

No campo Nome do log, está a indicação de onde o Windows Server 2003 grava o arquivo com os eventos do respectivo log. Cada opção de Log é gravada em seu próprio arquivo, isto é o log Aplicativo, por padrão, é gravado em C:\WINDOWS\system32\config\AppEvent.Evt, o log Segurança, por padrão, é gravado em C:\WINDOWS\System32\config\

SecEvent.Evt e o log Sistema, por padrão, é gravado em C:\WINDOWS\system32\config\SysEvent.Evt. Onde estou considerando WINDOWS a pasta onde está instalado o Windows Server 2003. Se o servidor foi migrado do NT Server 4.0 ou do Windows 2000 Server, para o Windows Server 2003, é provável que ao invés da pasta WINDOWS, esteja sendo utilizada a pasta WINNT.

Observe que o tamanho máximo para o Log de sistema esta definido em 16384 KB (16 MB). Este é o valor padrão, o qual pode ser alterado através das diretivas de segurança do domínio, que descreverei logo a seguir.

5. Aumente o tamanho do log para 32768 KB (32 MB).
6. Logo abaixo, estão disponíveis três opções a serem utilizadas quando log atingir o tamanho máximos, conforme descrito a seguir:
  - ◆ **Substituir eventos quando necessário:** A medida que o log alcança o tamanho máximo, os eventos mais antigos vão sendo excluídos para que novos eventos possam ser gravados. Não exige manutenção, porém você perde eventos mais antigos, os quais serão sobre-escritos pelos eventos mais novos. Esta é a opção selecionada por padrão.
  - ◆ **Substituir eventos com mais de X dias:** A medida que o log alcança o tamanho máximo, somente serão eliminados eventos gravados a X dias, conforme configurado nesta opção. Pode haver perda de eventos, dependendo do número e freqüência na geração dos eventos.
  - ◆ **Não substituir eventos (limpar log manualmente):** Requer que os eventos sejam manualmente eliminados pelo administrador. Especifica se eventos existentes serão retidos quando o log estiver cheio. Se o tamanho máximo do log for atingido, os eventos novos serão descartados. Esta opção requer que você esvazie o log manualmente. Selecione esta opção somente se você precisar reter todos os eventos.
7. Certifique-se de que a opção Substituir eventos conforme necessário esteja marcada.
8. Dê um clique em OK para aplicar estas configurações para o log do Sistema.
9. Feche o visualizador de eventos.

## Definindo as propriedades dos logs de auditoria, usando as diretivas de segurança do domínio:

Você pode definir uma série de propriedades e características dos logs do Windows Server 2003, usando as diretivas de segurança do domínio. Por exemplo, você pode definir um tamanho máximo para o log de segurança e um tamanho máximo para o log do sistema, para todos os servidores do domínio, usando para isso as diretivas de segurança do domínio, conforme descreverei no exemplo a seguir.

Exemplo: Para definir as diretivas de segurança relacionadas com as propriedades do log do Windows Server 2003, siga os passos indicados a seguir:

1. Faça o logon com uma conta com permissão de administrador.
2. Abra o console Diretiva de Segurança de Domínio: Iniciar -> Ferramentas administrativas -> Diretiva de segurança de domínio.
3. Será aberta a janela Configurações padrão de segurança de Domínio. Clique no sinal de +, ao lado de Configurações de segurança, para exibir as opções disponíveis.

---

**NOTA:** Você também pode utilizar o visualizador de eventos para acessar o log de outros servidores, remotamente através da rede. Para isso, clique com o botão direito do mouse na opção Visualizar eventos (local). No menu que é exibido clique na opção Conectar-se a outro computador... Na janela que surge basta digitar o nome ou o número IP do computador com o qual você deseja se conectar e clicar em OK. Feito isso o Windows Server 2003 conecta com o computador e exibe os logs de auditoria deste computador, desde que você tenha as devidas permissões para acessar os logs de auditoria do computador especificado.

---

4. Nas opções que surgem, dê um clique na opção Log de eventos . No painel da direita são exibidas as várias diretivas de auditoria disponíveis, as quais são indicadas na Figura 10.21 e explicadas logo a seguir. Observe ao lado do nome de cada diretiva, o status Não-definido, indicando que não existe definição para esta diretiva, isto é, é como se esta diretiva estivesse desabilitada, situação na qual estão valendo as diretivas do controlador de domínio ou, se estas também estiverem desabilitadas, os valores padrão do Windows Server 2003.

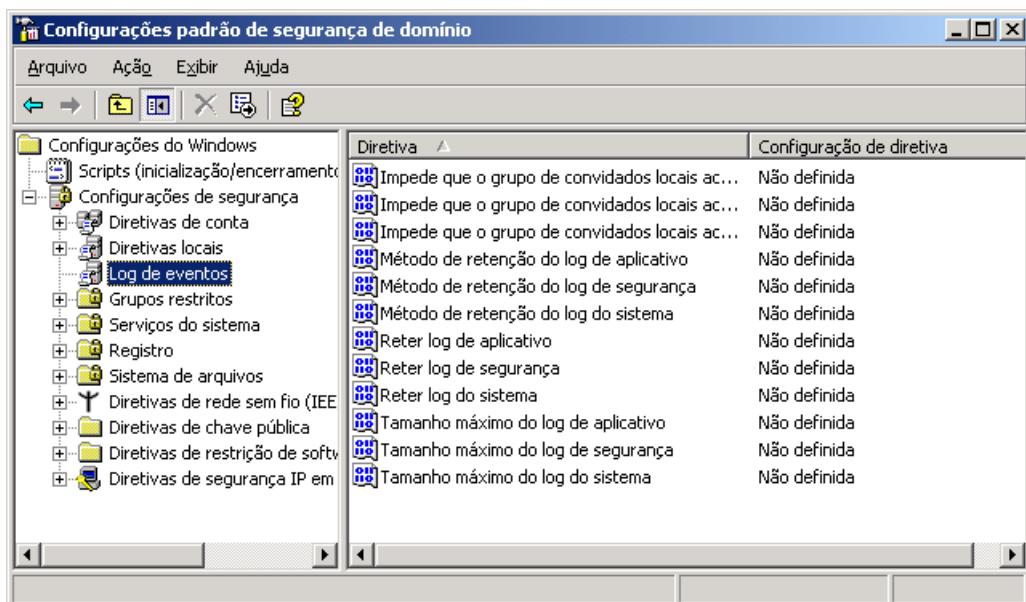


Figura 10.21 Opções para configuração das Diretivas de auditoria.

Descrição das diretivas de auditoria disponíveis:

- ◆ **Tamanho máximo do log de aplicativo:** É utilizada para definir o tamanho máximo do log Application (Aplicativo). O maior valor desta diretiva é 4GB e o valor definido nesta diretiva deve ser um múltiplo de 64 KB. Para configurar esta diretiva basta dar um clique duplo nela. Na janela que é exibida, informe o tamanho máximo do log de aplicativo, conforme exemplo da Figura 10.22 e clique em OK.

**NOTA:** Estas opções de auditoria também poderiam ser configuradas através da GPO (Group Policy Object) padrão do domínio.

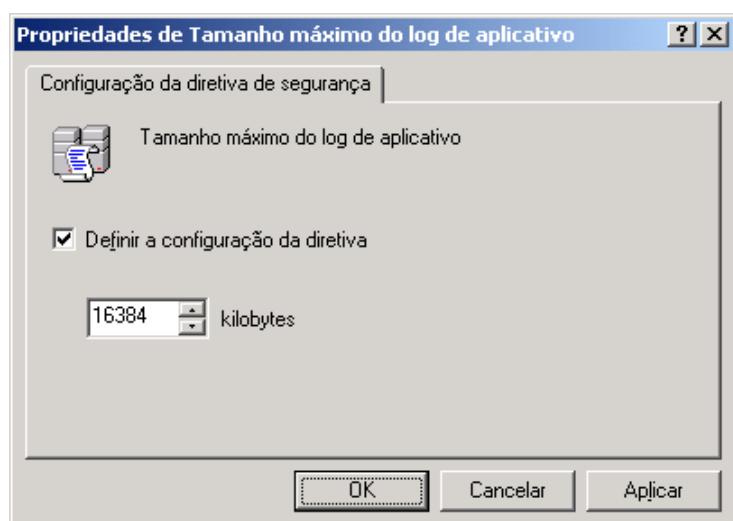


Figura 10.22 Definindo o tamanho máximo do log de aplicativos.

- ◆ **Tamanho máximo do log de segurança:** É utilizada para definir o tamanho máximo do log Security (Segurança). O maior valor que esta diretiva aceita é 4GB e o valor definido nesta diretiva deve ser um múltiplo de 64 KB. Para configurar esta diretiva basta dar um clique duplo nela. Na janela que é exibida, informe o tamanho máximo do log de segurança e clique em OK.
- ◆ **Tamanho máximo do log de sistema:** É utilizada para definir o tamanho máximo do log System (Sistema). O maior valor que esta diretiva aceita é 4GB e o valor definido nesta diretiva deve ser um múltiplo de 64 KB. Para configurar esta diretiva basta dar um clique duplo nela. Na janela que é exibida, informe o tamanho máximo do log de segurança e clique em OK.
- ◆ **Impede que o grupo de convidados locais acesse o log de aplicativo:** Esta diretiva é utilizada para definir se os membros do grupo Guests (Convidados) podem ou não acessar o log de aplicativo. Para configurar esta diretiva basta dar um clique duplo nela. Na janela que é exibida, marque a opção Definir a configuração da diretiva. Nas opções que são habilitadas, marque Habilitado, para permitir o acesso do grupo Guests ao log de aplicativo ou a opção Desabilitar, para impedir o acesso do grupo Guests ao log do aplicativo, conforme exemplo da Figura 10.23. Depois clique em OK. Esta diretiva somente tem efeito para computadores com versões do Windows anteriores ao Windows Server 2003, tais como o Windows 2000 Server e o Windows XP.



Figura 10.23 Definindo o acesso do grupo Guests (Convidados).

- ◆ **Impede que o grupo de convidados locais acesse o log de segurança:** Esta diretiva é utilizada para definir se os membros do grupo Guests (Convidados) podem ou não acessar o log de segurança. Para configurar esta diretiva basta dar um clique duplo nela. Na janela que é exibida, marque a opção Definir a configuração da diretiva. Nas opções que são habilitadas, marque Habilitado, para permitir o acesso do grupo Guests ao log de segurança ou a opção Desabilitar, para impedir o acesso do grupo Guests ao log de segurança. Depois clique em OK. Esta diretiva somente tem efeito para computadores com versões do Windows anteriores ao Windows Server 2003, tais como o Windows 2000 Server e o Windows XP.
- ◆ **Impede que o grupo de convidados locais acesse o log de sistema:** Esta diretiva é utilizada para definir se os membros do grupo Guests (Convidados) podem ou não acessar o log do sistema. Para configurar esta diretiva basta dar um clique duplo nela. Na janela que é exibida, marque a opção Definir a configuração da diretiva. Nas opções que são habilitadas, marque Habilitado, para permitir o acesso do grupo Guests ao log do sistema

ou a opção Desabilitar, para impedir o acesso do grupo Guests ao log do sistema. Depois clique em OK. Esta diretiva somente tem efeito para computadores com versões do Windows anteriores ao Windows Server 2003, tais como o Windows 2000 Server e o Windows XP.

- ◆ **Reter log de aplicativo:** Esta diretiva determina o número de dias (período em dias), para os quais deve ser mantido os eventos no log de aplicativo. Esta diretiva somente é utilizada se você tem uma política de armazenamento do log em períodos definidos. Você deve verificar que o tamanho máximo do log acomoda a quantidade de eventos gerados durante o período entre um e outro arquivamento.
- ◆ **Reter log de segurança:** Esta diretiva determina o número de dias (período em dias), para os quais deve ser mantido os eventos no log de segurança. Esta diretiva somente é utilizada se você tem uma política de armazenamento do log em períodos definidos. Você deve verificar que o tamanho máximo do log acomoda a quantidade de eventos gerados durante o período entre um e outro arquivamento.
- ◆ **Reter log de sistema:** Esta diretiva determina o número de dias (período em dias), para os quais deve ser mantido os eventos no log do sistema. Esta diretiva somente é utilizada se você tem uma política de armazenamento do log em períodos definidos. Você deve verificar que o tamanho máximo do log acomoda a quantidade de eventos gerados durante o período entre um e outro arquivamento.
- ◆ **Método de retenção do log de aplicativo:** Com esta diretiva você pode determinar um método de retenção para o log de aplicativo. O administrador pode definir um dos métodos descritos anteriormente: Substituir eventos periodicamente, Substituir eventos quando necessário ou Não substituir eventos (limpar log manualmente). Se não existir uma política de arquivamento de log, você deve definir esta diretiva com a opção Substituir eventos quando necessário, caso você tenha uma política de arquivamento deste log, em um período definido, configure esta diretiva com a opção Substituir eventos com mais de X dias, onde X representa o período de arquivamento.
- ◆ **Método de retenção do log de segurança:** Com esta diretiva você pode determinar um método de retenção para o log de segurança. O administrador pode definir um dos métodos descritos anteriormente: Substituir eventos periodicamente, Substituir eventos quando necessário ou Não substituir eventos (limpar log manualmente). Se não existir uma política de arquivamento de log, você deve definir esta diretiva com a opção Substituir eventos quando necessário, caso você tenha uma política de arquivamento deste log, em um período definido, configure esta diretiva com a opção Substituir eventos com mais de X dias, onde X representa o período de arquivamento.
- ◆ **Método de retenção do log do sistema:** Com esta diretiva você pode determinar um método de retenção para o log do sistema. O administrador pode definir um dos métodos descritos anteriormente: Substituir eventos periodicamente, Substituir eventos quando necessário ou Não substituir eventos (limpar log manualmente). Se não existir uma política de arquivamento de log, você deve definir esta diretiva com a opção Substituir eventos quando necessário, caso você tenha uma política de arquivamento deste log, em um período definido, configure esta diretiva com a opção Substituir eventos com mais de X dias, onde X representa o período de arquivamento.

5. Defina as diretivas de acordo com as necessidades do seu domínio.
6. Feche o console para configuração das diretivas de segurança do domínio.

## Mais configurações do log e exportação dos eventos do log de auditoria.

Utilizando o menu Ação, do console visualizador de eventos, o administrador pode definir mais algumas configurações e executar algumas ações relacionadas com os logs do Windows Server 2003.

Você pode utilizar o comando Ação -> Abrir arquivo de log..., para abrir um arquivo onde foram salvos eventos de auditoria. É comum, em redes maiores, que os eventos de vários servidores e até mesmo de computadores da rede,

sejam salvas em arquivos (conforme você aprenderá a fazer logo em seguida). Um administrador pode utilizar esta opção, para abrir e analisar os diversos arquivos contendo os eventos a serem analisados.

*Caso você precise de um banco centralizado de dados, com o arquivamento dos logs de auditoria de todos ou de um grande número de servidores de um domínio, o mais indicado é montar um esquema de arquivamento, onde os logs são periodicamente exportados, em cada servidor e depois importados em um banco de dados relacional, como o SQL Server 2000, ORACLE, DB2, etc. A importação pode ser automatizada mediante o uso de scripts.*

Você pode utilizar o comando Ação -> Salvar arquivo de log como..., para salvar os eventos em um arquivo, em diferentes formatos. Por exemplo, abra o console Visualizar eventos, clique na opção Sistema e selecione o comando Ação -> Salvar arquivo de log como.... Será aberta a janela Salvar "Sistema" como. Nesta janela você seleciona a pasta, o nome do arquivo onde serão salvos os eventos e o formato do arquivo. Estão disponíveis o formato Log de eventos (\*.evt) que é um formato que pode ser aberto somente no Visualizador de eventos; o formato Texto (delimit. por tab.) (\*.txt), que gera um arquivo do tipo texto, onde cada linha corresponde a um evento e os campos são separados por tabulação e o formato CSV (delimit. por vírg.) (\*.csv) que gera um arquivo do tipo texto, onde cada linha corresponde a um evento e os campos são separados por vírgula. O formato .csv é o mais indicado para importação em programas como o Excel e bancos de dados como o Access ou SQL Server 2000, ou seja, você exporta os logs para arquivos .csv e depois importa estes arquivos no Excel ou no Access, para análise, classificação e filtragem.

Na janela da Figura 10.24, os eventos do log Sistema estão sendo salvos, para um arquivo chamado log-sistema-Março-2004.csv, na pasta Meus documentos.

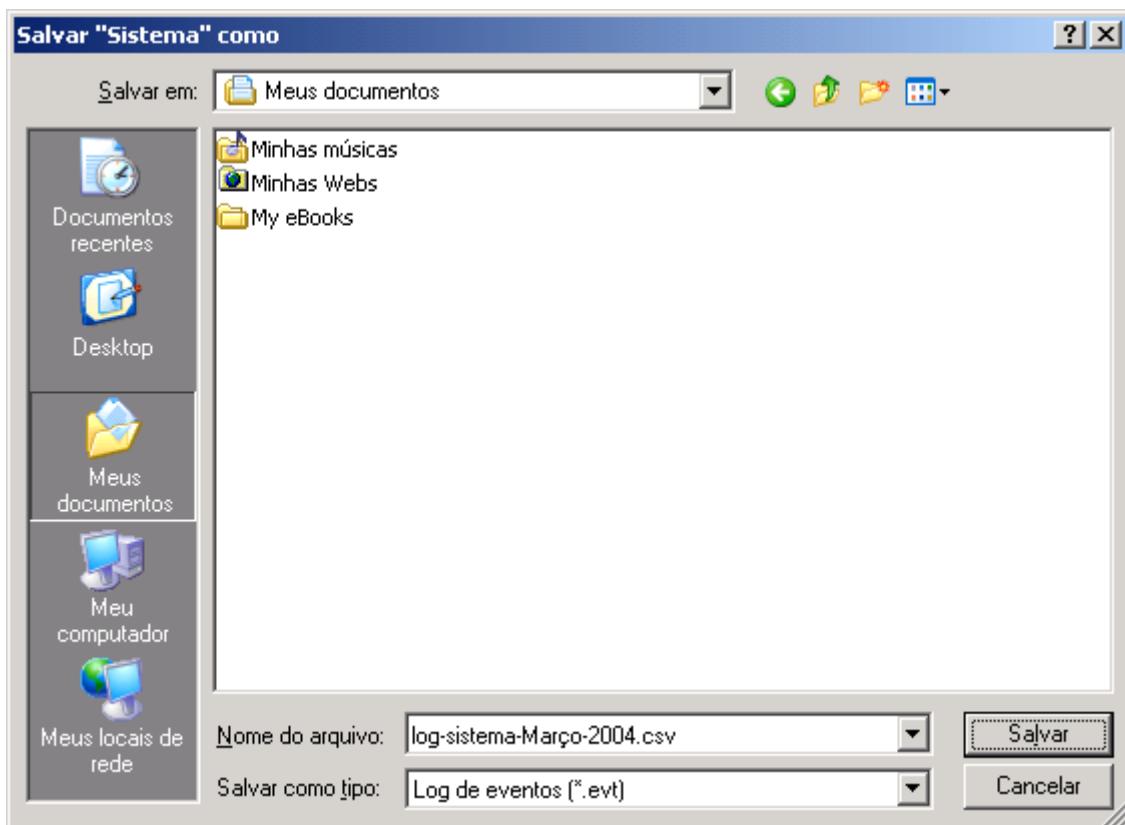


Figura 10.24 Salvando o log Sistema para um arquivo no formato .csv.

Ao clicar em Salvar o Windows Server 2003 salva uma cópia dos eventos, no arquivo especificado. Você pode abrir um arquivo .csv (que é um arquivo no formato texto), usando o bloco de Notas. Na Figura 10.25 mostro uma visão das primeiras linhas do arquivo log-sistema-Março-2004.csv, gerado anteriormente.

```
L/6/2003,22:30:44,LSASRV,warning,SPNEGO (Negotiator) ,40961,N/A,SRV-WIN2003,The Security System  
1/6/2003,22:30:43,LSASRV,warning,SPNEGO (Negotiator) ,40961,N/A,SRV-WIN2003,The security System  
1/6/2003,22:16:47,W32Time,Warning,None,12,N/A,SRV-WIN2003,"Time Provider NtpClient: This machine  
1/6/2003,21:30:41,LSASRV,warning,SPNEGO (Negotiator) ,40961,N/A,SRV-WIN2003,The security System  
1/6/2003,21:05:50,LSASRV,warning,SPNEGO (Negotiator) ,40961,N/A,SRV-WIN2003,The security System  
1/6/2003,20:30:39,LSASRV,warning,SPNEGO (Negotiator) ,40961,N/A,SRV-WIN2003,The security System  
1/6/2003,19:45:46,LSASRV,warning,SPNEGO (Negotiator) ,40961,N/A,SRV-WIN2003,The security System  
1/6/2003,19:30:36,LSASRV,warning,SPNEGO (Negotiator) ,40961,N/A,SRV-WIN2003,The security System  
1/6/2003,18:46:00,W32Time,Warning,None,12,N/A,SRV-WIN2003,"Time Provider NtpClient: This machine  
1/6/2003,18:35:34,LSASRV,warning,SPNEGO (Negotiator) ,40961,N/A,SRV-WIN2003,The security System  
1/6/2003,18:30:44,W32Time,Warning,None,12,N/A,SRV-WIN2003,"Time Provider NtpClient: This machine  
1/6/2003,18:30:30,LSASRV,warning,SPNEGO (Negotiator) ,40961,N/A,SRV-WIN2003,The security System  
1/6/2003,18:30:30,RemoteAccess,Information,None,20158,N/A,SRV-WIN2003,The user juliobattisti suc  
1/6/2003,18:24:04,W32Time,Warning,None,12,N/A,SRV-WIN2003,"Time Provider NtpClient: This machine  
1/6/2003,18:08:13,RemoteAccess,Information,None,20159,N/A,SRV-WIN2003,The connection to PopDisca  
1/6/2003,17:32:15,LSASRV,warning,SPNEGO (Negotiator) ,40961,N/A,SRV-WIN2003,The security System  
1/6/2003,17:32:14,LSASRV,warning,SPNEGO (Negotiator) ,40961,N/A,SRV-WIN2003,The security System  
1/6/2003,16:32:12,LSASRV,warning,SPNEGO (Negotiator) ,40961,N/A,SRV-WIN2003,The security System
```

Figura 10.25 O arquivo log-sistema-maio-2003.csv, aberto no Bloco de notas.

Você também pode limpar todos os eventos de um dos logs de auditoria. Para isso basta clicar com o botão direito do mouse no log desejado e, no meu de opções que é exibido, selecionar o comando Limpar todos os eventos. Surge uma janela pedindo se você deseja salvar os eventos atuais. Se você responder sim, será aberta a janela da Figura 10.24, para você definir o nome do arquivo, o formato e a pasta de destino; se você responder não os eventos serão excluídos e não poderão ser recuperados.

## Configurando a auditoria de acesso a arquivos, pastas e impressoras.

Conforme já descrevi brevemente, no início do Capítulo, a auditoria de acesso a objetos (pastas e impressoras compartilhadas), é um processo em duas etapas, conforme descrito a seguir:

1. Habilitar a Diretiva de auditoria: Auditoria de Acesso a objetos. Esta diretiva é habilitada, para sucesso, falha ou ambas as situações, utilizando o console Configurações locais de segurança, já descrito anteriormente. Em um dos exemplos anteriores você aprendeu a habilitar esta e outras diretivas de segurança. É também importante salientar que, para o Windows Server 2003, é considerado objeto, todo elemento que tiver uma Lista de Controle de Acesso – ACL (Access Control List). Com isso, entradas da Registry, todo e qualquer elemento do Active Directory, são considerados objetos.
2. Após ter habilitada a Diretiva de auditoria descrita no item 1, o administrador tem que configurar a auditoria em cada um dos objetos a serem auditados. Por exemplo, para monitorar o acesso a uma pasta e ao conteúdo desta pasta (subpastas e arquivos), o administrador deve acessar as propriedades desta pasta e configurar quais usuários/grupos terão o acesso monitorado. Por exemplo, o administrador pode definir que o grupo Gerentes terá o acesso a uma determinada pasta monitorada, tanto para evento de sucesso quanto de falha. Com isso, toda vez que um membro deste grupo acessar o conteúdo da pasta que está sendo monitorada, será gravado um evento no log de eventos.

A habilitação da Diretiva de auditoria já foi feita no item Habilitando/configurando os eventos do log de segurança. Utilizando os conhecimentos apresentados no referido item, certifique-se de que a diretiva Auditoria de acesso a objetos, esteja configurada para monitorar eventos de Sucesso e de Falha, conforme indicado ilustrado na Figura 10.26.

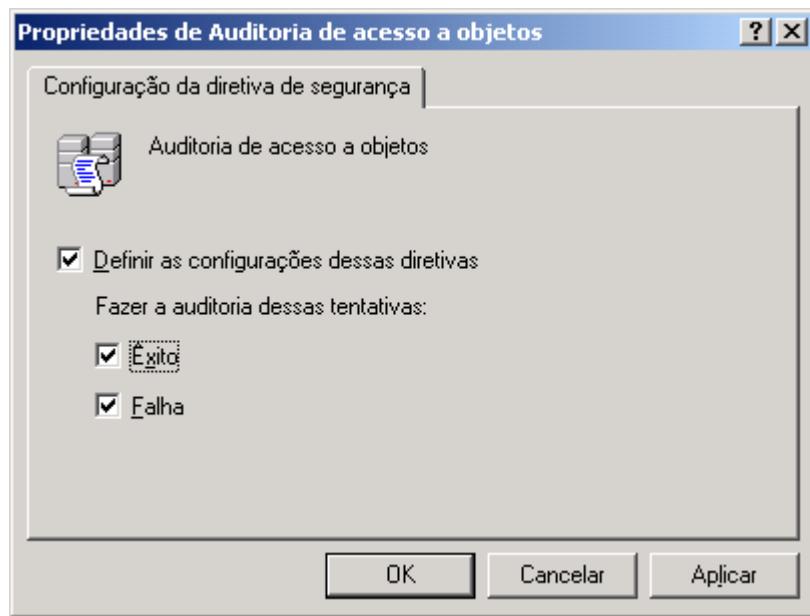


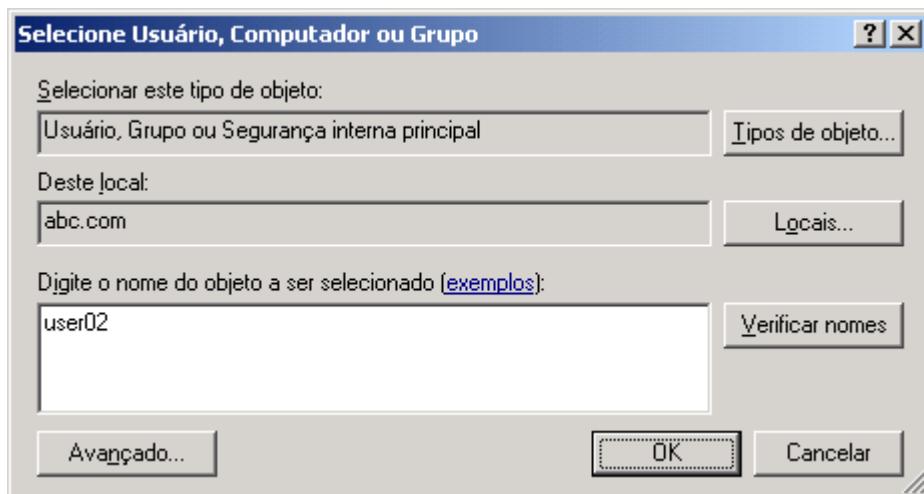
Figura 10.26 A diretiva Auditoria de acesso a objetos.

Neste item aprenderá, a título de exemplo, a configurar a pasta C:\Documentos, para que sejam monitorados os acessos a esta pasta e a seus arquivos. Ao fazer esta configuração, o administrador pode definir para quais usuários o acesso será monitorado. Para monitorar o acesso de todo e qualquer usuário, você deve utilizar o grupo Everyone (Todos). No exemplo proposto, você irá configurar o Windows Server 2003, para monitorar o acesso dos usuários user02 e user03 (utilize usuários do domínio da sua rede). Observe que você pode fazer com que seja monitorado o acesso de todo e qualquer usuário, ou apenas de determinados usuários. No exemplo que apresentarei, estou monitorando apenas o acesso de dois usuários. Esta situação pode ser utilizada, por exemplo, para monitorar tentativas de acesso sem permissão, para usuários que estão sob investigação ou sob suspeita na empresa.

Exemplo: Configurando a monitoração dos acessos na pasta C:\Documentos, para os usuários user02 e user03.

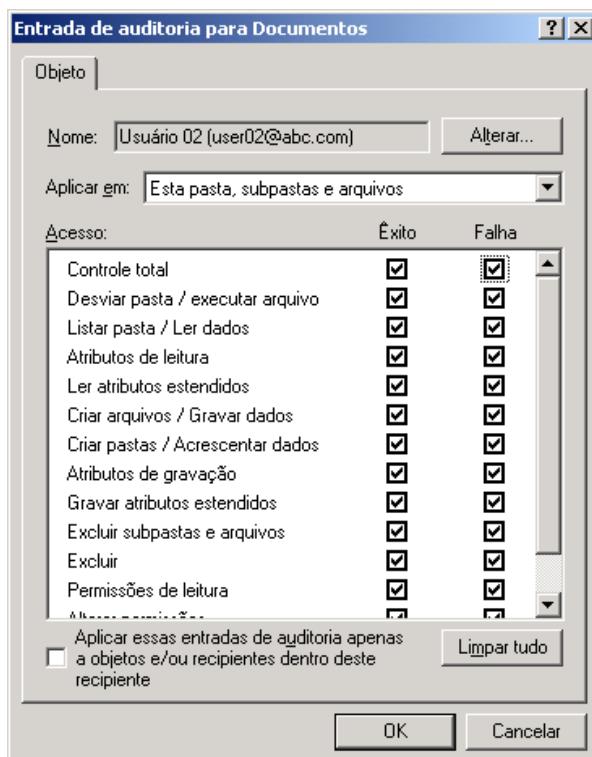
1. Faça o logon como Administrador ou com uma conta com permissões de administrador.
2. Usando o Meu computador ou o Windows Explorer, acessa a pasta C:\Documentos ou outra pasta qualquer, para a qual você deseja configurar o controle de acesso.
3. Clique com o botão direito do mouse na pasta e no menu que surge clique na opção Propriedades. Será exibida a janela de Propriedades da pasta.
4. Dê um clique na guia Segurança.
5. Clique no botão Avançado. Será exibida a janela Configurações de segurança avançadas para Documentos, onde Documentos é o nome da pasta que está sendo configurada.
6. Clique na guia Auditoria. Observe que por padrão não existe nenhum usuário na lista, ou seja, não estão sendo monitorados os acessos a pasta Documentos.
7. Dê um clique no botão Adicionar... Será aberta a janela Selecione Usuário, computador ou Grupo, que já foi utilizada em outros capítulos. Digite user02, conforme indicado na Figura 10.27 e clique em OK.

**IMPORTANTE:** Nunca é demais lembrar: as configurações de Auditoria somente estão disponíveis em volumes formatados com NTFS.



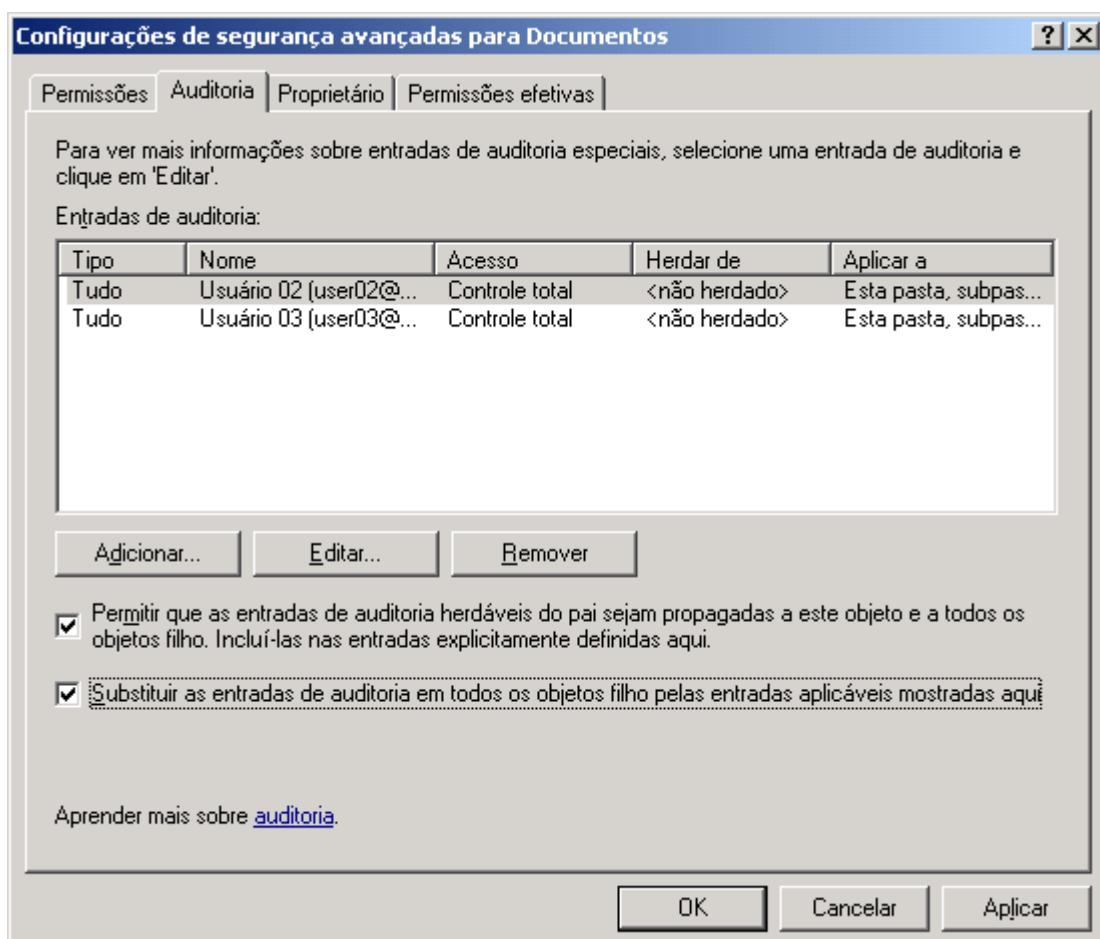
**Figura 10.27 Adicionando user02 à lista de usuários auditados na pasta Documentos.**

8. Será aberta a janela Entradas de auditoria para Documentos. Nesta janela você define o tipo de acesso que será monitorado para o usuário user2, na pasta Documentos. Por exemplo, pode ser que você queira monitorar apenas tentativas de alterações ou exclusões no conteúdo da pastas Documentos e das suas subpastas. No nosso exemplo vamos monitorar todos os tipos de acesso. Marque a opção Controle total, na coluna Êxito. Observe que todas as demais opções da coluna Êxito serão marcadas. Agora marque a opção Controle total, na coluna Falha. Observe que todas as demais opções da coluna Falha serão marcadas, conforme indicado na Figura 10.28. Com isso estamos pedindo que o Windows Server 2003 monitore todo e qualquer tipo de acesso do usuário user02, com sucesso ou com falha, à pasta Documentos e a todas as suas subpastas e arquivos. Marque a opção Aplicar essas entradas de auditoria apenas a objetos e/ou recipientes dentro deste recipiente, para fazer com que o Windows Server 2003 aplique estas configurações de auditoria à pasta Documentos e a todas as suas subpastas e arquivos. Clique em OK.



**Figura 10.28 Configurações de auditoria para o usuário user02.**

9. Repita os passos 7 e 8 para o usuário user03.
10. Você estará de volta à guia Auditoria, agora com os usuários user02 e user03 já adicionados à lista de usuários que serão auditados quando acessarem a pasta Documentos e o seu conteúdo, conforme indicado na Figura 10.29:



**Figura 10.29 Usuários user02 e user03 já adicionados à lista.**

11. Marque a opção Substituir as entradas de auditoria em todos os objetos filho pelas entradas aplicáveis mostradas aqui, para substituir outras configurações de auditoria, que por ventura estejam definidas para as subpastas e arquivos da pasta Documentos. Clique em OK. Você estará de volta à guia Segurança.
12. Clique em OK para fechar a janela de propriedades da pasta documentos. A partir de agora todos os acesso, com sucesso ou com falha, dos usuários user02 e user03 serão monitorados.

Para configurar a auditoria de acesso para uma impressora faça o seguinte:

1. Faça o logon como Administrador ou com uma conta com permissão de gerenciar a impressora a ser configurada.
2. Acesse as propriedades da impressora a ser configurada.
3. Clique com o botão direito do mouse na impressora a ser configurada e, no menu de opções que é exibido, clique em Propriedades.
4. Clique na guia Segurança e dentro da guia Segurança, clique no botão Avançado. Depois é só seguir os passos indicados no exemplo anterior, que são os mesmos, quer você esteja configurando a auditoria para pastas e arquivos ou para impressoras.

Com isso encerro o estudo sobre auditoria e logs de auditoria no Windows Server 2003. Para aqueles usuários que já trabalharam com auditoria de eventos no Windows 2000, verão que as configurações são muito semelhantes. No Windows 95/98 ou Me não estão disponíveis as funções de auditoria e log de eventos.

Na parte final do capítulo vou tratar sobre o conceito de serviços e vou mostrar como utilizar o console para administração de serviços.

## Gerenciando Serviços no Windows Server 2003.

Um Serviço é um componente de software que é inicializado automaticamente quando o Windows Server 2003 é inicializado, ou pode ser iniciado a qualquer momento, manualmente, pelo administrador. Um Serviço continua carregado e funcionando, mesmo quando não existe nenhum usuário logado no servidor. Por exemplo o serviço Spooler, responsável pela impressão continua trabalhando, mesmo quando não existe nenhum usuário logado. O mesmo é válido para qualquer serviço que rode no Windows Server 2003.

A maioria das funcionalidades de rede do Windows Server 2003 é fornecida por serviços. Por exemplo, para que um computador com o Windows Server 2003 possa atuar como servidor Web, é preciso instalar o serviço IIS – Internet Information Services (o qual será detalhado a partir no Capítulo 13). O Serviço Server permite que os usuários acessem o servidor através da rede. Existem uma infinidade de serviços disponíveis no Windows Server 2003 e outros podem ser acrescentados por programas que são instalados. Por exemplo, quando o Microsoft SQL Server 2000 é instalado (Servidor de Banco de dados da Microsoft), 4 novos serviços são adicionados.

### Acessando informações sobre serviços e administrando os serviços instalados.

Não seria exagero dizer que o Windows Server 2003 é um conjunto de Serviços que funcionam de maneira integrada. Temos os serviços principais, aqueles que forma o núcleo do Sistema Operacional, também conhecido como “Kernel” do sistema. Estes serviços são responsáveis por funções fundamentais tais como o gerenciamento de memória, gerenciamento do sistema de I/O (entrada e saída), detecção e configuração do Hardware, gerenciamento da interface gráfica e assim por diante.

Existem outros serviços que realizam funções específicas, como por exemplo serviços para envio e recebimento de mensagens de alerta e mensagens administrativas, serviços para o gerenciamento de impressão, serviço para compartilhamento de pastas e arquivos, serviços relacionados a segurança, serviços responsáveis pela disponibilização de recursos compartilhados e assim por diante.

O conceito de Serviços surgiu com as versões iniciais do Windows NT, também está presente no Windows 2000 e agora no Windows Server 2003. O conceito de serviço também existe no Windows NT Workstation 4.0, Windows 2000 Professional e Windows XP. No Windows 9x e Me não existe o conceito de serviços como o aqui apresentado.

Existem aplicativos que, ao serem instalados, adicionam serviços que são inicializados automaticamente para que o aplicativo possa funcionar corretamente. Por exemplo, ao instalar o IIS, automaticamente são instalados e inicializados serviços necessários para que o IIS possa atuar como um servidor de páginas e também um servidor de arquivos. Ao instalar o SQL Server 2000, por exemplo, novos serviços serão adicionados para que o SQL Server possa operar corretamente e assim por diante.

---

**NOTA:** Para maiores detalhes sobre o SQL Server 2000 consulte o livro de minha autoria: “SQL Server 2000 Administração & Desenvolvimento – Curso Completo”, publicado pela Editora Axcel Books ([www.axcel.com.br](http://www.axcel.com.br))

---

Neste tópico mostrarei como acessar informações sobre os diversos serviços instalados no Windows Server 2003, como verificar o status destes serviços, como configurar um serviço para iniciar automaticamente quando o Windows Server 2003 é inicializado e como iniciar um serviço manualmente quando necessário. Também mostrarei comandos que podem ser utilizados para parar e iniciar serviços através do Prompt de comando.

Exemplo 1: Acessando e configurando informações sobre os serviços instalados no servidor:

1. Faça o logon como Administrador ou com uma conta com permissões de administrador.
2. Abra o console Serviços. Iniciar -> Ferramentas administrativas -> Serviços.
3. Uma vez aberto o console Serviços surge a janela onde é exibida uma listagem com todos os serviços instalados no servidor. O console Serviços fornece dois modos de visualização: Estendido é um novo modo, o qual contém algumas opções a mais em relação ao modo Padrão. O modo Padrão é o modo disponível no Windows 2000 Server. Eu, particularmente, prefiro o modo Padrão, indicado na Figura 10.30:

The screenshot shows the Windows Services console window titled 'Serviços'. The menu bar includes 'Arquivo', 'Ação', 'Exibir', and 'Ajuda'. The toolbar contains icons for 'Novo', 'Abrir', 'Salvar', 'Copiar', 'Colar', 'Recortar', 'Iniciar', 'Parar', 'Reiniciar', and 'Finalizar'. The main pane displays a table of services with columns: Nome, Descrição, Status, Tipo de i..., and Fazer logon como. The table lists numerous services such as 'Acesso a dispositivo...', 'Adaptador de dese...', 'Agendador de tarefas', 'Ajuda e suporte', 'Alerta', 'Alocador Remote Pr...', 'Aplicativo de sistem...', 'Área de armazenam...', 'Armazenamento pr...', 'Armazenamento re...', 'Assistente de aquisi...', 'Assistente de conso...', 'Atualizações autom...', 'Áudio do Windows', 'Auxiliar NetBIOS TC...', 'Carregar Gerenciador', and 'Cartão inteligente'. The 'Status' column indicates the current state of each service. At the bottom of the table, there are two tabs: 'Estendido' and 'Padrão', with 'Padrão' being the selected tab.

| Nome                    | Descrição                  | Status     | Tipo de i...    | Fazer logon como |
|-------------------------|----------------------------|------------|-----------------|------------------|
| Acesso a dispositivo... | Permite acesso de ent...   | Desativado | Sistema local   |                  |
| Adaptador de dese...    | Fornece informações d...   | Manual     | Sistema local   |                  |
| Agendador de tarefas    | Permite que um usuári...   | Iniciado   | Automático      | Sistema local    |
| Ajuda e suporte         | Permite que o 'Centro ...  | Iniciado   | Automático      | Sistema local    |
| Alerta                  | Notifica os usuários e ... | Desativado | Serviço local   |                  |
| Alocador Remote Pr...   | Permite que clientes d...  | Manual     | Serviço de rede |                  |
| Aplicativo de sistem... | Gerencia a configuraç...   | Manual     | Sistema local   |                  |
| Área de armazenam...    | Permite que o 'Visualiz... | Desativado | Sistema local   |                  |
| Armazenamento pr...     | Protege o armazenam...     | Iniciado   | Automático      | Sistema local    |
| Armazenamento re...     | Gerencia e cataloga mí...  | Manual     | Sistema local   |                  |
| Assistente de aquisi... | Fornece serviços de a...   | Desativado | Serviço local   |                  |
| Assistente de conso...  | Permite que administra...  | Manual     | Sistema local   |                  |
| Atualizações autom...   | Ativa o download e ins...  | Iniciado   | Automático      | Sistema local    |
| Áudio do Windows        | Gerencia dispositivos d... | Iniciado   | Automático      | Sistema local    |
| Auxiliar NetBIOS TC...  | Forcene suporte a Net...   | Iniciado   | Automático      | Serviço local    |
| Carregar Gerenciador    | Gerencia as transferê...   | Manual     | Sistema local   |                  |
| Cartão inteligente      | Gerencia o acesso a c...   | Manual     | Serviço local   |                  |

Figura 10.30 Listagem dos serviços instalados no servidor.

**NOTA:** É importante salientar que no console Serviços são exibidos todos os serviços instalados. Porém nem todos os serviços são, obrigatoriamente, inicializados automaticamente durante a inicialização do Windows Server 2003. Para saber quais serviços foram inicializados observe a coluna Status. Nesta coluna aparece o Satatus Iniciado, somente para os serviços que estão em funcionamento, isto é, carregados na memória do servidor.

Na parte de baixo da lista de serviços, você tem as opções Estendido e Padrão. No modo de visualização Estendido, quando você clica em um determinado serviço, informações adicionais são exibidas sobre o serviço, no painel à esquerda da lista de serviços. Se você clicar na guia Padrão, será exibida a visualização que era utilizada nas versões anteriores, sem o painel de informações do lado esquerdo.

4. Observe que são exibidas as seguintes colunas de informação:

- ◆ **Nome:** Nome com o qual o serviço se registra no Windows Server 2003. É este nome que você deve fornecer para o comando net start, quando tiver que iniciar o serviço via linha de comando, ou para o comando net stop, quando você tiver que parar o serviço, via linha do comando. Se o nome do serviço contiver espaços, o nome do serviço deverá ser fornecido, entre aspas, para os comando net start e net stop.
- ◆ **Descrição:** Uma breve descrição da função do serviço.
- ◆ **Status:** Indica se o serviço está ou não carregado (Started).
- ◆ **Tipo de inicialização:** Indica se o serviço foi inicializado automaticamente (Automatic (Automático)) na inicialização do Windows Server 2003, manualmente pelo usuário ou por algum outro serviço (Manual) ou se o serviço está desativado (Disabled (Desativado)).
- ◆ **Fazer logon como:** Para que um serviço possa ser inicializado, deve ser fornecida uma conta de usuário e senha. Observe que a maioria dos serviços roda com a conta Loca System (Sistema Local) que é uma conta especialmente criada para esse fim. Um detalhe importante é que a conta Local System (Sistema Local) somente pode receber permissões para acessar recursos no próprio computador. Se um serviço precisar acessar recursos em outro computador da rede, a conta Local System (Sistema Local) não deverá ser utilizada para inicializar o serviço. Neste caso deverá ser utilizada uma conta que tenha permissão de acesso aos recursos que serão acessados pelo respectivo serviço, normalmente uma conta do domínio, especialmente criada para este fim.

5. Para ver maiores detalhes sobre um determinado serviço, dê um clique duplo na linha do serviço.  
6. Dê um clique duplo sobre o serviço Agendador de tarefas. Será exibida a janela indicada na Figura 10.31:

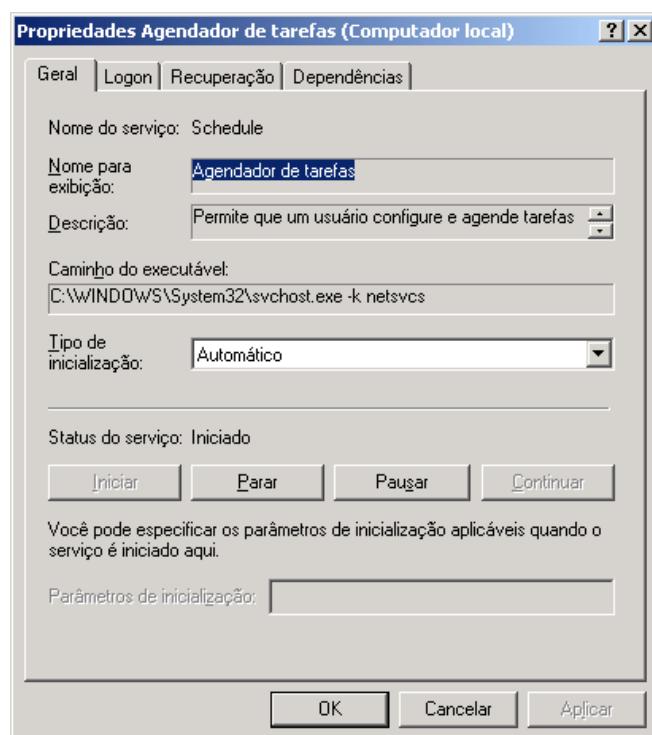
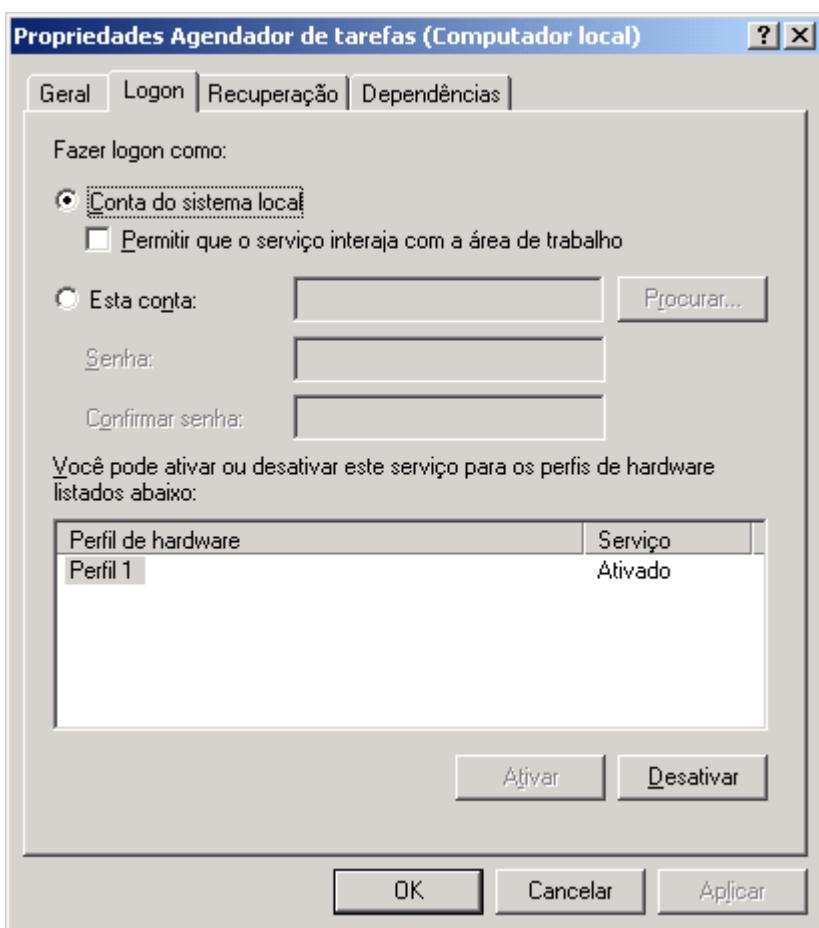


Figura 10.31 Propriedades do serviço agendador de tarefas.

7. Na guia Geral são exibidas diversas informações importantes, tais como o nome, descrição, caminho do arquivo executável (que é o arquivo que o Windows Server 2003 executa para carregar o serviço na memória). Por exemplo, para o serviço agendador de tarefas é utilizado o seguinte executável:  
**C:\WINDOWS\System32\svchost.exe -k netsvcs**
8. Muito importante na guia Geral é a seção Status do serviço. Nesta seção existe a indicação da situação atual: Started (Iniciado), Paused (Pausado), Disabled (Desativado) e assim por diante. Também estão disponíveis os botões para Iniciar, Parar, Pausar e Continuar.
9. Você pode utilizar o botão Iniciar para carregar um serviço que não foi inicializado automaticamente.
11. Dê um clique na guia Logon. Será exibida a janela indicada na Figura 10.32:

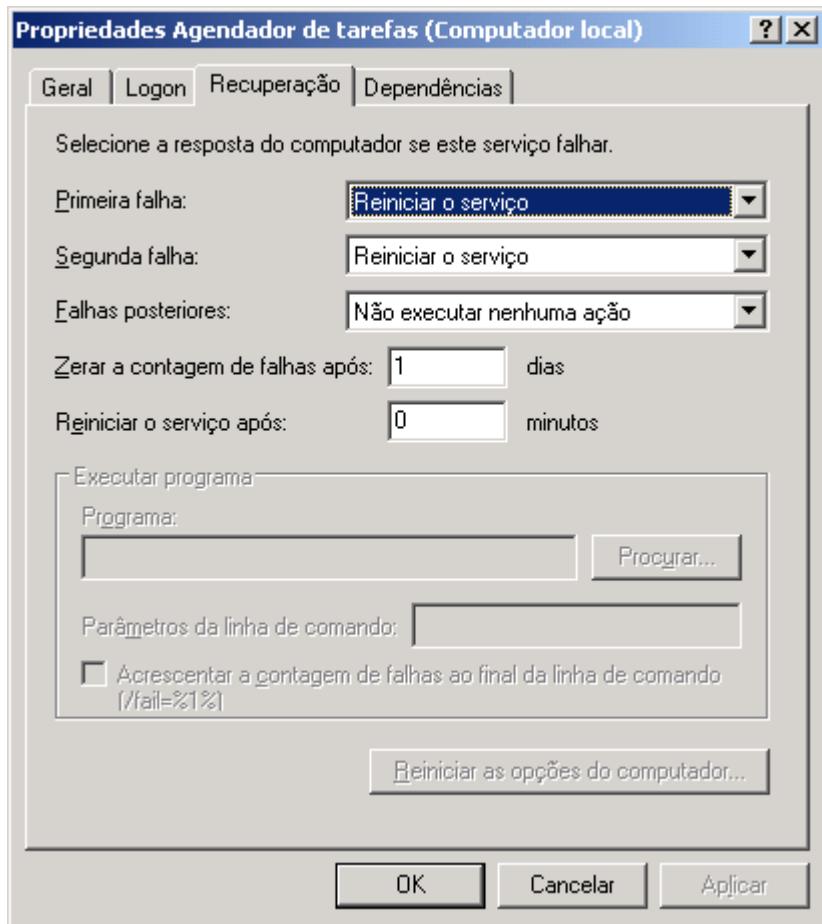


**Figura 10.32 Conta para a inicialização do serviço.**

**NOTA:** Se este serviço não estiver sendo executado, as tarefas agendadas não serão executadas nos horários e datas programados. Para maiores detalhes sobre o Agendamento de tarefas consulte o Capítulo 8

**IMPORTANTE:** É importante distinguir entre Parar e Pausar um serviço. Para aprender bem este conceito, vamos imaginar o serviço do servidor Web IIS. Imaginamos que existam 10 usuários conectados, se você Pausar o serviço, os 10 usuários continuam conectados, porém novas conexões não serão aceitas. Se você Parar o serviço não serão aceitas novas conexões e os 10 usuários atualmente conectados serão desconectados.

10. Nesta guia você pode configurar com qual conta o serviço irá rodar. A maioria dos serviços roda com a conta do Local System (Conta do sistema local). Para isso basta marcar a opção Conta do sistema local. Se você deseja especificar uma outra conta, clique na opção Esta conta. Informe o nome da conta e a respectiva senha. Confirme a senha digitada. Você também pode configurar em quais perfis de Hardware o serviço deve ser iniciado e em quais não deve.
11. Dê um clique na guia Recuperação. Será exibida a janela indicada na Figura 10.33:



**Figura 10.33 Definindo as opções de recuperação.**

12. Nesta guia você pode definir qual o comportamento do Windows Server 2003 quando o serviço falha pela Primeira vez, Segunda vez e para as Falhas posteriores. Conforme indicado na figura as ações podem ser:

- ◆ **Não executar nenhuma ação:** Neste caso se o serviço falhar o Windows Server 2003 não tentará reinicializá-lo automaticamente. Somente utilize esta opção se você deseja verificar pessoalmente as possíveis causas para a falha do serviço.
- ◆ **Reiniciar o serviço:** Se você selecionar esta opção o Windows Server 2003 tentará reinicializar o serviço automaticamente. Ao selecionar esta opção serão habilitados os campos Zera a contagem de falha após e Reiniciar o serviço após. A opção Zera a contagem de falha após, fornece um espaço para você digitar o número de dias que um serviço precisará ser executado com êxito antes que a contagem de falhas seja zerada. Quando a Contagem de falhas for zerada, a próxima falha acionará a ação definida para a primeira tentativa de recuperação. Se desejar que o serviço seja executado corretamente durante várias semanas entre falhas, digite um número maior. A opção Reiniciar o serviço após, fornece um espaço para você digitar a quantidade de minutos que se deve aguardar antes de reiniciar o serviço. Esta opção somente estará disponível se você selecionar Reiniciar o serviço como uma ação a ser executada quando um serviço falhar.
- ◆ **Executar um programa:** Com esta opção você pode especificar que o Windows Server 2003 execute um determinado arquivo quando o serviço falhar. Ao selecionar esta opção, o campo Programa será habilitado. Neste campo você digita o caminho para um arquivo executável válido. Pode ser um arquivo em lotes (.bat), um arquivo .cmd ou qualquer executável válido para o Windows Server 2003. No campo Parâmetros da linha de comando, você pode definir parâmetros que serão passados para o arquivo que será executado. Por exemplo,

você pode fazer que seja executado um Script que envia uma mensagem de email para o Administrador, informando sobre a falha no serviço.

- ◆ **Reiniciar o computador:** Esta opção fará com que o computador seja reinicializado em caso de falha do serviço. Somente deve ser utilizada para serviços realmente críticos em que qualquer falha possa representar uma ameaça à segurança. Se você selecionar esta opção, o botão Reiniciar as opções do computador (outra “obra de arte da tradução”). Obviamente que o título deste botão deveria ser “Opções de reinicialização do computador...”), será habilitado. Ao clicar neste botão será exibida a janela Reiniciar as opções de computador (mesmo comentário anterior em relação a tradução, ou seja, o correto seria: Opções de reinicialização do computador), na qual você pode definir em quanto tempo (minutos) o computador será reinicializado e uma mensagem a ser enviada aos computadores da rede, conforme exemplo da Figura 10.34. Na Figura é exibida a mensagem padrão do Windows Server 2003. Você pode alterar esta mensagem de acordo com suas necessidades. O envio da mensagem é útil, principalmente se o computador que será reinicializado estiver compartilhando pastas com os demais computadores da rede. Neste caso os outros usuários terão tempo de salvar e fechar os arquivos compartilhados que estão no computador que está sendo reinicializado. Isto evita que os usuários percam suas alterações.

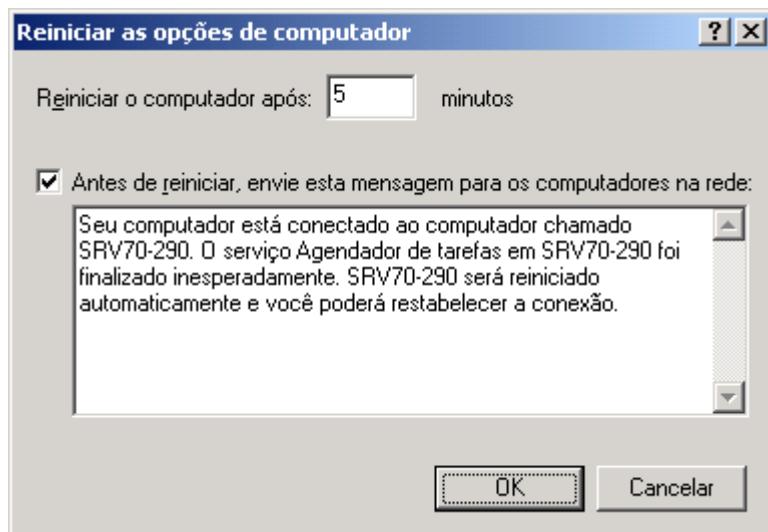


Figura 10.34 Definindo as configurações de reinicialização em caso de falha.

13. Dê um clique na guia Dependências. Será exibida a janela indicada na Figura 10.35.
14. Na parte de cima, são exibidos os serviços dos quais o serviço atual depende. No exemplo da Figura 10.35 é possível ver que o serviço Agendador de tarefas depende do serviço Chamada de procedimento remoto (RPC). Isto significa que para o serviço Agendador de tarefas poder iniciar é necessário que o serviço RPC já esteja carregado. O Windows Server 2003 utiliza as informações de dependência para definir a ordem de inicialização dos serviços. Por exemplo, como o serviço Agendador de tarefas depende do serviço Chamada de procedimento remoto, isto significa que o serviço Chamada de procedimento remoto deve ser inicializado antes do serviço Agendador de tarefas, pois caso contrário será gerado um erro e o serviço Agendador de tarefas não será inicializado. O Windows Server 2003 é encarregado de gerenciar as dependências entre os serviços, de tal forma que todos os serviços sejam inicializados na ordem correta.
15. Na parte de baixo é exibida lista de serviços que dependem do serviço Agendador de tarefas, no caso nenhum serviço depende do Agendador de tarefas.

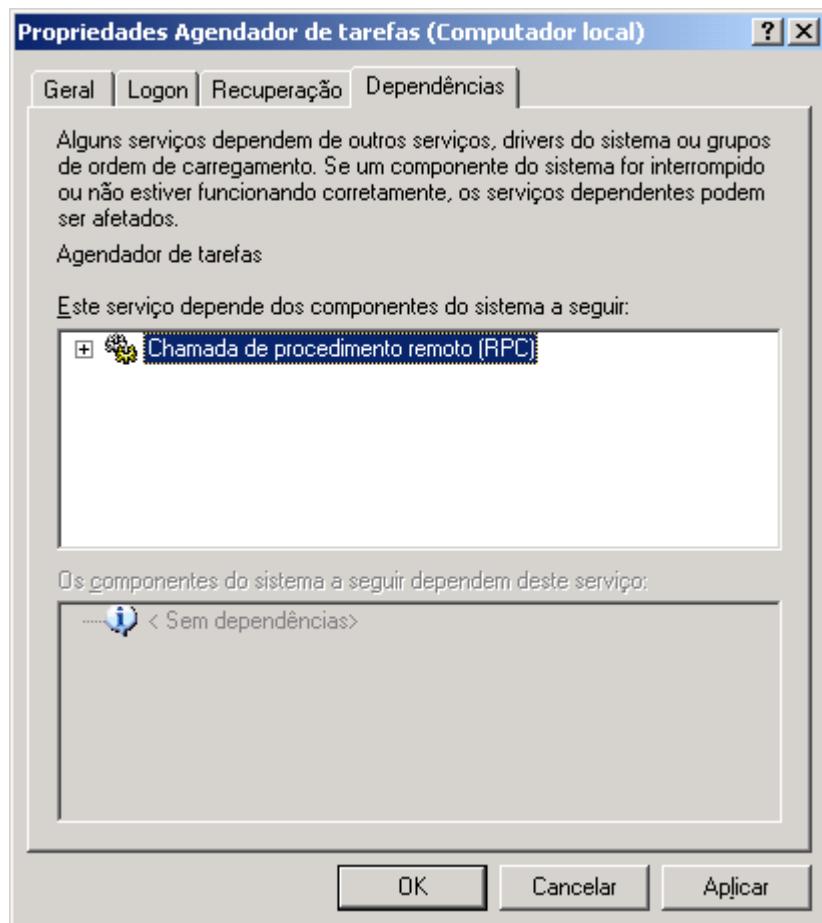


Figura 10.35 Exibindo as dependências do serviço.

16. Dê um clique em OK para fechar as propriedades do serviço Agendador de tarefas.
17. Feche o console Serviços.

Exemplo 2: Acessando as informações sobre Serviços em um computador remoto.

Você pode utilizar o console Serviços para se conectar e exibir as informações sobre os Serviços em um computador remoto. O computador remoto pode estar rodando o Windows NT, Windows 2000 Server ou Professional, Windows XP ou o Windows Server 2003.

Para acessar as informações sobre os serviços de um computador remoto, siga os passos indicados a seguir:

1. Faça o logon como Administrador ou com uma conta com permissões de administrador.
2. Abra o console Serviços. Observe que automaticamente é feita a conexão com o computador local.
3. Para conectar-se a um computador remoto, clique com o botão direito do mouse em Serviços (local). No menu de opções que é exibido clique em Conectar-se a outro computador... Será exibida a janela Selecionar Computador. No campo Outro computador digite o nome ou o endereço IP do computador com o qual você deseja se conectar, conforme exemplo

**DICA:** Um serviço que vale a pena ser comentado é o serviço Registro remoto. Este serviço é fundamental para que seja possível fazer a administração à distância, usando os consoles de administração do Windows Server 2003. Por exemplo, imagine que você irá abrir o console Gerenciamento do computador, no servidor SRV02. Agora você decide conectar o console Gerenciamento do computador, remotamente, com o servidor SRV02. Para que isso seja possível, o serviço Registro Remoto, deve ter sido inicializado, com sucesso, no servidor SRV02.

da Figura 10.36. Você pode utilizar o botão Procurar..., para selecionar o computador na lista de computadores da rede.

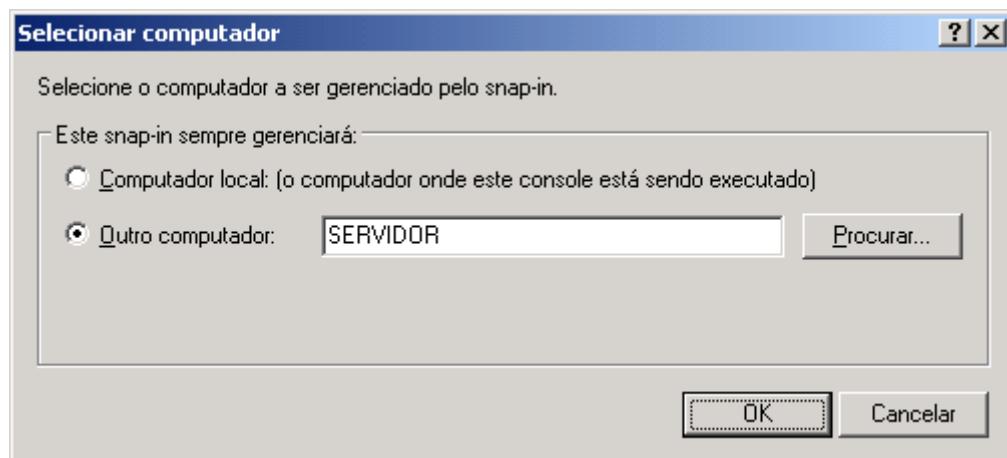


Figura 10.36 Informando o nome do computador a ser conectado.

4. Após ter especificado o nome do computador ou o número IP clique em OK. O Windows Server 2003 conecta-se com o computador especificado e exibe a lista de serviços deste computador.
5. Você pode escolher diferentes formas de exibição para a lista de serviços. Para alternar entre as diferentes opções de exibição utilize o menu Exibir, do console Serviços. Na Figura 10.37 temos a forma de exibição Ícones grandes, selecionada através do comando Exibir -> Ícones grandes.

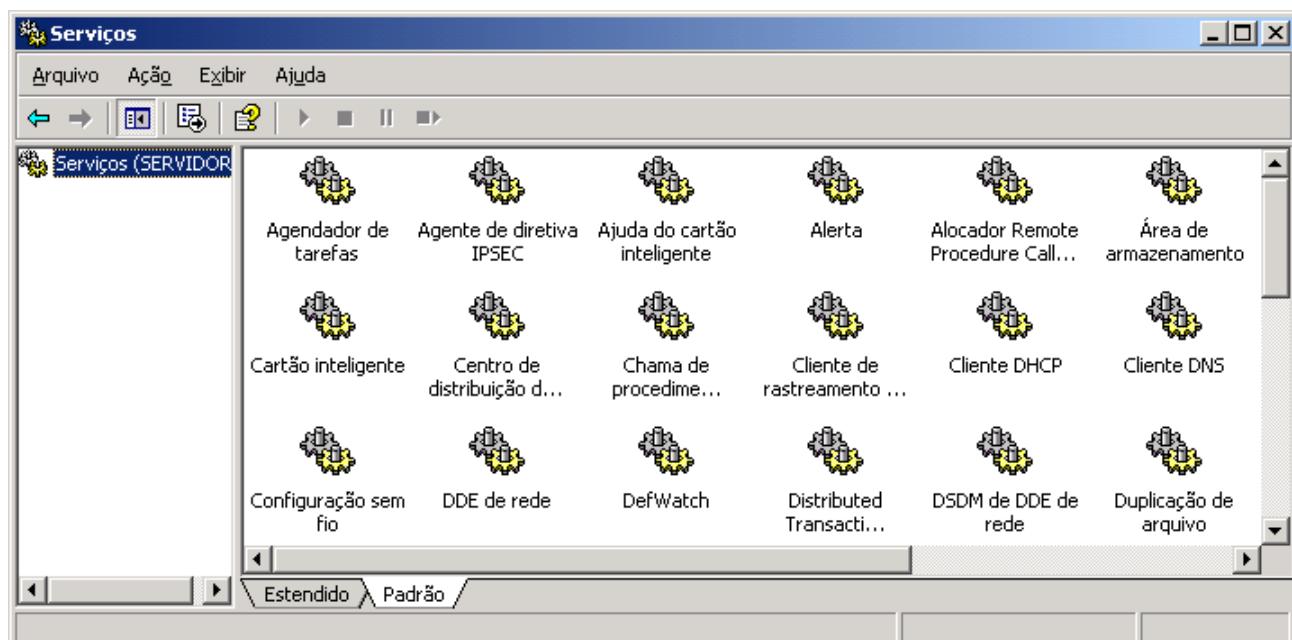


Figura 10.37 Exibição de ícones grandes.

6. Você também pode exportar as informações sobre a lista e as configurações de cada serviço, para um dos seguintes formatos:
  - ◆ Texto delimitado por tabulação (\*.txt).
  - ◆ Texto delimitado por vírgula (\*.csv).
7. Para exportar a lista de Serviços selecione o comando Ação -> Exportar lista... Será exibida a janela Exportar lista, na qual você define a pasta de destino, o nome e o formato do arquivo de destino.
8. Feche o console de serviços.

Exercício: Abra novamente o console Serviços. Verifique o status e as propriedades do serviço Server (Servidor). Acesse a guia de dependências para verificar quais serviços dependem do serviço Server. Exporte a lista de Serviços em execução para um arquivo chamado Serviços.txt, na pasta Meus documentos. Utilize o formato Texto delimitado por vírgula (\*.csv). Se você estiver conectado a uma rede com outros computadores, tente conectar o console Serviços a outro computador da rede. Você somente conseguirá realizar esta operação se a conta com a qual você estiver logado, tiver permissão de Administrador no computador com o qual você deseja se conectar.

## Conclusão.

Neste capítulo tratei de uma série de assuntos relacionados com logs de eventos e auditoria.

Iniciei o capítulo falando sobre o conceito de log e de auditoria. Em seguida fiz um longo estudo sobre a utilização e configuração dos logs de auditoria do Windows Server 2003.

Você aprendeu, através de uma série de exemplos práticos sobre quais os logs disponíveis, que cada log é configurado individualmente, que somente o administrador tem acesso ao log de Segurança e que as propriedades de cada log podem ser configuradas separadamente. Mostrei como filtrar os logs de evento por tipo de log, origem de log e outras opções.

Também mostrei como usar as diretivas de segurança do domínio para configurar uma série de opções que afetam as configurações dos logs e quais eventos são gravados no log. Por exemplo, você aprendeu que para fazer auditoria do acesso a pastas, arquivos ou impressoras, são necessários dois passos, conforme descrito a seguir:

1. Habilitar a seguinte diretiva de auditoria: “Auditoria de acesso a objetos”. Esta diretiva é habilitada, para sucesso, falha ou ambas as situações, utilizando o console Configurações locais de segurança, já descrito anteriormente. Você aprendeu, na prática, os passos necessários para configurar esta e outras diretivas de auditoria.
2. Após ter habilitada a Diretiva de auditoria descrita no item 1, o administrador tem que configurar a auditoria em cada um dos objetos a serem auditados. Por exemplo, para monitorar o acesso a uma pasta e ao conteúdo desta pasta (subpastas e arquivos), o administrador deve acessar as propriedades desta pasta e configurar quais usuários/grupos terão o acesso monitorado. Por exemplo, o administrador pode definir que o grupo Gerentes terá o acesso a uma determinada pasta monitorada, tanto para evento de sucesso quanto de falha. Com isso, toda vez que um membro deste grupo acessar o conteúdo da pasta que está sendo monitorada, será gravado um evento no log de eventos. Você também aprendeu as etapas práticas para configuração de auditoria em pastas, arquivos e impressoras.

Para finalizar o capítulo apresentei o conceito de serviços:

Um Serviço é um componente de software que é inicializado automaticamente quando o Windows Server 2003 é inicializado, ou pode ser iniciado a qualquer momento, manualmente, pelo administrador. Um Serviço continua carregado e funcionando, mesmo quando não existe nenhum usuário logado no servidor. Por exemplo o serviço Spooler,

responsável pela impressão continua trabalhando, mesmo quando não existe nenhum usuário logado. O mesmo é válido para qualquer serviço que rode no Windows Server 2003.

Em seguida mostrei como usar o console Services (Serviços) para gerenciar os serviços disponíveis no servidor. Também mostrei como conectar-se a outros servidores da rede, remotamente, para gerenciar os serviços em um servidor remoto.

No próximo capítulo falarei sobre a utilização do console de desempenho para a monitoração do desempenho do servidor e da taxa de ocupação dos principais serviços e recursos de hardware do servidor.

# Introdução

Neste capítulo tratarei sobre o conceito de monitoração de desempenho dos componentes de hardware e dos serviços de um servidor. A monitoração não é uma tarefa, digamos assim, obrigatória, ou seja, que se não for feita algum serviço deixa de funcionar.

Porém a monitoração é uma maneira do administrador acompanhar o aumento de carga em um ou mais servidores da rede, acompanhando qual a ocupação/utilização dos principais elementos de Hardware, tais como memória, processadores, interfaces de rede e sistemas de disco. Com o acompanhamento da carga de trabalho em cada um destes elementos, o administrador pode fazer uma estimativa com tempo de quando será necessário o upgrade de um ou mais destes elementos de hardware, como por exemplo adicionar mais memória RAM, trocar a placa controladora de discos por uma mais rápida e assim por diante. Se o administrador não tem este acompanhamento, o que acontece é que chega-se a um ponto onde os serviços tornam-se lentos e os usuários começam a reclamar. Neste ponto o administrador não sabe exatamente o que está acontecendo (apenas suspeita que pode ser sobrecarga no hardware do servidor). Como o administrador não fez a lição de casa, isto é não fez um monitoramento preventivo, terá que “tentar descobrir” quais os elementos de hardware que estão sobrecarregados, apresentar um relatório solicitando recursos, encomendar o hardware necessário para finalmente providenciar a troca. Ou seja, tudo na base do improviso, da pressa. Definitivamente esta não é uma boa maneira de trabalhar.

O monitoramento sistemático, isto é, com regras bem definidas e com uma metodologia de monitoramento, faz com que o administrador trabalhe de uma maneira pró-ativa (um amigo meu diria que este termo é ‘chique’), sempre prevendo com boa antecedência as necessidades de upgrade de hardware, evitando com isso que chegue-se ao ponto em que o desempenho caia exponencialmente e os usuários começem a reclamar. Outro fator que tem que ser considerado é que chega-se a um ponto onde o limite do servidor é atingido, ou seja, não é mais possível expandir a memória, não é possível adicionar novos processadores e assim por diante. Nestas situações faz-se necessária a troca do servidor por outro com maiores capacidades. Mais uma vez fica clara a importância do monitoramento para prever, com uma boa antecedência, uma necessidade de troca de servidor. Principalmente porque servidor e hardware de servidor não é como hardware de PC, que você encontra a pronta-entrega no mercado. Normalmente hardware de servidor é feito sob encomenda e demora alguns dias (ou até semanas) para estar disponível. Se o administrador não prever com uma boa antecedência a necessidade de troca, corre o risco de ter que conviver durante semanas com um ou mais servidores que não atendem as demandas dos usuários, com um desempenho sofrível e o que é o pior, com um telefone que não para de tocar, com usuários reclamando (e com toda a razão), do desempenho do sistema.

Neste capítulo você aprenderá a utilizar o console para monitoração de Desempenho, de forma a acompanhar a taxa de utilização dos principais elementos do sistema. Mostrarei uma série de assuntos relacionados com o monitoramento, otimização e manutenção do Windows Server 2003. Com os

# CAPÍTULO

## 11

### Monitoração de Desempenho e Logs de Alerta

conceitos e exemplos práticos vistos neste capítulo, você terá condições de fazer um monitoramento dos servidores, atuando de maneira pró-ativa.

Monitorar a utilização dos principais recursos de um servidor é uma tarefa importante para o administrador do servidor, principalmente em servidores que estão sendo utilizados para o compartilhamento de recursos (por ex. arquivos e impressoras) na rede. O desempenho de um servidor fica seriamente comprometido se um dos seguintes elementos estiver sobrecarregado:

- ◆ Memória RAM.
- ◆ Processador.
- ◆ Placa de rede.
- ◆ Sistema de discos.

Neste capítulo mostrarei como utilizar o console Desempenho, para acompanhar a taxa de ocupação de cada um destes elementos. Também mostrarei como configurar o Windows Server 2003 para que faça a coleta automática, em períodos definidos, da taxa de ocupação de determinados elementos, de tal maneira que você possa ter uma idéia da utilização destes elementos em condições normais de trabalho. Com este acompanhamento você também terá condições de verificar a evolução nas taxas de utilização de cada um dos elementos que estão sendo monitorados. Assim quando um determinado elemento tiver a sua taxa de utilização constantemente aumentada, é possível agir preventivamente, normalmente providenciando a substituição do elemento, como por exemplo a instalação de um processador mais rápido ou de uma quantidade adicional de memória RAM ou a substituição de discos IDE por um sistema de discos SCSI.

## Monitoração de desempenho – conceitos básicos.

Monitorar a utilização dos principais recursos de um servidor é uma tarefa importante para o administrador do sistema, principalmente em computadores que estão sendo utilizados por um grande número de usuários da rede, para acesso a recursos tais como pastas compartilhadas, impressoras, servidores Web de Intranet, servidores de banco de dados, DCs do domínio e assim por diante. Os principais elementos de hardware a serem monitorados são os seguintes:

- ◆ Memória RAM.
- ◆ Processador.
- ◆ Placa de rede.
- ◆ Sistema de discos.

Existem outros elementos que podem prejudicar o desempenho como um todo, porém estes quatro são os mais importantes. Podem existir situações, por exemplo, em que a utilização da memória RAM e do Processador esteja baixa, porém o Sistema de discos esteja sobrecarregado, e neste caso, o desempenho do sistema como um todo fica bastante prejudicado. Dependendo do tipo de função que o servidor está exercendo, um recurso de hardware pode ter mais ou menos influência no desempenho como um todo. Por exemplo, servidores de banco de dados são muito dependentes de bons processadores, já servidores de arquivos dependem de um bom sistema de disco e de uma conexão rápida com a rede.

---

**NOTA:** Em alguns livros e na documentação oficial do Windows Server 2003, o console Performance também é chamado de System Monitor (Monitor do Sistema). Neste capítulo utilizarei os termos System Monitor ou console Performance como sinônimos.

---

**IMPORTANTE:** Para o exame é muito importante que você conheça bem, quais os contadores e respectivos limites que podem representar um problema de sobrecarga do processador, memória, etc.

---

Quando um determinado componente está sobrecarregado, dizemos que este componente representa um “gargalo” para o sistema (do termo inglês “bottleneck”), isto é, é o componente que está limitando (“engargalando”, se é que existe esta palavra.), o desempenho do sistema como um todo. Ou seja, o desempenho de um sistema é tão bom quanto for o desempenho do seu componente mais lento. Por exemplo, de que adianta vários processadores, com muita memória RAM e com um sistema de discos antigo, extremamente lento.

Dependendo do papel que o servidor esteja desempenhando na rede, a utilização de cada um destes componentes será maior ou menor. Por exemplo, computadores que atuam como Servidores de Banco de dados (com o Microsoft SQL Server, por exemplo), ou Servidores de aplicação (com o Microsoft Transaction Server, por exemplo), fazem um uso muito intensivo dos Processadores. Neste caso pode ser recomendável, dependendo do número de usuários, a utilização de servidores multi-processados. Já no caso de Servidores de arquivos, a utilização da interface de rede e do sistema de discos pode ser bastante elevada, neste caso a utilização de placas mais velozes ou até mesmo de mais de uma placa de rede e de sistemas de discos mais rápidos, pode ser uma solução para melhorar o desempenho.

A monitoração do desempenho ajuda a determinar qual o componente que está sendo o principal limitador do desempenho do sistema (o ‘gargalo’ do sistema), além de permitir a análise da carga de trabalho a qual o respectivo componente está submetido (por exemplo, o processador está com 80% de utilização, o sistema de discos está constantemente com dados na fila de espera para leitura e gravação e assim por diante). O administrador também pode utilizar a monitoração do desempenho para fazer uma estimativa do crescimento na utilização dos componentes do sistema. Com isso fica mais fácil fazer uma previsão sobre as necessidades futuras de atualizações de Hardware. Além disso, de posse de dados de monitoração consistentes, fica mais fácil justificar o gasto envolvido na aquisição e atualização de componentes de hardware.

Conforme mostrarei nos próximos tópicos, a monitoração é feita através do console Desempenho, também conhecido como System Monitor. Este console é acessado através da opção Desempenho, no menu Ferramentas administrativas. No console de desempenho você adiciona “Objetos” a serem monitorados. Um exemplo de objeto pode ser um Processador, Memória, Disco físico, Fila de impressão, etc. Um objeto representa um elemento que pode ser monitorado pelo Windows Server 2003. Para cada objeto, estão disponíveis vários contadores que são indicativos da utilização dos recursos do respectivo objeto. Por exemplo para o objeto Processador, dentre outros, existem os seguintes contadores: “Porcentagem de tempo do processador”, “Interrupções por segundo” e assim por diante. Para o objeto Fila de impressão, existem os contadores “Total de páginas impressas”, “Trabalhos no spool”, e assim por diante.

Vários objetos e seus respectivos contadores são instalados durante a instalação do Windows Server 2003. A medida que novos serviços ou aplicativos são instalados, novos Objetos e contadores são adicionados. Por exemplo, ao instalar o Microsoft SQL Server 2000, novos objetos são adicionados. Outro exemplo, quando é instalado o servidor Web IIS, novos objetos são adicionados e assim por diante.

Saber exatamente quais objetos e quais contadores utilizar é um processo que envolve testes e muita paciência. Somente com a experiência é que o administrador saberá quais os contadores observar para verificar a existência de problemas de desempenho.

A otimização do desempenho é um processo contínuo. Muitas vezes em uma primeira análise, o administrador descobre que um dos componentes está sendo o gargalo do sistema, por exemplo, a memória RAM. Aí mais memória RAM é acrescentada ao servidor. Pode ser que outro componente passe a ser o gargalo, por exemplo a Placa de rede ou o processador. Monitorar e otimizar o desempenho é um desafio bastante grande, porém é uma necessidade. Não é possível simplesmente trocar de equipamento, toda vez que houver problemas de desempenho, pois isso seria um desperdício de dinheiro.

Também é possível configurar o console Desempenho para que seja feita a captura de dados automaticamente. O administrador pode configurar a captura de dados para que seja feita a captura apenas de determinados contadores de determinados objetos, ou seja, somente aqueles contadores que interessam ao administrador. Com base nesta captura é possível verificar os limites normais de operação para componentes como o Processador, memória RAM e assim por

diantre. Entenda-se por limites normais de operação, as taxas de utilização dos diversos componentes de hardware e software, durante o horário normal de expediente. Depois faz-se o agendamento de um monitoramento contínuo e compara-se os resultados obtidos com os limites de operação obtidos durante a primeira captura. Quando um determinado componente começar a apresentar aumento na sua taxa de utilização deve ser verificado o motivo para este aumento e, se for o caso, providenciar a substituição do dispositivo antes que a sua taxa de utilização atinja limites que possam comprometer o desempenho do servidor.

No próximo tópico você aprenderá a utilizar o console Performance (Desempenho), através de exemplos práticos.

## Utilização do console Desempenho

Neste tópico você verá vários exemplos práticos de utilização do console de desempenho, para monitoração dos principais elementos de hardware do servidor.

### Monitorando o Processador e a Memória do seu Servidor.

Neste item você aprenderá a utilizar o console Desempenho. Também verá como monitorar alguns contadores dos objetos Memória e Processador. Apresentarei diversos detalhes sobre a utilização da interface e das funcionalidades do console Desempenho. O console Desempenho já vem configurado para carregar o Snap-in para medição de desempenho.

Exemplo: Monitorando o uso da memória e do processador.

Para utilizar o console Desempenho, para monitorar a Memória e o Processador, siga os seguintes passos:

1. Faça o logon como Administrador, ou com uma conta com permissão de administrador.
2. Abra o console Desempenho: Iniciar -> Ferramentas administrativas -> Desempenho.
3. Será aberto o console Desempenho, conforme indicado na Figura 11.1:

**NOTA:** No Windows NT Server 4.0 existe um programa chamada Performance Monitor, o qual é utilizado para a monitoração de desempenho. A partir do Windows 2000 está disponível o console Desempenho, o qual está também disponível no Windows XP e no Windows Server 2003.

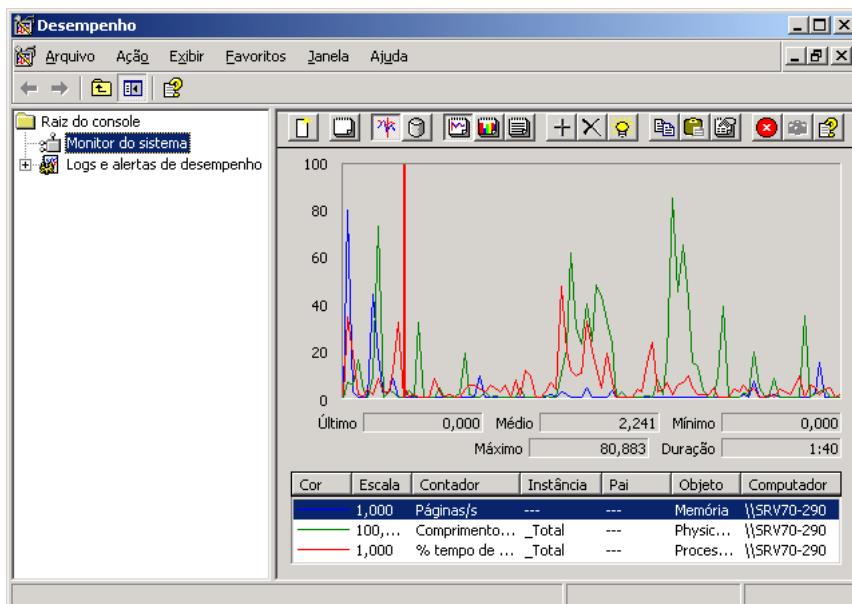


Figura 11.1 O console para monitoração do desempenho.

Observe que, por padrão, os seguintes contadores já estão adicionados e sendo monitorados:

- ◆ O contador Pages/sec do objeto Memory.
- ◆ Comprimento médio de fila de disco (Avg. Disk Queue Length) do objeto Physical Disk.
- ◆ O objeto %Tempo do processador (%Processor Time) do objeto Processor.

Para o exemplo proposto você irá excluir os contadores que foram adicionados automaticamente e adicionar outros contadores.

4. Clique no contador Páginas/s (na parte de baixo do painel, abaixo do gráfico, onde aparece a lista de contadores) e pressione a tecla Delete. Repita a operação para excluir os demais contadores.
5. Neste console, no painel da esquerda, é exibida a opção Monitor do sistema, que é a opção utilizada para adicionar novos contadores para os objetos a serem monitorados, no nosso exemplo a Memória e Processador. A opção Logs e alertas de desempenho será vista nos próximos itens.
6. Dê um clique na opção Monitor do Sistema, para seleciona-la.
7. Dê um clique no botão Adicionar na barra de ferramentas – botão com um sinal de + na barra de ferramentas ou pressione Ctrl+I. Será exibida a janela Adicionar contadores, na qual você pode selecionar objetos e adicionar os contadores a serem monitorados, conforme indicado na Figura 11.2.

**NOTA:** Os gráficos que vão sendo “desenhados” na tela do console, indicam os valores associados com cada um dos contadores. No exemplo da Figura 11.1 a taxa de ocupação do processador chegou a picos de 100% mas, na média, estava abaixo dos 20%.

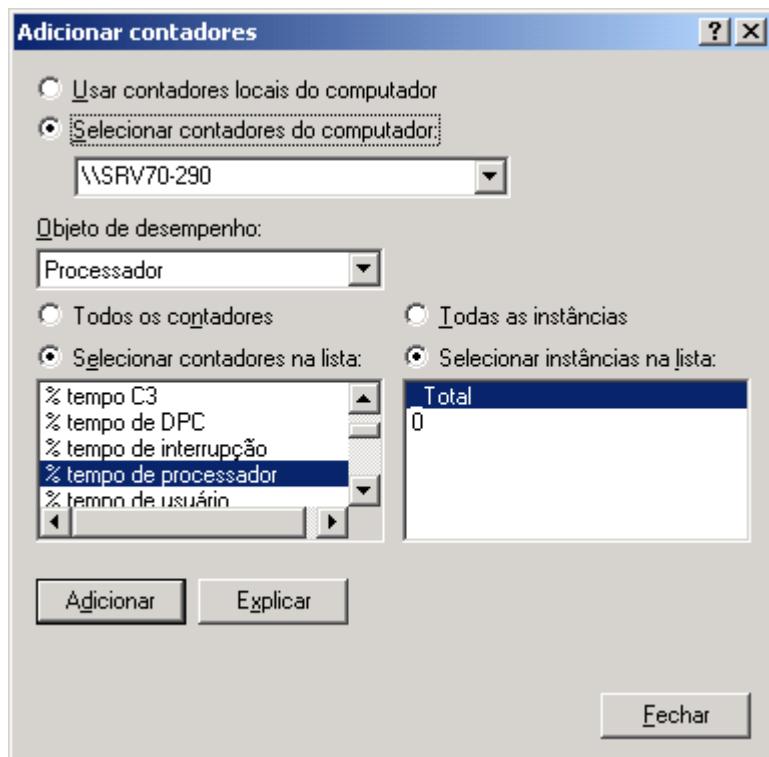


Figura 11.2 Janela para adicionar os contadores a serem monitorados.

Na lista Objeto de desempenho, por padrão já vem selecionado o objeto Processador. Nesta lista você pode selecionar um objeto para o qual serão adicionados contadores a serem monitorados. Ao selecionar um objeto na lista de objetos, na lista Selecionar contadores na lista, serão exibidos os contadores relacionados ao objeto selecionado. Um mesmo

contador pode ter uma ou mais instâncias. Por exemplo, ao selecionar o contador % tempo de processador, em um computador com dois processadores, na lista Selecionar instâncias na lista, serão exibidas as duas instâncias do referido contador, uma para cada processador. Você pode monitorar somente uma das instâncias ou ambas.

8. Certifique-se de que o objeto Processador esteja selecionado na lista de Objetos. Na caixa de listagem Selecionar contadores na lista, marque o contador % tempo de processado. Para ver uma explicação detalhada sobre o que significa este contador, dê um clique no botão Explicar. Será exibida uma janela com a descrição do contador selecionado, conforme indicado na Figura 11.3. Você pode utilizar o botão Explicar para obter um texto explicativo sobre qualquer contador selecionado.

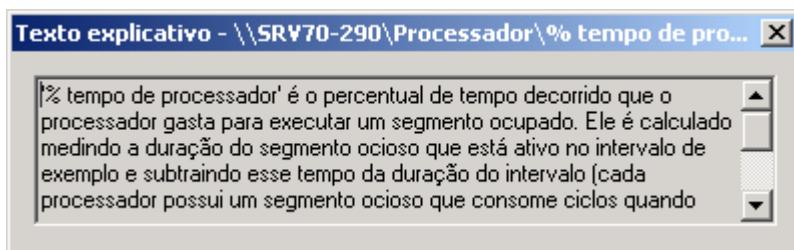


Figura 11.3 Janela que é exibida com a explicação sobre o contador selecionado.

9. Dê um clique no botão Adicionar, para adicionar o contador % tempo de processador.
10. Agora é hora adicionar um contador para a memória. Primeiro, na lista Objeto de desempenho, selecione o objeto Memória. Na caixa de listagem Selecionar contadores na lista, são exibidos os contadores disponíveis para o objeto Memória.
11. Dê um clique no contador % de bytes confirmados em uso. Clique no botão Adicionar e depois dê um clique no botão Fechar. Você estará de volta ao console de desempenho, sendo que agora os dois contadores que você adicionou já estão sendo monitorados, conforme mostrado pelo gráfico da Figura 11.4:

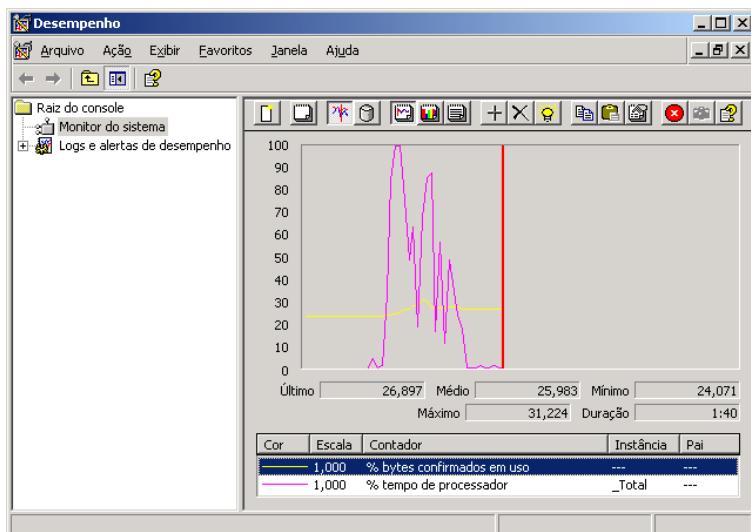


Figura 11.4 Um contador do Processador e outro da Memória, sendo monitorados.

**NOTA:** Um detalhe interessante é que, no mesmo console, você pode monitorar contadores de um ou mais computadores. Por exemplo, você pode monitorar a utilização do processador de dois ou mais computadores da rede, utilizando um único console Desempenho. Para isso, na janela da Figura 11.2, digite o nome do computador no campo Selecionar contadores do computador. Digite o nome do computador no formato \\NomeDoComputador. Ao digitar o nome e pressionar Enter serão exibidos os objetos do referido computador. Selecione um ou mais contadores. Você pode fazer isso para os diversos computadores que serão monitorados simultaneamente. Com isso, em um mesmo console, você poderá monitorar contadores de diferentes computadores da rede.

**NOTA:** Veja que no campo Selecionar contadores do computador, já vem, por padrão, o nome do computador local, onde foi aberto o console de desempenho. Podemos monitorar o desempenho de outros computadores da rede. Por exemplo, para acessar contadores de um computador chamado SERVER2, basta digitar \\SERVER2, neste campo e pressionar Enter. Em poucos instantes o Windows Server 2003 exibe uma listagem com os contadores do computador a ser monitorado. Você pode adicionar, para

**monitoração, contadores de diferentes computadores, conforme já descrito anteriormente. Por exemplo, você pode adicionar o Percentual de ocupação do processador para os diversos servidores da rede, para determinar qual ou quais estão com utilização excessiva do processador.**

---

12. Observe que o Processador teve picos de quase 100% de utilização. Já a memória tem se mantido em torno de 25%. Existem alguns indicadores que podem nos levar a certas conclusões interessantes. Por exemplo, se a taxa de utilização do Processador permanecer por longos períodos de tempo, sempre próxima ou acima de 80%, pode ser um indicativo de que o Processador é um gargalo para o sistema. O processador deve ser substituído por um Processador mais rápido, ou a utilização de mais do que um processador deve ser considerada. Por outro lado picos de 100% são perfeitamente normais. Quando você abre uma aplicativo é normal que a utilização do Processador chegue próxima dos 100%. O que não pode acontecer é uma alta taxa de utilização permanente próxima ou superior a 80%.
13. No nosso exemplo a utilização da memória (em torno de 25%), está em uma patamar ótimo. Até 60% seria um valor bastante razoável. Lembrando que picos podem acontecer, o que é um indicativo de sobrecarga em um dos componentes de hardware é uma taxa de utilização constante em patamares elevados.
14. O console de desempenho exibe uma série de informações para cada um dos contadores que estão sendo monitorados. Observe que cada um dos contadores possui um gráfico com cor diferente. Na parte de baixo do console, ao clicar em um contador, você irá seleciona-lo. Observe que logo abaixo do gráfico são exibidas diversas informações, dependendo do contador selecionado.
15. Ao selecionarmos o contador % tempo de processador, por exemplo, são exibidas diversas informações, tais como: valor médio, valor mínimo, valor máximo e assim por diante.
16. Para adicionar novos contadores, basta utilizar novamente o botão (Adicionar - botão com um sinal de +) ou pressionar Ctrl+I.
17. Quando você está monitorando diversos contadores, pode ser útil por em destaque o contador selecionado. Para isso basta pressionar Ctrl+H, que o contador selecionado será posto em destaque, isto é, ficará com a linha do gráfico mais espessa e destacada.
18. Para retirar o destaque do contador, basta pressionar Ctrl+H novamente.
19. Você pode excluir um contador, simplesmente clicando no contador, na parte de baixo do console, abaixo do gráfico e teclando Delete.
20. Você pode alterar diversas propriedades do gráfico que é exibido no console desempenho, como por exemplo: cor da linha, cor de fundo, exibir uma grade de referência, etc. Para acessar estas propriedades, dê um clique com o botão direito do mouse em qualquer parte do gráfico. No menu que surge clique em Propriedades.
21. Será exibida a janela Propriedades de Monitor do sistema, onde através das guias Geral, Fonte, Dados, Gráfico e Aparência, você pode alterar diversas propriedades da exibição do gráfico de desempenho. No exemplo da Figura 11.5, foram incluídas grades de referência. Esta configuração é feita através da guia Gráfico, da janela de propriedades.
22. Feche o console de desempenho.

---

**PRATIQUE UM POUCO:** Abra novamente o console desempenho e adicione alguns contadores do Processador e da Memória. Para o objeto Processador adicione os contadores Interrupções por segundo e % Tempo privilegiado. Utilize o botão Explicação para exibir a descrição destes contadores. Altere algumas propriedades do gráfico. Altere o campo atualizar automaticamente a cada, de 1 segundo para 2 segundos. Este campo é acessível através da guia Geral das propriedades do gráfico. Para acessar as propriedades clique com o botão direito do mouse em qualquer local do gráfico, e no menu que surge dê um clique na opção Propriedades.

---

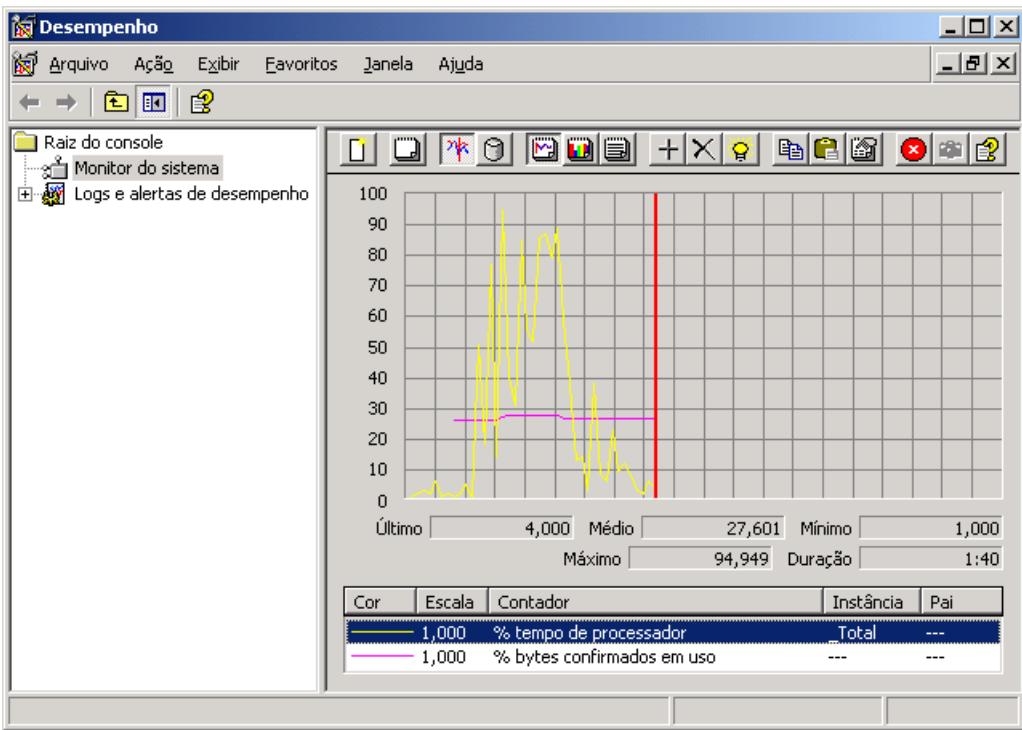


Figura 11.5 Alterando as propriedades do gráfico e incluindo grades de referência.

## Monitorando o acesso ao sistema de discos.

Neste item mostrarei como monitorar alguns contadores dos objetos Disco físico e Disco lógico. É importante lembrar que o objeto Disco físico se refere a um disco como um todo, independente de o disco estar dividido em partições (disco básico) ou volumes (disco dinâmico). Já o objeto Disco lógico, refere-se as partições ou volumes, independente de estarem localizadas em um único disco, ou distribuídas ao longo de vários discos, como no caso de um Volume RAID-5 ou de um Volume set.

Agora é hora de monitorar alguns contadores dos objetos Disco físico e Disco lógico.

Exemplo: Monitorando a atividade de discos, usando o console de desempenho.

Para monitorar a atividade do sistema de discos, siga os passos indicados a seguir:

1. Faça o logon como Administrador, ou com uma conta com permissão de administrador.
2. Abra o console Desempenho: Iniciar -> Ferramentas administrativas -> Desempenho.
3. No painel da esquerda, clique na opção Monitor do sistema, para marcá-la.
4. Dê um clique no botão Adicionar, na barra de ferramentas – botão com um sinal de + ou pressione Ctrl+I. Será exibida a janela Adicionar contadores, na qual podemos adicionar os objetos e respectivos contadores que serão monitorados.
5. No campo Objeto de desempenho, selecione o objeto Disco físico. Será exibida uma listagem com os discos instalados no seu computador e as partições (ou

**IMPORTANTES:** nunca é demais lembrar que no Windows NT 4.0 os contadores para o objeto Disco físico e Disco lógico estão desabilitados, por padrão. O objeto disco lógico nem sequer aparecia na listagem de objetos. O objeto Disco físico aparecia na listagem, mas se você adicionasse alguns dos seus contadores, estes ficariam sempre em zero, uma vez que estavam desabilitados. Para habilitar os contadores para os objetos Disco físico e Disco lógico, no NT 4.0, era necessário executar o seguinte comando: diskperf -y e reiniciar o computador para que os contadores sejam habilitados. NO WINDOWS SERVER 2003 NÃO É

volumes no caso de discos de Armazenamento dinâmico) criadas em cada um dos discos. No exemplo da Figura 11.6, são exibidos dois discos: Disco 0 e Disco 1. O espaço do Disco 0 é todo ocupado pelo Volume C: Já o espaço do Disco 1 é ocupado pelos volumes volume D:, E: e F: Observe que também é exibida uma instância denominada ‘\_Total’. A instância \_Total é utilizada para monitorar a atividade somada de todos os discos do sistema. Por exemplo, se você selecionar o contador Gravações em disco por segundo e selecionar a instância total, estará sendo monitorada a atividade total combinada de escrita em todos os discos do servidor.

**NECESSÁRIO ESTE PROCEDIMENTO, POIS OS CONTADORES,TANTO PARA DISCO FÍSCIO QUANTO PARA DISCO LÓGICO, ESTÃO HABILITADOS AUTOMATICAMENTE.**

---

**NOTA:** Para o exemplo proposto estou utilizando um computador com dois discos físicos, os quais estão divididos em um ou mais volumes. Para este exemplo estou utilizando um servidor com o Windows Server 2003, em Inglês, o que pode ser comprovado pelas telas em Inglês. Conforme visto no Capítulo 5, é possível criar mais de um volume (disco lógico) em um mesmo disco físico. Por exemplo, é possível dividir um disco de 40 GB em dois volumes de 20 GB. A cada volume estaria associada uma letra, como por exemplo: C: e E: Cada volume representa um disco lógico, isto é, uma unidade.

---

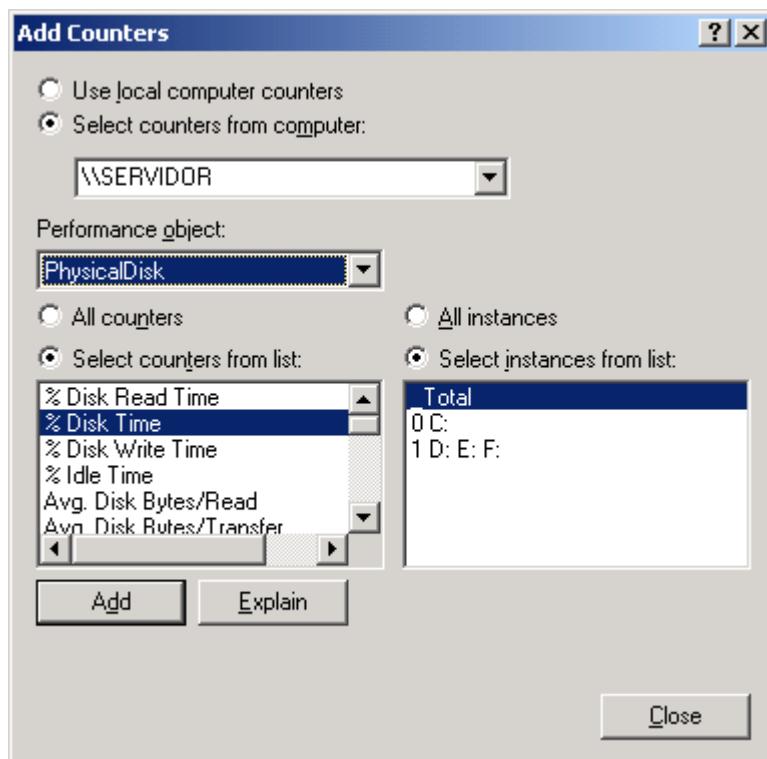
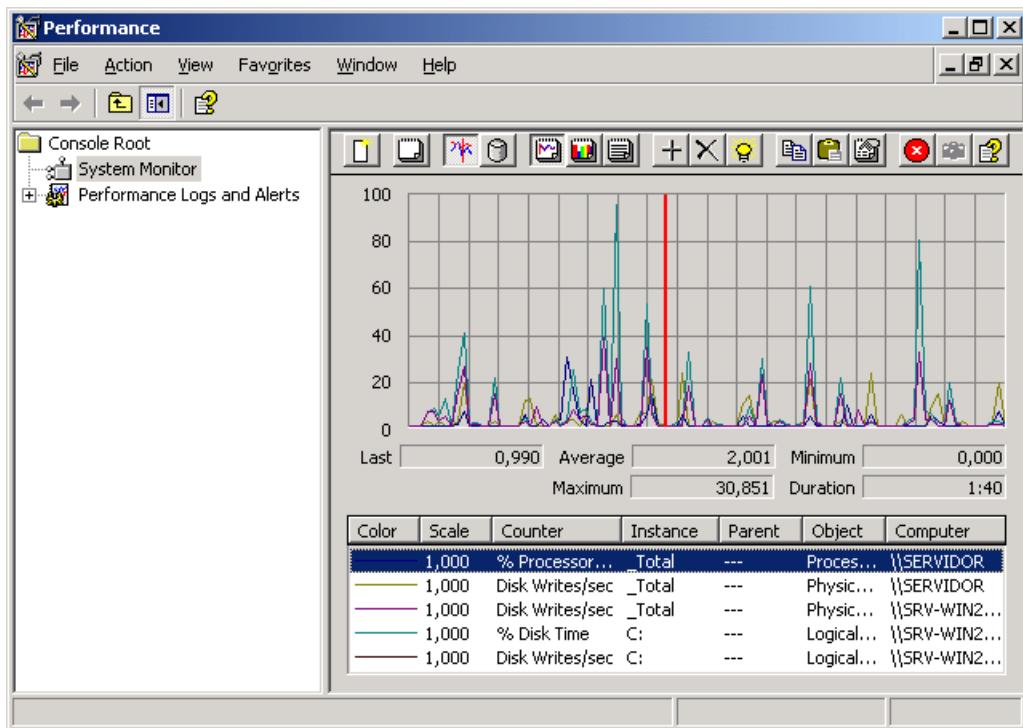


Figura 14.6 Monitorando o objeto Disco físico.

6. Na caixa de listagem Selecionar contadores na lista, selecione o contador Gravações em disco por segundo. Este contador é uma medida da freqüência das operações de gravação em disco. Ele irá indicar a atividade de gravação de informações no disco.
7. Na caixa de listagem Selecionar instâncias na lista, você tem a opção de definir se quer monitorar todos os discos físicos (\_Total), ou somente alguns deles. Esta caixa exibe todas as ocorrências do objeto Disco físico, isto é, exibe todos os discos instalados no computador. Por exemplo, para monitor apenas o Disco 0, clique na opção ‘0 C:’ para selecionar esta instância do contador Gravações em disco por segundo.
8. Dê um clique no botão Adicionar, para incluir este contador para monitoração.
9. Agora você irá monitorar a freqüência de gravação somente do volume E: Para isto, na lista Objeto de desempenho, selecione o objeto Disco lógico.
10. Na caixa de listagem Selecionar contadores na lista, selecione o contador Disk Gravações em disco por segundo.
11. Observe que na caixa de listagem da direita, é exibida uma lista com todas os volumes disponíveis. Dê um clique no volume E: (ou em um volume disponível no servidor que você está utilizando) para marcá-lo.

12. Dê um clique no botão Adicionar, para incluir este contador para monitoração.
13. Dê um clique no botão Fechar.
14. Você estará de volta ao console Desempenho, com contadores para monitorar a atividade de gravação do Disco 0 e da partição E:, conforme indicado pela Figura 11.7:



**Figura 11.7 Gráfico indicativo da atividade de gravação.**

15. A monitoração da atividade dos discos, através dos diversos contadores disponíveis é de grande importância, principalmente para servidores que atuam como servidores de disco (basicamente com compartilhamento de pastas e arquivos) ou Servidores Web para a Internet ou para uma Intranet. Normalmente o sistema de discos é a parte mais lenta do sistema. Muitas vezes pode ser necessária a atualização para discos mais rápidos ou para a implementação de níveis de RAID-5 ou RAID-10 baseados em Hardware. Porém estas utilizações somente se justificam em servidores com um volume de acesso elevado.
16. Feche o console Desempenho.

Exercício: Abra novamente o console Desempenho e monitore os seguintes contadores para o Disco físico, para o Disco 0: Leituras de disco por segundo e Transferência de disco por segundo. Utilize o botão Explicar para ver o que representa cada um destes contadores. Feche o console Desempenho.

## Contadores a serem monitorados em servidores.

Na tabela a seguir, da ajuda do Windows Server 2003, apresento uma lista de contadores que a Microsoft recomenda que sejam monitorados permanentemente nos servidores da rede.

| <b>Componente</b> | <b>Aspecto do desempenho</b> | <b>Contadores a monitorar sendo monitorado</b>   |
|-------------------|------------------------------|--|
| Disco             | Uso                          | PhysicalDisk\Leituras de disco/s<br>PhysicalDisk\Gravações de disco/s<br>LogicalDisk%\ de espaço livre   |
|                   |                              | Interprete cuidadosamente o contador % tempo de disco. Como a instância _Total desse contador pode não refletir com precisão o uso em sistemas de vários discos, é importante usar também o contador % Tempo ocioso. Observe que esses contadores não podem exibir um valor acima de 100%.           |
| Disco             | Gargalos                     | Disco físico\ Comprimento médio da fila de disco (todas as instâncias)   |
| Memória           | Uso                          | Memória\Bytes disponíveis<br>Memória\Bytes de cache  |
| Memória           | Gargalos ou vazamentos       | Memória\Páginas/s<br>Memória\Leituras de página/s<br>Memória\Falhas de transição/s<br>Memória\Bytes de pool paginável<br>Memória\Bytes de memória não-paginável  |
|                   |                              | Embora não sejam especificamente contadores do objeto Memória, as opções a seguir também são úteis para análise de memória:<br>Arquivo de paginação%\ uso (todas as instâncias)<br>Cache\Acertos de mapa de dados %<br>Servidor\Bytes de pool paginável e<br>Servidor\Bytes de memória não-paginável |
| Rede              | Taxa de transferência        | Contadores de transmissão de protocolo (varia de acordo com o protocolo de rede); para TCP/IP:<br>Interface de rede\Total de bytes/s<br>Interface de rede\Pacotes/s<br>Servidor\Total de bytes/s ou Servidor\Bytes transmitidos/s e Servidor\Bytes recebidos/s                                       |
| Processador       | Uso                          | Processador%\ tempo de processador ( todas as instâncias)  |
| Processador       | Gargalos                     | Sistema\Comprimento da fila de processador (todas as instâncias)<br>Processador\Interrupções/s<br>Sistema\Alternâncias de contexto/s   |

## Valores indicativos de limites de desempenho para contadores

Definir exatamente qual é o limite aceitável para o valor de um ou mais contadores não é uma ciência exata. Por exemplo, afirmar que sempre que a taxa de utilização do processador se mantiver em torno de 80%, por longos períodos, é um indicativo de queda no desempenho ou um indicativo de que o processador deve ser substituído, não é algo preciso. Claro que existem valores para determinados contadores que servem para disparar o alarme, isto é, servem para alertar o administrador que uma parte do sistema pode estar sendo responsável pela queda de desempenho, ou seja, pode estar sendo o que chamamos de ‘gargalo do sistema’.

Na tabela a seguir, da Ajuda do Windows Server 2003, apresento alguns valores para determinados contadores, valores estes que, pelas recomendações da Microsoft, devem servir de alerta ao administrador.

| Recurso | Objeto\Contador  | Limite sugerido                          | Comentários  |
|---------|--|--|--|
| Disco   | Disco físico\% de espaço livre   | 15%                                      |  |
|         | Disco lógico\% de espaço livre   |  |  |
| Disco   | Disco físico\% tempo de disco  | 90%                                      |  |
|         | Disco lógico\% tempo de disco  |  |  |
| Disco   | Disco físico\Leituras de disco/s,<br>Disco físico\Gravações de disco/s | Depende das especificações<br>fabricante | Verifique a taxa de<br>transferênciado<br>especificada para seus<br>discos, para ter certeza de<br>que ela não ultrapassa as<br>especificações. Em geral, os<br>discos Ultra Wide SCSI<br>podem gerenciar de 50 a<br>70 operações de E/S por<br>segundo. Observe que o<br>fato de a E/S ser seqüencial<br>ou aleatória pode ter um<br>forte efeito sobre os valores<br>de leituras de disco/s e<br>gravações de disco/s. |
| Disco   | Disco físico\Comprimento<br>da fila de disco atual                     | Número de eixos mais 2                   | Esse contador é instantâneo.<br>Observe seu valor durante<br>vários intervalos. Para obter<br>uma média ao longo do<br>tempo, use Disco físico\<br>Comprimento médio da fila<br>de disco.  |

| Recurso              | Objeto\Contador                    | Limite sugerido  | Comentários   |
|----------------------|------------------------------------|--|---|
| Memória              | Memória\Bytes disponíveis          | Para computadores com mais memória, mais de 4 MB                                 | Pesquise o uso da memória e adicione memória se necessário.   |
| Memória              | Memória\Páginas/s                  | $n$ páginas/s por arquivo de paginação   | Pesquise a atividade de paginação. Observe o volume de E/S transferido para os discos com arquivos de paginação.  |
| Arquivo de paginação | Arquivo de paginação%\ uso         | Acima de 70%   | Revise este valor juntamente com Bytes disponíveis e Páginas/s para entender a atividade de paginação do computador.  |
| Processador          | Processador%\ tempo de processador | 85%  | Descubra o processo que está usando uma alta porcentagem do tempo do processador. Atualize para um processador mais rápido ou instale um processador adicional.   |
| Processador          | Processador\Interrupções/s         | Depende do processador; um bom ponto de partida é 1.000 interrupções por segundo | Um aumento brusco no valor desse contador, sem um aumento correspondente na atividade do sistema, indica um problema de hardware. Identifique o adaptador de rede, o disco ou outro tipo de hardware que está causando as interrupções. |
| Servidor             | Servidor\Total de bytes/s          |  | Se a soma de Total de bytes/s para todos os servidores for aproximadamente igual às taxas de transferência máximas de sua rede, convém segmentar a rede.  |

| Recurso              | Objeto\Contador                                   | Limite sugerido          | Comentários  |
|----------------------|---|--------------------------|--|
| Servidor             | Servidor\Falta de itens de trabalho               | 3                        | <p>Se o valor atingir este limite, considere adicionar as entradas DWORD InitWorkItems (o número de itens de trabalho alocados para um processador durante a inicialização) ou MaxWorkItems (o número máximo de buffers de recebimento que um servidor pode alocar) ao Registro (em HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters). A entrada InitWorkItems pode variar de 1 a 512, enquanto MaxWorkItems pode variar de 1 a 65.535. Comece por qualquer valor para InitWorkItems e um valor igual a 4.096 para MaxWorkItems e dobre esses valores até que o limite de Servidor\Falta de itens de trabalho fique abaixo de 3.</p> |
| Servidor             | Servidor\Pico de pool paginável                   | Quantidade de RAM física | <p>Esse valor é um indicador do tamanho máximo do arquivo de paginação e da quantidade de memória física.</p>  |
| Servidor             | Filas de trabalho do servidor\Comprimento da fila | 4                        | <p>Se o valor atingir esse limite, poderá haver um gargalo no processador. Esse contador é instantâneo. Observe seu valor durante vários intervalos.</p>   |
| Vários processadores | Sistema\Comprimento da fila de processador        | 2                        | <p>Esse contador é instantâneo. Observe seu valor durante vários intervalos.</p>   |

Claro que estes são apenas valores sugeridos, os quais servem como alertas para o administrador. Conforme descrito anteriormente, o processo de monitoração é um processo contínuo, de acompanhamento na evolução dos principais contadores, sugeridos anteriormente.

A seguir apresento de uma forma resumida, os principais contadores e respectivos limites, ou seja, valores que podem indicar que o problema é com o respectivo componente:

- ◆ **Processador\% tempo de processador:** Não deve estar por longos períodos acima dos 80%
- ◆ **Sistema\Comprimento da fila de processador:** Não deve ser maior do que 2.
- ◆ **LogicalDisk\Comprimento da fila de disco atual:** Se este valor estiver constantemente acima de 2, o sistema de discos deve ser substituído por um sistema mais rápido. Por exemplo, se os discos forem IDE, você pode substituir por um sistema SCSI. Outra alternativa é implementar um Volume Set sem Paridade.
- ◆ **LogicalDisk\Comprimento da fila de disco atual:** Valem os mesmos comentários do item anterior.
- ◆ **Memória\Páginas/s:** Um valor maior do que 20, pode indicar a necessidade de um Upgrade de memória, normalmente com a adição de mais memória RAM.
- ◆ **Memória\Bytes confirmados:** Deve ser sempre menor do que a quantidade total de memória instalada.

## Configurando o console Desempenho para capturar dados automaticamente.

Na introdução sobre a monitoração de desempenho, falei sobre a possibilidade de configurar o console Desempenho para efetuar a captura automática de dados, conforme destacado no trecho a seguir:

*“Também é possível configurar o console Desempenho para que seja feita a captura de dados automaticamente. O administrador pode configurar o console desempenho para que sejam capturados dados sobre os Objetos/contadores a serem monitorados. Com base nesta captura, o administrador pode verificar os limites normais de operação para componentes como o Processador, memória RAM e assim por diante. Depois faz-se um monitoramento contínuo e compara-se os resultados obtidos com os limites de operação obtidos em outras medições. Quando um determinado componente começar a apresentar aumento na sua taxa de utilização o administrador deve verificar o motivo para este aumento e, se for o caso, providenciar a substituição do elemento que está apresentando elevação em suas taxas de utilização, antes que a sua taxa de utilização atinja limites que possam comprometer o desempenho do servidor.”*

Conforme pode ser concluído pelo parágrafo anterior, o principal objetivo em configurar a coleta automática de dados é para determinar quais as taxas normais de utilização dos componentes a serem monitorados, em situação normal de uso. Depois são feitas novas observações para acompanhar a evolução destas taxas de ocupação, para poder agir preventivamente quando um determinado componente estiver atingindo níveis elevados de utilização.

A captura automática de dados é feita utilizando a opção Logs e alertas de desempenho, do console Desempenho. Com esta opção, você pode coletar automaticamente dados de desempenho de computadores locais ou remotos. Você pode visualizar os dados que foram gravados no log usando a opção Monitor do sistema ou exportar os dados para programas de planilha ou banco de dados, para fins de análise e geração de relatórios. Por exemplo, você pode importar os dados gravados em um log de desempenho, para um banco de dados do Microsoft Access e utilizar estes dados para a criação de relatórios personalizados.

---

**IMPORTANTE:** Certifique-se de que você conhece os limites para os contadores da lista anterior e que entendeu o funcionamento de cada um destes contadores. Este é um ponto importante para o exame.

---

Com a opção Logs e alertas de desempenho, estão disponíveis os seguintes recursos:

- ◆ Coleta de dados em formato separado por vírgulas ou por tabulações para facilitar a importação por programas de planilha ou programas de banco de dados. É fornecido também um formato de arquivo de log binário para registro em log circular ou para registro em log de instâncias, como segmentos ou processos, que podem começar depois do início da coleta de dados. (O registro em log circular é o processo de registro contínuo de dados em um único arquivo, sobrepondo os dados anteriores com novos dados.)
  - ◆ Você também pode coletar dados em formato de banco de dados SQL. Essa opção define o nome de um banco de dados SQL e conjunto de logs existentes dentro do banco de dados em que os dados de desempenho serão lidos ou gravados. Esse formato de arquivo é útil ao coletar e analisar dados de desempenho de toda a empresa, em vez de servidor por servidor. Por exemplo, a partir de um único console Desempenho, você pode obter dados sobre diversos servidores da rede e armazenar estes dados centralizadamente em um único banco de dados do SQL Server.
  - ◆ Os dados do contador coletados podem ser visualizados durante a coleta ou após seu término.
- Como o log funciona da mesma maneira que um serviço do Windows Server 2003, a coleta de dados ocorre independentemente de haver um usuário logado ou não, no servidor que está sendo monitorado.
- ◆ Você pode definir os momentos de início e parada, nomes de arquivos, tamanho máximo de arquivo e outros parâmetros para a geração automática do log.
  - ◆ Você pode gerenciar várias sessões de log em uma única janela de console.
  - ◆ Você pode definir um alerta em um contador, especificando que uma mensagem seja enviada, um programa seja executado e uma entrada seja feita no log de eventos do Windows Server 2003 ou um log seja iniciado quando o valor do contador selecionado for superior ou inferior a uma configuração especificada. Por exemplo, você pode monitorar a taxa de utilização do processador e solicitar que o Administrador seja avisado quando esta taxa ultrapassar um determinado patamar, digamos 85 %, ou você pode monitorar o espaço livre em todas as unidades de disco ou em todos os volumes, de todos os servidores da rede e pedir que seja disparado um alerta para o administrador, sempre que uma unidade apresentar espaço livre inferior a 20%.

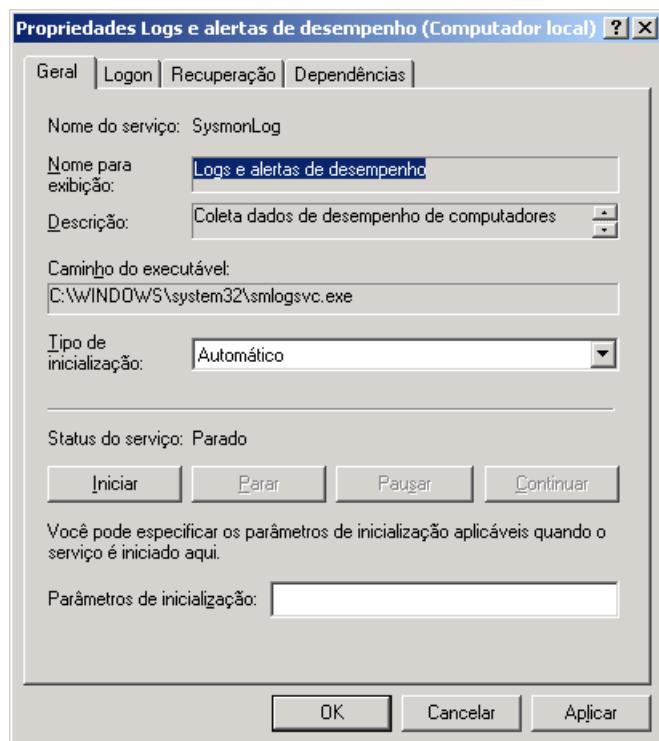
Exemplo: Verificando as opções de configuração e inicialização do serviço “Logs e alertas de desempenho”.

1. Faça o logon como Administrador ou com uma conta com permissão de administrador..
2. Abra o console Serviços que está disponível no menu Ferramentas administrativas.
3. Localize o serviço Logs e alertas de desempenho e verifique o valor indicado na coluna Tipo de inicialização. Se o valor desta coluna estiver em Manual, significa que o serviço não está sendo inicializado automaticamente. Se for este o caso, dê um clique duplo no serviço para exibir a janela com as propriedades do serviço.

**IMPORTANTE:** Lembre-se que quando houver a necessidade de capturar dados de desempenho de diversos servidores e consolidar estas dados em um único banco de dados, a opção mais indicada é fazer com que os dados obtidos, sejam gravados em um banco de dados do SQL Server 2000.

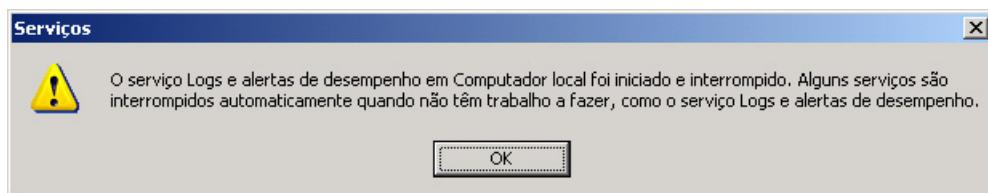
**NOTA:** Para que a coleta de dados possa funcionar corretamente, o serviço “Logs e alertas de desempenho” deve ter sido inicializado corretamente. Antes de prosseguir você irá verificar (no exemplo logo a seguir) se este serviço está configurado para inicialização automática. Caso não esteja, irá configurá-lo para que seja inicializado automaticamente.

4. Na janela de propriedades do serviço, na guia Geral, altere o tipo de inicialização para Automática, conforme indicado na Figura 11.8:



**Figura 11.8 Configurando o serviço Logs e alertas de desempenho para iniciar automaticamente.**

5. Clique no botão Iniciar para fazer com que o serviço seja inicializado imediatamente.  
6. Surge a mensagem indicada na Figura 11.9:



**Figura 11.9 Mensagem sobre o serviço Logs e alertas de desempenho.**

Esta mensagem informa que o serviço foi inicializado e encerrado, pois no momento não existe nenhuma coleta de dados em andamento. Porém o Windows Server 2003 irá iniciar o serviço automaticamente, quando uma coleta de dados for configurada. O Windows Server 2003 detecta que o serviço deve estar ativo para que a coleta de dados possa ser feita e inicializa o serviço automaticamente.

7. Clique em OK para fechar a mensagem de aviso. Você estará de volta à janela de propriedades do serviço. Clique em OK para fecha-la.  
8. Feche o console Serviços.

Uma vez estando configurado corretamente o serviço Logs e alertas de desempenho, temos à disposição às seguintes funcionalidades:

- ◆ Iniciar e parar o log manualmente, por demanda ou automaticamente, com base em um agendamento definido pelo usuário.
- ◆ Definir configurações adicionais para log automático, como renomear o arquivo automaticamente e definir parâmetros para parar ou iniciar um log com base no tempo decorrido ou no tamanho do arquivo.
- ◆ Criar logs de rastreamento. Usando o provedor de dados do sistema padrão do Windows Server 2003 ou outro provedor de aplicativos, os logs de rastreamento registram detalhadamente os eventos de aplicativos do sistema, quando ocorrem certas atividades, como uma operação de entrada/saída (E/S) de disco ou uma falha de página. Quando o evento ocorre, o Windows Server 2003 registra os dados em um arquivo de log especificado pelo serviço de logs e alertas de desempenho. Isso difere da operação dos logs de contadores. Quando eles estão em uso, o serviço obtém dados do sistema no fim do intervalo de atualização, em vez de esperar por um evento específico. Uma ferramenta de análise é necessária para interpretar o resultado do log de rastreamento.
- ◆ Definir um programa que seja executado quando um log for parado. Por exemplo, você pode configurar que seja executado um script que copia os arquivos com os dados para um drive da rede, onde o arquivo será importado em um banco de dados. O script também pode ser configurado para enviar uma mensagem para o Administrador.

Agora você acompanhará alguns exemplos práticos de coleta de dados.

Exemplo 1: Configurar o serviço de logs e alertas para monitorar a taxa de ocupação do Processador. Serão monitorados os seguintes contadores:

- ◆ % tempo de processador
- ◆ Interrupções/s

Os dados deverão ser obtidos em intervalos de 05 segundos e salvos em um arquivo do tipo texto. Os dados deverão ser gravados no arquivo C:\Monitora o processador\_000001.csv.

Para fazer o acompanhamento proposto e gerar o arquivo de log, siga as seguintes etapas:

1. Faça o logon como Administrador, ou com uma conta com permissão de administrador.
2. Abra o console Desempenho: Iniciar -> Ferramentas administrativas -> Desempenho.
3. No painel da esquerda, clique no sinal de + ao lado da opção Logs e alertas de desempenho. Serão exibidas as opções indicadas na Figura 11.10.

**NOTA:** Se você desejar exportar dados do log para o Microsoft Excel, o serviço de logs e alertas de desempenho deverá ser parado, porque o Microsoft Excel exige acesso exclusivo ao arquivo de log. Não há informações sobre outros programas que exijam esse acesso exclusivo. Portanto, você geralmente pode trabalhar com dados de um arquivo de log enquanto o serviço estiver coletando dados para esse arquivo. Para parar o serviço de logs e alertas utilize o console Serviços, conforme descrito no exemplo anterior.

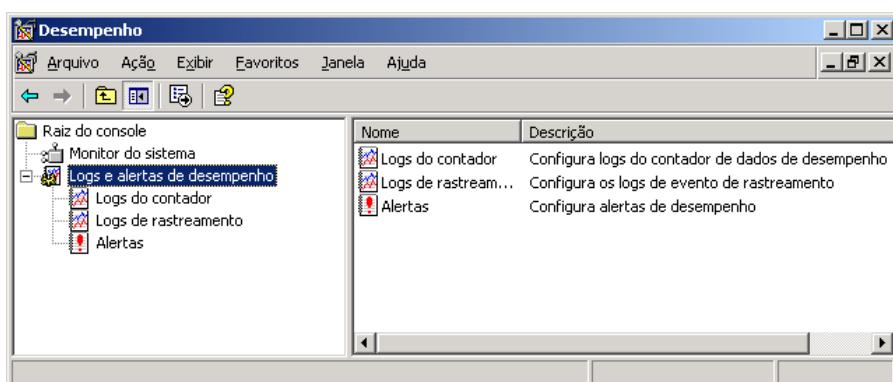


Figura 11.10 Opções de configuração para logs e alertas de desempenho.

4. Clique na opção Logs do contador. Observe que, por padrão, já existe um log configurado. Este log, chamado Visão geral do sistema, coleta dados de um conjunto de objetos/contadores, os quais fornecem uma visão geral do desempenho do servidor. Você pode iniciar a coleta de dados para este log, clicando nele para marcá-lo e depois selecionando o comando Ação -> Iniciar ou clicando no botão Iniciar (botão com o desenho de um pequeno triângulo para a direita).
5. Neste exemplo você irá criar um novo log. Para criar um novo log clique na opção Logs do contador e selecione o comando Ação -> Novas configurações de log. Surge uma janela solicitando o nome do novo Log. Digite Monitora o processador, conforme indicado na Figura 11.11 e clique em OK.

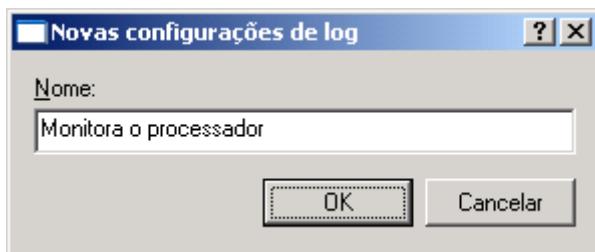


Figura 11.11 Definindo um nome para o novo log.

Surge a janela Monitora o processador, na qual nos temos as seguintes guias:

- ◆ **Geral:** Esta guia é utilizada para definir quais objetos/contadores farão parte do log, definir uma descrição para o log, definir o intervalo de coleta dos dados e definir se o log executará no contexto do usuário padrão do sistema ou no contexto de uma conta de usuário específica.
- ◆ **Arquivos de log:** Nesta guia você define o formato para o arquivo de log, a forma de nomeação dos arquivos, um comentário e se os arquivos existentes devem ser sobreescritos ou mantidos. Você somente poderá acessar esta guia se tiver adicionado pelo menos um objeto ou contador, usando a guia Geral.
- ◆ **Agendar:** Nesta guia o administrador pode definir um agendamento para a coleta. Por exemplo, de segunda a sexta-feira, das 8:00 as 18:00.

---

**NOTA:** Não pode haver nenhum log selecionado, senão a opção Novas configurações de log..., não será exibida no menu Ação. Se esta opção não estiver sendo exibida, clique novamente na opção Logs do contador, no painel da esquerda. Isso fará com que qualquer log que esteja marcado, seja desmarcado.

---

Agora você adicionará os contadores % tempo de processador e Interrupções/s, do objeto Processador.

6. Clique na guia Geral. Clique no botão Adicionar contadores... Será exibida a janela Adicionar contadores que você já utilizamos nos exemplos anteriores. Adicione os contadores % tempo de processador e Interrupções/s, do objeto Processador e clique em Fechar.
7. No campo Intervalo, defina um intervalo de 5 segundos para a coleta dos dados. A guia Geral deve estar conforme indicado na Figura 11.12:

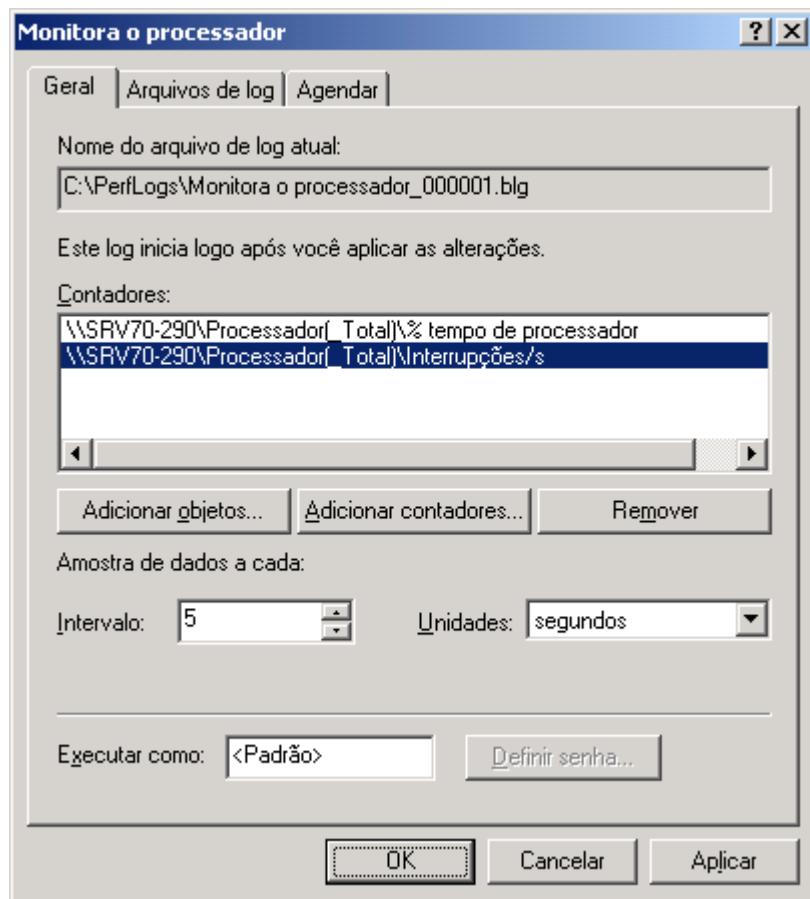


Figura 11.12 Configurações da guia Geral, para o exemplo proposto.

8. Clique na guia Arquivos de log. Para o formato selecione Arquivo de texto (delimitado por vírgulas). Clique no botão Configurar... para definir o local onde será criado o arquivo de log e um tamanho máximo.
9. Ao clicar no botão Configurar será exibida a janela Configurar Arquivos de log. Defina as configurações indicadas na Figura 11.13:

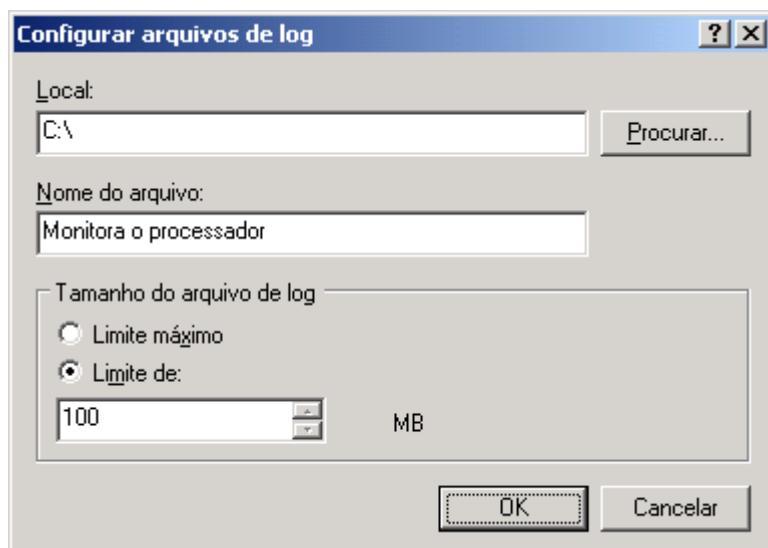


Figura 11.13 Definindo configurações para o arquivo de log.

10. Clique em OK para fechar a janela Configurar arquivos de log.
11. Você estará de volta à guia Arquivos de log. Clique na guia Agendar.
12. Defina um agendamento para que a coleta seja iniciada e encerrada. Por exemplo, configure o log para iniciar em uma data e horário específicos, conforme exemplo indicado na Figura 11.14. Nesta guia você também pode definir o que deve ser feito, caso o arquivo de log atinja o seu tamanho máximo. Estão disponíveis as seguintes opções: Iniciar um novo arquivo de log ou Executar este comando.

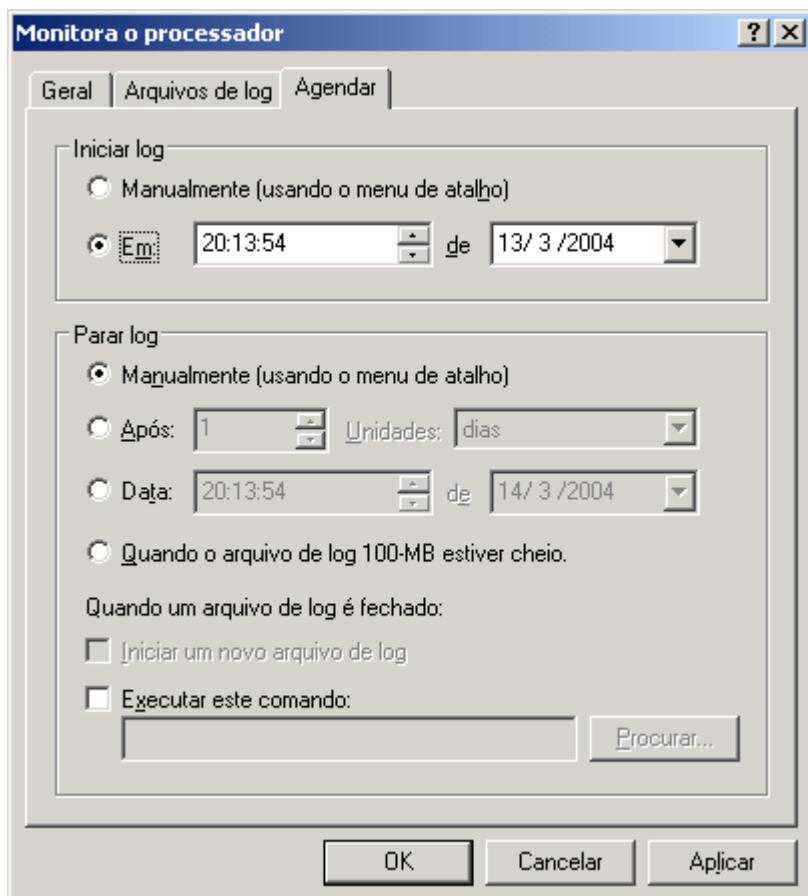


Figura 11.14 Definindo um agendamento para a coleta de dados.

13. Clique em OK. Você estará de volta ao console Desempenho. O log Monitora o processador foi criado e iniciará a coleta de dados no horário determinado, conforme configurações definidas na guia Agendar. Observe que o log Monitora o processador já aparece na lista de logs, juntamente com o log Visão geral do sistema, sendo que este último é automaticamente criado pelo Windows Server 2003, conforme descrito anteriormente.
14. O administrador pode fazer com que o log inicie a coleta de dados imediatamente, independente do agendamento definido. Para isso clique no log Monitora o processador para marcá-lo e selecione o comando Ação -> Iniciar.
15. O log será inicializado e os dados começarão a ser capturados e salvos no arquivo C:\Monitora o processador\_000001.csv. Aguarde uma meia-hora para que o Windows Server 2003 possa coletar uma boa quantidade de dados. Observe que após ser inicializado, o pequeno ícone, ao lado do nome do log alterna para a cor verde. Este é um indicativo de que o log está em execução.

---

**NOTA:** Se você precisar alterar alguma configuração de um log, basta dar um clique duplo no respectivo log que será exibida a janela com as propriedades do log, onde você terá acesso às guias Geral, Arquivos de log e Agendar.

16. Para suspender a execução do log e a coleta dos dados, basta clicar no log a ser suspenso e depois selecionar o comando Ação -> Parar. Você também pode clicar com o botão direito do mouse no log e, no menu que é exibido, clicar na opção Parar.

17. Após meia-hora de coleta, suspenda a execução do log.

Agora vamos analisar os dados obtidos, os quais foram gravados no arquivo C:\Monitora o processador\_000001.csv.

18. Feche o console desempenho.

Exemplo 2: Analisando os dados obtidos com o log Monitora o processador, criado no exemplo anterior.

Para abrir o arquivo com os dados obtidos, faça o seguinte:

1. Faça o logon como Administrador ou com uma conta do tipo Administrador do computador.
2. Abra o Bloco de notas.
3. Abra o arquivo C:\Monitora o processador\_000001.csv.
4. Na listagem a seguir temos uma amostra dos dados de monitoração que foram salvos:

“05/01/2002 16:31:04.511”,”99.99991106930112”,”237.43538236310363”,”Monitora o processador”  
“05/01/2002 16:31:09.518”,”3.0029057285789862”,”281.7091259002674”,”Monitora o processador”  
“05/01/2002 16:31:14.526”,”2.2029296933507747”,”250.63934155863382”,”Monitora o processador”  
“05/01/2002 16:31:19.533”,”2.6029177109648804”,”240.65353587347821”,”Monitora o processador”  
“05/01/2002 16:31:24.540”,”2.0029356845437163”,”233.86324638545705”,”Monitora o processador”  
“05/01/2002 16:31:29.548”,”1.0029656405084575”,”230.06868469153261”,”Monitora o processador”  
“05/01/2002 16:31:34.555”,”2.6029177109648804”,”236.65902223849881”,”Monitora o processador”  
“05/01/2002 16:31:39.562”,”3.0029057285789862”,”245.64630670524917”,”Monitora o processador”  
“05/01/2002 16:31:44.570”,”1.0029656405084575”,”232.46519458083583”,”Monitora o processador”  
“05/01/2002 16:31:49.577”,”18.602438415529178”,”298.36987599426584”,”Monitora o processador”  
“05/01/2002 16:31:54.584”,”31.602048987987665”,”277.20116678260399”,”Monitora o processador”  
“05/01/2002 16:31:59.592”,”3.0029057285789862”,”237.8575213706925”,”Monitora o processador”  
“05/01/2002 16:32:04.599”,”3.4028937461930919”,”238.45647244632733”,”Monitora o processador”  
“05/01/2002 16:32:09.607”,”2.0029356845437163”,”232.46529833970988”,”Monitora o processador”  
“05/01/2002 16:32:14.614”,”2.4029237021578331”,”233.66353396326622”,”Monitora o processador”  
“05/01/2002 16:32:19.621”,”2.4029237021578331”,”235.86035744808296”,”Monitora o processador”  
“05/01/2002 16:32:24.629”,”1.2029596493155048”,”229.66911893931493”,”Monitora o processador”  
“05/01/2002 16:32:29.636”,”2.8029117197719389”,”237.45805673646964”,”Monitora o processador”  
“05/01/2002 16:32:34.643”,”1.802941675736669”,”235.46093262598629”,”Monitora o processador”  
“05/01/2002 16:32:39.651”,”2.6029177109648804”,”235.26065580456452”,”Monitora o processador”  
“05/01/2002 16:32:44.658”,”2.8029117197719389”,”240.25447283770185”,”Monitora o processador”  
“05/01/2002 16:32:49.665”,”6.6027978871059485”,”330.12472597415723”,”Monitora o processador”  
“05/01/2002 16:32:54.673”,”4.4028637902283618”,”238.25672027892747”,”Monitora o processador”  
“05/01/2002 16:32:59.680”,”3.6028877550001503”,”239.85475287258555”,”Monitora o processador”  
“05/01/2002 16:33:04.687”,”2.2029296933507747”,”235.26124646664911”,”Monitora o processador”

**NOTA:** Além do menu Ação, você também pode utilizar o botão direito do mouse, clicando no respectivo log, para ter acesso aos comandos Iniciar e Parar. Na barra de ferramentas do console Desempenho, existe o botão Iniciar - botão com o desenho de um pequeno triângulo e o botão Parar - botão com o desenho de um pequeno quadrado.

“05/01/2002 16:33:09.695”,”3.0029057285789862”,”248.0428006830586”,”Monitora o processador”  
“05/01/2002 16:33:14.702”,”1.6029476669296105”,”234.86158573592209”,”Monitora o processador”  
“05/01/2002 16:33:19.709”,”1.802941675736669”,”240.8528989677138”,”Monitora o processador”  
“05/01/2002 16:33:24.717”,”1.6029476669296105”,”237.05892288973411”,”Monitora o processador”  
“05/01/2002 16:33:29.724”,”3.0029057285789862”,”237.25834432542132”,”Monitora o processador”  
“05/01/2002 16:33:34.731”,”2.6029177109648804”,”241.45210288853528”,”Monitora o processador”  
“05/01/2002 16:33:39.739”,”2.8029117197719389”,”242.45101580959104”,”Monitora o processador”  
“05/01/2002 16:33:44.746”,”2.2029296933507747”,”243.8488266800569”,”Monitora o processador”  
“05/01/2002 16:33:49.754”,”0.80297163170139907”,”238.05704786936531”,”Monitora o processador”  
“05/01/2002 16:33:54.761”,”2.4029237021578331”,”237.05864514051027”,”Monitora o processador”  
“05/01/2002 16:33:59.768”,”3.2028997373860446”,”238.65630457220965”,”Monitora o processador”  
“05/01/2002 16:34:04.776”,”2.0029356845437163”,”234.06288045367026”,”Monitora o processador”  
“05/01/2002 16:34:09.783”,”2.8029117197719389”,”236.06013571127014”,”Monitora o processador”  
“05/01/2002 16:34:14.790”,”3.6028877550001503”,”240.25373559434755”,”Monitora o processador”  
“05/01/2002 16:34:19.798”,”3.6028877550001503”,”239.45538124481718”,”Monitora o processador”  
“05/01/2002 16:34:24.805”,”1.802941675736669”,”234.46240981460366”,”Monitora o processador”  
“05/01/2002 16:34:29.812”,”2.8029117197719389”,”235.86018637754623”,”Monitora o processador”  
“05/01/2002 16:34:34.820”,”3.8028817638072088”,”291.58010386253267”,”Monitora o processador”  
“05/01/2002 16:34:39.827”,”2.0029356845437163”,”234.66201751967793”,”Monitora o processador”  
“05/01/2002 16:34:44.834”,”2.4029237021578331”,”236.85895914831343”,”Monitora o processador”  
“05/01/2002 16:34:49.842”,”3.2028997373860446”,”239.8546458154506”,”Monitora o processador”  
“05/01/2002 16:34:54.849”,”3.0029057285789862”,”238.85597698173174”,”Monitora o processador”  
“05/01/2002 16:34:59.856”,”3.2028997373860446”,”242.65053880935429”,”Monitora o processador”  
“05/01/2002 16:35:04.864”,”2.6029177109648804”,”241.85174327309008”,”Monitora o processador”  
\*\*\*\*\*

A listagem apresenta dados para cerca de 4 minutos, com início em 16:31:04.511 e término em 16:35:04.864. A primeira coluna representa o horário da coleta do dado, a segunda coluna é o valor correspondente ao contador % tempo do processador, a terceira coluna é o valor correspondente ao contador Interrupções/s. A quarta e última coluna é o nome do log, nome este que é definido pelo usuário quando da criação do log, conforme visto anteriormente.

Observe que existe um intervalo de 5 segundos entre uma linha e outra, que é exatamente o intervalo que você configurou no exemplo de criação do log.

##### 5. Feche o Bloco de Notas.

Com os dados no formato .csv, você pode importá-los facilmente para o Excel ou para o Access, para fazer uma série de análises, usando as ferramentas destes programas. Por exemplo, você pode utilizar os dados para calcular a taxa média de ocupação do processador, ou o número médio de interrupções por segundo. O formato .csv pode ser aberto diretamente no Excel e é facilmente importado pelo Microsoft Access.

A seguir coloco uma lista resumida (em relação a lista apresentada anteriormente) dos contadores mais comumente utilizados para verificação do desempenho do computador como um todo e que são candidatos a serem configurados para coleta automática, utilizando logs de desempenho. Esta lista é obtida na documentação oficial do Windows Server 2003.

Contadores para identificar gargalos em recursos de memória:

- ◆ Memória\Bytes disponíveis
- ◆ Memória\Páginas/s

Contadores para identificar gargalos em recursos de disco:

- ◆ PhysicalDisk -> % tempo de disco e % Tempo ocioso
- ◆ PhysicalDisk -> Leituras de disco/seg e Gravações de disco/seg
- ◆ PhysicalDisk -> Comprimento médio da fila de disco
- ◆ LogicalDisk -> % de espaço livre

Contadores para identificar gargalos em recursos do processador:

- ◆ Processador -> Interrupções por segundo
- ◆ Processador -> % tempo de processador
- ◆ Processo(processo) -> % tempo de processador
- ◆ Sistema -> Comprimento da fila de processador

Contadores para identificar gargalos em recursos de rede:

- ◆ Interface de rede -> Total de bytes/segundo, Bytes enviados/s e Bytes recebidos/s
- ◆ Objeto\_de\_camada\_de\_protocolo -> Segmentos recebidos/s, Segmentos enviados/s, Quadros enviados/s e Quadros recebidos/s
- ◆ Servidor -> Total de bytes/segundo, Bytes recebidos/s e Bytes enviados/s

Contadores para identificar gargalos em recursos de impressora:

- ◆ Fila de impressão -> Bytes impressos/s
- ◆ Fila de impressão -> Erros de trabalhos

## Montando gráficos de desempenho a partir de informações de arquivos de log.

É possível utilizar o console Desempenho para acessar as informações gravadas em um arquivo de log, como o que criamos no exemplo anterior. Ao abrir o arquivos podemos especificar para quais contadores queremos montar o gráfico. Quando abrimos um arquivo de log, evidentemente, somente estarão disponíveis os contadores para os quais foram salvas informações no arquivo.

Vamos a um exemplo prático, onde acessaremos informações do arquivo C:\Monitora o processador\_000001.csv, criado no exemplo anterior.

Exemplo: Acessando os dados de um arquivo de log já existente.

**IMPORTANTE:** Monitore contadores de memória para determinar se a paginação excessiva está sobrecarregando o disco. Quando o computador tem pouca memória, o Windows Server 2003 é obrigado a utilizar intensivamente o arquivos de paginação (Swap). O arquivo de trocas fica na raiz do disco C:, com o nome de pagefile.sys ou pode também ficar em outros discos e até mesmo distribuídos em dois ou mais discos, conforme configurações efetuadas pelo administrador. Com o uso intenso do arquivo de trocas, as taxas de utilização do disco rígido aumentam significativamente, porém o problema não é com o sistema de discos e sim devido a falta de memória (que é a causa da paginação excessiva). Ao acrescentar mais memória RAM, você irá reduzir a utilização do arquivo pagefile.sys e, consequentemente, reduzir as taxas de utilização do disco rígido.

**NOTA:** Um número muito elevado de Interrupções por segundo pode ser causado por problemas em um dispositivo de Hardware, ou em um driver de hardware, conforme descrito anteriormente.

Para acessar os dados do arquivo C:\Monitora o processador\_000001.csv, siga os seguintes passos:

1. Faça o logon como Administrador, ou com uma conta com permissão de administrador.
2. Abra o console Desempenho: Iniciar -> Ferramentas administrativas -> Desempenho.
3. Será aberto o console de monitoração de desempenho, com alguns indicadores já adicionados, conforme descrito anteriormente.
4. Para limpar as configurações atuais clique no botão Novo conjunto de contadores, que é o primeiro botão da barra de ferramentas ou pressione Ctrl+E. Todos os contadores serão excluídos. Agora você irá carregar o arquivo de log C:\Monitora o processador\_000001.csv, criado anteriormente.
5. Clique no botão Exibir dados de logs, que é o quarto botão da esquerda para a direita, na barra de ferramentas, ou pressione Ctrl+L. Será exibida a janela Propriedades do Monitor do sistema, com a guia Fonte já selecionada. Você utiliza a guia Fonte para informar o arquivo de log a ser carregado.
6. Na guia Fonte clique na opção Arquivos de log e depois clique no botão Adicionar... Será aberta a janela Selecionar Arquivo de Log. Selecione o arquivo C:\Monitora o processador\_000001.csv, conforme indicado na Figura 11.15:

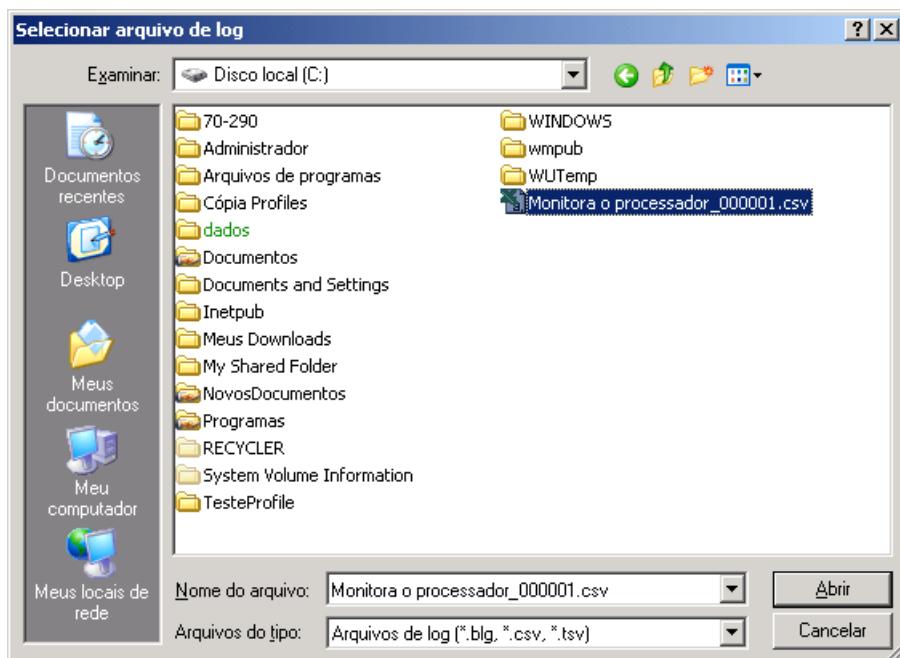


Figura 11.15 Selecionando o arquivo de log a ser carregado.

7. Clique no botão Abrir. Você estará de volta a guia Fonte, com o arquivo C:\Monitora o processador\_000001.csv já selecionado.
8. Clique em OK e o arquivo de log será carregado. Por padrão ainda não estão sendo exibidas informações sobre os contadores do arquivo de log. Esta é a próxima etapa, dentre os contadores que existem no arquivo de log, para qual ou quais queremos exibir informações??
9. Clique no botão Adicionar - botão com um sinal de + ou pressione Ctrl+I. Será exibida a janela Adicionar contadores. Abra a lista objeto de desempenho. Observe que somente aparece o objeto Processador. Isto acontece porque, no arquivo de log que abrimos, somente existem informações sobre os contadores % tempo do processador e Interrupções/s do objeto Processador.
10. Na lista Seleccione contadores da lista, selecione o contador % tempo do processador e clique no botão Adicionar.

- Clique em Fechar.
- Você estará de volta ao console Desempenho. Observe que foi montado um gráfico com os valores do contador % tempo do processador Time, para o período contido no arquivo de log, que conforme podemos observar na Figura 11.16 é de 20 minutos e 1 segundo.

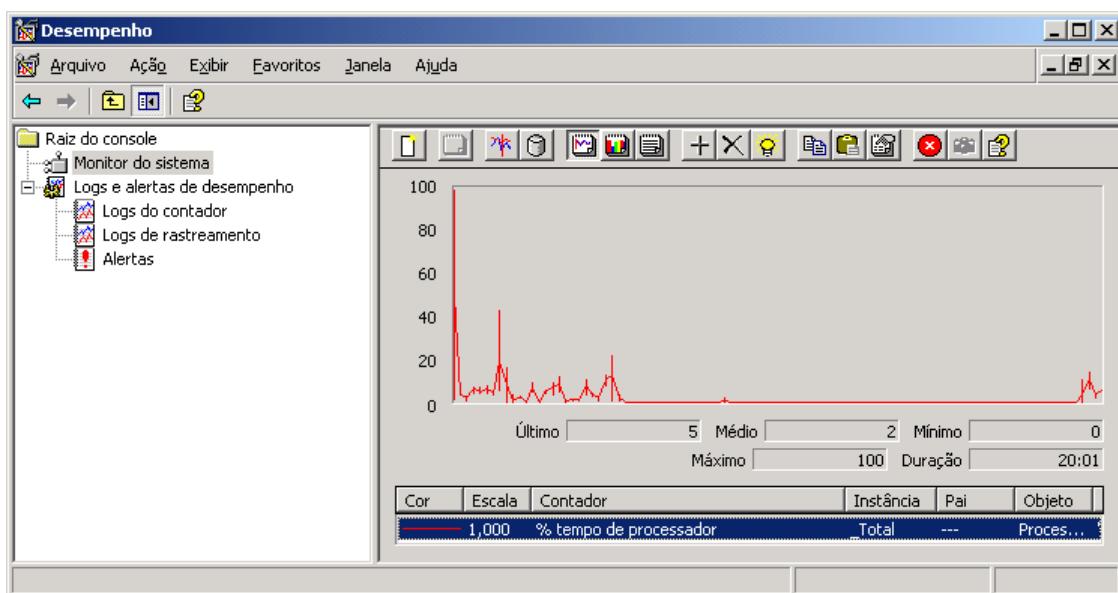


Figura 11.16 Gráfico montado com informações do arquivo de log.

Você pode fazer com que o gráfico seja baseado apenas em um determinado período e não em toda a janela de tempo do arquivo de log. Agora você aprenderá a limitar o período de tempo no qual o gráfico é baseado.

- Clique com o botão direito do mouse em qualquer parte do gráfico. No menu de opções que é exibido clique em Propriedades.

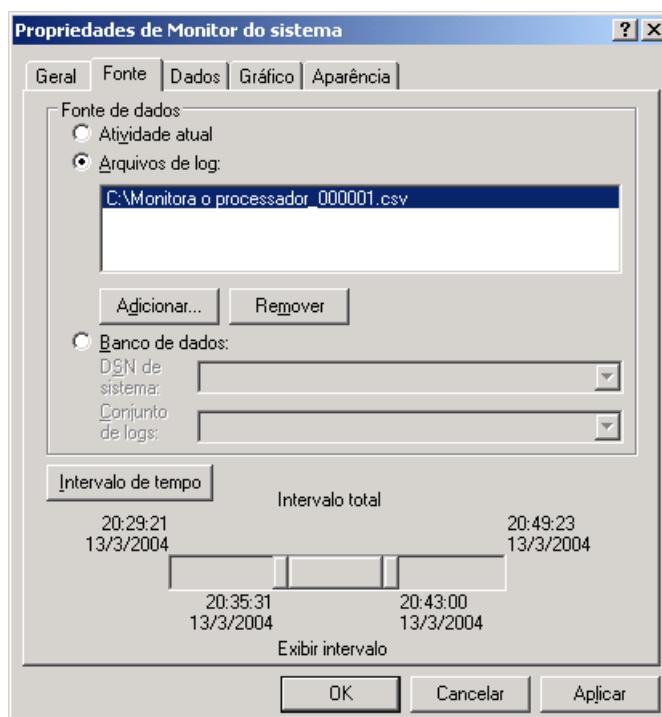
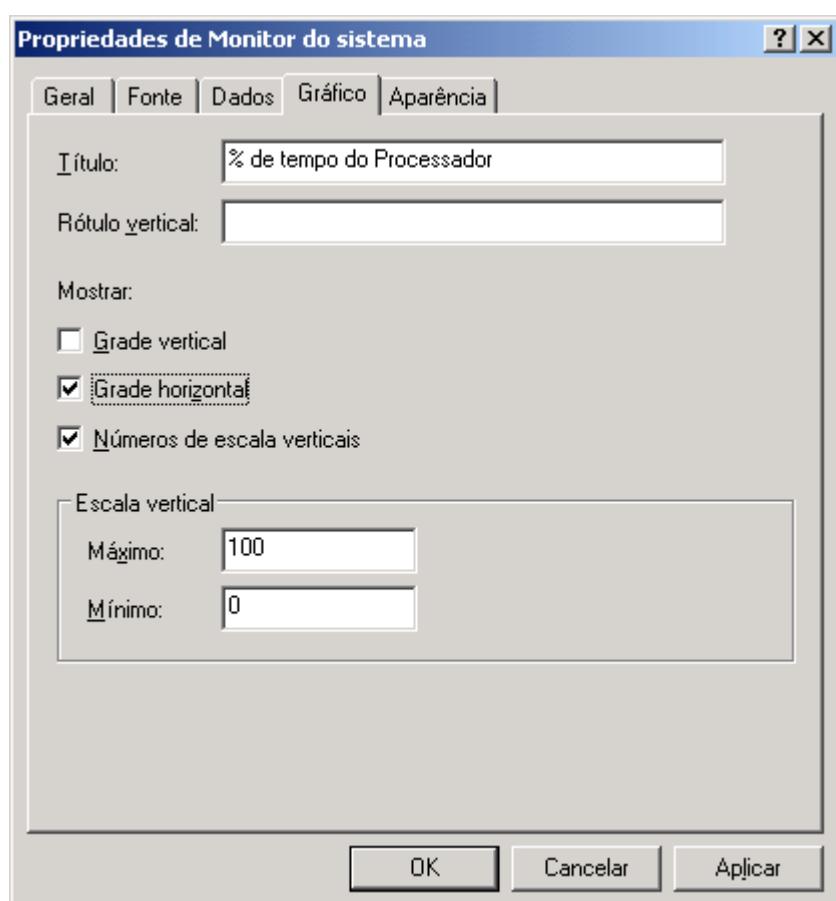


Figura 11.17 Definindo uma janela de tempo.

14. Na janela de propriedades que é exibida, dê um clique na guia Fonte.
15. Na parte de baixo da janela existem dois controles deslizantes, que você pode deslocar para definir uma janela de tempo na qual o gráfico será baseado, conforme exemplo da Figura 11.17.
16. Defina uma janela de tempo e clique em OK.
17. Você estará de volta ao console Desempenho.
18. Observe que o período dos dados já foi limitado, conforme pode ser conferido no campo Duração, nos campos logo abaixo do gráfico.
19. Agora você irá configurar algumas propriedades do gráfico.
20. Clique com o botão direito do mouse em qualquer parte do gráfico. No menu de opções que é exibido clique em Propriedades.
21. Na janela de propriedades que é exibida, dê um clique na guia Gráfico. Nesta guia você pode definir um título para o gráfico, se serão exibidas grades verticais e horizontais, bem como definir a escala do eixo vertical. Defina as opções conforme indicado na Figura 11.18:



**Figura 11.18 Configurando opções do gráfico.**

22. Clique em OK e observe que as alterações já são aplicadas ao gráfico.
23. Veja que o gráfico fica com um aspecto bem melhor, conforme indicado na Figura 11.19:

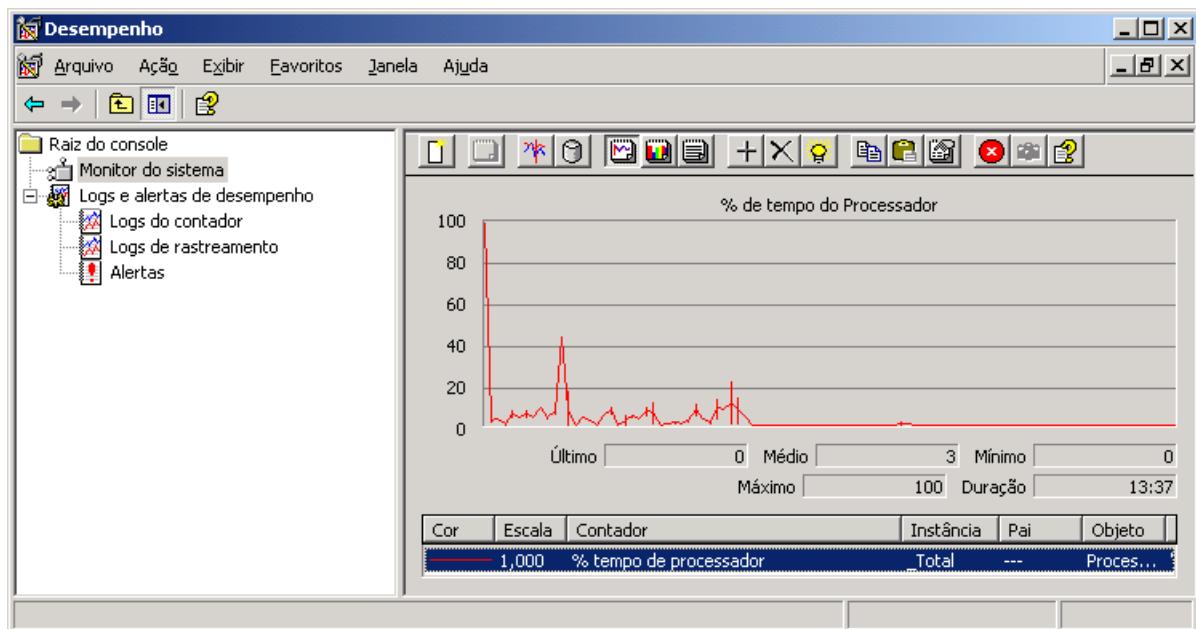


Figura 11.19 O gráfico após as formatações.

24. Feche o console Desempenho.

## Utilizando Alertas para monitorar situações limite.

O administrador pode configurar alertas com base em contadores de desempenho. Por exemplo, posso configurar um alerta que é disparado sempre que um determinado contador atinge um valor limite. Podem ser configuradas diferentes ações como resposta a um alerta: Enviar uma mensagem para um usuário, normalmente o Administrador, Gravar um evento no log de eventos do Windows Server 2003, executar um programa ou iniciar a captura de dados de desempenho, com base nas configurações de um log pré-definido.

A seguir apresento um exemplo prático de criação de um alerta com base no valor limite de um contador.

**Exemplo:** Criar um alerta que será disparado sempre que o contador % tempo do processador ultrapassar 5%. Como resposta ao alerta, uma mensagem deve ser enviada para o usuário Administrador.

Para criar o alerta proposto siga os seguintes passos indicados a seguir:

1. Faça o logon como Administrador, ou com uma conta com permissão de administrador.
2. Abra o console Desempenho: Iniciar -> Ferramentas administrativas -> Desempenho.
3. No painel da esquerda, clique no sinal de + ao lado da opção Logs e alertas de desempenho.
4. Clique na opção Alertas. Observe que, por padrão, nenhum Alerta é criado.
5. Vou criar um novo Alerta para monitorar o contador % tempo de processador.
6. Para criar um novo Alerta selecione o comando Ação -> Novas configurações de alerta...

---

**NOTA:** Evidentemente que 5% é um valor muito baixo. Estou utilizando este valor apenas para forçar que o alerta seja disparado e com isso você possa conferir se a mensagem está realmente sendo enviada para o Administrador.

---

7. Surge uma janela solicitando que você digite um nome para o Alerta que está sendo criado. Digite Alerta-Teste, conforme indicado na Figura 11.20 e clique em OK.

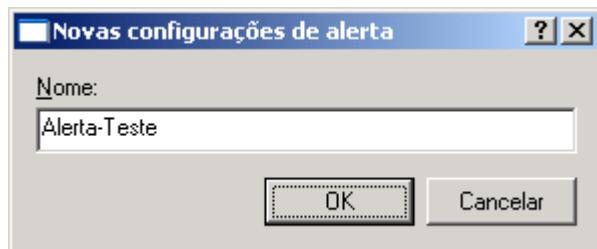


Figura 11.20 Definindo o nome do Alerta que está sendo criado.

8. Será exibida a janela Alerta-Teste com as guias Geral, Ação e Agendar, na qual você define as características do Alerta que está sendo criado.
9. O primeiro passo é adicionar o contador (ou os contadores) que serão monitorados. Na guia Geral dê um clique no botão Adicionar... Será exibida a janela Adicionar contadores, a qual já foi utilizada em exemplos anteriores. Na lista de objetos selecione Processador e na lista de contadores selecione % tempo de processador. Clique no botão Adicionar e depois clique no botão Fechar. Você estará de volta à guia Gera) da janela do alerta.
10. Na guia Geral você também pode definir um comentário e o valor limite para o contador que foi adicionado. No nosso exemplo digite 5, no campo Limite e certifique-se de que na lista Alertar quando o valor for, esteja selecionado Superior a. Com isso estou configurando o alerta para ser disparado quando o contador % tempo de processador atingir um valor superior a 5%. Suas configurações devem estar conforme indicado na Figura 11.21:

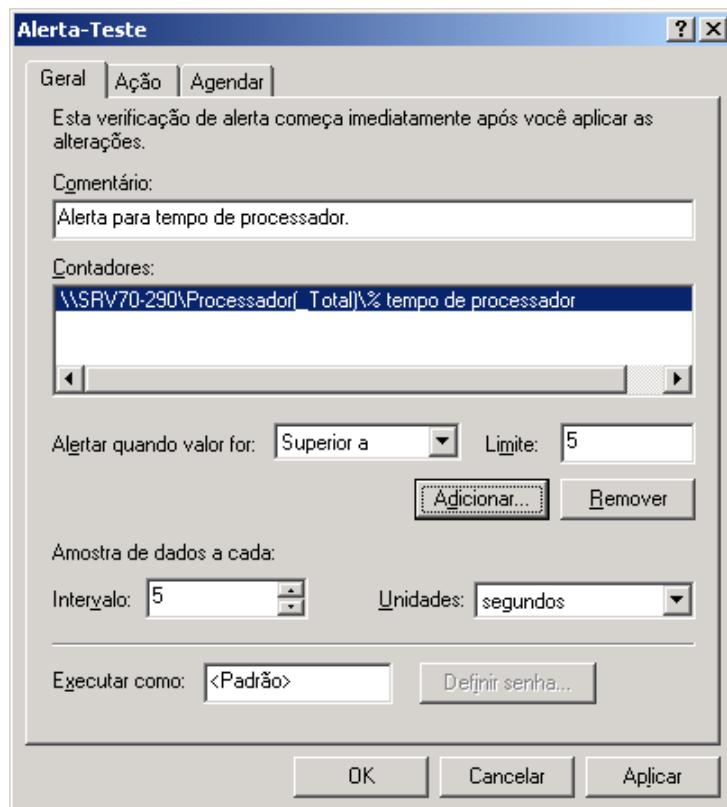


Figura 11.21 Configurações da guia Geral.

11. Dê um clique na guia Ação. Nesta guia você define uma ou mais ações que serão executadas quando o Alerta for disparado. Para o nosso exemplo quero apenas que uma mensagem seja enviada para o usuário Administrador. Defina as configurações conforme indicado na Figura 11.22:

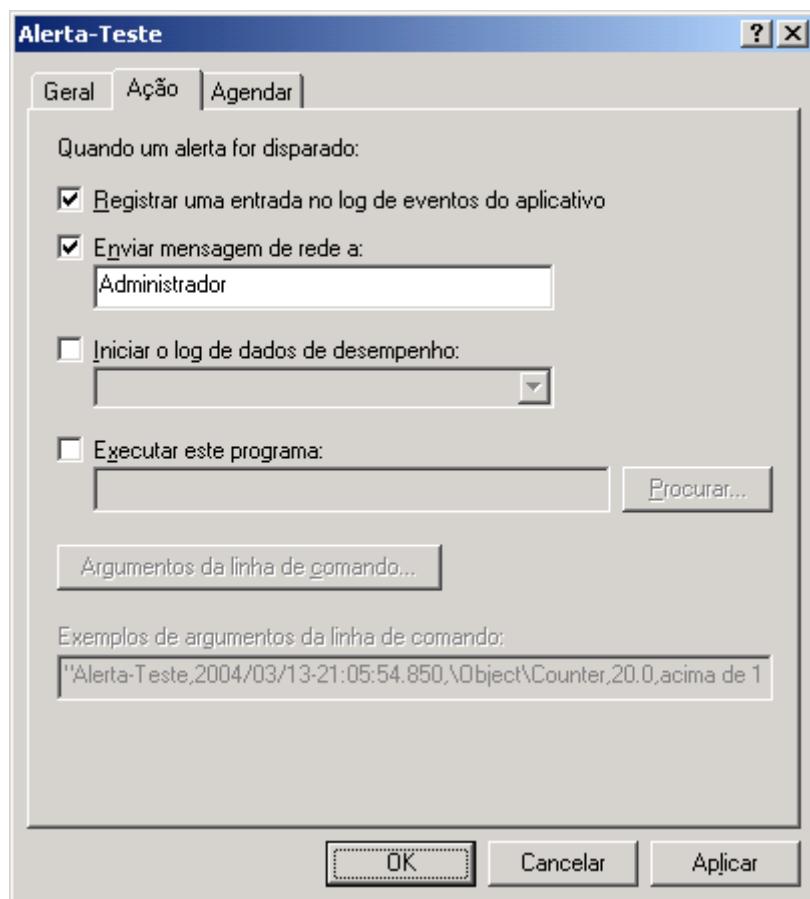


Figura 11.22 Configurações da guia Ação.

12. Clique em OK e o Alerta será criado e já será inicializado. Alertas podem ser iniciados e parados, assim como Logs para a captura automática de dados que também podem ser iniciados e parados. Para parar um Alerta que está em andamento, clique no botão Parar - botão com o desenho de um quadradinho ou clique com o botão direito do mouse no Alerta e, no menu de opções que é exibido, clique em Parar. A ação associada ao Alerta somente será disparada enquanto o Alerta estiver em execução.
13. Na Figura 11.23 mostro o exemplo da mensagem que é enviada para o usuário Administrador quando o Alerta deste exemplo é disparado, ou seja, quando o contador % tempo de processador atingir mais do que 5%. Esta mensagem foi enviada na estação de trabalho onde o administrador estava logado, que no exemplo era uma estação de trabalho com o Windows XP Professional. Ou seja, a mensagem é enviada para onde o administrador estiver logado, independente do servidor onde está configurado o alerta.

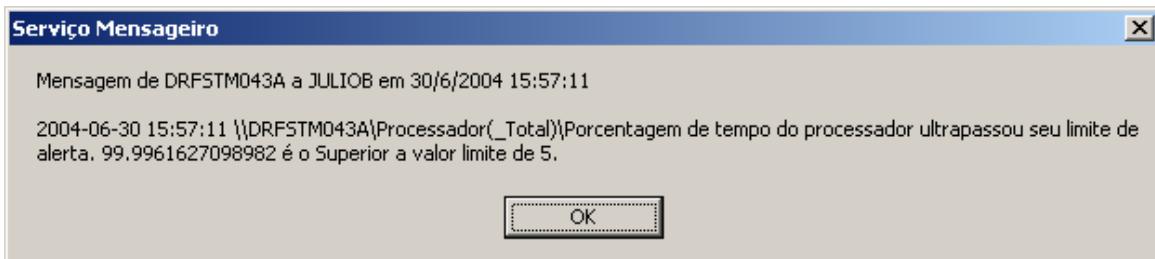


Figura 11.23 Mensagem enviada em resposta ao Alerta.

14. Feche o console Desempenho.

## Conclusão

Neste capítulo você aprendeu sobre a importância da monitoração de diversos elementos de hardware dos servidores, para trabalhar de uma maneira pro-ativa, antecipando futuras necessidades de atualização de hardware.

Tratei de diversos assuntos relacionados a monitoração de desempenho do servidor. Você aprendeu a utilizar as diversas opções do console desempenho, para executar ações tais como:

- ◆ Criar um gráfico de monitoração de desempenho.
- ◆ Configurar a captura automática de dados de desempenho.
- ◆ Criar alertas.

Também apresentei a lista dos principais contadores e respectivos valores limites, ou seja, valores que quando atingidos durante períodos prolongados de tempo, são indicativos de problemas no desempenho.

No próximo capítulo você aprenderá sobre a recuperação a desastres, ou seja, como botar o servidor para funcionar, após a ocorrência de problemas mais graves, os quais muitas vezes fazem com que o Windows Server 2003 deixe de inicializar.

# Introdução

Neste capítulo trataremos de assuntos relacionados com a inicialização do Windows Server 2003 (processo de boot) e com técnicas para recuperação do Windows Server 2003 quando por algum motivo (configurações incorretas, erros de operação, etc) o sistema não consegue inicializar normalmente ou inicializa com problemas que impedem o seu correto funcionamento. Trataremos, dentre outros, dos seguintes assuntos:

- ◆ O Processo de boot do Windows Server 2003.
- ◆ O Registro do sistema – Registry.
- ◆ O Modo Seguro de inicialização.
- ◆ Last Known good Configuration.
- ◆ Entendendo e usando o Console de Recuperação do Windows Server 2003.
- ◆ Criando disquetes de recuperação e de boot.

---

**NOTA:** Também é parte importante do processo de recuperação a desastres do Windows Server 2003, as operações de Backup e Restore do Active Directory, as quais foram abordadas no Capítulo 8.

---

Vamos iniciar o capítulo falando sobre o processo de boot do Windows Server 2003. Mostrarei que, em grande parte, este processo é muito semelhante ao processo de boot do Windows 2000 e do Windows XP. Será apresentada a seqüência de passos do processo de boot, bem como detalhes sobre os problemas que podem ocorrer em cada etapa. É importante que o leitor entenda o processo de boot do Windows Server 2003, pois em determinadas situações é muito mais simples corrigir um problema que ocorre na inicialização do que ter que reinstalar o Windows Server 2003 novamente. Para o usuário residencial, que tem um único computador, reinstalar o Windows Server 2003 pode não ser problema em termos do tempo necessário para esta tarefa. Agora imagine a situação de uma rede empresarial, com milhares de computadores conectados em rede. Sempre que possível, a equipe de suporte deve resolver o problema e não simplesmente reinstalar o Windows Server 2003. Pois além de economizar tempo, o usuário poderá voltar a utilizar a máquina quanto antes, o que significa menor tempo de parada.

Ainda dentro do contexto do processo de boot do Windows Server 2003 falarei sobre a Registry do Windows Server 2003. A Registry é um banco de informações sobre as configurações do Windows Server 2003 e dos diversos aplicativos instalados. A Registry é de fundamental importância para o Windows, a ponto de o Windows Server 2003 simplesmente não inicializar se ele não tiver acesso ao banco de informações da Registry. Antes do lançamento do Windows 2000 havia rumores de que a Registry seria extinta e todas as informações de configuração seriam armazenadas no Active Directory. Porém forem apenas Rumores, ou seja, mesmo no Windows Server 2003 a Registry continua presente e fundamental para o funcionamento do Sistema. As informações da Registry ficam gravadas

# CAPÍTULO

# 12

## Ferramentas de recuperação a desastres

em arquivos na seguinte pasta: C:\WINDOWS\system32\config. Supondo que o Windows Server 2003 esteja instalado no drive C:, na pasta C:\Windows.

Em seguida trataremos de dois tópicos importantes para a resolução de problemas de inicialização no Windows Server 2003. O Modo seguro é uma opção de inicialização, na qual podemos carregar o Windows Server 2003 apenas com um número mínimo de drivers, necessários ao seu funcionamento. Podemos utilizar o Modo Seguro para inicializar o Windows Server 2003 e desinstalar algum driver com problemas ou alterar configurações que foram feitas incorretamente e estão impedindo a inicialização do Windows Server 2003 no modo normal. A opção Last Known Good Configuration está relacionada com as configurações da Registry e será explicada em detalhes neste capítulo.

É importante salientar que os tópicos apresentados neste capítulo são valiosos, principalmente para quem dá suporte a computadores com o Windows Server 2003 instalado. São tópicos que ajudam a restaurar o Windows Server 2003 a um estado normal de funcionamento quando surgem problemas.

## Entendendo o processo de boot do Windows Server 2003

Neste tópico mostrarei como funciona o processo de boot (inicialização) do Windows Server 2003. O processo de boot começa quando você liga o computador e se encerra com o logon no sistema. Analisarei as cinco fases do processo de boot:

- ◆ Seqüência de pré-boot
- ◆ Seqüência de boot
- ◆ Carga do kernel
- ◆ Inicialização do kernel
- ◆ logon

Para que cada fase do processo de boot possa acontecer com sucesso, determinados arquivos são necessários. Na tabela 12.1 estão listados os arquivos necessários a cada fase do processo de boot. Systemroot indica a pasta onde estão os arquivos do Windows Server 2003 estão instalado, por padrão é C:\Windows, mas pode ser uma pasta diferente, dependendo de onde foi instalado o Windows Server 2003.

**Tabela 12.1 Arquivos utilizados no processo de boot do Windows Server 2003.**

| Arquivo        | Localização                     | Fase                    |
|----------------|---------------------------------|-------------------------|
| Ntldr          | Raiz da partição de sistema C:\ | Pré-boot e boot         |
| Boot.ini       | Raiz da partição de sistema C:\ | boot (*)                |
| Bootsect.dos   | Raiz da partição de sistema C:\ | boot                    |
| Ntdetect.com   | Raiz da partição de sistema C:\ | boot                    |
| Ntoskrnl.exe   | systemroot\System32             | Carga do kernel.        |
| Hal.dll        | systemroot\System32             | Carga do kernel         |
| System         | systemroot\System32\Config      | Inicialização do kernel |
| Device drivers | systemroot\System32\Drivers     | Inicialização do kernel |

Na seqüência, apresentamos um pequeno resumo de cada uma das fases envolvidas no processo de boot.

1. Seqüência de pré-boot: Após ligado o computador, uma série de testes de hardware e detecção de dispositivos Plug and Play é processada. O partição ativa é localizada e o setor de boot desta partição é carregado na memória e executado. O arquivo Ntldr é carregado na memória e inicializado. Este arquivo é que inicia o processo de carga do Windows Server 2003.
2. Seqüência de boot: Após ter carregado o arquivo Ntldr na memória, a seqüência de boot detecta informações sobre o hardware e os respectivos drivers, em preparação para as fases de carregamento do Windows Server 2003. Dentro da fase de seqüência de boot, temos quatro etapas bem distintas, conforme descrito a seguir:
  - ◆ **Fase inicial de carga do boot:** Nesta subfase, o Ntldr altera o processador do modo real de memória para o modo de 32 bit, o qual é requerido para a carga das demais funções. Um suporte mínimo de sistema de arquivos é carregado, para que o Ntldr possa achar e carregar o Windows Server 2003, a partir de uma partição FAT ou NTFS.
  - ◆ **Seleção do Sistema Operacional:** Nesta subfase, o Ntldr lê o arquivo Boot.ini (que detalharei no próximo item) e apresenta um menu de opções, de tal forma que o usuário possa escolher qual o sistema operacional será carregado, no caso de existir mais de um Sistema operacional instalado. Caso o arquivo Boot.ini tenha sido eliminado por acidente, o Ntldr tenta carregar o Windows Server 2003 a partir da primeira partição do primeiro disco rígido.
  - ◆ **Detecção de hardware:** É feita pelos arquivos Ntdetect.com e Ntoskrnl.exe. Os dispositivos de hardware detectados pelo arquivo NTDETECT.COM são passados para o arquivo NTLDR, o qual gravará estas informações na Registry, na chave HKEY\_LOCAL\_MACHINE\HARDWARE. O Windows Server 2003 detecta, automaticamente, dispositivos tais como: Portas de comunicação, processadores de ponto flutuante, drives de disquete, teclado, mouse, portas paralelas, dispositivos SCSI, adaptadores de vídeo e assim por diante.
  - ◆ **Seleção de configuração:** Após a detecção do hardware, você terá a oportunidade de acessar uma lista com diferentes Perfis de Hardware, caso você tenha criado outros perfis além do perfil padrão. Um Perfil de Hardware é uma configuração que pode fazer com que o Windows Server 2003 ignore determinados componentes de hardware e com isso não carregue os drivers para estes componentes, quando da inicialização do sistema.
3. Carga do kernel: Durante esta fase, o arquivo Ntoskrnl.exe é carregado, porém ainda não é inicializado. O arquivo hal.dll é carregado na memória. Os drivers para dispositivos de hardware de baixo nível, como por exemplo, discos rígidos, são carregados. Dispositivos de hardware de baixo nível, são aqueles dispositivos que precisam ser inicializados antes do que os demais, de tal forma que o processo possa prosseguir. Uma série de retângulos, em seqüência, é exibida na tela, a medida que os dispositivos são carregados. Neste momento ainda não foi carregada a interface gráfica do Windows Server 2003. Nesta fase a chave da Registry HKEY\_LOCAL\_MACHINE\SYSTEM é carregada a partir do arquivo Systemroot\System32\Config\System. Conforme comentado na introdução deste capítulo, as informações da Registry estão

**NOTA: (\*.sys): (\*) -> Este arquivo somente está presente quando temos outros sistemas operacionais instalados no mesmo computador. Por exemplo, quando temos o Windows 98 e o Windows Server 2003 instalados, no mesmo computador, teremos este arquivo. Esta situação dificilmente acontecerá, afinal quem iria instalar o Windows 98, com uma partição FAT, junto com o Windows Server 2003 em um servidor?**

**NOTA: Esta seqüência é idêntica (para não dizer igual) a seqüência de boot do Windows 2000. Compare o texto deste item com o texto da Lição 7 da Unidade IX, do livro "Série Curso Básico & Rápido Microsoft Windows 2000 Server", de minha autoria, publicado pela Axcel Books ([www.axcel.com.br](http://www.axcel.com.br)).**

gravadas em arquivos na pasta Systemroot\System32\Config, onde Systemroot representa a pasta onde o Windows Server 2003 foi instalada. Em seguida um “control set” (conjunto de controle) é selecionado e carregado. Um control set representa um conjunto de configurações que definem quais drivers e serviços serão carregados e inicializados automaticamente pelo Windows Server 2003. Conforme veremos no item sobre Last Know Good Configuration (Última configuração válida), o conceito de control set é importante na recuperação do sistema quando usamos a opção Last Know Good Configuration.

4. Inicialização do kernel: Após ter sido completada a fase da carga do kernel, este é inicializado e o Ntldr passa o controle para o kernel do sistema. Nesta etapa é exibida uma tela gráfica, com uma barra de status indicando o andamento do processo. Nesta etapa os drivers de dispositivos de baixo nível, carregados na fase anterior, são inicializados. Também é nesta fase, que os diversos Serviços configurados para inicializar automaticamente, são inicializados. Por exemplo o DNS, Inetinfo (Servidor Web – Internet Information Server), e qualquer outro serviço instalado no Windows Server 2003 As seguintes etapas são executadas durante esta etapa:
  - ◆ A chave HKEY\_LOCAL\_MACHINE\HARDWARE é criada usando como base as informações coletadas na etapa de Detecção de Hardware da fase de Seqüência de boot, descrita anteriormente.
  - ◆ Criação de uma cópia do control set utilizado – Clone Control set: É feita uma cópia do control set utilizado. Esta cópia poderá ser utilizada posteriormente, caso alterações feitas no control set atual, impeçam a inicialização do Windows Server 2003.
  - ◆ Os drivers de hardware que foram carregados na fase de Carga do Kernel são agora inicializados. Cada driver possui um parâmetro de configuração chamado ErrorControl. Este parâmetro define a maneira como o Windows Server 2003 irá proceder, caso algum erro aconteça na inicialização do driver. Os valores possíveis para este parâmetro são os seguintes:
    - a. **0x0:** Ignore. Caso ocorra algum erro na inicialização do driver, o Windows Server 2003 simplesmente ignora o erro e continua a inicialização dos demais drivers. Nenhuma mensagem de erro será exibida.
    - b. **0x1:** Normal. Uma mensagem de erro será exibida e o processo de Inicialização do Kernel continua.
    - c. **0x2:** Severe. O processo de boot falha, o computador será reinicializado e serão utilizadas as configurações definidas no control set Last Know Good Configuration (Última configuração válida), ou seja, as configurações que foram gravadas como sendo as configurações da última inicialização com sucesso serão utilizadas. Se o erro ocorrer novamente, quando o computador já está utilizando o control set Last Know Good Configuration, o erro será ignorado e a inicialização do Kernel continuará com a inicialização dos demais drivers.
    - d. **0x3:** Critical. O processo de boot falha, o computador será reinicializado e serão utilizadas as configurações definidas no control set Last Know Good Configuration, ou seja, as configurações que foram gravadas como sendo as configurações da última inicialização com sucesso serão utilizadas. Se o erro ocorre novamente, quando o computador já está utilizando o control set Last Know Good Configuration, a seqüência de boot será interrompida e uma mensagem de erro será exibida. Este valor é utilizado para os dispositivos de hardware que são fundamentais para a inicialização do sistema. Por exemplo, o boot não tem como continuar se o Windows Server 2003 não conseguir inicializar os drivers para acesso ao sistema de discos.
  - ◆ Os serviços configurados para inicialização automática são inicializados e carregados na memória do computador. Os serviços são inicializados em uma ordem específica, de acordo com as dependências existentes entre os respectivos serviços. Por exemplo, vários serviços dependem do serviço Remote Procedure Call (RPC). O serviço RPC deve ser inicializado antes dos serviços que dele dependem, caso contrários a inicialização destes últimos irá falhar.

5. Logon: Nesta fase o subsistema Win32 automaticamente inicializa o serviço Winlogon.exe, o qual inicializa a Autoridade local de segurança – LSA – Local Security Authority (Lsass.exe), e finalmente a janela de logon é exibida. O processo de inicialização do Windows Server 2003, somente é considerado OK, quando o usuário efetua o logon com sucesso. Após o logon ter sido feito com sucesso o Windows Server 2003 copia as configurações do Clone control set para o Last Known Good Configuration control set, ou seja, o Windows Server 2003 considera que as configurações atuais representam a última configuração que permitiu uma inicialização com sucesso.

Pode parecer um pouco complexo, porém conhecer o processo de boot do Windows Server 2003 é de fundamental importância para o Administrador do sistema e para os técnicos de suporte, principalmente quando surgem problemas e o computador não consegue inicializar com sucesso. Informações mais detalhadas sobre o processo de boot podem ser encontradas na Ajuda do Windows Server 2003.

Agora passaremos a analisar alguns tópicos importantes para a inicialização e manutenção do Windows Server 2003 em funcionamento. Vamos iniciar por um estudo detalhado do arquivo Boot.ini e depois falaremos um pouco mais sobre a Registry do Windows Server 2003.

## O arquivo Boot.ini e caminhos ARC

O arquivo Boot.ini é criado durante a instalação do Windows Server 2003. Este arquivo é gravado na partição ativa, ou seja, na partição que é utilizada para inicializar o Windows Server 2003. Normalmente a partição ativa é o drive C:\. Durante a fase de inicialização do Windows Server 2003, o arquivo NTLDR lê o conteúdo do arquivo Boot.ini e utiliza este conteúdo para montar o menu de opções, no qual você pode selecionar o Sistema Operacional a ser carregado, caso haja mais de um sistema operacional instalado no servidor. O arquivo Boot.ini é bastante útil quando temos mais de um Sistema Operacional instalado no mesmo computador. Neste caso, as informações do arquivo Boot.ini são utilizadas pelo NTLDR para exibir um menu, no qual selecionamos o Sistema Operacional a ser instalado.

Por exemplo, tenho um computador de teste onde estão instaladas versões de avaliação do Windows 98, do Windows 2000 Server em Inglês, do Windows 2000 Server em Português, do Windows 2000 Professional e do Windows XP Professional. Ao inicializar este computador é exibido um menu como os diferentes Sistemas operacionais instalados, no qual selecionei qual o sistema desejo carregar.

Na listagem a seguir coloco uma cópia do arquivo boot.ini do computador citado no parágrafo anterior:

Arquivo boot.ini de um computador com cinco versões diferentes do Windows instaladas:

```
[boot loader]
timeout=30
default=multi(0)disk(0)rdisk(1)partition(2)\WXPPRO
[operating systems]
multi(0)disk(0)rdisk(1)partition(2)\WXPPRO="Microsoft Windows Server 2003 Professional" /fastdetect
multi(0)disk(0)rdisk(1)partition(1)\WINNT="Microsoft Windows 2000 Server - Portugues" /fastdetect
multi(0)disk(0)rdisk(1)partition(1)\W2KSRVIN="Microsoft Windows 2000 Server" /fastdetect
multi(0)disk(0)rdisk(1)partition(2)\WINNT="Microsoft Windows 2000 Professional" /fastdetect
C:=\"Microsoft Windows 98"
O arquivo boot.ini possui duas seções distintas:
[boot loader]
[operating systems]
```

Na seção [boot loader] é informado qual o Sistema Operacional padrão, ou seja, qual o Sistema Operacional será carregado caso o usuário não selecione uma das opções do menu. Nesta seção também é definido durante quanto tempo o menu será exibido. No nosso exemplo, o menu será exibido durante 30 segundos: timeout=30. Neste exemplo

também está definido que será carregado o Sistema Operacional instalado na partição default=multi(0)disk(0)rdisk(1)partition(2)\WXPPRO. O sistema definido como padrão (default), será carregado se o usuário não selecionar nenhuma opção do menu.

Na seção [operating systems] é exibida a lista de Sistemas Operacionais instalados e disponíveis para uso. Cada linha indica um Sistema Operacional instalado e para indicar a pasta onde estão os arquivos do respectivo Sistema Operacional é utilizado o caminho ARC, que será detalhado logo em seguida. Após o caminho podem ser fornecidas chaves que alteram a maneira como o respectivo Sistema é inicializado, como no exemplo a seguir, onde foi utilizada a chave /fastdetect. Estudaremos as chaves disponíveis mais adiante.

```
multi(0)disk(0)rdisk(1)partition(2)\WXPPRO="Microsoft Windows Server  
2003 Professional" /fastdetect
```

O que vem após o sinal de igual (=), entre aspas, é simplesmente uma descrição. Esta é a descrição que é exibida no menu de inicialização.

Agora precisamos detalhar dois pontos importantes:

- ◆ A sintaxe dos caminhos ARC.
- ◆ As chaves que podem ser utilizadas no arquivo Boot.ini.

## Entendendo a sintaxe dos caminhos ARC.

Vamos detalhar as diversas partes que compõem um caminho ARC. Considere os dois exemplos a seguir:

- ◆ multi(0)disk(0)rdisk(1)partition(2)\WXPPRO
- ◆ scsi(0)disk(0)rdisk(1)partition(2)\WXPPRO
- ◆ **multi ou scsi:** Na primeira parte do caminho temos duas opções: multi ou scsi. Utilizamos scsi em uma única situação: quando temos uma controladora SCSI com a BIOS desabilitada, o que é uma situação muito rara. Em todas as demais situações utilizamos multi para a primeira parte do caminho ARC. O número entre parênteses indica a ordem em que os adaptadores são carregados. Por exemplo, se você tiver um computador com dois adaptadores IDE instalados. O caminho dos discos do primeiro adaptador inicia com multi(0) e o caminho dos discos do segundo adaptador inicia com multi(1).
- ◆ **disk:** Indica a posição (ID) do disco SCSI e somente é utilizado quando a primeira parte do caminho começa com scsi. Quando a primeira parte for multi, esta parte será sempre disk(0).
- ◆ **rdisk:** Um número que identifica o disco dentro da controladora. Para controladores SCSI este número será ignorado. Sempre inicia com o valor zero. Por exemplo, se você tiver um computador com duas controladoras IDE e dois discos em cada controladora, teremos as seguintes combinações possíveis:  
multi(0)disk(0)rdisk(0) -> Primeiro disco da primeira controladora.  
multi(0)disk(0)rdisk(1) -> Segundo disco da primeira controladora.  
multi(1)disk(0)rdisk(0) -> Primeiro disco da segunda controladora.  
multi(1)disk(0)rdisk(1) -> Segundo disco da segunda controladora.

**NOTA:** Logo em seguida falarei sobre a sintaxe utilizada pelo arquivo Boot.ini para indicar a partição onde estão gravados os arquivos do Sistema Operacional associado a cada opção. No nosso exemplo temos o caminho: default=multi(0)disk(0)rdisk(1)partition(2)\WXPPRO. Este caminho também é conhecido como caminho ARC - Advanced RISC Computing.

**NOTA:** Observe que para o Windows 9x ou Me, é fornecido o caminho tradicional, no nosso exemplo C:\="Microsoft Windows 98", informando que o Windows 98 está na partição C:. O que vem após o sinal de igual (=), entre aspas, é simplesmente uma descrição. Esta é a descrição que é exibida no menu de inicialização.

- ◆ **Partition:** Indica o número da partição dentro do disco. O valor entre parênteses começa com 1, diferente dos valores dos outros parâmetros que iniciam sempre com zero. Por exemplo, se você tiver um computador com duas controladores IDE e dois discos em cada controladora. No primeiro disco da primeira controladora você tem uma única partição e nos demais discos duas partções, teremos as seguintes combinações possíveis:  
 multi(0)disk(0)rdisk(0)partition(1)-> Primeira partição do primeiro disco da primeira controladora.  
 multi(0)disk(0)rdisk(1)partition(1)-> Primeira partição do segundo disco da primeira controladora.  
 multi(0)disk(0)rdisk(1)partition(2)-> Segunda partição do primeiro disco da primeira controladora.  
 multi(1)disk(0)rdisk(0)partition(1)-> Primeira partição do primeiro disco da segunda controladora.  
 multi(1)disk(0)rdisk(0)partition(2)-> Segunda partição do primeiro disco da segunda controladora.  
 multi(1)disk(0)rdisk(1)partition(1)-> Primeira partição do segundo disco da segunda controladora.  
 multi(1)disk(0)rdisk(1)partition(2)-> Segunda partição do segundo disco da segunda controladora.

O que vem após o caminho ARC é o nome da pasta, dentro da partição especificada pelo caminho ARC, onde estão os arquivos do Sistema Operacional. No exemplo que demos no início deste tópico temos o seguinte caminho:

**multi(0)disk(0)rdisk(1)partition(2)\WXPPRO**

O que representa esta caminho? Lendo de trás para frente temos a seguinte interpretação:

|                          |    |              |
|--------------------------|----|--------------|
| A pasta WXPPRO           | -> | \WXPPRO      |
| da segunda partição      | -> | partition(2) |
| do segundo disco         | -> | rdisk(1) *   |
| da primeira controladora | -> | multi(0) *   |

(\*): Lembre que para multi, disk e rdisk os valores iniciam em zero e para partition os valores iniciam em um.

## As chaves que podem ser utilizadas no arquivo Boot.ini.

Conforme descrito anteriormente, existem algumas chaves que podem ser utilizadas no arquivo Boot.ini, para alterar a maneira como cada Sistema Operacional é utilizado. A seguir descrevemos as chaves disponíveis.

- ◆ **/basevideo:** Esta chave faz com que o Sistema Operacional seja inicializado utilizando um driver VGA com configurações padrão mínimas, suportadas pela maioria dos adaptadores de vídeo e monitores. Esta opção pode ser utilizada se você instalou um novo adaptador de vídeo (ou um novo monitor), os quais não estão funcionando corretamente, a ponto de após feito o logon, não ser possível ler as informações exibidas na tela. Neste caso você pode fazer a inicialização no Modo seguro, que descreverei mais adiante, alterar o arquivo boot.ini adicionando a chave /basevideo. Quando o Windows Server 2003 for inicializado serão utilizadas configurações básicas do driver VGA. Você poderá fazer o logon e corrigir as configurações que estão impedindo o funcionamento correto do adaptador de vídeo ou do monitor. Feitas as correções você pode retirar a chave /basevideo para que o Windows Server 2003 carregue as configurações de vídeo normalmente. No exemplo a seguir temos uma ilustração do uso desta chave:

**multi(0)disk(0)rdisk(1)partition(2)\WXPPRO /basevideo**

- ◆ **/fastdetect= comx ou /fastdetect= comx, y,z ou /fastdetect:** Com esta chave a detecção de mouse serial na inicialização será desabilitada. Comx é utilizada para especificar se a detecção deve ser desabilitada em um única porta com, como por exemplo Com1 ou Com2. É possível desabilitar a detecção em duas ou mais portas, como por exemplo Com1,2. Se não for especificada a porta Com, a detecção será desabilitada em todas

as portas. Por padrão a chave /fastdetect, sem a especificação de porta, é incluída em todas as opções de Sistema Operacional do arquivo boot.ini, com exceção de linhas que correspondem ao Windows 9x ou Me.

- ◆ **/maxmem:n:** Com esta chave é possível definir a quantidade máxima de memória RAM disponível para o Windows Server 2003. Por exemplo, em um computador com 256 MB de RAM instalados, se você quiser utilizar apenas 128, utilize a seguinte chave: /maxmem:128. A única justificativa para o uso desta chave é se você quiser detectar se um determinado pente de memória está com problemas.
- ◆ **/noguiboot:** Inicializa o Windows Server 2003 sem exibir a tela gráfica com informações sobre o andamento (Status) da inicialização.
- ◆ **/sos:** A medida que os drivers de dispositivos vão sendo carregados, o nome dos arquivos que estão sendo carregados será exibido no vídeo. Esta opção é útil quando o Windows Server 2003 não consegue inicializar corretamente e você quer detectar em que ponto da inicialização está o problema. Por exemplo, se você utilizar esta chave e a inicialização for interrompida no momento da carga do driver da placa de rede, este é um bom indicativo de que o problema pode ser com este driver ou com algum driver relacionado.

## Configurações de inicialização através do utilitário System (Sistema).

Existe opções relacionadas a inicialização do computador e de recuperação no caso de falhas, tal como a famosa “Blue Screen of Death” (Tela azul da morte), que podem ser configuradas através da opção System (Sistema) do Painel de controles. A tela azul da morte é exibida quando ocorre um erro grave, que impede o Windows Server 2003 de continuar sendo executado. Normalmente este tipo de erro está relacionado com problemas em drivers de dispositivos de hardware. Quando ocorre um destes erros, o Windows Server 2003 faz um dump (cópia/despejo) do conteúdo da memória RAM em um arquivo no disco. Estas informações podem ser de grande utilidade para a equipe de suporte técnico poder analisar e tentar descobrir as causas do problema.

A seguir apresento um exemplo prático, passo-a-passo, mostrando as opções de configurações da opção Sistema, relacionadas com a inicialização do Windows Server 2003.

Exemplo: Para configurar as opções de inicialização do Windows Server 2003, usando a opção Sistema, siga os passos indicados a seguir:

1. Faça o logon como administrador ou com uma conta com permissão de administrador.
2. Abra o Painel de controle: Iniciar -> Painel de controle.
3. Dê um clique duplo na opção Sistema.
4. Dê um clique na guia Avançado. Nesta guia você tem acesso a diversas opções de configuração, que afetam a aparência, o desempenho, o processo de boot e a geração de relatórios de erros no Windows Server 2003. Neste exemplo mostrarei como configurar as diversas opções disponíveis nesta guia, opções estas indicadas na Figura 12.1.
5. Clique no primeiro botão Configurações..., dentro do grupo Desempenho. Será aberta a janela de configurações de desempenho, na qual estão disponíveis as guias Efeitos visuais e Avançado. Na guia Efeitos Visuais você pode habilitar/desabilitar uma série de novos efeitos visuais que foram introduzidos inicialmente no Windows XP e que estão presente também no Windows Server 2003. Um detalhe importante é que os efeitos visuais utilizam recursos de memória e processamento. Por isso, se você está utilizando o Windows Server 2003 em um servidor da rede (a qual é a utilização mais comum para o Windows Server 2003) é aconselhável desabilitar todos os efeitos visuais, já que dificilmente você trabalhará diretamente no console do servidor e o mais importante será realmente o desempenho do servidor.

---

**DICA:** Um atalho para abrir a opção Sistema é clicar com o botão direito do mouse em Meu computador e, no menu de opções que é exibido, clicar em Propriedades.

---

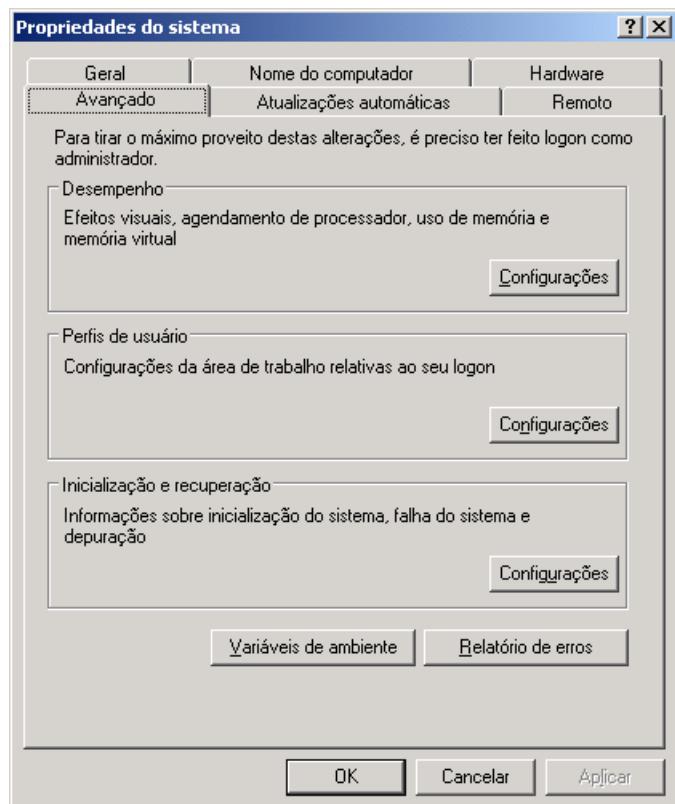


Figura 12.1 Opções avançadas do sistema.

Na guia Visual Efeitos visuais, você tem as opções indicadas na Figura 12.2 com a explicação.

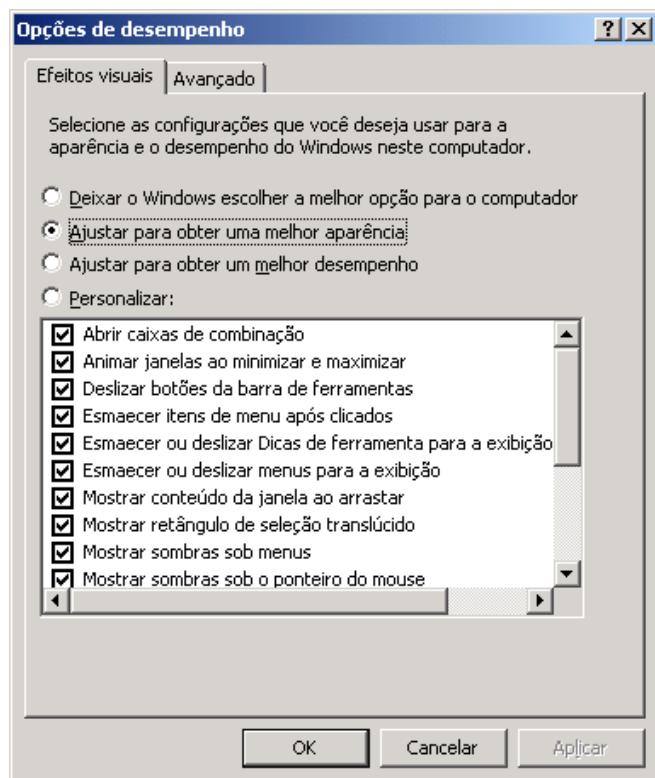


Figura 12.2 Configurando Efeitos visuais.

- ◆ Deixar o Windows escolher a melhor configuração para o meu computador: Ao selecionar esta opção, o próprio Windows Server 2003 definirá quais efeitos visuais estarão habilitados e quais estarão desabilitados, com base nos serviços instalados e na ocupação dos recursos de hardware. A medida que aumenta a ocupação do processador e da memória RAM, o Windows Server 2003 vai desabilitando mais efeitos visuais, para liberar estes recursos.
  - ◆ Ajustar para obter uma melhor aparência: Ao marcar esta opção, todos os efeitos visuais serão habilitados. Lembre-se que os efeitos visuais causam uma utilização de maior de processamento e memória.
  - ◆ Ajustar para obter um melhor desempenho: Ao marcar esta opção, todos os efeitos visuais serão desabilitados. Esta é a opção mais indicada para servidores, de tal forma que os recursos sejam liberados para os serviços executados pelo servidor.
  - ◆ Personalizar: Ao marcar esta opção, você poderá definir quais recursos visuais serão habilitados e quais serão desabilitados.
6. Defina as configurações desejadas e clique na guia Avançado. Serão exibidas as opções indicadas na Figura 12.3:

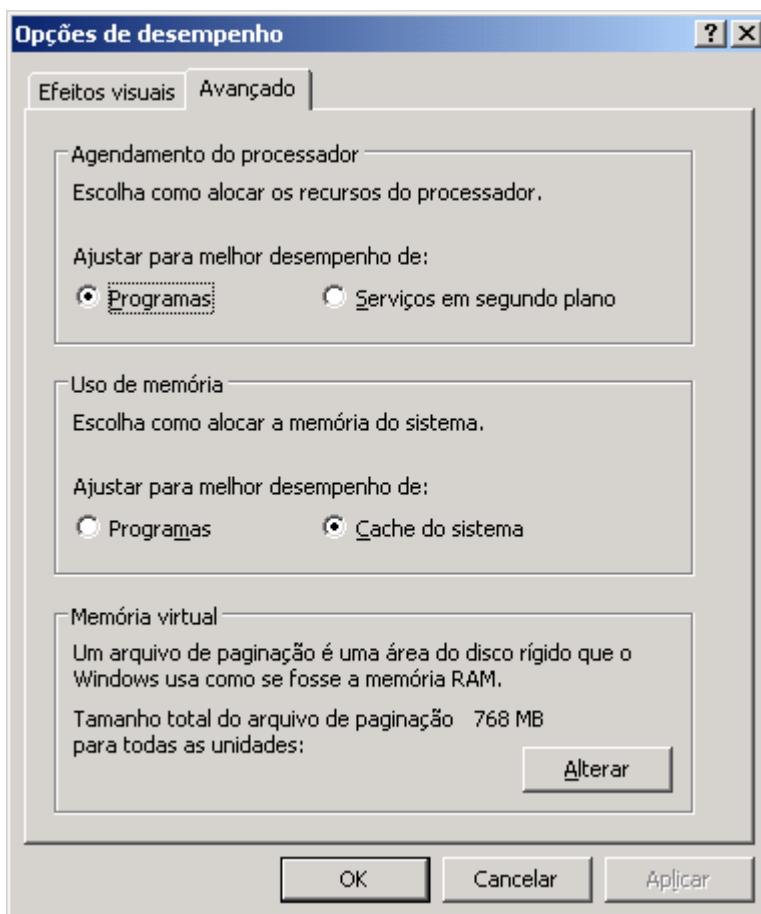


Figura 12.3 Configurando opções avançadas.

7. Nesta guia você configura opções relacionadas a prioridade que o Windows Server 2003 dará para programas do usuário em relação aos serviços do sistema operacional e outras opções relacionadas ao desempenho dos programas e serviços. Na opção Agendamento do processador, você define se os programas executados em primeiro plano, tais como o Word, Excel, Corel Draw, etc, terão prioridade no uso do processador (opção Programas) ou se os serviços que executam em segundo plano, tais como DNS, DHCP, WINS, RRAS, IIS, etc, terão prioridade no uso

do processador (opção Serviços em segundo plano). Nos servidores da rede, tais como DCs, servidores DNS, DHCP, servidores da Intranet, rodando o IIS, é aconselhável que você marque a opção Serviços em segundo plano, pois dificilmente você usará estes servidores para execução de programas de usuário, mas sim para serviços da rede. Ao marcar esta opção você dá prioridade no uso dos recursos de processamento, para os serviços de rede, que é a opção mais indicada para servidores. Os mesmos comentários são válidos em relação as opções do gru Uso de memória. Se o computador está sendo utilizado como um servidor, marque a opção Cache do sistema; se o computador estiver sendo utilizado como uma estação de trabalho, executando programas de usuário, marque a opção Programas.

8. O Windows Server 2003 (a exemplo das demais versões do Windows), utiliza um arquivo de memória virtual em disco. Este arquivo também é conhecido como arquivo de troca. O Kernel do Windows Server 2003 fica constantemente monitorando a memória do computador e move conteúdo da memória RAM para o arquivo de trocas no disco rígido e do arquivo de trocas de volta para a memória RAM. São movidos para o arquivo de troca, páginas de memória que estão há algum tempo sem serem utilizadas. Com este procedimento, o Windows Server 2003 libera memória para a execução das páginas de memória que estão sendo constantemente utilizadas. Claro que o acesso ao disco é bem mais lento do que o acesso a memória RAM. Por isso o uso de memória virtual em disco não deve ser visto como uma opção para expandir a memória do servidor. Em situações onde está havendo um uso muito intensivo do arquivo de paginação, haverá, certamente, uma queda no desempenho do servidor. Nestas situações o mais indicado é adicionar mais memória RAM, para reduzir o uso intensivo do arquivo de paginação. Para definir as configurações do arquivo de paginação, clique no botão Alterar. Será exibida a janela Memória virtual, indicada na Figura 12.4:

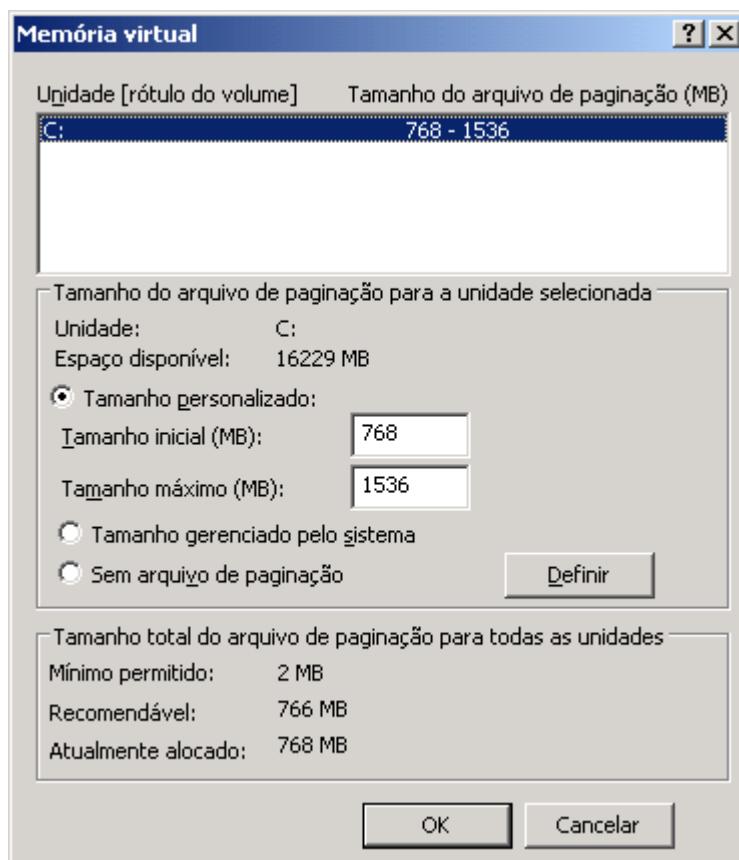


Figura 12.4 Configurando opções avançadas.

9. Nesta janela você define o tamanho do arquivo de paginação. O arquivo de paginação é gravado com o nome de pagefile.sys, na raiz de um ou mais volumes do servidor. Também é possível criar um arquivo de paginação distribuído por dois ou mais volumes. Por exemplo, suponhamos que você tem um servidor com 6 volumes: C, D, E, F, G e H. Você pode criar uma arquivo de paginação de 4 GB, utilizando a seguinte configuração: 1 GB em D:, 1GB em E, 1GB em F e 1 GB em G ou outra combinação qualquer. Uma das recomendações é, se possível, colocar o arquivo de paginação em um volume em um disco diferente do disco onde está o volume onde o Windows Server 2003 está instalado. Ao fazer isso, você evita um acesso intensivo ao disco, pois teríamos o acesso aos arquivos do Windows Server 2003 e o acesso ao arquivo de paginação, simultaneamente, no mesmo disco. Por isso a recomendação de deslocar o arquivo de paginação para um ou mais volumes, localizados em outros discos que não o disco onde está instalado o Windows Server 2003. Para definir o tamanho que o arquivo de paginação irá ocupar em cada volume, basta clicar no respectivo volume e digitar o tamanho a ser utilizado, nos campos Tamanho inicial e Tamanho máximo. Após ter definido o tamanho clique em Definir. Outra recomendação é utilizar um arquivo de paginação, com um tamanho de, no mínimo, o dobro da quantidade de memória RAM instalado. Por exemplo, se você tem 1 GB de RAM instalada, crie um arquivo de paginação de 2 GB. A seguir mais algumas observações/recomendações em relação ao arquivo de paginação, para obter um melhor desempenho do servidor:

- ◆ Você pode colocar um arquivo de paginação em outras unidades de disco. Se você tiver vários discos rígidos, é uma boa idéia dividir o arquivo de paginação, pois isso deve acelerar o tempo de acesso (leituras simultâneas em vários discos) e reduzir o acesso concorrente ao arquivo de paginação e aos arquivos do Windows Server 2003. Se você tiver dois discos rígidos e dividir o arquivo de paginação, ambos os discos rígidos poderão acessar informações simultaneamente, aumentando muito a taxa de transferência. Entretanto, se você tiver dois discos rígidos e um disco rígido for mais rápido do que o outro, pode ser melhor armazenar o arquivo de paginação apenas no disco rígido mais rápido.
- ◆ Você pode aumentar o tamanho do arquivo de paginação. Quando você inicia o Windows Server 2003 ele cria automaticamente um arquivo de paginação (Pagefile.sys) no disco onde está instalado o sistema operacional. O Windows Server 2003 usa o arquivo de paginação para fornecer a memória virtual. O tamanho recomendado para o arquivo de paginação equivale a duas vezes à quantidade de memória RAM disponível no seu sistema. No entanto, o tamanho do arquivo também depende do espaço livre disponível em seu disco rígido quando o arquivo é criado. Você pode descobrir qual o tamanho do arquivo de paginação do seu sistema verificando o tamanho de arquivo mostrado para Pagefile.sys no Windows Explorer.
- ◆ Apesar de você poder redefinir os tamanhos inicial e máximo do arquivo de paginação, é melhor expandir o tamanho do arquivo de paginação inicial, em vez de forçar o sistema operacional a alocar mais espaço para o arquivo de paginação conforme os programas forem iniciados, o que fragmenta o disco.
- ◆ Se o arquivo de paginação alcançar seu tamanho máximo, será exibido um aviso e o sistema poderá ser interrompido. Para ver se seu arquivo de paginação está se aproximando do limite superior antes de alcançar este limite, verifique o tamanho real do arquivo e compare-o à configuração do tamanho máximo de arquivo de paginação. Se esses dois números estiverem próximos do mesmo valor, considere aumentar o tamanho do arquivo de paginação inicial ou executar menos programas.
- ◆ Os contadores do arquivo de paginação, podem ser utilizados no Console Desempenho e oferecem outra maneira de verificar se o tamanho do arquivo Pagefile.sys está apropriado:
  - ◆ Paging File\ % Usage (% Uso)
  - ◆ Paging File\ % Usage Peak (% Uso máximo)

Se o valor % Usage Peak se aproximar da configuração máxima do arquivo de paginação ou se % Usage se aproximar de 100%, considere aumentar o tamanho de arquivo inicial.

7. Defina as configurações desejadas e clique em OK. Você estará de volta à guia Avançado da janela Opções de desempenho. Dê um clique em OK para fechá-la. Você estará de volta à guia Avançado, da janela de configurações do sistema. Agora você aprenderá a configurar as opções de inicialização do sistema. Clique no botão Configurações, ao lado da opção Inicialização e recuperação. Será exibida a janela Inicialização e recuperação, indicada na Figura 12.5:

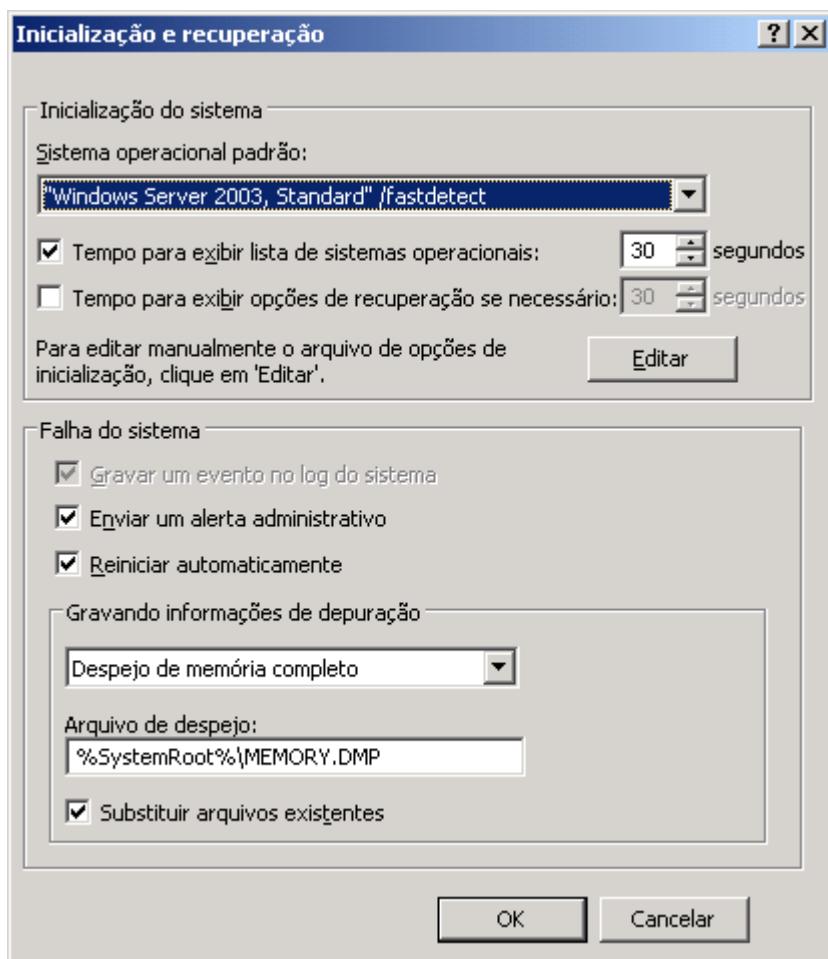


Figura 12.5 Opções de inicialização e recuperação.

**NOTA:** Se vários arquivos de paginação estiverem espalhados por várias unidades de disco, o nome do caminho de cada arquivo aparecerá como um exemplo do tipo de objeto Arquivo de paginação. É possível adicionar um contador a cada arquivo de paginação ou selecionar o exemplo \_Total para verificar os dados de uso combinados para todos os seus arquivos de paginação.

8. Na lista Sistema operacional padrão, você seleciona qual será a versão do Windows a ser carregada por padrão, caso haja mais de uma versão instalada no computador. No campo Tempo para exibir a lista de sistemas operacionais:, você define quantos segundos a lista de sistemas operacionais será exibida, caso haja mais de uma versão do Windows instalada. Este menu é montado com base nas informações do arquivo boot.ini, conforme descrito anteriormente. Se uma opção não for selecionada, dentro do tempo definido neste campo, o sistema operacional definido como padrão será carregado. No campo Tempo para exibir a lista de opções de recuperação se necessário, você define o tempo que serão exibidas as opções de recuperação, quando você estiver inicializando o servidor para fazer uma recuperação com base em um disquete de recuperação (que será descrito mais adiante, conhecido como disquete ASR) ou uma recuperação a partir do CD-ROM. Se você clicar no botão Editar, o arquivo boot.ini será carregado no Bloco de notas, para que você possa fazer alterações manualmente. No grupo Falha do sistema, você define qual o comportamento do Windows Server 2003 no caso de uma falha grave, na

qual é exibida a famosa Blue screen of death (Tela azul da morte). Por padrão as opções Enviar um alerta administrativo e Reiniciar automaticamente. Ao marcar a opção Enviar um alerta administrativo, será enviada uma mensagem para os usuários do grupo Administradores. Esta mensagem é enviada usando o comando net send e é exibida no computador onde o usuário está logado, no formato de uma caixa de mensagens. Na lista Gravando informações de depuração, você define se uma cópia do conteúdo atual da memória deve ser gravada em um arquivo de dump. O nome e o caminho do arquivo é definido no campo Dump file (por incrível que pareça, a tradução oficial para Dump file foi: Eliminar arquivo. Pergunto, o que tem a ver Eliminar arquivo com o arquivo de Dump de memória. Absolutamente nada. Ou seja, tradução literal, sem levar em consideração os aspectos técnicos). O caminho padrão é %SystemRoot%\MEMORY.DMP, onde %SystemRoot%\\ representa a pasta onde o Windows Server 2003 está instalado.

8. Defina as configurações desejadas e clique em OK. Você estará de volta à guia Avançado de configurações do sistema. Agora você aprenderá a configurar as opções de geração de relatório de erros quando um programa falha. Este tipo de erro ocorre quando um programa simplesmente congela e você tem que fechá-lo manualmente (na marra, usando Ctrl+Alt+Del ou Gerenciador de tarefas, usando o gerenciador de tarefas, que será descrito mais adiante. Clique no botão Relatório de erros. Será exibida a janela Relatório de erros, indicada na Figura 12.6:

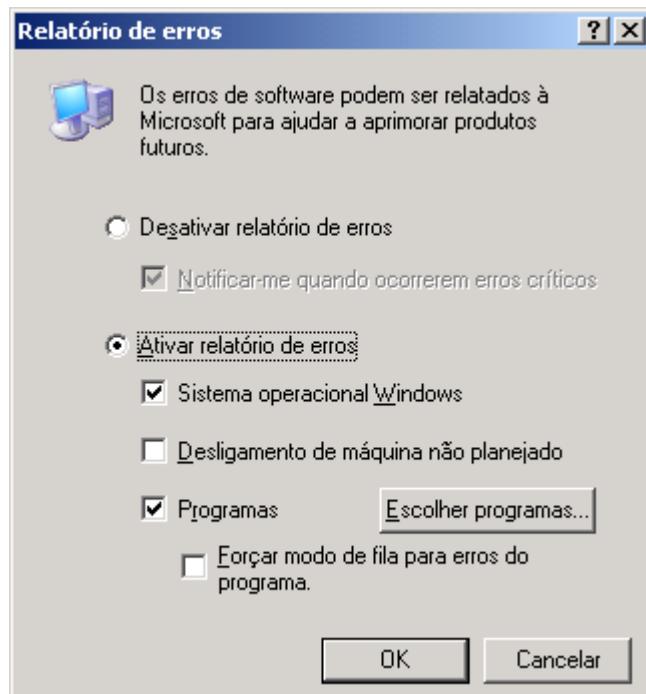


Figura 12.6 Configurando a geração de relatório de erros.

9. Para desabilitar completamente a geração de relatórios de erros clique em Desativar relatórios de erros. Ao marcar esta opção, você poderá habilitar/desabilitar a opção Notificar-me quando ocorrerem erros críticos. Ao marcar a opção Ativar relatórios de erros, você pode configurar para quais tipos de erros serão gerados relatórios, tais como: erros do Windows Server 2003, erros de desligamentos não planejados, como por exemplo uma queda de energia e erros para programas. Você pode usar o botão Escolher programas..., para definir para quais programas você quer que seja feito um relatório de erro em caso de falha/trancamento do programa
10. Defina as configurações desejadas e clique em OK. Você estará de volta à guia Avançado de configurações do sistema. Clique em OK para fechá-la e aplicar as configurações efetuadas. Dependendo das alterações que foram feitas (principalmente no arquivo de paginação), pode ser necessário reinicializar o servidor.

Com isso concluímos o nosso estudo sobre o processo de boot (inicialização) do Windows Server 2003. No próximo tópico veremos alguns detalhes sobre a Registry do Windows Server 2003.

## A Registry do Windows Server 2003.

A Registry é um banco de dados (hierárquico), onde o Windows Server 2003 armazena uma série de informações de configurações sobre o Hardware e o Software do computador. Informações importantes de inicialização do Sistema Operacional estão contidas na Registry. Se o Windows Server 2003 não puder acessar estas informações, não será possível fazer a inicialização do Sistema. As informações necessárias para a inicialização de drivers de hardware, de inicialização e carga de serviços, também estão armazenadas na Registry. A maioria dos aplicativos, ao serem instalados, armazenam informações na Registry do Windows Server 2003. Estas informações são necessárias para o correto funcionamento das respectivas aplicações.

Em resumo, a Registry é um banco de dados com informações vitais para o funcionamento do Windows Server 2003 e dos aplicativos instalados.

As informações da Registry estão armazenadas na seguinte pasta: C:\WINDOWS\system32\config. Supondo que o Windows Server 2003 esteja instalado no drive C:, na pasta C:\Windows.

A seguir descrevo algumas características gerais da Registry:

- ◆ As informações da Registry são divididas em categorias. Por exemplo, existe uma categoria na qual estão configurações do computador, ou seja, que são aplicadas a qualquer usuário que fizer o logon no computador. Existe uma outra categoria onde estão configurações de usuários, onde é mantido um conjunto de configurações separado para cada usuário. Por isso que é possível manter um ambiente personalizado para cada usuário. Observe que esta separação entre configurações do computador e configurações do usuário é o mesmo princípio utilizado pelo recurso de Group Policy Objects - GPO. Não poderia deixar de ser desta maneira, uma vez que o recurso de GPO trabalha intimamente relacionado com a Registry. Quando as configurações de uma GPO são aplicadas a um computador ou usuário, o que está sendo feito é aplicar uma série de alterações na Registry, alterando-a de acordo com as opções que foram definidas na GPO que está sendo aplicada.
- ◆ Os dados da Registry são gravados em arquivos binários, na pasta %Windir%\system32\config, onde %Windir% representa a pasta onde o Windows Server 2003 foi instalado. A única maneira de ter acesso a estes dados é utilizando o editor da Registry, conforme você aprenderá mais adiante ou usando programação. Por exemplo, em linguagens de programação como Delphi e VB.NET, dentre outras, você tem comandos para ler informações na Registry, criar novas chaves, alterar o valor de chaves existentes e assim por diante.
- ◆ As entradas da Registry onde são armazenados os valores, são conhecidas como chaves. Cada chave é definida como de um

---

**IMPORTANTE:** A maioria dos usuários provavelmente não necessite ter acesso e fazer alterações na Registry. Já para o Administrador do sistema e para os técnicos de suporte a Registry é uma ferramenta importante, a qual deve ser bem conhecida. Também é importante salientar que alterações incorretas, feitas na Registry, podem fazer com que o Windows Server 2003 deixe, inclusive, de inicializar. Por isso que somente devem ter acesso a fazer alterações na Registry, os usuários com o conhecimento adequado e que saibam exatamente o significado das alterações que estão fazendo.

determinado tipo de dado (que serão descritos mais adiante). Também é possível definir permissões de acesso aos elementos da Registry, de tal maneira que seja possível restringir quais usuários tem permissão a um ou mais conjuntos de chaves.

## Acessando e alterando informações na Registry do Windows Server 2003.

Vamos ver um exemplo prático, no qual iremos navegar através das diversas opções da Registry e aprender a executar algumas operações.

Exemplo: Acessando a Registry do Windows Server 2003.

1. Faça o logon como Administrador ou com uma conta do tipo Administrador do computador.
2. Selecione o comando Iniciar -> Executar. A janela Executar será aberta.
3. No campo Abrir digite regedt32 e clique em OK.
4. O Registry Editor (Editor do Registro) será aberto, conforme indicado na Figura 12.7:

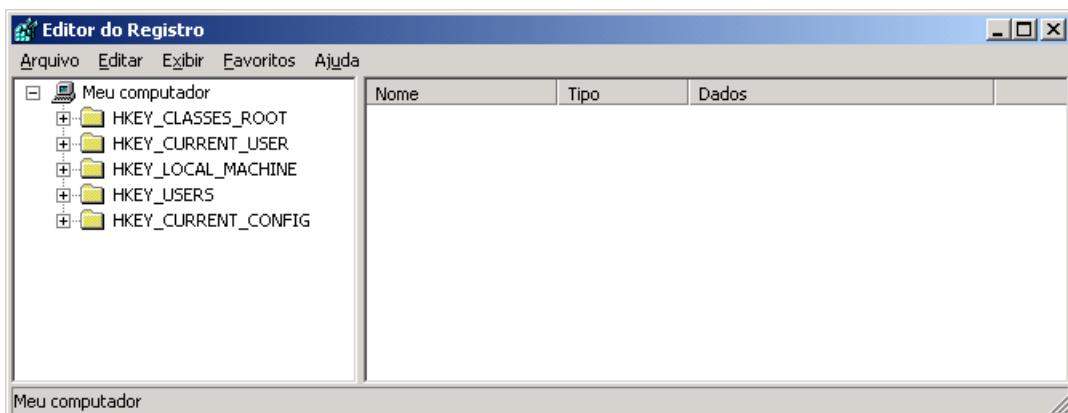


Figura 12.7 O editor da Registry do Windows Server 2003.

O banco de dados de Registry é um banco de dados hierárquico. Usando o Editor de Registro podemos navegar através do banco de dados da Registry, o qual é acessado na forma de uma estrutura de árvore de navegação, exatamente igual a estrutura de pastas e subpastas exibida no Windows Explorer.

O banco de dados da Registry está dividido em cinco grandes segmentos, os quais são a seguir descritos. Estes segmentos são chamados de subchaves da Registry.

Descrição das subchaves da Registry:

- ◆ **HKEY\_CLASSES\_ROOT:** É uma subchave de HKEY\_LOCAL\_MACHINE\Software, porém é exibida no primeiro nível para facilitar o acesso. As informações armazenadas nesta subchave garantem que o programa correto será aberto quando você abrir um arquivo usando o Windows Explorer. Em outras palavras, nesta subchave estão informações que associam uma determinada extensão de arquivo com o respectivo programa (.doc com o Word, .xls com o Excel e assim por diante). Por exemplo, quando você dá um clique duplo no ícone de um arquivo .doc, o Windows abre o Word e carrega o arquivo. Isto acontece porque o Windows associa a extensão do arquivo - .doc, com o Microsoft Word. Esta associação é feita através de informações gravadas nesta subchave, informações estas que relacionam as extensões dos arquivos com os respectivos programas. Por exemplo: arquivos .xls com o Microsoft Excel, arquivos .mdb com o Microsoft Access, arquivos .txt com o Bloco de Notas e assim por diante.

- ◆ **HKEY\_CURRENT\_USER:** Contém a base das informações de configuração para o usuário que estiver logado no momento. As configurações de pastas, de cores de tela e do Painel de controle do usuário são armazenadas aqui. Essas informações são chamadas de perfil do usuário. Conforme descrito no Capítulo 4, o Windows Server 2003 mantém um ambiente personalizado para cada usuário que faz o logon no computador. Este ambiente é mantido através de uma estrutura de pastas e subpastas dentro da pasta Documents and Settings, da partição onde o Windows Server 2003 está instalado. As informações que definem o ambiente do usuário são carregadas para esta subchave da Registry, quando o usuário faz o logon.
- ◆ **HKEY\_LOCAL\_MACHINE:** Contém informações de configurações específicas do computador, independentemente do usuário que estiver logado. Por exemplo informações sobre os aplicativos instalados (HKEY\_LOCAL\_MACHINE\SOFTWARE), sobre o control set a ser utilizado (HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet) e assim por diante.
- ◆ **HKEY\_USERS:** Contém a base de todos os perfis do usuário no computador. HKEY\_CURRENT\_USER é uma subchave de HKEY\_USERS.
- ◆ **HKEY\_CURRENT\_CONFIG:** Contém informações sobre o perfil de hardware usado pelo computador na inicialização do sistema.

A forma de navegação da Registry é idêntica a do Windows Explorer. Você clica no sinal de + ao lado de um chave e o Windows Server 2003 exibe as opções da respectiva chave. Algumas opções podem levar a outras. A forma de navegação é exatamente a mesma do Windows Explorer, onde vamos acessando pastas, subpastas e os arquivos de cada pasta. Ao acessar uma opção da Registry, no painel do lado direito são exibidos os diversos itens da opção selecionada. Um item, também chamado de entrada ou chave da registry, contém um valor associado. Antes de prosseguirmos, vamos definir os diversos tipos de componentes da Registry:

- ◆ **Sub-árvore (Subtree):** Uma sub-árvore representa para a Registry, o mesmo conceito que a pasta raiz representam para um volume no Windows Explorer. Uma sub-árvore é uma divisão lógica da Registry. Por padrão existem as seguintes sub-árvores: HKEY\_LOCAL\_MACHINE e HKEY\_USERS. Porém para facilitar a localização e edição das informações, o Editor de Registro exibe as informações divididas em cinco sub-árvores: HKEY\_CLASSES\_ROOT, HKEY\_CURRENT\_USER, HKEY\_LOCAL\_MACHINE, HKEY\_USERS e HKEY\_CURRENT\_CONFIG. Na prática é apenas uma maneira de facilitar a visualização, já que existem sub-árvores que, na prática, são parte integrante de outras. Como por exemplo a sub-árvore HKEY\_CURRENT\_USER que faz parte da sub-árvore HKEY\_USERS.
- ◆ **Chaves e subchaves:** Cada sub-árvore pode ser dividida em chaves e subchaves. Este conceito é idêntico a divisão de um volume em pastas e subpastas. Por exemplo, existe a sub-árvore HKEY\_LOCAL\_MACHINE já descrita anteriormente, dentro da qual existem as chaves HKEY\_LOCAL\_MACHINE\SOFTWARE, HKEY\_LOCAL\_MACHINE\SYSTEM, e assim por diante. Dentro da chave HKEY\_LOCAL\_MACHINE\SOFTWARE podem existir outras sub-chaves e assim por diante. É esta subdivisão que caracteriza o formato hierárquico da Registry.

---

**NOTA:** Para cada subchave destas existem dezenas, centenas de outras opções, sendo que cada opção pode levar a novas ramificações e novos valores de itens da registry. Existem livros inteiros somente sobre a Registry do Windows Server 2003.

- ◆ **Entrada:** Uma entrada é um item da Registry que possui um valor a ele associado. Dentro de uma chave ou subchave podem existir diversas entradas. Cada entrada possui um valor associado. Por exemplo considere a seguinte entrada: HKEY\_CURRENT\_USER\Control Panel\Keyboard\InitialKeyboardIndicators=2

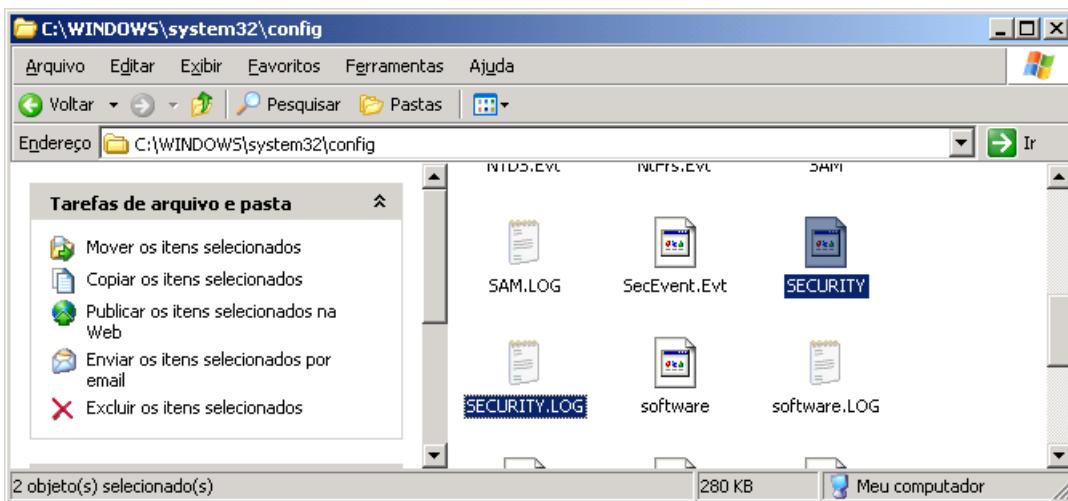
Estamos na sub-árvore HKEY\_CURRENT\_USER, dentro da qual estamos na chave Control Panel, dentro da qual na subchave Keyboard. Dentro da subchave Keyboard estamos considerando a entrada InitialKeyboardIndicators=2, a qual tem um valor definido como 2.

Existem diferentes tipos de entradas que podem ser criadas. Para cada tipo de entrada existe um conjunto de valores possíveis. Ao definir o tipo associado com uma Entrada da Registry estamos definindo os valores que podem ser atribuídos a respectiva entrada. No Windows Server 2003 temos os seguintes tipos possíveis de entrada da Registry:

- REG\_SZ:** Define a entrada como sendo do tipo String, ou seja, esta entrada aceita valores do tipo Texto.
- REG\_BINARY:** Esta entrada deve receber um valor na forma de uma String de dígitos Hexadecimais, como por exemplo: 0C 12 B6 D4. Cada par de valores Hexadecimais é interpretado como um byte.
- REG\_DWORD:** Esta entrada deve receber um valor na forma de uma String de 1 a 4 bytes Hexadecimais, como por exemplo: 0C 12 B6 D4. Este tipo de chave é normalmente utilizado para valores do tipo ligado/desligado, on/off, onde 0 indica desligado e 1 indica ligado.
- REG\_MULTI\_SZ:** Este tipo de entrada aceita múltiplos valores. Por exemplo, a lista de servidores DNS e a lista de servidores WINS, configurados nas propriedades do protocolo TCP/IP, são armazenados em uma chave do tipo REG\_MULTI\_SZ.
- REG\_EXPAND\_SZ:** Semelhante a REG\_SZ, com a diferença que este tipo de entrada pode conter um variável que é substituída pelo valor associado. Por exemplo, podemos criar uma chave deste tipo que contém a variável %CurrentUser%. Quando o usuário faz o logon, o valor desta entrada é definido como sendo o nome de logon do usuário atual, através da substituição da variável %CurrentUser% pelo respectivo nome de logon do usuário atual.

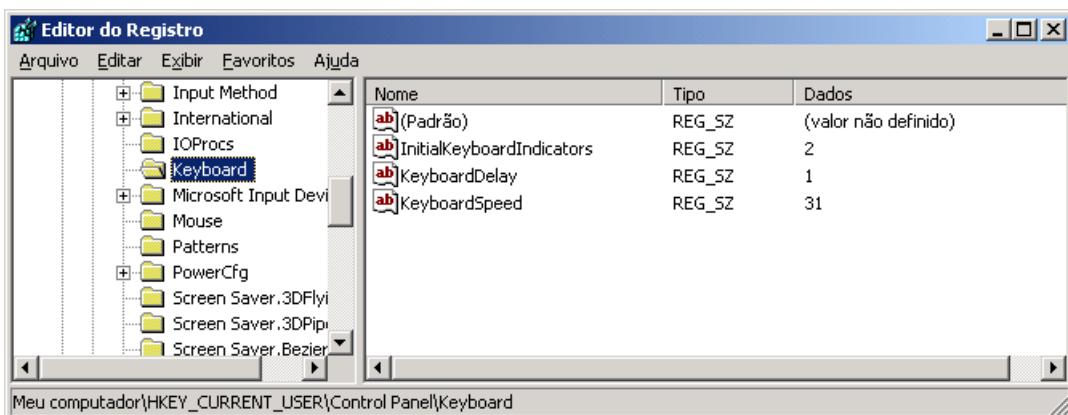
**NOTA:** A entrada InitialKeyboardIndicators define se a tecla NumLook aparecerá ligada ou desligada durante a inicialização do Windows Server 2003. A maioria dos usuários espera que esta tecla esteja ligada durante a inicialização, principalmente para usuários que fazem o logon em uma rede baseada no Windows 2000 Server ou Windows NT Server e utilizam dígitos como parte da senha. Se a tecla NumLook estiver desligada o teclado numérico estará desabilitado, sendo que os números deverão ser digitados nas teclas numéricas do teclado tradicional. O valor 2 indica que a tecla NumLook deve ser ligada durante a inicialização do Windows Server 2003. Este exemplo nos dá uma boa noção sobre a variedade de aspectos que são controlados pela Registry. Conforme já descrito anteriormente, está fora do escopo deste livro uma ampla descrição das entradas da Registry. Existem livros, até o momento apenas em Inglês, somente sobre a Registry do Windows 2000 e outros sobre a Registry do Windows Server 2003.

**Hive:** Uma Hive é um conjunto definido de Chaves, subchaves e as respectivas entradas, conjunto este normalmente associado a um determinado assunto, como por exemplo segurança. As entradas associadas a uma Hive são gravadas em um mesmo arquivo, na pasta %systemroot%\ System32\Config. Para cada Hive é criado um arquivo com o nome da Hive e sem extensão e um arquivo com o nome da Hive e a extensão .log. Por exemplo, para a Hive SECURITY, são criados os arquivos SECURITY e SECURITY.LOG, conforme indicado na Figura 12.8:



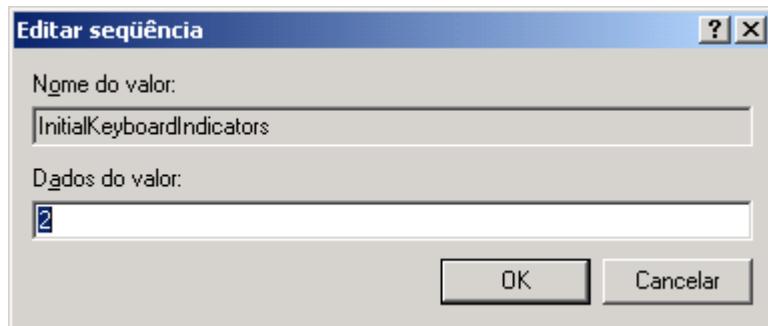
**Figura 12.8 Arquivos associados a Hive SECURITY.**

5. Clique no sinal de + ao lado de HKEY\_CURRENT\_USER para exibir as opções desta sub-árvore.
6. Nas opções que são exibidas, abaixo de HKEY\_CURRENT\_USER, clique no sinal de + ao lado da chave Control Panel. Serão exibidas as subchaves de Control Panel.
7. Nas subchaves de Control Panel clique em Keyboard, para exibir as entradas desta subchave. Observe no Painel da direita que são exibidas as entradas para a subchave Keyboard, conforme indicado na Figura 12.9:



**Figura 12.9 As entradas da subchave HKEY\_CURRENT\_USER\Control Panel\Keyboard\.**

8. Verifique se o valor da entrada InitialKeyboardIndicators está definido em 2. Se não estiver, vamos editá-lo, a título de exemplo.
9. Para editar uma entrada da Registry basta dar um clique duplo na respectiva entrada que o Windows Server 2003 exibe uma janela com o valor atual da entrada. Nesta janela você pode alterar o valor desejado, conforme indicado na Figura 12.10:

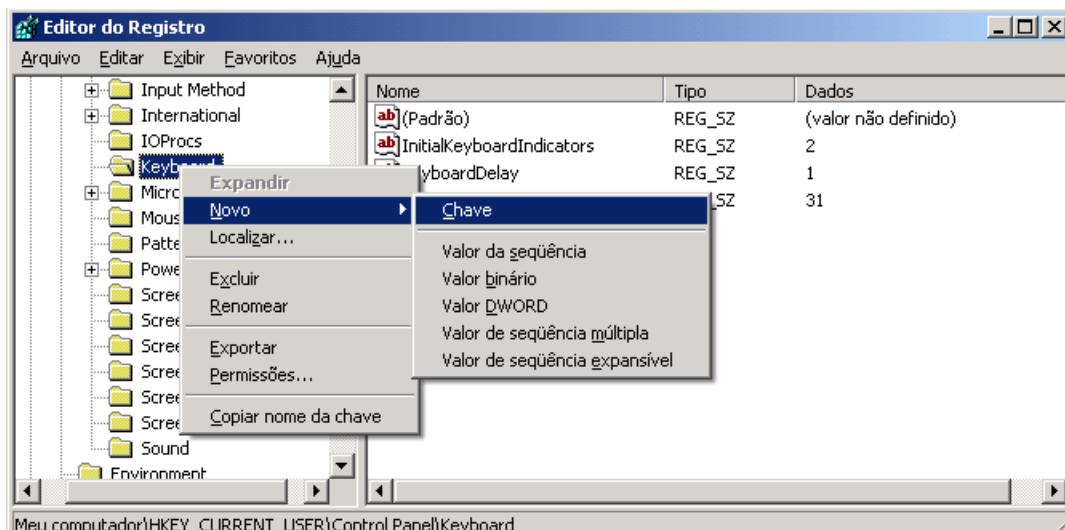


**Figura 12.10 Editando o valor da entrada InitialKeyboardIndicators.**

10. Se o valor estiver diferente de 2 digite 2 e clique em OK. Você estará de volta ao Editor da Registry.

Em determinadas situações pode ser que seja necessária a criação de novas chaves ou de novas entradas na Registry. Na prática, a maioria das chaves da Registry são criadas, automaticamente, pelo Windows Server 2003 e pelos aplicativos quando estes são instalados. Porém em determinadas situações pode ser necessária a criação de chaves ou entradas diretamente na Registry. Você deve tomar muito cuidado com este procedimento e somente criar chaves ou entradas quando este procedimento for recomendado pela documentação do Windows Server 2003, pela documentação do aplicativo ou pelo manual de algum dispositivo de hardware.

Para criar uma nova chave ou entrada, basta clicar com o botão direito do mouse no local onde a chave/entrada deve ser criada e selecionar o comando Novo. Será exibido um menu de opções onde você pode selecionar se deseja criar uma nova chave ou uma nova entrada de um dos cinco tipos descritos anteriormente, conforme indicado na Figura 12.11:



**Figura 12.11 Criando novas chaves/entradas na Registry.**

Para excluir uma chave ou entrada da Registry basta clicar no elemento a ser excluído e pressionar o botão Delete. Cuidado que ao excluir uma chave, todas as suas subchaves e respectivas entradas serão excluídas. Todos os cuidados que foram recomendados para a adição e alteração de chaves e entradas também são válidas, só que em dobro, para a exclusão. Se você excluir, por engano, chaves utilizadas pelo Windows Server 2003, poderemos ter situações em que o Windows Server 2003 não poderá mais reiniciar corretamente.

Podem existir situações em que partes inteiras da Registry de um computador tenha que ser copiadas para um computador semelhante. Esta por exemplo é uma maneira rápida de copiar as configurações da registry feitas em um servidor para

vários outros servidores, sem ter que repetir as configurações manualmente em cada servidor. Para copiar partes da Registry utilizamos os seguintes passos:

- ◆ No computador de origem exporte a parte da registry a ser copiada para outro (ou outros) computador. Para exportar uma chave e suas subchaves, basta clicar com o botão direito do mouse na chave a ser exportada. No menu que é exibido clique em Exportar. Será exibida a janela Exportar arquivo de Registro. Nesta janela você define a pasta e o nome do arquivo onde as configurações serão salvas. As configurações são salvas em um arquivo .reg.
- ◆ No computador de origem, onde as configurações devem ser copiadas basta abrir o Windows Explorer, localizar o arquivo .reg, gerado no passo anterior e dar um clique duplo no arquivo. O Windows Server 2003 emite uma mensagem pedindo a confirmação para a importação das entradas contidas no arquivo .reg para a Registry do sistema, conforme indicado na Figura 12.12. Clique em Sim e as entradas serão importadas.

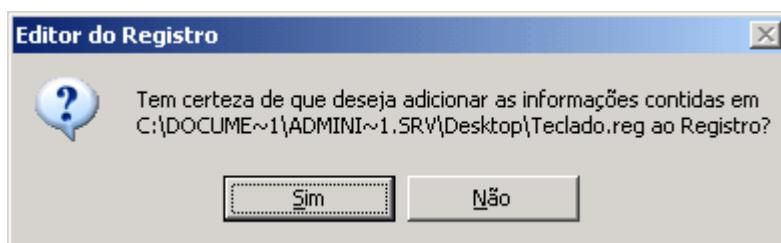


Figura 12.12 Importando as entradas de um arquivo .reg.

Existem permissões associadas com as chaves e subchaves da Registry. Através das permissões o Windows Server 2003 controla quais usuários e grupos podem acessar, alterar e, até mesmo, excluir chaves e subchaves da registry. Para configurar as permissões associadas a uma chave basta localizar a respectiva Chave, clicar com o botão Direito do mouse e, no menu que é exibido, clicar em Permissões. Será exibida a janela de Permissões para a chave selecionada, janela esta indicada na Figura 12.13.

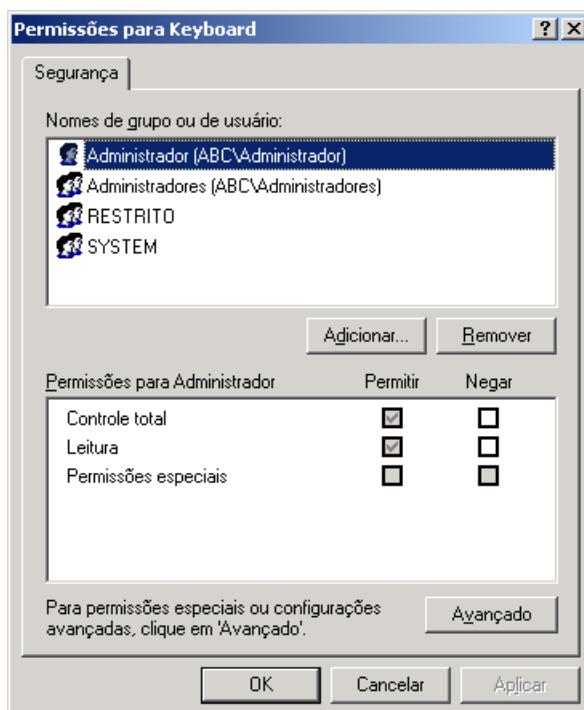
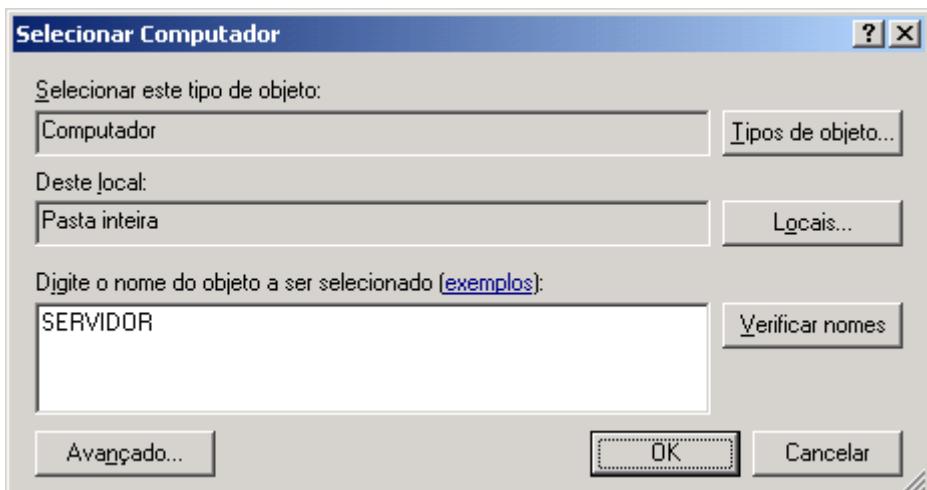


Figura 12.13 Janela para definir permissões na Registry.

A janela de permissões é semelhante a janela de permissões para pastas e subpastas, descrita no Capítulo 6. É possível, inclusive, definir auditoria em chaves da Registry, para que fique registrado quais usuários fizeram acesso e quais as operações executadas por cada usuário. A auditoria é definida para cada chave individualmente. As configurações de Auditoria são acessadas através do botão Avançado.

Você também pode se conectar com a Registry de outros computadores da rede, desde que tenha a devida permissão para isso. Para se conectar com a Registry de outro computador basta utilizar o comando Arquivo -> Conectar Registro da rede... Será exibida a janela Selecionar computador. Digite o nome do computador do qual você deseja acessar a Registry, conforme exemplo da Figura 12.14 e clique em OK.



**IMPORTANTE:** Lembre que para habilitar a auditoria em chaves da registry, antes você deve habilitar a diretiva de auditoria: Auditoria de acesso a objetos. Esta diretiva deve ser habilitada quando você deseja fazer a auditoria de acesso em pastas e arquivos, em impressoras, em OUs, em chaves da Registry, enfim, quando você deseja fazer auditoria em qualquer tipo de objeto que tenha uma lista de permissões associada (ACL – Access Control List).

Figura 12.14 Conectando com a Registry de outro computador, remotamente.

O Editor de Registro faz a conexão e exibe as informações da Registry do computador remoto, conforme indicado na Figura 12.15:

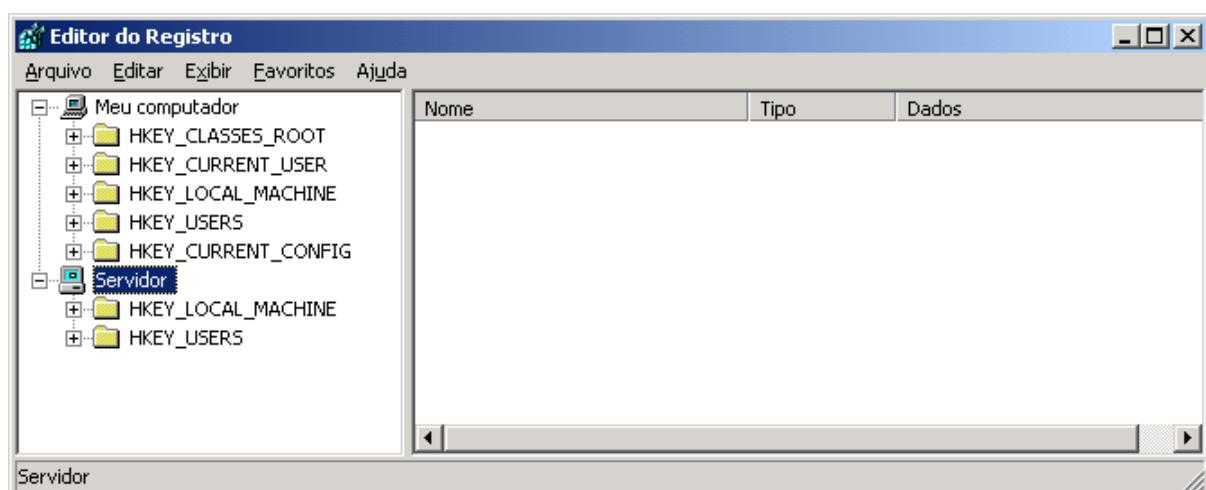


Figura 12.15 Informações da Registry de outro computador da rede (Servidor).

11. Feche o Editor de Registro.

12. Reinicialize o Windows Server 2003 e verifique se a tecla NumLook é ligada automaticamente, mesmo antes de você fazer o logon no Windows Server 2003. Isto comprova que a alteração que fizemos na Registry, definindo o valor da chave HKEY\_CURRENT\_USER\Control Panel\Keyboard\InitialKeyboardIndicators=2 está funcionando corretamente.

## O Modo Seguro, Last Know Good Configuration e Control Sets..

Neste tópico veremos conceitos importantes, principalmente quando acontecem problemas na reinicialização do sistema. Vamos tratar dos seguintes tópicos:

- ◆ Opções de inicialização do Windows Server 2003 e o Modo seguro.
- ◆ Last Know Good Configuration e Control Sets.

### Opções de inicialização do Windows Server 2003 e o Modo seguro.

Ao inicializar o Windows Server 2003, será exibido um menu de opções (caso esteja instalada mais de uma versão do Windows Server 2003), menu este que é montado a partir de informações do arquivo boot.ini, conforme descrito anteriormente. Este menu somente é montado e exibido se existirem, pelo menos duas opções de inicialização diferentes, no arquivo boot.ini. Consideramos como sendo “diferentes opções de inicialização”, diferentes versões do Windows (9x, Me, NT, 2000 ou XP) ou uma mesma versão com diferentes chaves de inicialização como por exemplo /fastdetect e /basevideo. Se houver uma única opção o menu não será exibido.

Quando o menu é exibido você pode selecionar uma das opções do menu e pressionar Enter. Logo após pressionar Enter é exibida a mensagem Iniciando ... Se neste momento você pressionar a tecla F8, será exibido um menu de opções avançadas de inicialização. Se não for exibido o menu, ou seja, se houver uma única opção de inicialização, você deve ficar atento à tela do computador. Quando as primeiras mensagens começarem a aparecer na tela, você deve pressionar a tecla F8 para exibir o menu com as opções avançadas de inicialização, opções estas que serão descritas neste item.

- ◆ Safe Mode (Modo seguro)
- ◆ Safe Mode with Networking (Modo seguro com rede)
- ◆ Safe Mode with Command Prompt (Modo seguro com prompt de comando)
- ◆ Enable Boot Logging (Ativar log de inicialização)
- ◆ Enable VGA Mode (Ativar modo VGA)
- ◆ Last Known Good Configuration (Última configuração válida)
- ◆ Directory Service Restore Mode (Modo de restauração de serviços de diretório (só control. de domínio))
- ◆ Debugging Mode (Modo de depuração)

---

**NOTA: No Windows Server 2003 você pode pressionar a tecla F8 enquanto o menu de inicialização, com as diferentes versões do Windows estiver sendo exibido. Ao pressionar F8 será exibido o menu de opções avançadas do Windows, no qual são exibidas as seguintes opções de inicialização:**

---

É comum utilizarmos o menu de opções avançadas quando estamos com problemas na inicialização do Windows Server 2003. Nestas situações, as opções do menu avançado podem nos ajudar na solução de problemas, conforme veremos na seqüência. Vamos analisar cada uma destas opções, iniciando pelas opções de Modo seguro.

## Entendendo o Modo seguro de inicialização – Safe mode.

Quando o Windows Server 2003 não está conseguindo inicializar no modo Normal, temos a opção de inicializa-lo no Modo seguro. No Modo seguro apenas os drivers e serviços estritamente necessários à inicialização do sistema são carregados. O sistema é inicializado utilizando um driver de vídeo padrão VGA, com resolução de 640x480 e com suporte a milhões e cores (24 bits), com suporte ao mouse, teclado, monitor, sistema de armazenamento local (discos rígidos, disquete, etc). Os programas configurados para serem inicializados automaticamente são ignorados no Modo seguro. Todo este cuidado é tomado para que o Windows Server 2003 possa inicializar, mesmo que com um conjunto mínimo e drivers e serviços. Uma vez inicializado, você poderá alterar as configurações que estão impedindo que o Windows Server 2003 inicialize no modo Normal.

A maioria das ferramentas de configuração estão disponíveis no modo Seguro, para que você possa fazer as configurações necessárias, para corrigir os problemas que estão impedindo o Windows Server 2003 de inicializar no modo Normal. Por exemplo, no modo Seguro temos acesso ao Painel de controle, às Ferramentas Administrativas, ao utilitário de Backup, ao Editor de registro, às configurações de rede e assim por diante.

Se você desconfia que o problema é com algum hardware recém instalado ou com o driver de hardware instalado, utilize o Gerenciador de dispositivos para verificar se existe algum problema de hardware. Se o Windows Server 2003 consegue inicializar no modo Seguro é porque os serviços básicos do Sistema Operacional estão funcionando corretamente. Se o Windows Server 2003 deixou de inicializar normalmente após a instalação de um driver é provável que o respectivo driver seja a causa do problema. Estando no Modo Seguro você pode utilizar o Gerenciador de Dispositivos para desinstalar ou desabilitar o driver que está causando problemas. Uma vez desabilitado o referido driver, o Windows Server 2003 deverá voltar a inicializar normalmente.

Ao fazer a inicialização no Modo Seguro, o Windows Server 2003 vai exibindo cada driver e serviço que vai sendo carregado. A inicialização no Modo Seguro utiliza a chave /sos, já descrita anteriormente. Ao iniciar o computador no modo Seguro você deve fazer o logon como Administrador ou com uma conta do tipo Administrador do computador, para que você possa ter acesso a todas as configurações do Windows Server 2003 e fazer as alterações necessárias. Após fazer o logon uma mensagem é emitida, avisando sobre as limitações do Modo seguro e perguntando se você realmente deseja entrar neste modo, conforme indicado na Figura 12.16. Clique em Sim e o Windows Server 2003 será carregado no Modo seguro.

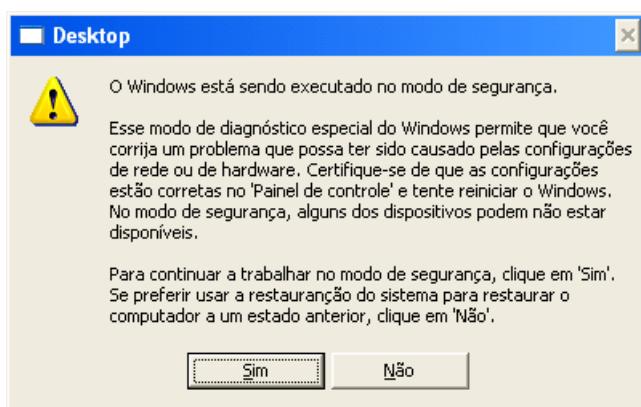


Figura 12.16 Confirmação para entrar no Modo Seguro.

Uma vez tendo feita as alterações necessárias você deve reiniciar o computador para testar se as alterações que foram feitas surtiram o efeito desejado, qual seja, permitir que o Windows Server 2003 possa voltar a inicializar no modo Normal.

Se você precisa acessar recursos da rede, ao invés da opção Modo seguro, deve selecionar a opção Modo seguro com rede. Com esta opção o sistema de rede do Windows será carregado (desde que não existam problemas que impeçam a carga dos componentes de rede) e, mesmo no Modo Seguro, você terá acesso aos recursos da rede.

A opção Modo seguro com prompt de comando carrega o Windows Server 2003 porém não carrega a interface gráfica, mas sim a interface de linha de comando (Cmd.exe) com suporte a todos os comandos reconhecidos pelo Windows Server 2003. Devido às facilidades da interface gráfica, dificilmente alguém vai optar por esta opção, a não ser que você seja um fã de carteirinha da interface baseada na linha de comando.

Em resumo podemos afirmar que o Modo Seguro (ou Modo de Segurança) é uma ferramenta especialmente útil quando o Windows Server 2003 está com problemas para inicializar no Modo Normal. Nestas situações podemos inicializar no Modo Seguro e fazer as alterações necessárias para que o Windows Server 2003 possa voltar a inicializar no modo Normal.

Agora vamos entender um pouco melhor a opção Ultima configuração válida (Last Know Good Configuration) e a sua relação com os chamados Control Sets. Na parte final deste item trataremos das demais opções do Menu de opções avançadas do Windows.

## Last know good configuration e Control Sets.

A opção Última configuração válida é indicada em situações onde a instalação de um novo driver está causando problemas sérios, impedindo que o Windows Server 2003 possa inicializar normalmente. Vamos supor que você baixou da Internet uma nova versão para o driver da placa de rede do servidor. Você instala a nova versão do driver e ao reiniciar o computador, o Windows Server 2003 não consegue inicializar normalmente. Nesta situação você pode inicializar utilizando as opções avançadas do menu de inicialização e selecionar a opção Last know good configuration. Com isso serão carregadas as configurações da última configuração com a qual o Windows Server 2003 conseguiu inicializar normalmente, ou seja, as configurações anteriores a atualização do driver que está causando o problema.

Ao selecionar a opção Last know good configuration o Windows Server 2003 será inicializado usando as informações da Registry que o Windows Server 2003 salvou na última vez que você fez o logon no Windows Server 2003 com sucesso, ou seja, as informações da Última configuração válida. As informações sobre a Última configuração válida são armazenadas na Registry do Windows Server 2003.

Ao inicializar um computador com o Windows Server 2003 estão disponíveis duas configurações para inicialização: Default and LastKnownGood. Estas configurações são conhecidas como Control Sets. Um Control Set é um conjunto de configurações da Registry, configurações estas utilizadas para inicializar o computador. Quando você faz o logon no Windows Server 2003 normalmente e faz alterações nas configurações, como por exemplo instalar uma nova versão de um driver, estas alterações são salvas no Current control set. Ao encerrar o Windows Server 2003 (Shutdown) as alterações são copiadas para o control set Default. Na próxima vez que você fizer o logon com sucesso, as configurações do control set Default serão copiadas para o control set Last Known Good Configuration. Se você não conseguir fazer o logon com sucesso devido às últimas alterações, você tem a opção de reiniciar o sistema e utilizar a opção Last know good configuration. Observe que as configurações da Última configuração válida somente são

---

**NOTA: O Modo Seguro também é conhecido como Modo de Segurança. As duas expressões são sinônimos.**

---

**IMPORTANTE: O Modo seguro com rede não funcionará em computadores portáteis que estão utilizando cartões PCMCIA de rede. O suporte a cartões PCMCIA é desabilitado no Modo seguro, mesmo quando você seleciona a opção Modo seguro com rede.**

---

sobrescritas depois que você faz as alterações, reinicializa o computador e consegue fazer o logon com sucesso. Se devido às alterações você não conseguir fazer o logon ou sequer reinicializar o Windows Server 2003, as configurações da Última configuração válida não serão sobreescritas e você terá a opção de carregá-las na próxima inicialização, revertendo as alterações que foram feitas e estão impedindo o Windows Server 2003 de inicializar corretamente.

Você pode utilizar a Última configuração válida em situações tais como:

- ◆ Você instalou uma novo driver ou uma nova versão de um driver existente e o Windows Server 2003 não consegue mais inicializar corretamente. Nesta situação você pode reinicializar utilizando a opção Last know good configuration. Com isso as configurações anteriores a alteração que não está funcionando serão carregadas e o Windows Server 2003 volta a inicializar normalmente.
- ◆ Por engano ou por sabotagem um dispositivo fundamental, como por exemplo o controlador IDE foi desabilitado. Se um dispositivo como o controlador IDE for desabilitado, o Windows Server 2003 não conseguirá inicializar normalmente. Nestas situações você pode utilizar a Última configuração válida para restaurar as configurações que estavam funcionando normalmente.

## Outras opções de configuração do Menu de opções avançadas do Windows

Vamos analisar as demais opções do Menu de opções avançadas.

- ◆ **Ativar log de inicialização:** Ao selecionar esta opção o Windows Server 2003 cria um log com a descrição da carga e inicialização de drivers e serviços. Este log é gravado em um arquivo chamado NTBTLOG.TXT, o qual é gravado na pasta onde o Windows Server 2003 está instalado. Ao inicializar o Windows Server 2003 no Modo Seguro este log também é automaticamente criado.
- ◆ **Ativar modo VGA:** Esta opção inicializa o Windows Server 2003 utilizando um driver VGA com configurações mínimas. Esta opção é útil quando você está tendo problemas com o driver da placa de vídeo ou do monitor.
- ◆ **Última configuração válida:** Já descrita anteriormente.
- ◆ **Modo de depuração:** Inicializa o Windows Server 2003 no modo de depuração do Kernel.

---

**IMPORTANTE:** Lembre que se após ter feito alguma alteração, o Windows Server 2003 reiniciar e você conseguir fazer um logon, as configurações do control set Last Know Good Configuration serão sobreescritas pelas configurações atuais. Nesta situação você não poderá mais utilizar a opção Última configuração válida, para voltar à situação anterior. Para estas situações é que existe a opção Restauração do sistema, a qual veremos mais adiante.

---

## Diversas ferramentas de recuperação a desastres.

Neste tópico apresentarei uma série de itens relacionados a recuperação de um servidor em caso de problemas diversos, tais como quando um arquivo fundamental é corrompido ou quando um driver de hardware causa instabilidade do sistema e assim por diante. Você também aprenderá sobre o uso do Console de recuperação. Mostrarei como instalar o Console de recuperação e quais os principais comandos disponíveis.

## O recurso ASR – Automated System Recovery Disks

No Windows NT Server 4.0 e no Windows 2000 Server o administrador pode criar um disco chamado ERD – Emergency Repair Disk. Este disco contém informações que podem ser utilizadas para reparar o servidor em situações de

emergência, como por exemplo quando um arquivo de inicialização (ntldr, ntoskrnl.exe, etc.) é corrompido. O administrador pode dar um boot usando o CD do Windows 2000 Server, iniciar a instalação e bem no início informar que será feita uma reparação de uma instalação já existente. Neste momento é que será necessário o disquete ERD. Já no Windows Server 2003 este procedimento mudou bastante. Não existe mais o conceito de ERD. Ao invés disso foi criado o chamado ASR - Automated System Recovery (recuperação automatizada do sistema).

O administrador pode criar um conjunto de discos ASR, regularmente, como parte de um plano de recuperação do sistema em caso de falhas. Os discos do ASR contém informações fundamentais para o funcionamento do Windows Server 2003, informações estas que podem ser utilizadas para substituir arquivos corrompidos, corrigir defeitos no setor de boot e no ambiente de inicialização do Windows Server 2003. O recurso ASR deve ser utilizado como uma última tentativa de recuperar o sistema, depois que várias outras tentativas foram esgotadas, tais como usar o modo seguro, a opção Last Known Good Configuration e o console de recuperação (que será descrito mais adiante).

O recurso ASR é composto de duas partes: O backup ASR e o restore ASR. Para fazer o Backup ASR, utilizamos o Automated System Recovery Preparation (Assistente de preparação para a recuperação do sistema) do ASR, o qual está disponível como uma das opções do utilitário de backup. Este assistente faz o backup do estado do sistema, dos serviços configurados e de todos os discos associados com a instalação do Windows Server 2003. Também é criado um disquete, qual contém informações sobre o backup, configurações dos discos do sistema (incluindo informações dos discos básicos e discos dinâmicos) e informações sobre como deve ser efetuada a restauração do sistema. Este disquete é denominado ASR disk ou disco ASR.

Para fazer a restauração do sistema, usando os discos criados pelo assistente de backup do ASR, você deve iniciar uma instalação normal do Windows Server 2003 (por exemplo, a partir de um boot pelo CD-ROM, usando o CD de instalação do Windows Server 2003). Em uma das etapas da instalação, bem no início, ainda na parte de texto, tem uma mensagem informando que você pode pressionar a tecla F2 para fazer uma restauração do sistema. Nesta etapa você pressiona F2 e será solicitado que você insira o disquete ASR no drive. O ASR lê as informações sobre os discos do sistema a partir do disquete ASR e restaura todas as assinaturas de discos, volumes e partições, pelo menos nos discos necessários para que o Windows Server 2003 seja inicializado. O ASR tentará restaurar as configurações de todos os discos e volumes/partições, mas pode acontecer de ele não conseguir restaurar as informações sobre todos os volumes. O ASR irá instalar uma versão simplificada do Windows Server 2003, apenas com o suficiente para iniciar um restore a partir do backup feito pelo ASR, utilizando o Automated System Recovery Wizard, backup este que normalmente é feito em fita em fita.

Observações sobre o ASR:

- ◆ O ASR não faz o backup dos arquivos de dados, apenas dos arquivos do sistema, necessários ao funcionamento do ASR. O backup dos dados deve ser feito separadamente, usando uma política de backup e agendamento de tarefas de backup, conforme descrito no Capítulo 8.
- ◆ O ASR tem suporte a volumes FAT16 com tamanho máximo de 2.1 GB. O ASR não tem suporte para volumes FAT16 com tamanho de 4 GB, volumes estes que utilizam um tamanho de cluster de 64 Kb. Se o servidor tiver uma partição FAT 16 de 4 GB (o que é muito pouco provável), primeiro você deve converter este volume para NTFS, para depois usar o ASR. Para converter um volume de FAT16 ou FAT32 para NTFS basta usar o comando convert. Por exemplo, para converter o drive C: de FAT para NTFS, utilize o seguinte comando:

**convert C: /fs:NTFS**

A seguir mostrarei como usar o assistente de backup e o Assistente de preparação para a recuperação do sistema.

Exemplo: Usar o assistente de backup e o Assistente de preparação para a recuperação do sistema, para criar um conjunto de discos para recuperação automática do sistema. Para isso siga os passos indicados a seguir:

1. Faça o logon como administrador ou com uma conta com permissão de administrador.
2. Abra o utilitário de backup: Iniciar -> Todos os programas -> Acessórios -> Ferramentas do sistema -> Backup.
3. Se for aberto o assistente de backup clique na opção Modo avançado, para abrir o utilitário de backup no modo avançado.
4. O utilitário de backup será aberto, com a guia Bem vindo selecionada por padrão. Nesta guia está disponível a opção Assistente para recuperação automática do sistema, conforme indicado na Figura 12.17:

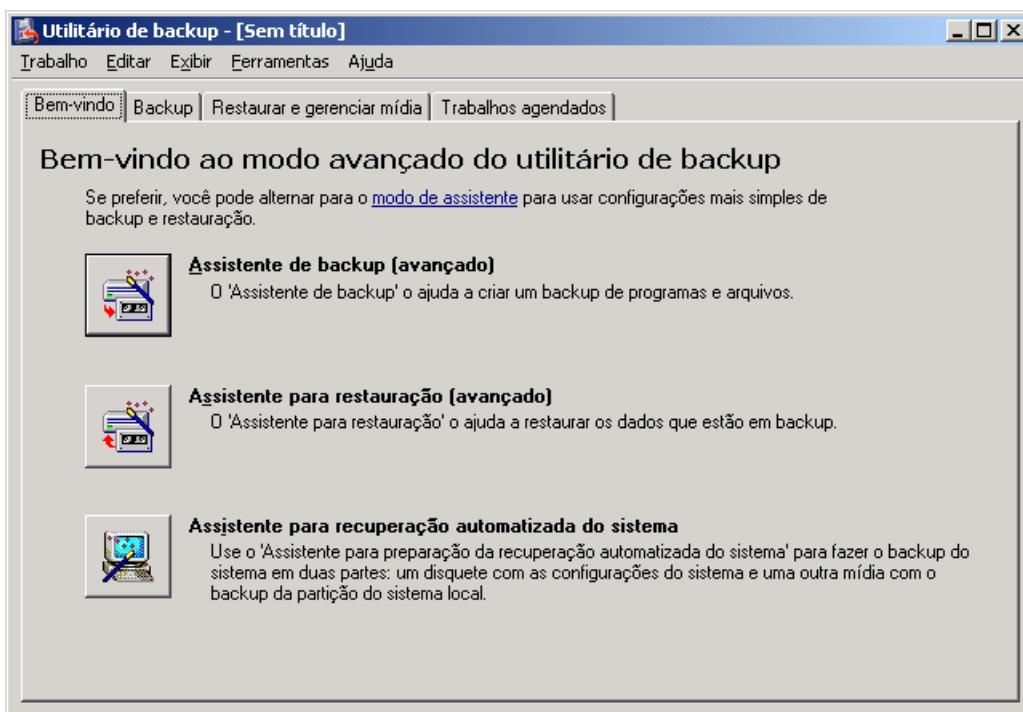
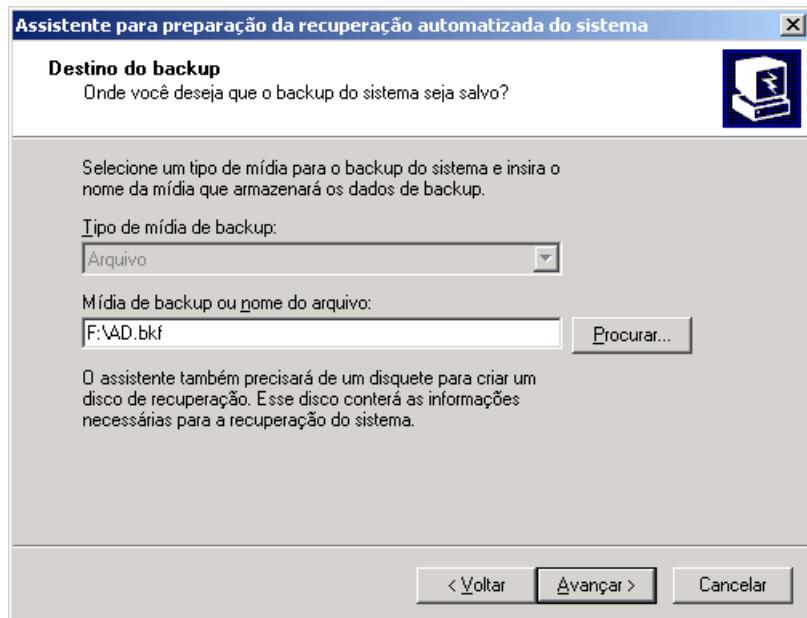


Figura 12.17 O assistente do ASR.

5. Clique nesta opção.
6. Será iniciado o assistente Assistente para preparação da recuperação automatizada do sistema. A primeira tela do assistente é apenas informativa. Clique em Avançar, para seguir para a próxima etapa do assistente.
7. Nesta etapa você deve selecionar o destino para o backup. Se você tiver um drive de fita instalado, poderá gravar em fita. Esta é a opção mais recomendada. Você também pode gravar o backup em disco, preferencialmente em um disco da rede. Afinal de nada adiantaria gravar o backup do ASR no mesmo disco onde está instalado o Windows Server 2003, pois se este disco apresentasse problemas, você perderia o disco e também o backup, ou seja, ficaria sem nada. Selecione o destino para o backup, conforme exemplo da Figura 12.18 e clique em Avançar, para seguir para a próxima etapa do assistente.



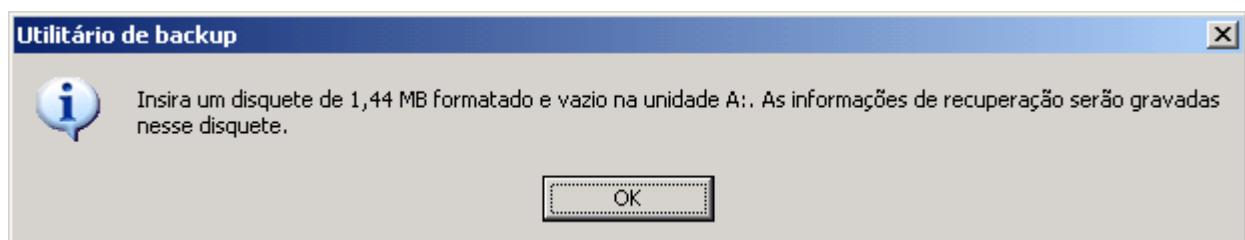
**Figura 12.18 Selecionando o destino para o backup do ASR.**

8. Será exibida a tela final do assistente. Clique em Concluir. O processo de backup para gerar as informações necessárias para um restauração do sistema será iniciado.
9. Após a conclusão do backup do ASR, o Windows emite uma mensagem solicitando que você insira um disco em branco na unidade de disquete, conforme indicado na Figura 12.19:

---

**NOTA: O backup do ASR não poderá ser feito diretamente em CD ou DVD, mesmo que você tenha um drive gravador de CD ou gravador de DVD.**

---



**Figura 12.19 Criação do disquete do ASR.**

10. Clique em OK para iniciar a criação do disquete do ASR.
11. O disquete será criado e uma mensagem será exibida, orientando você a identificar o disquete e guardá-lo em local seguro. Clique em OK para fechar a mensagem de aviso.

Pronto, o backup do ASR foi criado e poderá ser utilizado para restaurar o servidor em caso de falhas graves. Para usar o backup do ASR você deve iniciar uma instalação do Windows Server 2003 normalmente e, em uma das etapas iniciais, fique atento a mensagem que indica que você deve pressionar a tecla F2 para restaurar o estado do sistema usando um backup do ASR.

O que é contém o disquete do ASR: O disquete do ASR é como se fosse um “mapa” para encontrar as demais informações necessárias ao processo de restauração. No disquete do ASR são gravados os seguintes arquivos:

- ◆ **Setup.log:** Contém a localização dos arquivos do sistema.
- ◆ **Asr.sif:** Contém informações sobre os discos, partições, volumes e sobre a mídia utilizada para fazer o backup do ASR.
- ◆ **Asrpnp.sif:** Contém informações sobre os dispositivos de hardware, instalados no servidor, e que são compatíveis com o padrão Plug and Play.

**DICA:** Sempre que você estiver para fazer alterações importantes no servidor, tais como instalação de novos dispositivos de hardware ou instalação de novos serviços e sistemas, é recomendado que, antes de fazer as modificações, você faça um backup do ASR. Com isso, você poderá usar este backup para restaurar o servidor a uma situação de normalidade, caso aconteça algum erro grave, devido as modificações que estão sendo feitas. É importante salientar novamente, que o restore a partir de um backup do ASR deve ser considerado como uma última alternativa, quando outros recursos como o Modo de segurança e a última configuração válida já falharam. Alterações tais como inserção de um novo disco ou exclusão de volumes e criação de novos volumes também podem ser consideradas grande alterações e, consequentemente, antes de fazer estas alterações, crie um novo backup do ASR. Após ter feito as alterações e o servidor estar funcionando normalmente, é hora de criar o backup do ASR novamente, para que agora ele já contenha as últimas alterações, as quais estão funcionando sem problemas.

## Criando um disquete de boot.

O conceito de disquete de boot no Windows NT, Windows 2000, Windows XP ou Windows Server 2003 é bem diferente do conceito de disquete de boot no Windows 95/98/Me. No Windows 95/98/Me ao usar um disquete de boot, o sistema é inicializado no modo caractere, é aberto um prompt de comando e você tem acesso ao disco rígido e demais unidades de disco. Já no Windows NT/2000/XP/2003, o disquete de boot não inicializa o sistema no modo caractere, com um prompt de comando e acesso aos volumes (C:, D:, etc). Além disso, o uso do disquete de boot terá pouca utilidade, principalmente com a disponibilidade do Console de recuperação, o qual descreverei mais adiante.

Mas existem algumas circunstâncias em que o disquete de boot pode ser útil, mais especificamente para auxiliar na inicialização do sistema, quando ocorrer um dos seguintes problemas:

- ◆ Quando o setor de boot do disco rígido estiver corrompido.
- ◆ Quando o MBR – master boot Record do disco rígido estiver corrompido.
- ◆ Quando um vírus tiver infectado o MBR.
- ◆ Quando os arquivos ntldr ou ntdetect.com estiverem corrompidos ou tiverem sido excluídos por engano.

Exemplo: Para criar um disquete de boot para um determinado servidor, siga os passos indicados a seguir:

1. Faça o logon como administrador ou com uma conta com permissão de administrador.
2. Insira um disquete em branco no drive de disquete
3. Abra um Prompt de comando: Iniciar -> Todos os programas -> Acessórios -> Prompt de comando.
4. Execute o comando format a: /u
5. Aguarde a conclusão do comando e copie os arquivos Ntdetect.com e Ntldr, da pasta i386 do CD de instalação do Windows Server 2003, para o disquete. Copie também o arquivo Boot.ini, que se encontra na raiz do C:\.

**NOTA:** Outra situação prática em que o disco de boot pode ser útil é quando você tem um volume espelhado, no qual está instalado o Windows Server 2003. Pode acontecer do disco principal do espelhamento (aquele a partir do qual o Windows Server 2003 é carregado) apresentar problemas. Neste caso você pode usar um disquete de boot, alterando o

6. Pronto, está criado o CD de boot, o qual é específico para o servidor onde foi criado e que poderá ser utilizado nas situações descritas no início deste tópico.

## O Console de Recuperação.

O Console de Recuperação foi uma das novidades introduzidas com o Windows 2000 Server e que também está presente no Windows XP Professional e no Windows Server 2003. O Console de Recuperação não é instalado, automaticamente, quando o Windows Server 2003 é instalado. Neste item mostrarei como instalar o Console de Recuperação.

Após instalar o console de recuperação, este será adicionado como uma opção do menu de inicialização do computador, conforme descrito anteriormente. Ao selecionar a opção para inicializar no modo de recuperação, o servidor será inicializado em um modo muito parecido com o Prompt de comando. Neste modo estarão disponíveis uma série de comandos (descritos mais adiante). Estão disponíveis comandos para acessar os arquivos do disco rígido, para habilitar/desabilitar drivers e assim por diante.

Se o modo de segurança e outras opções de inicialização não funcionarem, você poderá considerar o uso do Console de recuperação (claro que este deve ter sido instalado previamente). No entanto, esse método é recomendado somente se você for um usuário avançado ou administrador que possa usar comandos básicos para identificar e localizar drivers e arquivos com problemas.

Para usar o Console de recuperação, você precisa efetuar o logon na conta Administrador. Esse console fornece comandos que podem ser usados para executar operações simples, como mudar de diretório ou exibir um diretório, e operações mais complexas, como corrigir o setor de inicialização. Você pode acessar a Ajuda para os comandos no Console de recuperação digitando help no prompt de comando do Console de recuperação.

Ao usar o Console de recuperação, você pode iniciar e interromper serviços, ler e gravar dados em uma unidade local (inclusive unidades formatadas com o sistema de arquivos NTFS), copiar dados de um disquete ou CD, formatar unidades, corrigir o setor de inicialização ou o registro de inicialização mestre (MBR) e executar outras tarefas administrativas. O Console de recuperação será especialmente útil se você precisar reparar o sistema copiando um arquivo de um disquete ou CD-ROM para a unidade de disco rígido ou se precisar reconfigurar um serviço que está impedindo o computador de ser iniciado corretamente. Por exemplo, o Console de recuperação poderia ser usado para substituir um arquivo de driver sobreescrito ou danificado por uma cópia perfeita a partir do disquete.

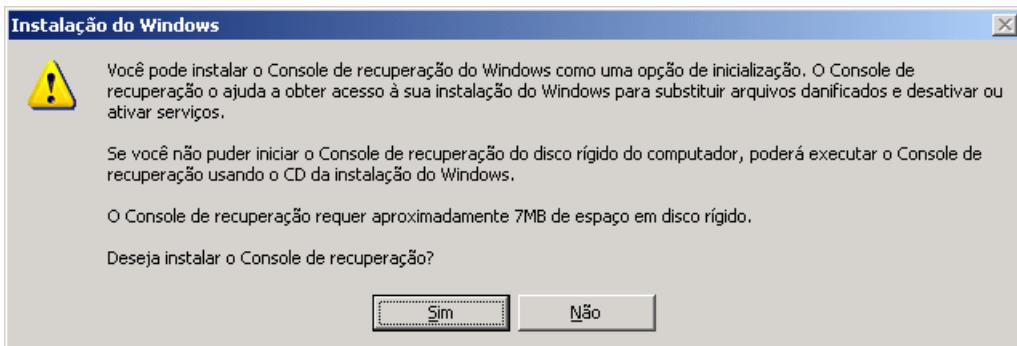
Exemplo: Para instalar o console de recuperação, siga os passos indicados a seguir:

1. Faça o logon como administrador ou com uma senha com permissão de administrador.
2. Abra um Prompt de comando e acesse a pasta i386, do cd de instalação do Windows Server 2003.

arquivo boot.ini para que carregue o Windows Server 2003 a partir do disco que ainda está funcionando. O Windows Server 2003 é carregado normalmente. Aí você desfaz o espelhamento, desliga o servidor e substitui o disco com problemas. Em seguida você usa o disquete de boot novamente para inicializar o servidor, reconhece o disco recém instalado e refaz o espelhamento. Pronto, o próximo boot já pode ser feito a partir do novo HD instalado e devidamente espelhado. Este método dá bem menos trabalho (e tem bem menos probabilidade de dar problemas) do que usando um backup tradicional, principalmente se o servidor for um DC, onde são necessários cuidados especiais para o restore do Active Directory, conforme descrito no Capítulo 8.

**IMPORTANTE:** O disco de boot que você cria em um servidor, servirá para inicializar este servidor e não qualquer servidor com o Windows Server 2003. Na prática outros servidores poderão ser inicializados, mas somente se tiverem exatamente as mesmas configurações de discos e de volumes, do servidor onde foi feito o disquete de boot.

3. Para instalar o console de recuperação, execute o seguinte comando:  
**winnt32 /cmdcons**
4. Será exibida uma mensagem informando que você pode instalar o console de recuperação como uma das opções de inicialização do computador, conforme indicado na Figura 12.20:



**Figura 12.20 Instalando o console de recuperação.**

5. Clique em Sim, para prosseguir com a instalação do console de recuperação.
6. A instalação é concluída e uma mensagem é exibida informando que o console de recuperação foi adicionado como uma das opções de inicialização e que você pode utilizar o comando HELP, para ver uma lista dos comandos disponíveis. Clique em OK para fechar esta mensagem e pronto, o console de recuperação está instalado. No próximo exemplo mostrarei como utilizar o console de recuperação.

Exemplo: Para utilizar o console de recuperação, após tê-lo instalado, siga os passos indicados a seguir:

1. Reinicialize o servidor.
2. Será apresentado um menu, onde a primeira opção é a instalação normal do Windows Server 2003. Se houver outras versões do Windows, estas serão exibidas na seqüência. A última opção é Microsoft Windows Recovery Console (Console de Recuperação do Microsoft Windows). Selecione esta opção e pressione Enter.
3. Após alguns instantes, será exibido um novo menu de opções para que você selecione qual instalação do Windows você deseja acessar. Este menu será exibido mesmo que haja uma única instalação do Windows. Digite o número da instalação a ser carregada e pressione Enter. Nesta etapa você também pode digitar Exit e pressionar Enter para reiniciar o computador.
4. Será solicitada a senha de acesso. Se o servidor for um DC, é importante salientar que está não é a senha da conta Administrator (Administrador) do domínio, mas sim a senha que foi definida durante a instalação do Active Directory, senha esta que também é utilizada para inicializar o servidor no modo de Restauração do Active Directory, conforme descrito no Capítulo 8. Digite a senha e pressione Enter.
5. A inicialização usando o console de recuperação será completada e será exibido um prompt de comando. Para obter uma lista completa dos comandos disponíveis digite help e pressione Enter. Será exibida uma lista com todos os comandos disponíveis no console de recuperação.
6. Para obter ajuda sobre um comando específico, digite help nome\_do\_comando e tecle Enter. Por exemplo para obter ajuda sobre o comando enable, digite help enable e pressione enter.
7. Para sair do console de recuperação e reiniciar o servidor, digite EXIT e pressione Enter. O servidor será reiniciado, agora selecione o modo normal de inicialização. A seguir apresento uma descrição resumida dos principais comandos disponíveis no console de recuperação.

Principais comandos disponíveis no console de recuperação:

- ◆ **ATTRIB:** É o bom e velho attrib da época do MS-DOS. É utilizado para alterar os atributos de pastas e arquivos.
- ◆ **BATCH:** É utilizado para executar uma seqüência de comandos contidos em um arquivo de texto. A saída dos comandos é exibida na tela ou pode ser redirecionada para um outro arquivo de texto.
- ◆ **BOOTCFG:** É utilizado para exibir e modificar as configurações do arquivo boot.ini.
- ◆ **CD (CHDIR):** O bom e velho comando CD, igualzinho ao que você utiliza no prompt de comando. É utilizado para alterar a pasta ativa.
- ◆ **CHKDSK:** Utilitário para verificação e correção de erros em unidades de disco. Foi descrito e exemplificado no Capítulo 10.
- ◆ **CLS:** Por incrível que possa parecer é ele mesmo: Clear Screen. Utilizado para limpar a tela, desde a época do MS-DOS 1.0.
- ◆ **COPY:** Mesmo comentário do item anterior. É utilizado para copiar pastas e arquivos. Por exemplo, você pode utilizar este comando para copiar um arquivo de inicialização que tenha sido corrompido, do CD de instalação do Windows Server 2003 para o disco rígido, substituindo desta forma o arquivo corrompido, o que fará com que o Windows Server 2003 possa ser inicializado normalmente.
- ◆ **DELETE (DEL):** Utilizado para excluir pastas e arquivos.
- ◆ **DIR:** Ele mesmo, com todas as tradicionais opções que você já conhece a décadas.
- ◆ **DISABLE:** Este é um dos comandos mais importantes e normalmente utilizados. Ele é utilizado para desabilitar um driver ou serviço. Por exemplo, se o que está impedindo o Windows Server 2003 de inicializar normalmente é um serviço, você pode inicializar o servidor no modo Console de Recuperação. Em seguida você utiliza o comando LISTSVC para listar todos os serviços instalados no servidor. Anote o nome do serviço a ser desabilitado e em seguida utilize o seguinte comando:  
**DISABLE NOME\_DO\_SERVIÇO**

pronto, agora você pode inicializar o Windows Server 2003 no modo normal e corrigir os problemas com o serviço que estava impedindo o Windows Server 2003 de ser inicializado no modo normal.

- ◆ **EXIT:** Sai do console de recuperação e reinicializa o servidor.
- ◆ **EXPAND:** Utilizado para descompactar um arquivo compactado.
- ◆ **FIXBOOT:** Este também é um comando muito utilizado. Este comando recria o código de boot do Windows Server 2003, na partição de boot, sobrescrevendo o código atualmente existente. É indicado para casos em que o código de boot foi corrompido, o que está impedindo o servidor de inicializar normalmente.
- ◆ **FIXMBR:** Também muito utilizado. É utilizado para reparar o Master Boot Record (MBR) da partição de boot. Normalmente é utilizado em situações onde o MBR foi danificado por vírus, o que está impedindo o Windows Server 2003 de ser inicializado. Você deve tentar outros recursos antes de usar este comando. Primeiro tente utilizar um anti-vírus atualizado. Não é comum, mas pode acontecer de este comando danificar a MBR ao invés de corrigir. Nestas situações você pode perder completamente o acesso ao disco e somente uma reinstalação do Windows Server 2003 e uma restauração a partir do backup, para voltar o sistema ao estado normal.
- ◆ **FORMAT:** O bom e velho format, utilizado para formatar volumes e disquetes.

---

**NOTA:** O comando LISTSVC lista os serviços e os drivers instalados no servidor, bem com o status de cada um.

---

- ◆ **HELP:** Exibe uma lista de todos os comandos disponíveis no console de recuperação. Para obter ajuda sobre um comando específico, digite help nome\_do\_comando e tecle Enter. Por exemplo para obter ajuda sobre o comando enable, digite help enable e pressione enter.
- ◆ **LISTSVC:** Exibe uma lista dos serviços e drivers instalados no servidor, bem como o status de cada um.
- ◆ **LOGON:** Exibe uma lista de todas as instalações disponíveis, para as seguintes versões do Windows: NT, XP, 2000 e Server 2003. É exibido um menu, você digita o número da instalação que você quer acessar. Será solicitada a senha de acesso. Se você digitar a senha incorretamente três vezes, o servidor será reinicializado.
- ◆ **MAP:** Exibe uma lista das letras de drives em uso, o sistema de arquivos de cada drive e o tamanho de cada partição.
- ◆ **MD (MKDIR):** Ele mesmo, velho conhecido. Utilizado para criar pastas e subpastas.
- ◆ **MORE:** Mais um velho conhecido. É utilizado para paginar a saída de um comando, quando a saída que é exibida na tela é muito extensa. Usando o comando more em conjunto com outros comandos, os resultados são exibidos uma tela por vez. Para exibir a próxima tela basta pressionar a barra de espaços.
- ◆ **RD (RMDIR):** Outro velho conhecido. Utilizado para excluir uma pasta. A pasta deve estar vazia para que o comando seja executado com sucesso.
- ◆ **REN (RENAME):** Utilizado para renomear um arquivo.
- ◆ **SET:** Permite que sejam definidas características de execução do console de recuperação. Com o comando SET você pode definir as seguintes características:
  - ◆ **AllowWildCards:** Define se será permitido o uso de caracteres coringa (\*, ?) no console de recuperação.
  - ◆ **AllowAllPaths:** Define se será permitido acesso a todas as pastas do disco rígido.
  - ◆ **AllowRemovableMedia:** Define se será permitida a cópia de arquivos para mídias móveis, tais como um disquete ou um Zip Drive.
  - ◆ **NoCopyPrompt:** Permite a utilização do comando copy, para sobrescrever arquivos, sem que seja exibida uma mensagem de aviso.
- ◆ **SYSTEMROOT:** Altera para a pasta definida como %systemroot%, ou seja, a pasta onde o Windows Server 2003 está instalado.
- ◆ **TYPE:** É utilizado para exibir o conteúdo de um arquivo de texto.

## A opção Roll Back Driver.

Outra opção útil é a opção para reinstalar a versão anterior do driver de um dispositivo de hardware. Esta opção é útil quando a instalação de uma nova versão de um driver está causando problemas. Desde problemas como por exemplo consumo excessivo de memória e processador, até problemas mais graves, como simplesmente fazer com que o dispositivo de hardware deixe de funcionar após a atualização do driver. Nestas situações, você pode orientar o Windows Server 2003 a voltar a versão anterior do driver, versão esta que estava funcionando corretamente. No exemplo a seguir, listo os passos para fazer o Roll Back de um driver.

Exemplo: Para fazer o Roll Back de um driver de dispositivo, siga os passos indicados a seguir:

1. Faça o logon como administrador ou com uma conta com permissão de administrador.
2. Abra o console Gerenciamento do computador: Iniciar -> Ferramentas Administrativas -> Gerenciamento do computador.
3. Acesse a opção Ferramentas do Sistema -> Gerenciador de Dispositivos.
4. Localize o dispositivo cujo drive está com problemas e clique com o botão direito nele. No menu de opções que é exibido clique em Propriedades.

5. Na janela de propriedades que é exibida, clique na guia Driver. Em seguida clique no botão Roll Back Driver (Reverter driver), conforme indicado na Figura 12.21. Pronto, será instalada a versão anterior do driver.

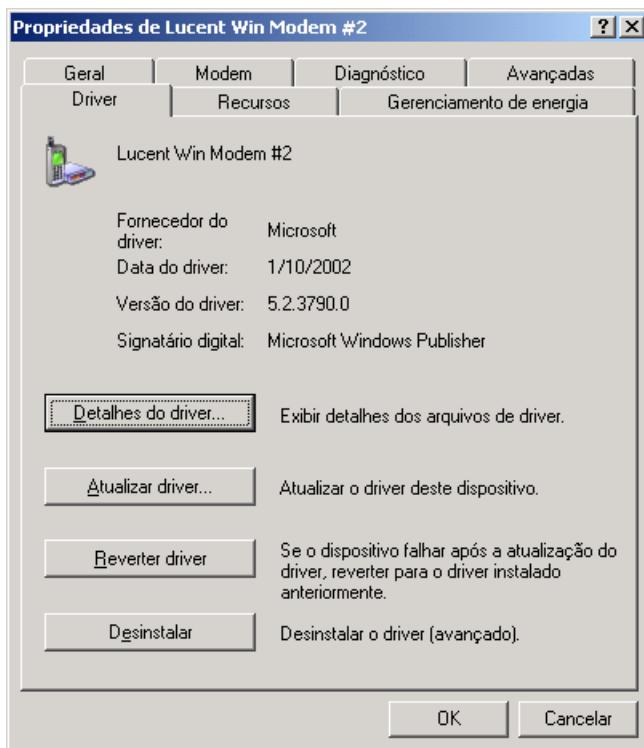


Figura 12.21 A opção Roll Back Driver.

## Conclusão

Neste capítulo tratei de uma série de assuntos importantes, todos relacionados a manutenção do Windows Server 2003 em funcionamento e do retorno do Windows Server 2003 ao funcionamento normal quando ocorrerem problemas.

Foram abordados os seguintes tópicos:

- ◆ O Processo de boot do Windows Server 2003.
- ◆ Registry.
- ◆ Opções avançadas de inicialização do sistema.
- ◆ O Modo seguro.
- ◆ A Última configuração válida – Last Known Good Configuration.
- ◆ Outras opções avançadas de inicialização.
- ◆ O ASR – Automatic System Recovery
- ◆ O console de recuperação.
- ◆ O recurso de Roll Back driver.

Todas são ferramentas importantes para restaurar o Windows Server 2003 a sua normalidade em caso de problemas. Mas a principal ferramenta de recuperação a desastres, sem dúvidas, é um bom planejamento. Planejar com cuidado a segurança física e lógica das informações, bem com um bom sistema de backup e anti-vírus sempre atualizados. Combinando os recursos tecnológicos com uma educação e treinamento contínuo para os usuários, você terá um ambiente bem mais seguro, produtivo e preparado para enfrentar os problemas que fatalmente virão.

# Introdução

Neste capítulo mostrarei como instalar, configurar e utilizar os serviços Web em um servidor com o Windows Server 2003. O servidor Web da Microsoft é o Internet Information Services, que com o Windows Server 2003 chega a sua versão 6.0, mais conhecido como IIS 6.0. As configurações que você aprenderá se aplicam tanto se você estiver usando a edição Windows Server 2003 Web Edition ou qualquer uma das outras edições do Windows Server 2003, com o IIS 6.0 instalado e configurado. O desenvolvimento de software atualmente é baseado em um modelo Web. Por isso posso citar várias situações onde o uso do Windows Server 2003 como um servidor Web é indicado:

- ◆ Vamos iniciar por uma das aplicações mais simples. Imagine que você esteja utilizando o Windows Server 2003 para montar uma rede de uma pequena empresa ou de um pequeno escritório com, digamos, umas 10 máquinas. Você pode utilizar o Windows Server 2003 como um servidor Web, para compartilhar documentos como manuais, apostilas de treinamentos e outras informações que devam estar disponíveis para todos os usuários da rede. Desta maneira os usuários acessam estes documentos utilizando o Internet Explorer para acessar a Intranet da empresa. Quando um dos documentos for alterado no Servidor, automaticamente os usuários passarão a ter acesso a esta nova versão, sem necessidade de distribuir uma cópia da nova versão para todos os usuários. Desta maneira garantimos que todos terão acesso às versões mais atualizadas e ainda economizamos espaço no disco rígido de cada estação de trabalho. Agora estenda este exemplo para uma rede com milhares de usuários.
- ◆ Agora vamos a um uso mais sofisticado, onde temos o acesso a bancos de dados através do uso da tecnologia ASP – Active Server Pages ou ASP.NET, a nova tecnologia de páginas dinâmicas que faz parte da iniciativa .NET da Microsoft. Vamos imaginar que existem bancos de dados nos quais os usuários da rede devam fazer pesquisas. Por exemplo, pode ser um banco para consulta ao CEP, uma lista de produtos e preços, uma lista de clientes e assim por diante. Neste caso podemos armazenar os referidos bancos de dados no computador configurado como servidor Web e criar formulários de pesquisa usando páginas ASP ou ASP.NET. Desta maneira todos os usuários da rede dispõem de uma maneira rápida e sempre atualizada de realizar pesquisas nos bancos de dados utilizados pela empresa. Além disso não é preciso instalar um programa em cada um dos computadores, pois todo o acesso é feito simplesmente usando um navegador como o Internet Explorer ou o Netscape Navigator. Se um formulário de pesquisa for modificado no servidor Web, automaticamente todos os usuários passarão a acessar a nova versão do formulário. Com a tecnologia ASP ou ASP.NET podemos criar não só formulários de pesquisa mas também formulários para cadastramento e alteração de informações.

Em resumo podemos dizer que com o uso de um servidor Web podemos facilitar o acesso às informações, ao mesmo tempo em que a disponibilizar informações e aplicativos torna-se um processo bem mais simples.

# CAPÍTULO

# 13

## Internet Information Services 6.0 – IIS 6.0 e Software Update Services – SUS

Vou iniciar o capítulo mostrando como a fazer a instalação do IIS – Internet Information Services. O IIS é o servidor Web da Microsoft. Ao instalarmos o IIS estamos transformando o computador em um servidor de páginas e de arquivos, com suporte as tecnologias ASP e ASP.NET. Na seqüência você aprenderá sobre o acesso ao servidor Web e sobre a formação de endereços.

Em seguida mostrarei como configurar e a utilizar os diversos serviços oferecidos pelo IIS, desde a simples criação de pastas virtuais até as configurações de segurança disponíveis no IIS.

O segundo tópico a ser abordado neste capítulo é o SUS – Software Update Services. No Windows Server 2003, em Português, este serviço é denominado de Serviço de Atualizações Automáticas. Já há alguns anos, que a Microsoft disponibiliza o site Windows Update, através do qual você pode baixar e instalar atualizações e correções de segurança para as diferentes versões do Windows. Porém o usuário deve tomar a iniciativa de usar o comando Windows Update, para conectar o seu computador com o site do Windows Update, para fazer a instalação das últimas correções disponíveis. O SUS leva este processo um nível a frente. Você estala o SUS em um servidor da rede e pode configurar este servidor para baixar, automaticamente, as atualizações a partir do site Windows Update. Depois de baixadas para o servidor, estas atualizações poderão ser aplicadas, automaticamente, em todos os demais computadores da rede. Este processo tem inúmeras vantagens, as quais serão descritas neste capítulo.

## Instalação do IIS 6.0.

Para que você possa tornar um servidor com o Windows Server 2003 em um servidor Web, você precisa instalar o IIS – Internet Information Services. O IIS é o serviço responsável pela disponibilização dos serviços http (para disponibilização de páginas) e ftp (para cópia de arquivos). Outros serviços também são disponibilizados pelo IIS, tais como serviços de SNMT e NNTP. Para maiores detalhes sobre os serviços de SNMT e NNTP, consulte o Capítulo 24, do livro: Windows Server 2003 – Curso Completo, 1568 páginas. A versão do IIS disponível com o Windows Server 2003 é a versão 6.0. Neste capítulo farei referência simplesmente utilizando IIS.

Caso você não tenha instalado o IIS quando da instalação do Windows Server 2003, é possível fazer a instalação quando for necessário. No próximo exemplo, você aprenderá passo-a-passo a instalar o IIS 6.0. Nunca é demais lembrar que sem o IIS 6.0, não será possível testar os exemplos práticos, propostos neste capítulo.

Antes de instalar o IIS, é importante fazer algumas observações, relacionadas com a segurança do IIS. No Windows 2000 Server, ao instalar o IIS, por padrão, são habilitadas uma série de funcionalidades. O problema é que muitas destas funcionalidades não são necessárias em muitas situações práticas. O mais grave é que muitas das falhas de segurança do IIS 5.0, estavam justamente nestas funcionalidades que eram habilitadas automaticamente durante a instalação do produto. Já com o IIS 6.0, no Windows Server 2003, é adotada uma política de habilitar apenas um conjunto mínimo de serviços, durante a instalação. A medida que o administrador precisa de novas funcionalidades ele as habilita. Obviamente que os problemas de segurança detectados no IIS 5.0 já foram corrigidos através do uso de Service Packs no Windows 2000 Server e não estão presentes no IIS 6.0. Mas habilitar somente os serviços realmente necessários, é uma política bem mais sensata, tanto em termos de segurança, quanto em termos de uso de recursos do servidor.(tais como memória e processador). Quando houver necessidade de utilizar uma funcionalidade que não está habilitada, basta que o Administrador configure o IIS para habilitar a respectiva funcionalidade.

Durante a instalação do IIS você terá a opção de selecionar quais componentes do IIS você deseja instalar. Por exemplo, você pode optar por instalar ou não o gerenciamento do próprio IIS via navegador e assim por diante. No exemplo prático, logo a seguir, iremos instalar todos os componentes do IIS. Conforme descrito anteriormente, mesmo instalando todos os componentes, somente será habilitado um conjunto mínimo de funcionalidades. A medida que novas funcionalidades se mostrarem necessárias, o administrador pode habilita-las.

Exemplo: Para instalar o IIS 6.0, siga os passos indicados a seguir:

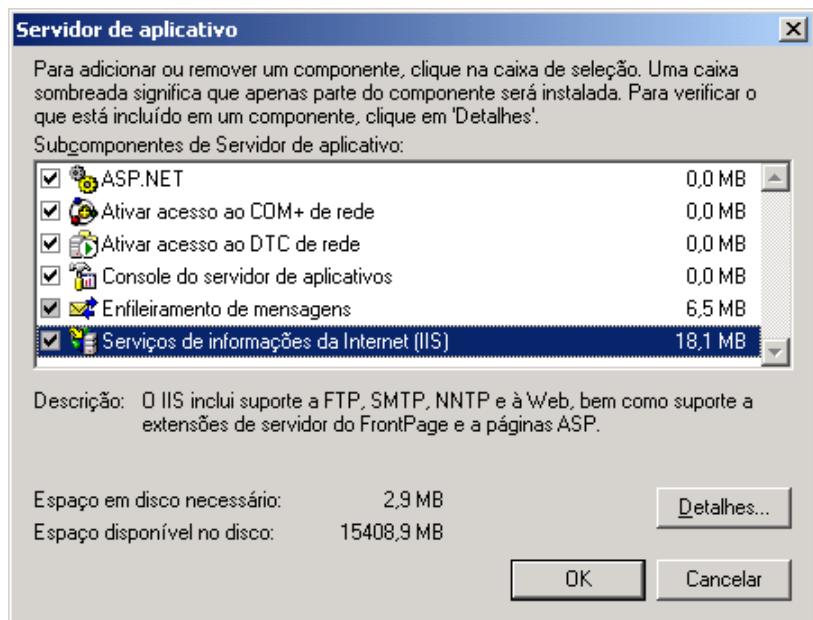
1. Faça o logon com a conta Administrador ou com uma conta do tipo Administrador do computador.
2. Abra o Painel de controle: Iniciar -> Painel de controle.
3. Abra a opção Adicionar ou remover programas.
4. Surgirá a janela Adicionar ou remover programas.
5. No lado esquerdo da janela, dê um clique na opção Adicionar/remover componentes do Windows.
6. Será aberto o Assistente de componentes do Windows. Com este assistente podemos adicionar componentes do Windows Server 2003 que não foram instalados durante a instalação original ou remover componentes que não sejam mais necessários.
7. Vá descendo com a barra de rolagem vertical, até localizar o item Servidor de aplicativo e clique neste item para marcá-lo, conforme indicado na Figura 13.1

**IMPORTANTE: Quando você instala o IIS, o serviço é instalado em um modo de alta segurança. Por padrão, ele está configurado para servir apenas conteúdo estático (páginas HTML padrão). Para que possam ser executados conteúdos dinâmicos - páginas ASP e ASP.NET, scripts CGI, Internet Server Application Programming Interface (ISAPI) e Web Distributed Authoring and Versioning (WebDAV) – estes recursos devem ser habilitados pelo administrador, conforme mostrarei neste capítulo.**



Figura 13.1 O grupo Servidor de aplicativo.

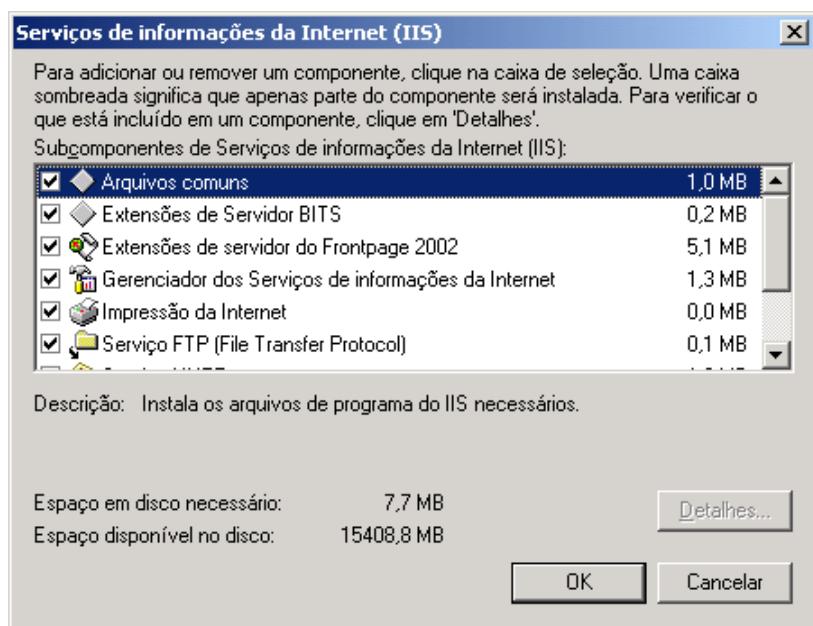
8. Clique no botão Detalhes. Será exibida uma lista com os diversos serviços relacionados ao desenvolvimento de aplicações. Marque a opção Serviços de informações da Intenet (IIS), conforme indicado na Figura 13.2:



**Figura 13.2 Selecionando o IIS para instalação.**

9. Observe que ao marcar esta opção, o botão Detalhes... é habilitado. O IIS é formado por uma série de componentes e funcionalidades. Existe um servidor de páginas (servidor HTTP), um servidor de ftp, um servidor de notícias (NNTP) e assim por diante. Ao instalarmos o IIS, podemos escolher um ou mais dos seus componentes, dependendo das necessidades do nosso servidor Web. Não é necessário que todos os componentes do IIS sejam instalados. Por exemplo, se o serviço de cópia de arquivos não for necessário, não temos porque instalar o serviço de FTO. No nosso exemplo iremos instalar todos os componentes.
10. Clique no botão Detalhes... Será exibida uma lista com os componentes do IIS.
11. Na lista de opções disponíveis, exibida na Figura 13.3, certifique-se de que todas as opções estejam marcadas, conforme indicado na Figura 13.3. Não esqueça de usar a barra de rolagem vertical, para marcar também os componentes que não são exibidos na tela:

**DICA:** Na prática, em um servidor da sua rede, instale somente os serviços realmente necessários. Não é uma boa idéia instalar todos os serviços disponíveis, mesmo que somente alguns sejam utilizados. Quanto mais serviços instalados, maiores as possibilidades de ataque e quebra da segurança do site, por parte de um hacker, além da maior utilização de memória e processador no servidor.



**Figura 13.3 Instalando todos os componentes do IIS.**

12. A opção Serviço World Wide Web Service também é dividida em vários componentes. Clique nesta opção para marca-la. Em seguida clique no botão Detalhes.... Será exibida a janela com os componentes do serviço World Wide Web Service. Certifique-se de que todas as opções estejam marcadas, conforme indicado na Figura 13.4.

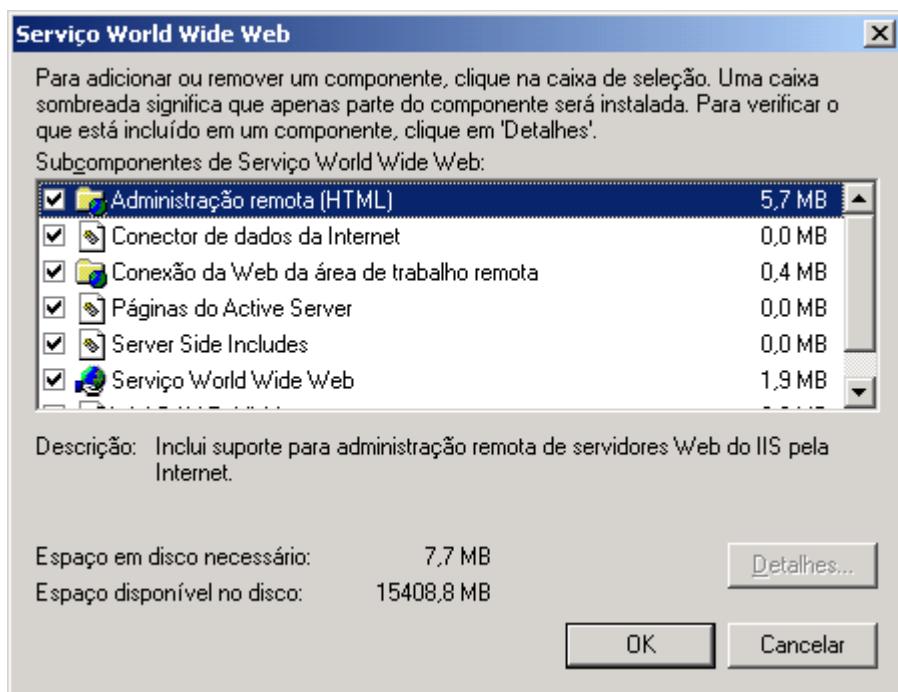


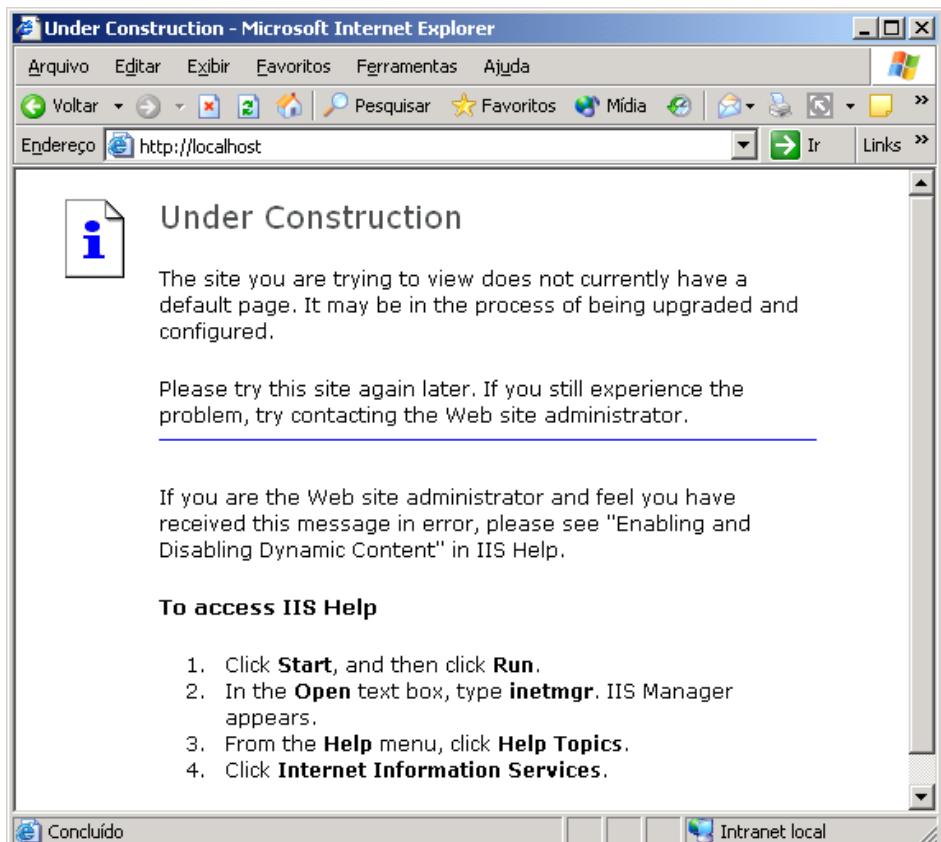
Figura 13.4 Opções do Servidor World Wide Web.

13. Clique em OK para fechar a janela da Figura 13.4. Você estará de volta à janela Serviços de informações da Internet, indicada na Figura 13.3. Clique em OK para fechá-la e aplicar as configurações selecionadas.
14. Você estará de volta à janela do Assistente de componentes do Windows. Observe, que após ter selecionado os componentes a serem instalados, o Windows Server 2003 exibe o espaço em disco necessário para a instalação dos novos componentes selecionados.
15. Dê um clique no botão Avançar, para ir para a próxima etapa do assistente.
16. O Windows Server 2003 exibe uma janela indicando o progresso da Instalação
17. Caso o Windows Server 2003, não encontre os arquivos necessários à instalação do IIS, no Disco rígido, você será solicitado a inserir o CD de instalação do Windows Server 2003.
18. Insira o CD e aguarde. O Windows detecta que o CD foi inserido e inicia, automaticamente, o processo de cópia dos arquivos.
19. Após concluída a cópia dos arquivos, o Assistente emite uma mensagem dizendo que o processo foi concluído com sucesso.
20. Dê um clique no botão Concluir para encerrar o Assistente.
21. Você estará de volta à janela Adicionar ou remover programas. Dê um clique no botão Fechar para sair desta janela.
22. Você estará de volta ao Painel de controle. Feche o Painel de controle.
23. Agora o IIS está instalado e pronto para ser utilizado, pelo menos as funcionalidades básicas do IIS.

Agora que já temos o IIS instalado vamos testar se ele está funcionando corretamente.

Para testar se o IIS foi instalado com sucesso, siga os seguintes passos:

1. Abra o Internet Explorer.
2. Digite o seguinte endereço: <http://localhost>
3. Será aberta uma página padrão (iisstart.htm), que é uma página apenas com um aviso de que o site está em construção, conforme indicado na Figura 13.5:



**IMPORTANTE:** Nunca é demais repetir que a instalação de todos os componentes esta sendo feita apenas para uso didático, para que você aprenda a utilizá-los. Na prática, devem ser instalados apenas os componentes realmente necessários, por motivos já expostos anteriormente.

Figura 13-5 O IIS instalado e funcionando e a página padrão sendo exibida.

4. Esta é a página inicial do IIS logo após a instalação. A pasta padrão do IIS é em C:\Inetpub\wwwroot. Falaremos mais sobre pasta padrão e como criar pastas virtuais, mais adiante. Isto comprova que o IIS foi instalado com sucesso. Feche o Internet Explorer.

## Preparando o seu computador para acompanhar os exemplos práticos de utilização do IIS.

Neste item vamos criar uma pasta chamada exemplos. Dentro desta pasta vamos criar uma subpasta para outros assuntos, tais como: documentos, aplicativos e assim por diante. Depois aprenderemos a tornar esta pasta, parte integrante do servidor IIS. Não são todas as pastas de um servidor que podem ser acessadas através do IIS.

## Criando a estrutura de pastas e subpastas.

Utilizando o Windows Explorer, crie uma estrutura de pastas e subpastas, conforme indicado a seguir. É importante que você não utilize acentos para o nome das subpastas, uma vez que os nomes das pastas passarão a fazer parte do endereço de acesso, quando estas pastas forem configuradas para fazer parte do IIS.

Cria as seguintes pastas:

- ◆ C:\exemplos\aplicativos
- ◆ C:\exemplos\documentos

Agora vamos fazer com que a pasta exemplos (e consequentemente, todas as suas subpastas), passem a fazer parte do servidor IIS. O computador que estou utilizando para os exemplos tem o nome de srv70-290 e faz parte do domínio abc.com. Para acessar a página inicial deste servidor utilizo o seguinte endereço: <http://srv70-290.abc.com>. Substitua srv70-290.abc.com pelo nome do computador e domínio que você estiver utilizando para acompanhar os exemplos deste livro.

Ao instalar o IIS por padrão a pasta C:\Inetpub\wwwroot é definida como a pasta home. Dentro da pasta home, um ou mais arquivos podem ser definidos como o arquivo padrão. Quando um usuário acessa o computador, simplesmente especificando o seu endereço, como por exemplo: <http://srv70-290.abc.com>, será carregado o arquivo padrão, da pasta home, que no caso do IIS 6.0 é o arquivo iisstart.htm, já citado anteriormente. Outras pastas podem ser criadas e definidas para ser parte do servidor IIS. Estas pastas são conhecidas como pastas virtuais. Aprenderemos a cria-las logo em seguida. Também veremos como fica o endereço de acesso para as pastas virtuais e para arquivos contidos nestas pastas.

## Tornando a pasta exemplos parte dos servidores IIS – criando uma pasta virtual.

Agora vamos aprender passo-a-passo, como tornar a pasta exemplos (e as suas subpastas), parte do servidor IIS. Para isso utilizaremos o console Gerenciador dos Serviços de informações da Internet (IIS), do Windows Server 2003. Este console, que está disponível através do menu Ferramentas administrativas, nos dá acesso a todas as opções de configuração do IIS.

Exemplo: Para tornar a pasta exemplos, parte do servidor IIS srv70-290.abc.com, siga os passos indicados a seguir:

1. Faça o logon como Administrador ou com uma conta com permissões de administrador.
2. Clique em Iniciar -> Ferramentas administrativas -> Gerenciador dos Serviços de informações da Internet (IIS).
3. Será aberta a janela Internet Information Services (IIS) Manager, conforme indicado na Figura 13.6:

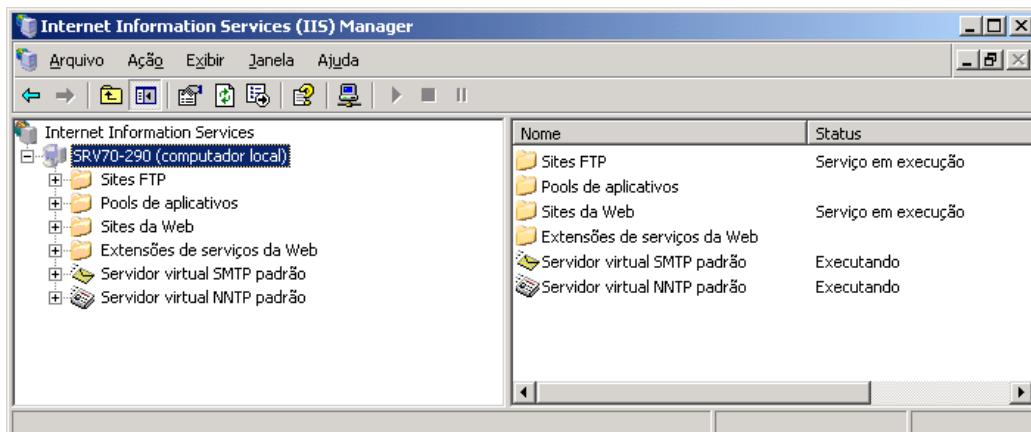


Figura 13.6 O console Internet Information Services.

Comparando WebDav com FTP:

| Protocolo | Senha de segurança   | Criptografia de dados   |
|-----------|--|---|
| WebDAV    | Sempre que o servidor Web estiver usando a SSL; às vezes quando ele não estiver usando | Sempre que o servidor Web estiver usando a SSL; nunca quando ele não estiver usando |
| FTP       | Nunca  | Nunca   |

O WebDAV protege a senha e os dados criptografados quando você envia informações para um servidor Web executando SSL (Secure Sockets Layer). Se o servidor não estiver executando a SSL, o WebDAV poderá proteger a sua senha se ele estiver configurado para usar a autenticação do Windows. Entretanto, você não pode criptografar os dados enviados ao servidor, se este não estiver usando SSL. Se o servidor estiver executando a SSL, o endereço do servidor na Internet será iniciado por https:// em vez de http://.

O FTP não usa criptografia ou outro mecanismo de segurança para proteger a sua senha quando você faz logon em um servidor. Além disso, você não pode criptografar os dados quando usar o FTP para enviar arquivos para/de um servidor. Isso coloca suas informações em risco, pois qualquer pessoa que use hardware ou software de rede pode capturá-las à medida que são transferidas.

O uso do WebDAV para a transferência de arquivos, pastas e outros dados para servidores Web que executam a SSL é a maneira mais segura de transferir informações.

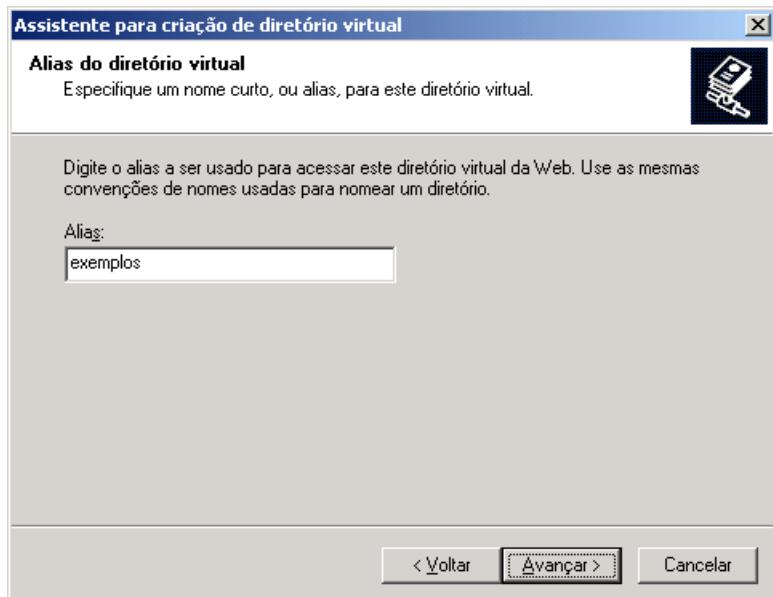
4. Dê um clique na opção Sites da Web. No lado direito será exibida a lista dos sites configurados durante a instalação do IIS. Com o IIS é possível ter mais de um site no mesmo servidor. O site Site da Web padrão é, como o nome sugere, o site padrão do servidor. A pasta raiz deste site é C:\Inetpub\wwwroot, conforme citado anteriormente.
5. Dê um clique no sinal de +, ao lado da opção Site da Web padrão, para expandir esta opção. As opções que aparecem, são as pastas que já fazem parte do site. Por padrão a pasta home é definida como sendo C:\Inetpub\wwwroot. A pasta home do serviço de ftp é definida como sendo c:\inetpub\ftproot.
6. Dê um clique com o botão direito do mouse, na opção Site da Web padrão. No menu que surge, execute o comando Novo -> Diretório virtual...
7. Será exibida a primeira tela do Assistente para a criação de diretório virtual. Esta tela é apenas informativa. Dê um clique no botão Avançar, para ir para a segunda etapa do assistente.
8. Nesta segunda etapa, você precisa definir um nome (Alias), para esta pasta virtual. Este nome fará parte do endereço para acessar a referida pasta, conforme

**NOTA:** Você pode usar a opção Extensões de serviços da Web para configurar quais extensões do servidor IIS estarão habilitadas e quais estarão desabilitadas. Para habilitar/desabilitar uma determinada extensão, basta clicar na extensão a ser habilitada/desabilitada para marca-la. Em seguida clique no botão Permitir, para habilitar a extensão ou no botão Proibir, para desabilitar a extensão. Ao clicar em Permitir, para habilitar uma extensão, será exibida uma janela pedindo confirmação para a habilitação. Clique em Sim, para prosseguir com a habilitação. Nunca é demais lembrar que somente devem ser habilitadas as funcionalidades realmente necessárias, para evitar problemas de segurança e uso desnecessário dos recursos do servidor.

**IMPORTANTE:** A extensão WebDav deve estar habilitada, para que você possa criar os chamados Web Folders (Pastas Web). Ao acessar uma pasta de um servidor IIS, usando o Internet Explorer, se a extensão WebDav não estiver habilitada, você receberá uma mensagem de que não foi possível exibir a pasta como uma pasta Web e perguntando se você deseja exibi-la usando o modo padrão (modo usado no Windows Explorer). Isso acontece quando a extensão WebDav está desabilitada no

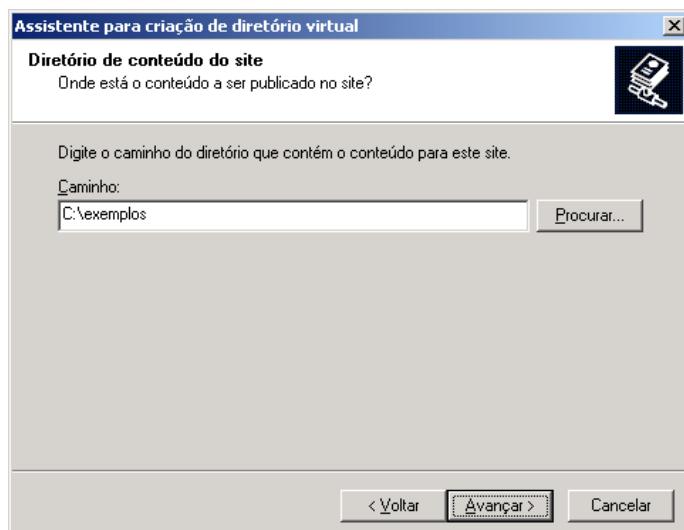
veremos mais adiante no item sobre formação de endereços. Utilizaremos o mesmo nome da pasta: exemplos. Porém não é obrigatório que utilizemos o mesmo nome. Por questão de facilidade de administração e gerenciamento, sempre utilizo nomes iguais para o nome da pasta no disco rígido e o nome no utilizado pelo IIS.

- Digite exemplos, conforme indicado na Figura 13.7. Dê um clique no botão Avançar, para ir para a terceira etapa do assistente.



**Figura 13.7** Digitando um nome para o diretório virtual que está sendo criado.

- Na terceira etapa, o assistente pergunta qual a pasta a ser associada com o nome virtual informado na etapa anterior. Nesta etapa você pode digitar o caminho completo para a pasta, ou utilizar o botão procurar, para localizar a pasta desejada. No nosso exemplo, vamos digitar C:\exemplos. Com isso estamos associando a pasta C:\exemplos, com o diretório virtual exemplos, do servidor IIS.
- Digite C:\exemplos, conforme indicado na Figura 13.8, e dê um clique no botão Avançar, para ir para a quarta etapa do assistente.



**Figura 13.8** Informando o caminho da pasta C:\exemplos.

**servidor IIS. O WebDAV (Web Distributed Authoring and Versioning), também conhecido como pastas da Web, é um protocolo de transferência de arquivos que oferece suporte à transferência de arquivos segura em intranets e na Internet. Com o WebDAV, é possível carregar, fazer o download e gerenciar arquivos em um computador remoto, através da intranet e pela Internet. O WebDAV é semelhante ao protocolo de transferência de arquivo (FTP); entretanto, o WebDAV proporciona um ambiente mais seguro para a transferência de arquivos pela Web.**

12. Na quarta etapa do assistente, podemos configurar as permissões de acesso à pasta exemplos. Certifique-se de que as opções: Leitura e Executar Scripts (ASP por exemplo), estejam marcadas, conforme indicado pela Figura 13.9. Se a opção Executar Scripts (ASP por exemplo), não estiver marcada, o código ASP será ignoradas pelo IIS e as páginas ASP não serão processadas.

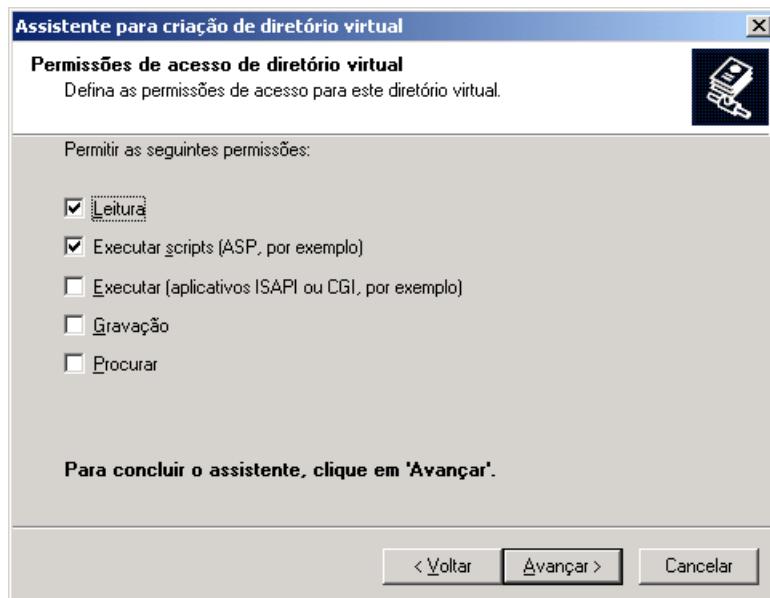


Figura 13.9 Configurando as opções de segurança.

13. Dê um clique em Avançar. Surge a tela final do assistente.  
 14. Dê um clique no botão Concluir, para finalizar o assistente.  
 15. Você estará de volta ao Gerenciador do Internet Services.  
 16. Observe que um novo diretório virtual chamado exemplos, já aparece como parte integrante do servidor IIS, conforme indicado pela Figura 13.10. Caso o diretório exemplo ainda não apareça na listagem, pressione F5 para atualizar a listagem. Clique no sinal de + ao lado de Exemplos e observe que as subpastas Aplicativos e Documentos também são exibidas.

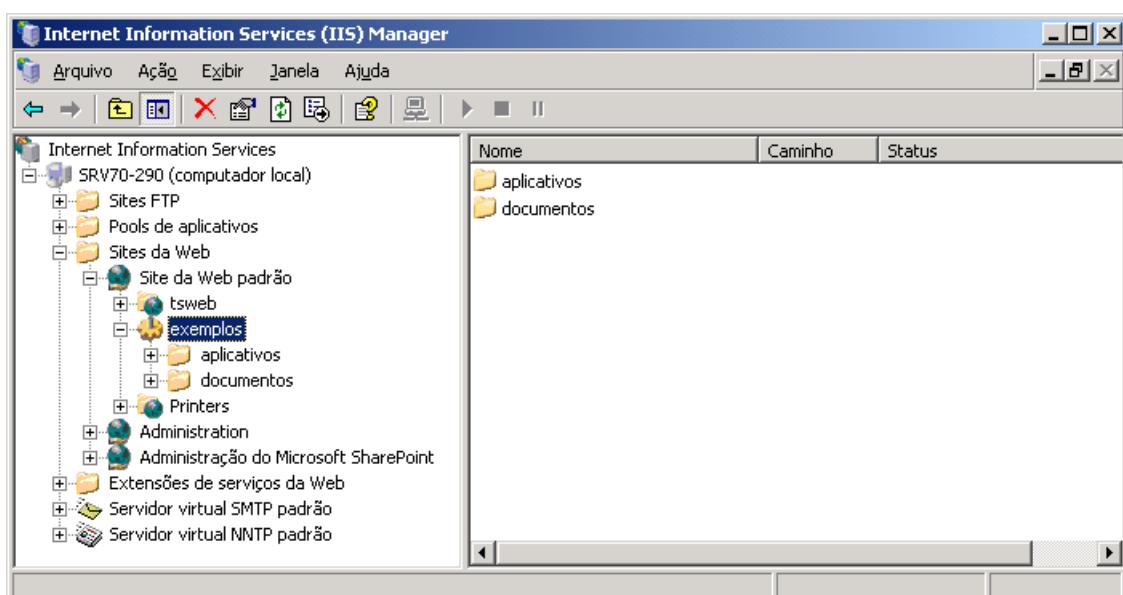


Figura 13.10 O diretório virtual exemplos, recém criado.

17. Feche o console de gerenciamento do IIS.

## Como são formados os endereços de acesso à páginas do IIS?

Uma vez criado o diretório virtual exemplos, o qual está associado à pasta C:\Exemplos, como posso acessar o conteúdo que for colocado dentro deste diretório, ou em uma das suas subpastas ? Por exemplo, se eu colocar um arquivo chamado avisos.htm no diretório virtual Exemplos, qual o endereço que os usuários devem utilizar para acessar a página avisos.htm?

A resposta para a questão acima, é bastante simples, basta que entendamos como são formados os endereços em um servidor como o IIS. No nosso exemplo, vamos imaginar o endereço do servidor como sendo: http://srv-win2003.abc.com. Ao digitarmos este endereço, estamos acessando a página principal do servidor que, por padrão, está na pasta C:\Inetpub\wwwroot, conforme descrito anteriormente. Vamos supor que dentro do diretório Exemplos, fosse colocada uma página chamada avisos.htm, como faríamos para acessar esta página, através do Navegador? O endereço da página em questão, seria o seguinte:

**http://srv-win2003.abc.com/exemplos/avisos.htm**.

A Figura 13.11, descreve em detalhes a formação deste endereço:

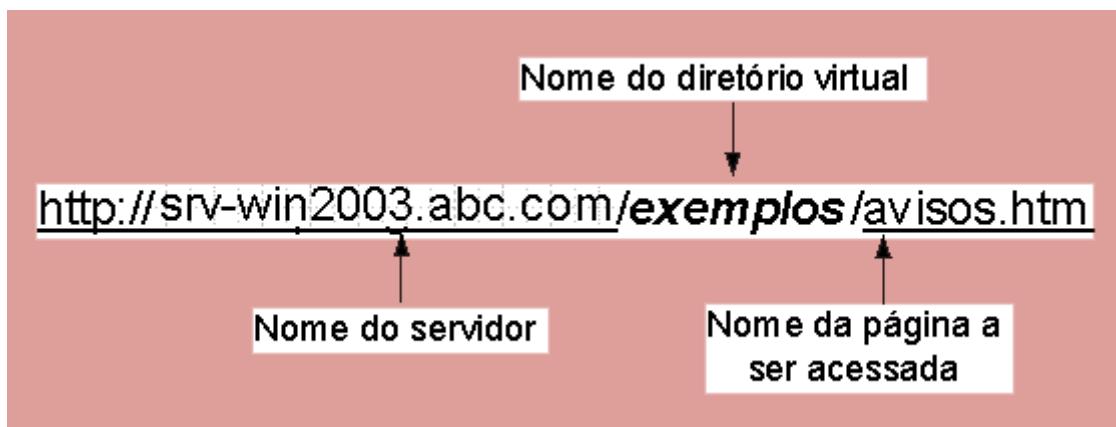


Figura 13.11 A formação de endereços no servidor IIS.

Observe que primeiro vem o nome do servidor (srv-win2003.abc.com), depois o nome do diretório virtual (exemplos) e, finalmente, o nome da página a ser acessada (avisos.htm).

Seguindo o mesmo raciocínio anterior, fica fácil responder a esta pergunta. Vamos supor que você queira acessar uma página chamada cep.asp, que está na subpasta aplicativos, a qual está no diretório virtual exemplos. Como fica o endereço para acessar esta página ? A Figura 13.12, responde esta questão:

---

**IMPORTANTE:** Como é que fica o endereço, quando eu quero acessar uma página que está dentro de uma subpasta do diretório virtual exemplos?

---

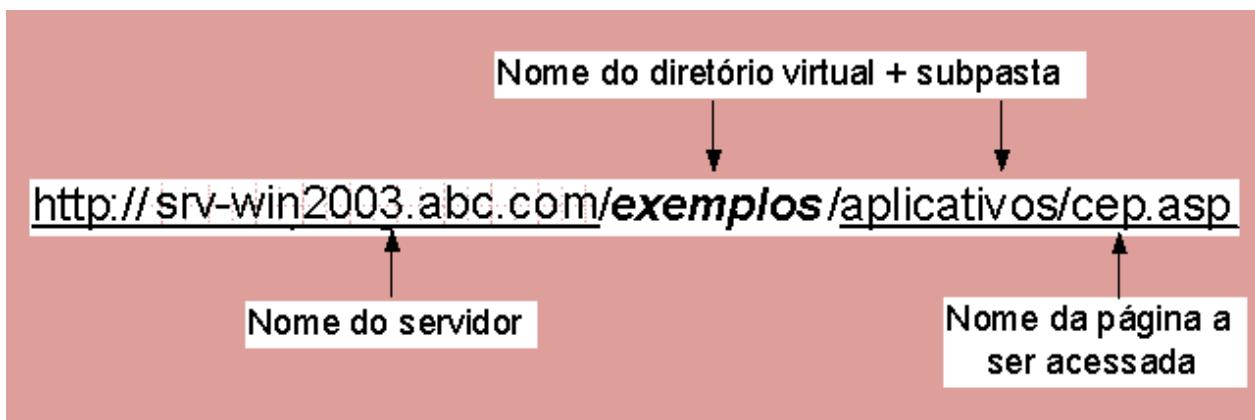


Figura 13.12 A formação de endereços em subpastas do diretório virtual, no servidor IIS.

Com isso, podemos ver que existe uma lógica bem definida para a formação dos endereços. Apenas para confirmar, vamos dar mais alguns exemplos de formação de endereços. Considere os casos abaixo indicados:

*Qual o endereço de uma página chamada teste.htm, gravada na pasta Documentos?*

Resposta: <http://srv-win2003.abc.com/exemplos/documentos/teste.htm>

*Qual o endereço de uma página chamada cadastro.asp, gravada na pasta Aplicativos?*

Resposta: <http://srv-win2003.abc.com/exemplos/aplicativos/cadastro.asp>

É importante que você entenda bem a maneira como o servidor IIS constrói os endereços de acesso para as páginas gravadas em seus diretórios virtuais. Observe que o diretório virtual, é simplesmente um nome que nos leva até o diretório real, gravado no disco. Podemos criar diversos diretórios virtuais, em um único servidor IIS.

Uma vez criada uma estrutura de diretórios virtuais é só criar as páginas com o conteúdo a ser disponibilizado para os usuários da rede. Para a criação de páginas html simples você pode utilizar o Microsoft Word, o qual é capaz de converter para html, diversos formatos de documentos. Para páginas mais sofisticadas você pode utilizar editores específicos como o Front Page da Microsoft ou o Dreamweaver da Macromedia.

Tudo o que foi visto para o servidor http também é válido para o serviço de ftp. Por exemplo, você pode criar uma pasta C:\pub e associar à esta pasta um diretório virtual de ftp chamado pub. Para acessar o conteúdo desta pasta, o usuário utiliza o seguinte endereço:

<ftp://srv-win2003.abc.com/pub>.

Para criar uma pasta virtual de ftp você utiliza o console Internet Services Manager. Também é possível configurar o nível de acesso a uma pasta de ftp, como por exemplo: somente leitura ou leitura e escrita.

Com estas configurações o seu computador já está configurado para atuar como um servidor http e um servidor de ftp. Você pode criar novos diretórios virtuais a adicionar conteúdo. Depois é só criar uma página principal onde são colocados os links para o conteúdo disponível.

A seguir veremos mais algumas configurações do IIS. Veremos configurações para que possamos personalizar o servidor IIS, bem como configurações de segurança.

# Configurando opções do servidor de páginas e do servidor ftp.

Após ter criado um diretório virtual, quer seja de http ou de ftp, você pode configurar uma série de opções para este diretório. As configurações podem ser configuradas para o servidor como um todo, neste caso as configurações serão válidas para todos os diretórios virtuais do servidor. As configurações também podem ser feitas em cada diretório virtual, individualmente. No caso de conflito entre as configurações do servidor e as configurações de um diretório virtual, prevalecem as configurações do nível mais inferior, ou seja, do diretório virtual. Também é possível definir configurações individuais para pastas e subpastas de um diretório virtual, quer seja do servidor de páginas (http), quer seja do servidor de arquivos (ftp).

Vamos ver alguns exemplos de configurações do IIS.

Exemplo 1: Configurando opções do Default Web Site (Site da Web padrão).

Para configurar as opções básicas do Servidor Web Padrão, siga os passos indicados a seguir:

1. Faça o logon como Administrador ou com uma conta com permissões de administrador.
2. Abra o console Gerenciador dos Serviços de informações da Internet (IIS): Iniciar -> Ferramentas administrativas -> Gerenciador dos Serviços de informações da Internet (IIS).
3. Clique no sinal de + ao lado do nome do Computador para exibir as opções disponíveis. Observe que são exibidas as opções Sites da Web e Sites FTP, dentre outras opções disponíveis.
4. Clique no sinal de + ao lado da opção Sites da Web, para exibir os sites disponíveis. Por padrão é possível “hospedar” mais de um site, com endereços diferentes, em um mesmo servidor IIS. Para maiores detalhes sobre a hospedagem de vários sites em um único servidor, consulte o Capítulo 24 do livro Windows Server 2003 – Curso Completo, 1568 páginas, de minha autoria, publicado pela Editora Axcel Books. Observe que é exibida a opção Site da Web padrão. Este é o site criado, automaticamente, durante a instalação do IIS.
5. Clique no sinal de + ao lado de Site da Web padrão. Serão exibidos os diretórios virtuais criados durante a instalação, mais o diretório exemplos, criado no exercício anterior, conforme indicado na Figura 13.13:

---

**NOTA:** Dependendo dos componentes do IIS que você instalou, outras opções poderão ser exibidas no console Gerenciador dos Serviços de informações da Internet (IIS).

---

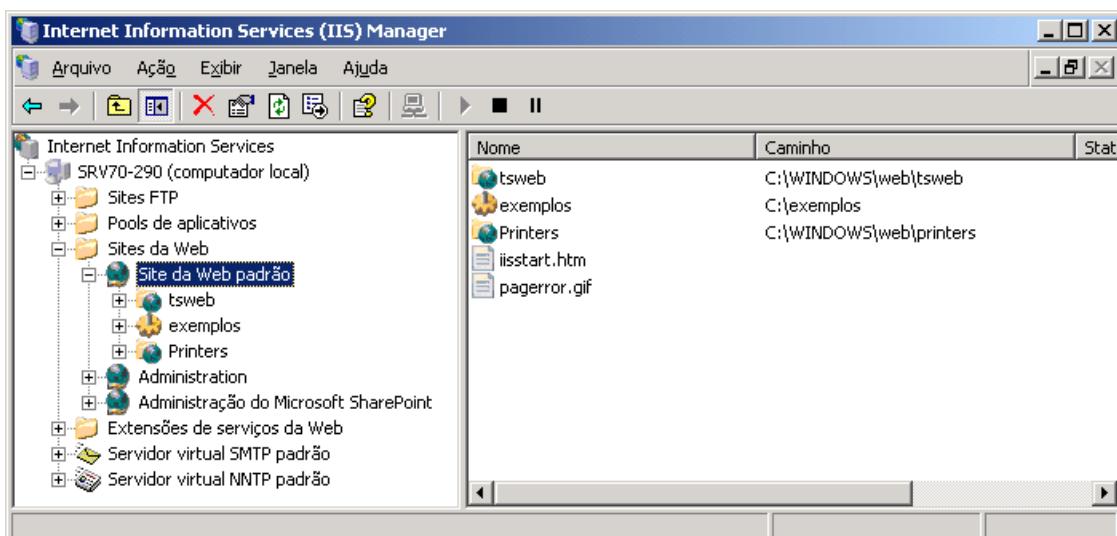


Figura 13.13 Site da Web padrão, criado durante a instalação do IIS.

Conforme descrito anteriormente podemos definir configurações diretamente no Site da Web padrão, configurações estas que serão válidas para todos os diretórios virtuais do site. Também podemos definir configurações personalizadas em um determinado diretório virtual. Neste caso valerão as permissões definidas ao nível do diretório virtual. Ao definir configuração no Site da Web padrão, se houver diretórios virtuais com configurações diferentes, o IIS abre uma janela perguntando se você deseja aplicar as novas configurações a todos os diretórios virtuais ou deseja manter, nos diretórios virtuais, as configurações já existentes, mesmo que estas sejam diferentes das configurações que estão sendo aplicadas no site principal.

6. Clique com o botão direito do mouse em Site da Web padrão. No menu de opções que é exibido clique em Propriedades. Será exibida a janela de Propriedades, com a guia Site da Web já selecionada, conforme indicado na Figura 13.14:

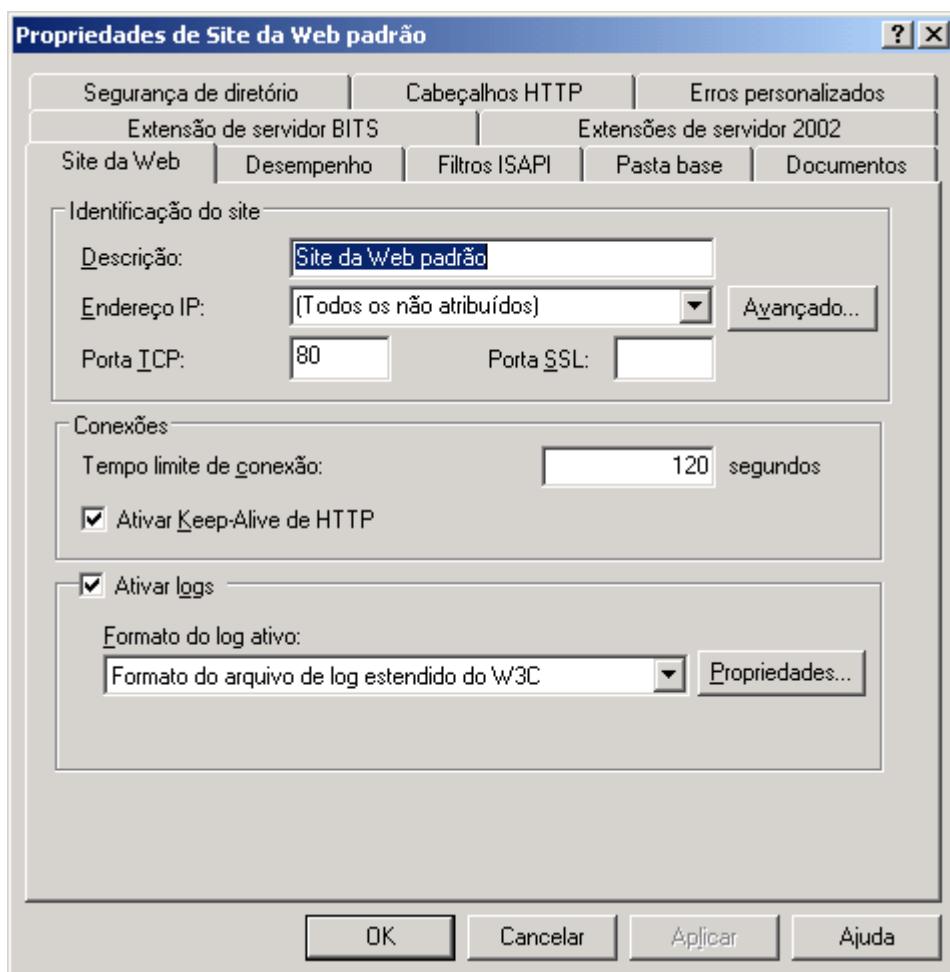


Figura 13.14 A guia Site da Web.

Nesta guia podemos definir diversas configurações.

No grupo Identificação do site da Web, você pode definir as seguintes configurações:

- ◆ **Descrição:** Neste espaço você pode digitar uma descrição para o site, como por exemplo: Documentos e Manuais. A descrição padrão é Site da Web padrão, a qual é definida durante a instalação do IIS.
- ◆ **Endereço IP:** Caso você tenha mais de um endereço IP configurado na mesma placa de rede, ou tenha mais de uma placa de rede, é possível definir qual endereço IP será associado com o site. Por padrão Todos os endereços

IP estão associados com o site padrão. O uso de múltiplos endereços IP em uma mesma placa de rede ou de múltiplas placas de rede, com diferentes endereços IP permite que sejam criados diferentes sites para diferentes grupos de usuários.

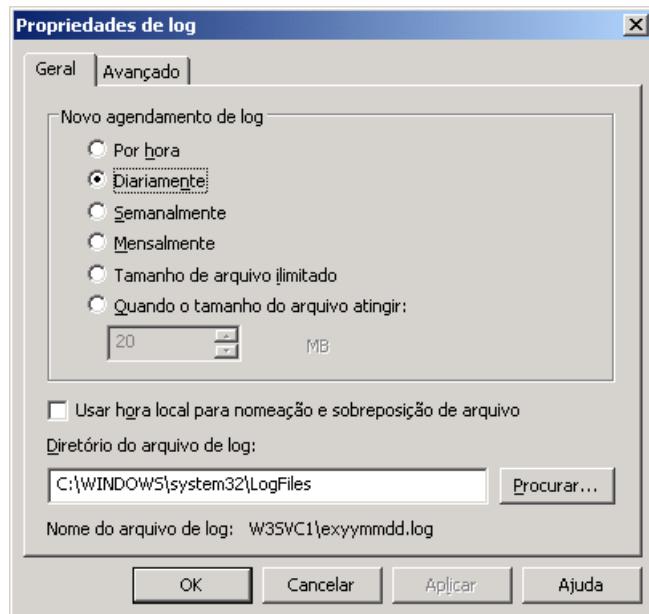
- ◆ **Porta TCP:** Cada serviço no protocolo TCP/IP é configurado para trabalhar em uma porta específica. O protocolo HTTP, por padrão, é configurado para responder na porta 80. Se você definir uma porta diferente da 80, o número da porta deverá ser informado no endereço de acesso. Por exemplo, se você definir a porta 470, o endereço para acesso ao site fica da seguinte maneira: <http://srv-win2003.abc.com:470>. Observe que o número da porta é informado após o endereço, separado deste pelo sinal de dois pontos (:).

No grupo Conexões você pode definir as seguintes configurações:

- ◆ **Tempo limite de conexão:** Define por quanto tempo (em segundos) o IIS tenta atender uma determinada requisição. Quando o tempo limite for atingido, o cliente receberá uma mensagem que o servidor não está respondendo.
- ◆ **Ativar Keep-Alive de http:** Por padrão, o navegador do cliente faz a solicitação de uma página para o servidor, estabelece uma conexão, recebe o conteúdo e fecha a conexão. Se uma nova requisição for feita logo em seguida, uma nova conexão será estabelecida, o conteúdo fornecido e a conexão será fechada. Este processo de abrir e fechar uma conexão, a cada requisição do cliente, faz com que sejam consumidos recursos de memória e processamento no servidor. Os navegadores atuais permitem que seja mantida a conexão entre o cliente e o servidor e que várias requisições possam ser feitas, dentro da mesma conexão. Esse procedimento é chamado de HTTP Keep-Alives (manter ativada). Keep-alive é uma especificação do protocolo HTTP que permite uma melhora considerável no desempenho do servidor. Sem ele, um navegador precisaria fazer numerosas solicitações de conexão para uma página com diversos elementos, como elementos gráficos. Por exemplo, para uma página com 20 figuras seriam necessárias 21 conexões: uma para a página e um para cada uma das figuras. Uma conexão separada precisaria ser feita para cada elemento. Essas solicitações e conexões adicionais requerem atividade e recursos adicionais do servidor, como memória e processador, diminuindo sua eficiência. Elas também tornam um navegador muito mais lento e as páginas menos aptas a responder, especialmente em uma conexão de alta latência (lenta), como por exemplo o acesso discado. Por padrão, o HTTP Keep-Alives fica ativado durante o processo de instalação. É recomendado que você mantenha esta opção sempre ativada.

**IMPORTANTE: Você deve conhecer o número de porta utilizado pelos principais serviços.  
http – 80, ftp – 21, SSL – 443, smtp – 25, DNS – 53, pop3 – 110, ldap – 389.**

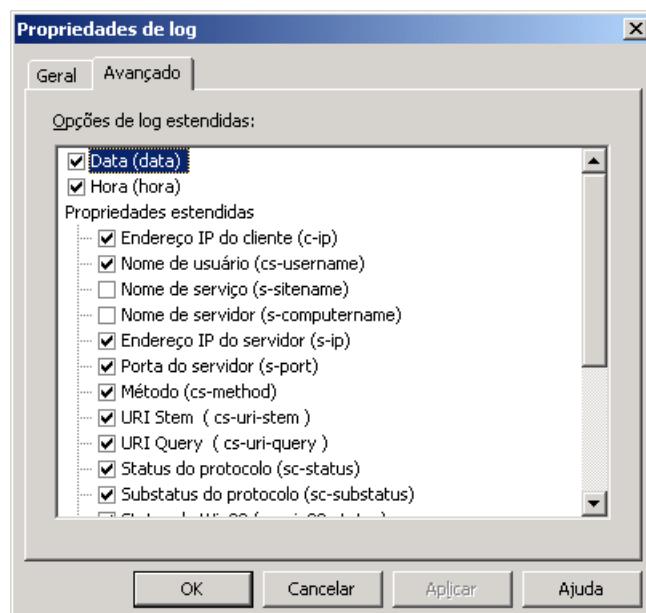
No grupo Ativar logs você pode definir se deve ser mantido ou não um log de acesso aos recursos do IIS. Existem vários formatos diferentes de log. Por padrão é utilizado o formato do arquivo de log estendido do W3C. É recomendado que você mantenha este formato, pois este é um formato padrão que pode ser lido por muitos dos programas geradores de estatísticas de acesso, com base nos logs de acesso. Para personalizar o log de acesso dê um clique no botão Propriedades. Será exibida a janela indicada na Figura 13.15.



**Figura 13.15 Configurando as propriedades do log.**

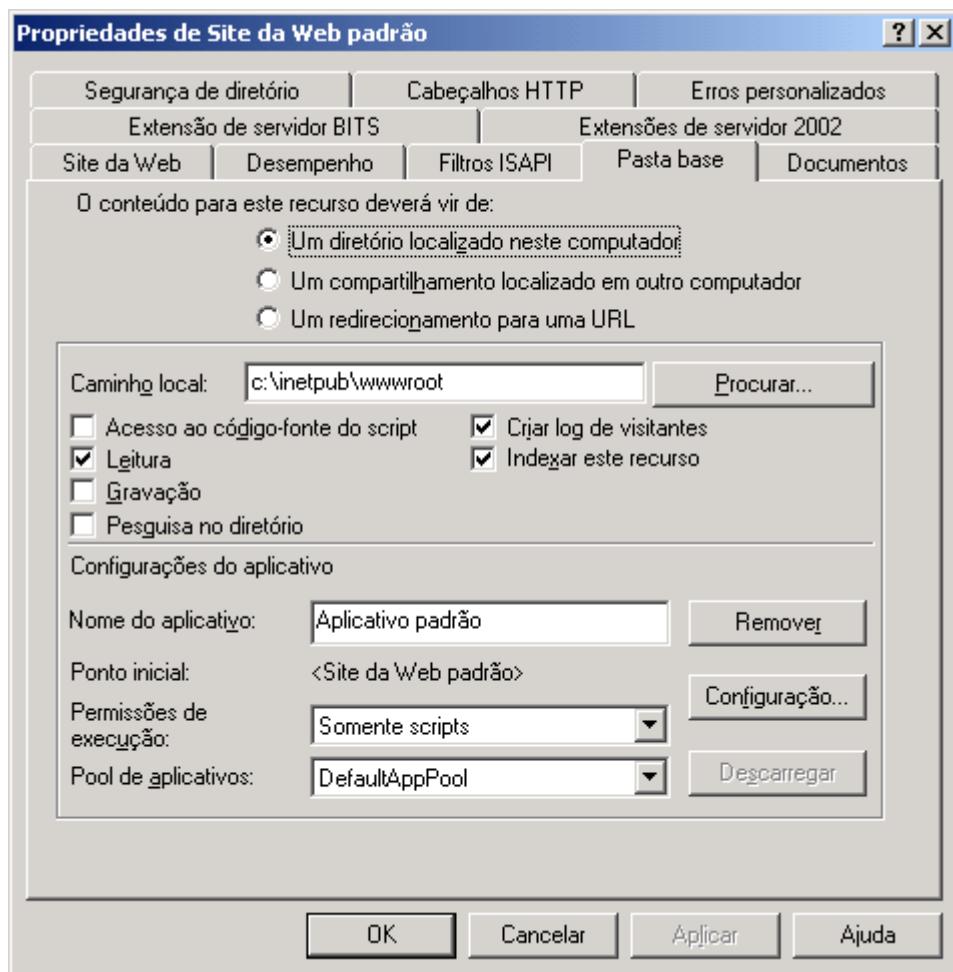
Na guia Geral você define de quanto em quanto tempo um novo arquivo de log deve ser gerado: Por hora, diariamente, semanalmente, Mensalmente, Tamanho de arquivo ilimitado (usa sempre o mesmo arquivo) ou Quando o tamanho do arquivo atingir (x MB). A opção a ser escolhida depende das políticas de segurança e do volume de acesso ao site. Por exemplo, para sites muito acessados a opção por hora pode ser a mais indicada. Na guia Propriedades gerais também é possível definir a pasta onde os arquivos de log serão gravados. Por padrão é definida a pasta: C:\WINDOWS\System32\LogFiles, onde C:\ é o drive onde está instalado o Windows Server 2003 e WINDOWS é a pasta onde o Windows Server 2003 foi instalado. Este caminho poderá ser diferente, dependendo do local e do drive onde foi instalado o Windows Server 2003.

Na guia Avançado, indicada na Figura 13.16, podemos definir informações adicionais a serem gravadas no log, como por exemplo: Nome do usuário, Nome do serviço, Nome do servidor e assim por diante.



**Figura 13.16 A guia Propriedades avançadas.**

- Defina as configurações desejadas e clique em OK. Você estará de volta à guia Site da web, da janela de propriedades do site padrão.
- A guia Filtros ISAPI é utilizada para a adição ou remoção de Filtros ISAPI, os quais são componentes de Software utilizados para responder a solicitações específicas do usuário. Por exemplo, o processador de páginas ASP é um filtro ISAPI.
- Dê um clique na guia Pasta base. Esta guia é utilizada para definir qual o diretório padrão do servidor IIS e a qual pasta ele está associado. Por padrão o diretório base está associado a pasta c:\inetpub\wwwroot, conforme indicado na Figura 13.17:



**Figura 13.17 A guia Diretório base.**

Observe que o diretório base não precisa, necessariamente, estar associado com uma pasta localizada no mesmo computador onde o IIS está instalado. Observe que além da opção Um diretório localizado neste computador, temos as opções: Um compartilhamento localizado em outro computador e Um redirecionamento para uma URL.

Nesta guia também podemos definir as permissões de acesso ao conteúdo do diretório base que, por padrão, está definido apenas como leitura – Ler. Uma opção que deve estar sempre desmarcada é a opção Pesquisa no diretório. Se esta opção estiver marcada e não existir uma página padrão configurada (conforme mostrarei logo a seguir) e o usuário digitar o endereço para o diretório, sem especificar uma página, será exibida uma listagem com todo o conteúdo do diretório, o que pode ser um problema de segurança. Na Figura 13.18 temos o exemplo da listagem que é exibida quando a opção Pesquisa no diretório está marcada e o diretório é acessado.

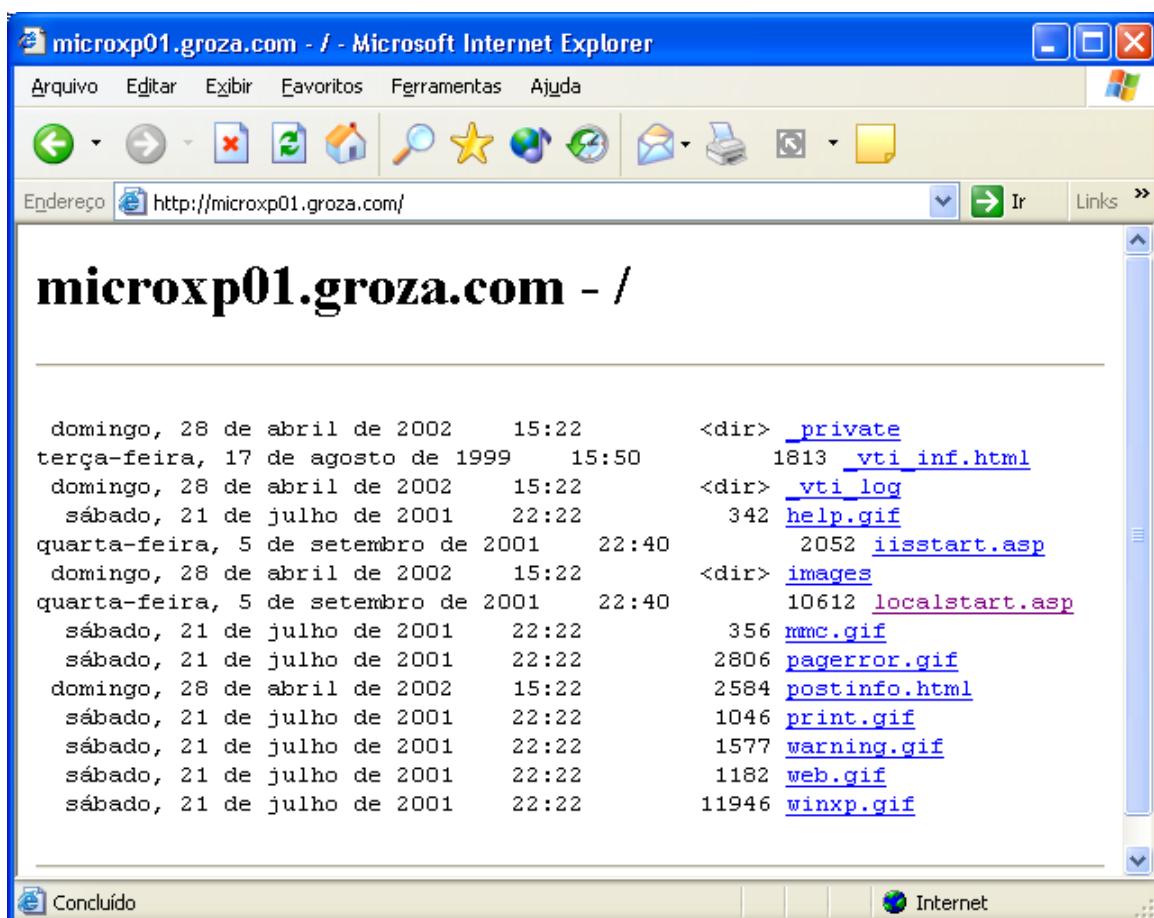


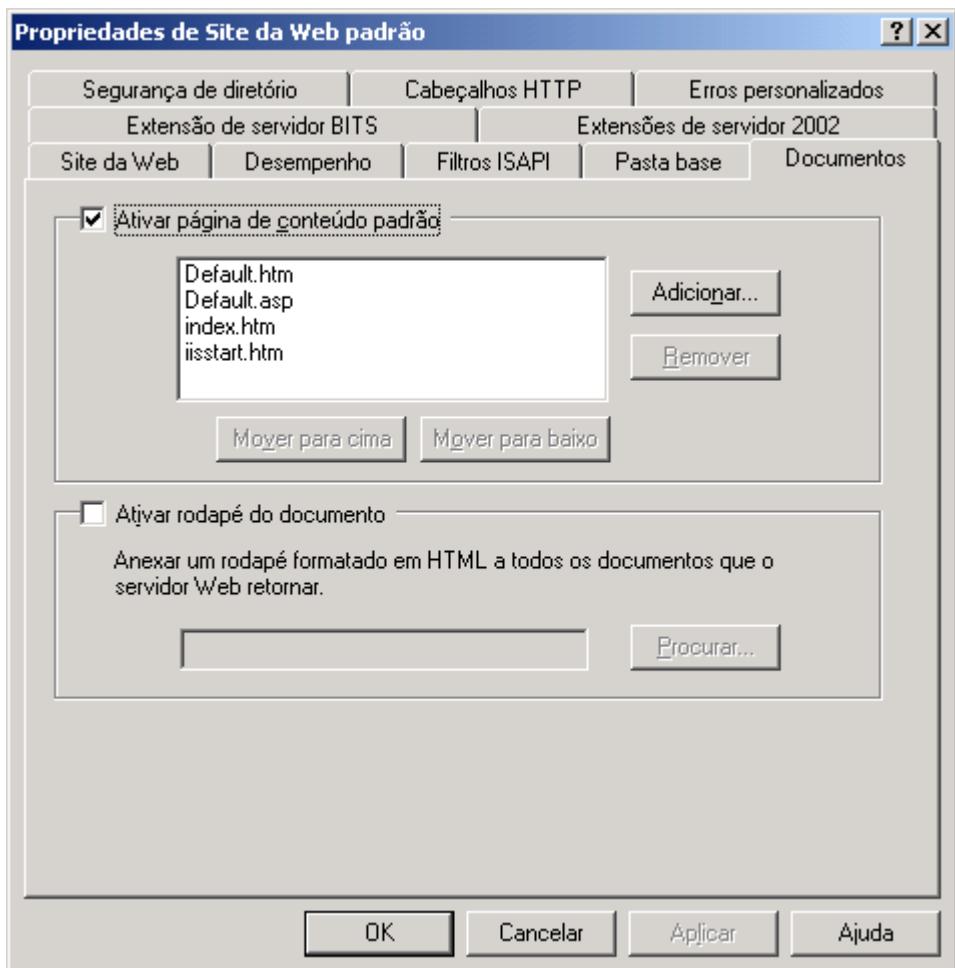
Figura 13.18 Listagem de todo o conteúdo do diretório.

10. Dê um clique na guia Documentos. Nesta guia você pode definir uma lista de documentos como sendo o conteúdo padrão do diretório. Por exemplo, se você define a página index.asp como sendo a página padrão e o usuário acessa o site, sem especificar um nome de página: <http://srv-win2003.abc.com> - será carregada a página definida como padrão. Para adicionar uma página como padrão clique no botão Adicionar... Para remover uma página da lista utilize o botão Remover. Com os botões de seta para cima e seta para baixo, você pode alterar a ordem dos documentos na lista. É possível ter mais do que uma página definida como padrão, conforme indicado na Figura 13.19. Neste caso o IIS irá tentar carregar a primeira página da lista, se esta não for encontrada o IIS tenta carregar a segunda e assim por diante.

Com a opção Ativar rodapé do documento, é possível configurar o IIS para inserir automaticamente um arquivo em formato HTML na parte inferior de todas as páginas da Web enviadas pelo servidor (não há suporte para a anexação de rodapés às páginas ASP). Por exemplo, o arquivo pode conter instruções de formatação HTML para adicionar uma mensagem de texto simples e um logotipo da empresa em todas as páginas do site.

Nota da documentação do IIS: Os rodapés de documentos podem reduzir o desempenho do servidor Web, especialmente se uma página da Web for acessada com freqüência.

11. Na guia Erros personalizados você pode associar páginas com mensagens de erro personalizadas para cada tipo de erro. Por exemplo, o erro mais tradicional é o erro 404, o qual indica que a página solicitada não foi encontrada. Quando este erro ocorre é exibida uma mensagem de erro padrão. Você pode criar uma página HTML mais elaborada e configurar esta página para ser exibida quando o erro 404 ocorrer. A página pode conter um link para o usuário voltar ao site principal e um email para que o usuário informe ao Administrador do site sobre o problema ocorrido. A guia Erros personalizados é utilizada para associar páginas HTML personalizadas com um determinado tipo de erro.



**Figura 13.19 A guia Documentos.**

12. Defina as configurações desejadas e clique no botão OK. Se algum dos diretórios virtuais apresentar configurações diferentes das definidas para o site principal, uma janela será exibida, listando os diretórios com configurações diferentes das do site principal. Você pode optar por aplicar as configurações do site principal a um ou mais dos diretórios ou a nenhum deles.

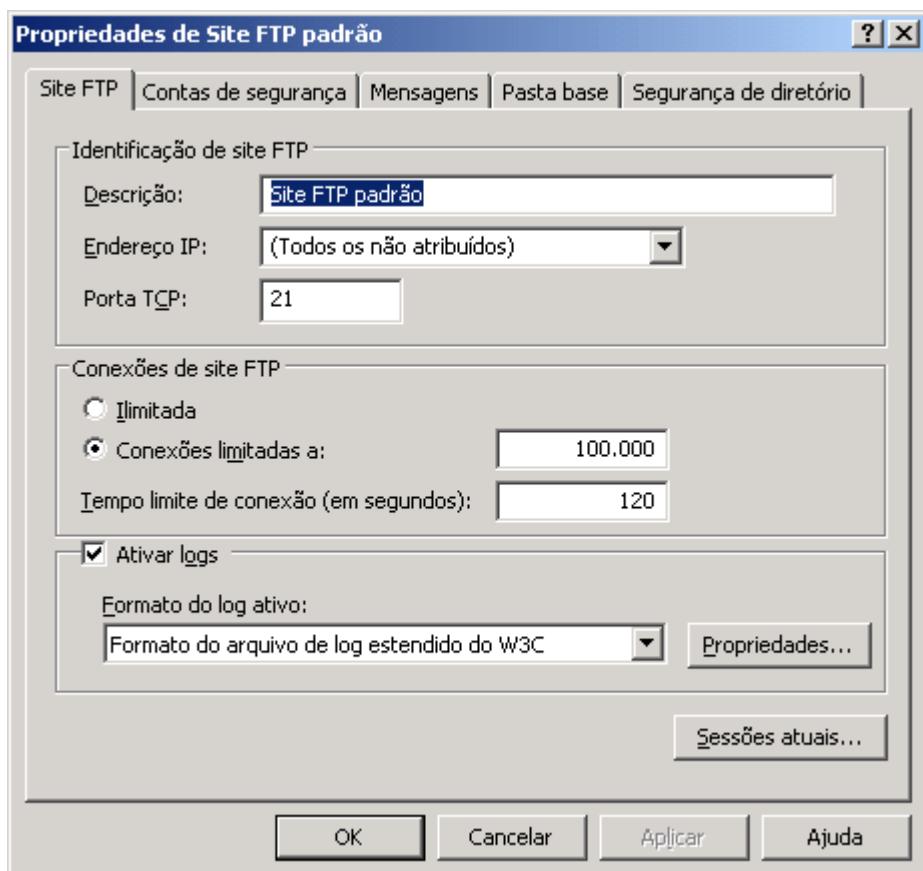
Exemplo 2: Para configurar as opções do servidor de arquivos – Site FTP padrão, siga os passos indicados a seguir:

1. Faça o logon como Administrador ou com uma conta com permissão de administrador.
2. Abra o console Gerenciador dos Serviços de informações da Internet (IIS): Iniciar -> Ferramentas administrativas -> Gerenciador dos Serviços de informações da Internet (IIS).
3. Clique no sinal de + ao lado do nome do Computador para exibir as opções disponíveis. Observe que são exibidas as opções Sites da Web e Sites FTP.
4. Clique no sinal de + ao lado da opção Sites FTP, para exibir os sites de ftp disponíveis. Por padrão é possível “hospedar” mais de um site de ftp, com endereços diferentes, em um mesmo servidor IIS. Observe que é exibida a opção Site FTP padrão. Este é o site de ftp criado, automaticamente, durante a instalação do IIS.

**NOTA:** Para uma descrição completa dos diferentes tipos de erros consulte a documentação do IIS.

**NOTA:** Dependendo dos componentes do IIS que você instalou, outras opções poderão ser exibidas no console Internet Services Manager.

- Clique no sinal de + ao lado de Site FTP padrão. Observe que por padrão ainda não foi criado nenhum diretório virtual além do diretório root do ftp que por padrão é o seguinte: c:\inetpub\ftproot.
- Clique com o botão direito do mouse na opção Site FTP padrão e no menu de opções que é exibido dê um clique em Propriedades. Será exibida a janela de propriedades do site FTP padrão com a guia Site FTP selecionada, conforme indicado na Figura 13.20:



**Figura 13.20 Janela de propriedades do site FTP padrão.**

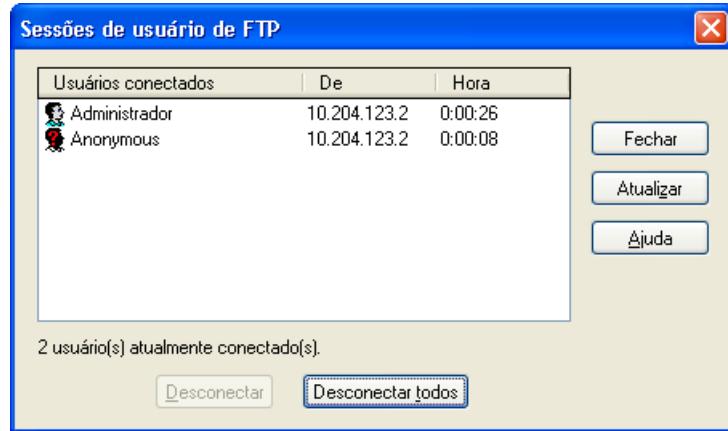
Na guia Site FTP temos opções semelhante às encontradas na guia Site da Web, da janela de propriedades do Site Web padrão.

As opções do grupo Identificação são idênticas às descritas no exemplo anterior. Para maiores detalhes consulte o Exemplo 1. A única diferença é a porta na qual é acessado o serviço de FTP que é a porta 21, ao invés da porta 80 usada pelo serviço HTTP.

No grupo conexão podemos definir se o site de ftp aceitará um número ilimitado de conexões simultâneas ou se iremos limitar o número de conexões. A configuração padrão é limitar a 100.000 (cem mil) conexões simultâneas. Você também pode definir um tempo limite para a conexão. Caso não exista uma resposta dentro do tempo limite, a conexão será encerrada e uma mensagem de erro será retornada para o usuário.

Na guia Site ftp você também pode configurar as opções para o log do serviço de ftp. Estas configurações são semelhantes as vistas no Exemplo 1 para o site Web padrão.

- Clique no botão Sessões atuais... Será exibida uma janela com a lista de usuários conectados e o tempo de conexão de cada usuário, conforme indicado na Figura 13.11:

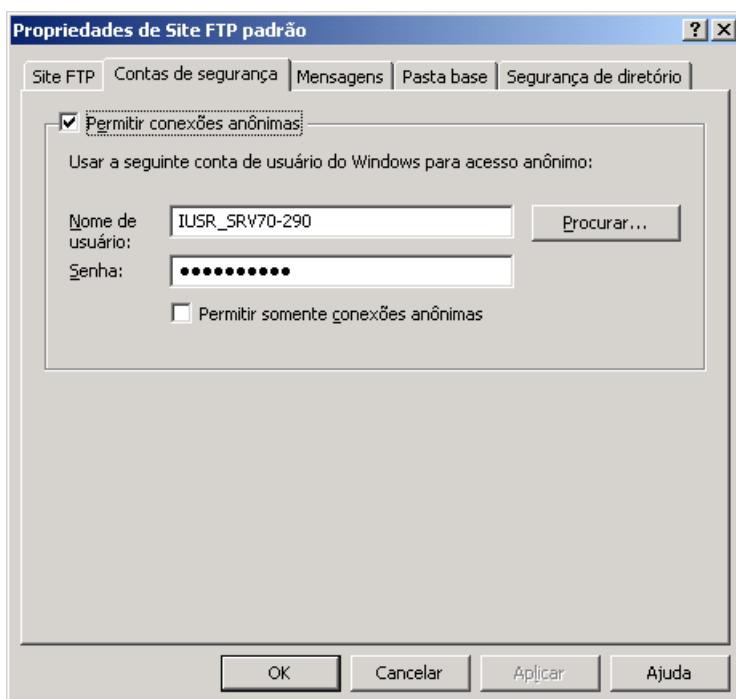


**Figura 13.21** Lista de usuários conectados ao site de FTP.

Você pode desconectar um determinado usuário. Para isso clique no usuário a ser desconectado e depois clique no botão Desconectar-se. Se você clicar no botão Desconectar todos, todos os usuários serão desconectados e suas sessões serão encerradas.

8. Clique no botão Fechar para fechar a janela Sessões de usuário de FTP.
9. Você estará de volta à janela de propriedades do site FTP padrão. Dê um clique na guia Contas de segurança.

Nesta guia você define se serão permitidas ou não Conexões anônimas e qual a conta será utilizada para conexões anônimas. Ao instalar o IIS é criada, automaticamente, uma conta com o nome IUSR\_Nome\_do\_computador. Por exemplo, em um servidor com o nome SRV-WIN2003, será criada a conta IUSR\_SRV-WIN2003. Durante a instalação do IIS esta conta é criada e configurada para ser utilizada como conta de acesso anônimo. Com o acesso anônimo, os usuários podem acessar o site de FTP sem ter que especificar um nome de usuário e uma senha. Esta configuração é ideal quando você quer criar um site de FTP para acesso público ou para acesso interno para os usuários da sua rede. Com o acesso anônimo os usuários não precisam fazer um logon para ter acesso aos arquivos que estão disponíveis no servidor de ftp. Isto facilita e simplifica o acesso. As opções desta guia estão indicadas na Figura 13.22:



**Figura 13.22** A guia Contas de segurança.

10. Clique na guia Mensagens. Nesta guia você pode definir mensagens que serão enviadas para o usuário quando um dos seguintes eventos ocorre: Boas vindas – quando o usuário conecta-se com o servidor; Saída - quando o usuário encerra a conexão e Nº máximo de conexões – quando o usuário tenta conectar-se mas o número máximo de conexões já foi atingido. Também está disponível a opção Faixa. Neste campo você define uma mensagem que será exibida antes da conexão ser estabelecida. Defina as mensagens desejadas.

11. Dê um clique na guia Pasta base.

Nesta guia você define qual o diretório padrão do servidor de ftp, que por padrão é c:\inetpub\ftproot. Você também define se o diretório padrão está associado com uma pasta no computador local ou com uma pasta compartilhada em outro computador. É possível definir permissões de acesso de Leitura, Gravação e se um log deve ser gravado com informações sobre o acesso ao diretório.

12. Defina as opções desejadas e clique em OK para aplicá-las.

13. Você estará de volta ao console de gerenciamento do IIS. Feche-o.

Com isso aprendemos a configurar as principais opções do site Web padrão e do site FTP padrão. Caso você crie sites adicionais, as configurações serão as mesmas. Quando tenho mais de um site (http ou ftp) as configurações são mantidas, separadamente, para cada site. O IIS utiliza, além do registro do Windows Server 2003, uma base de configurações conhecida como Metabase. Para maiores informações sobre a Metabase consulte a documentação do IIS.

## Questões e configurações de segurança com o IIS.

Neste tópico mostrarei algumas questões relacionadas com a segurança no acesso às informações disponibilizadas pelo IIS. Vamos iniciar falando sobre os tipos de autenticação existentes.

### Porque devo me preocupar com segurança?

Quando se fala de Internet nos dias de hoje, o assunto mais tratado, sem nenhuma dúvida, é sobre Segurança, principalmente devido aos inúmeros vírus difundidos nos últimos meses: I Love You, Nimda, Sircam, Klez, MSBlast, NetSky e tantas outras pragas que provocaram estragos e prejuízos mundo a fora. Muitos relatos, alguns verdadeiros e outros mais fantasiosos, sobre invasões mirabolantes, roubo de número de cartões de créditos, acesso a informações sigilosas de órgãos governamentais e assim por diante.

Não podemos negar que o problema de segurança existe e é crítico, principalmente hoje em que o Comércio Eletrônico é, mais do que uma realidade, uma necessidade e um diferencial competitivo para as empresas. O diferencial competitivo não é entrar ou não no mundo do Comércio Eletrônico, o diferencial é criar serviços agregados ao comércio eletrônico, capazes de gerar diferenciais que atraem o cliente. Assuntos como fidelização do cliente, melhorias nos sistemas de CRM – Customer Relationship Management (Gerenciamento das Relações com o Cliente), B2B – Business to Business, B2C – Business to Consumer e outros, estão em evidência.

Porém sistemas de Comércio Eletrônico, CRM e assemelhados, exigem acesso a um conjunto de dados estratégicos da empresa. Uma vez que estes sistemas estão acessíveis através da Internet, os dados empresariais precisam estar protegidos. Neste ponto é que a questão segurança é de fundamental importância. O ponto de acesso a estes dados é através de aplicações Web, hospedadas em um servidor Web. Por isso a importância de conhecer os mecanismos de segurança do IIS e a integração destes com o Sistema Operacional e com o sistema de banco de dados utilizado.

Existem os mais variados tipos de ataques pela Internet. Um engano comum é pensar que único tipo de ataque capaz de causar prejuízos é aquele que rouba ou destrói dados. No caso de um site de comércio eletrônico, qualquer ataque que torne o site indisponível por um determinado período de tempo, causa prejuízos incalculáveis, pois além das compras

que deixaram de ser feitas no período de indisponibilidade, tem a questão da imagem da empresa, sem contar que o cliente pode ter feito a compra no site do concorrente e passar a fazer as próximas compras no site do concorrente.

Por todos estes motivos é que a questão de segurança é fundamental e deveria ser prioritária quando tratamos de aplicações Web. Outro fato importante a ser mencionado é que a maioria dos ataques, ao contrário do que muitos pensam, é originado dentro da Intranet da própria empresa, ou seja, por funcionários da empresa. Pode ser um funcionário descontente ou desonesto, ou um usuário com permissões de acesso indevidas que causa algum prejuízo por imperícia técnica. O fato é que a questão de segurança não deve ser tratada apenas como uma questão de proteção contra “as forças do mal que vem da Internet”. Precisamos definir uma política de segurança que permita que todos possam realizar o seu trabalho, porém com os níveis de permissão adequados – nem mais nem menos do que o necessário.

Além de definir uma política de segurança, é necessário a ampla divulgação desta. É alarmante constatar que muitas empresas não possuem uma política de segurança definida e amplamente divulgada e em constante revisão e atualização.

Outro erro bastante comum é achar que a questão de segurança é responsabilidade somente da equipe de informática/ tecnologia. Na verdade o item segurança é bastante complexo e exige que todos estejam comprometidos. Veja bem, não é “envolvidos” e sim “comprometidos”. A diferença básica entre “comprometido” e “envolvido” é ilustrada pela seguinte história: “Quando você come ovos com bacon no café da manhã, a galinha está envolvida já o porquinho está comprometido”. É isso.

Conforme veremos existem aspectos de segurança que são de responsabilidade do desenvolvimento e outros que são de responsabilidade da Administração de rede. Na verdade o que se faz é criar várias barreiras para que o hacker não tenha sucesso em sua tentativa de invasão. Algumas destas barreiras são criadas na própria rede da empresa e outras no servidor Web.

Neste site são divulgados boletins sobre segurança dos produtos Microsoft. Sempre que algum novo problema é descoberto, são divulgadas informações sobre o problema, bem como a maneira de corrigi-los. Também são disponibilizados arquivos para Download. Estes arquivos normalmente contém correções (Hotfix) que devem ser aplicados para corrigir problemas de segurança.

## Autenticação de usuários com o IIS.

Quando um usuário tenta acessar uma página no servidor IIS, a primeira coisa que o servidor precisa determinar é a identidade deste usuário, isto é, o IIS precisa conhecer “quem” está tentando acessar a página. Uma das maneiras de saber quem é o usuário que está acessando o site, é através da utilização de um Username e senha. Porém não seria nada “simpático” apresentar uma tela de logon para o usuário a primeira vez que ele está acessando o site. Também não seria prático apresentar uma tela de logon para o funcionário que está acessando a Intranet da empresa. Até mesmo nas próximas tentativas de acesso, a necessidade de logon pode acabar “afastando” o usuário.

Através da autenticação do usuário, podem ser definidos os níveis de acesso a informação que ele tem, bem como podem ser feitos registros das ações realizadas pelo usuário, mediante a gravação de logs de acesso. Existem diversos tipos de autenticação possíveis com o IIS. Passaremos a estudá-los individualmente. Os tipos de autenticação existentes são os seguintes:

- ◆ Autenticação anônima.
- ◆ Autenticação básica.

---

**NOTA:** Quando trabalhamos com tecnologias da Microsoft como ADO, Windows Server 2003 e IIS, o endereço a seguir é de consulta obrigatória para assuntos relacionados a segurança de tecnologias Microsoft: <http://www.microsoft.com/security>.

---

- ◆ Autenticação avançada.
- ◆ Autenticação integrada ao Windows.
- ◆ Autenticação com certificados.

## O acesso anônimo.

Um tipo de autenticação bastante comum é o que permite o acesso anônimo. O IIS permite que seja configurado um tipo de acesso chamado Acesso anônimo, no qual não é necessário que o usuário forneça um Username e senha para ter acesso ao site. Este acesso anônimo está ligado a uma única Conta de usuário do Windows Server 2003, a conta IUSR\_Nome\_do\_Computador já descrita anteriormente. Todo o usuário que acessar um site configurado para permitir Acesso anônimo, será identificado como se estivesse autenticado usando a Conta de usuário configurada para o acesso anônimo.

A conta de usuário para Acesso anônimo é automaticamente criada quando instalamos o Internet Information Services. Por padrão esta conta possui o seguinte nome:

**IUSR\_NOME\_DO\_COMPUTADOR**

Por exemplo, ao instalarmos o IIS em um servidor chamado SERVER02SP, será criada a seguinte conta para permitir o Acesso anônimo:

**IUSR\_SERVER02SP**

A autenticação anônima fornece aos usuários acesso a áreas públicas do seu site, sem solicitar um nome de usuário ou uma senha.

Por padrão, a conta IUSR\_NOME\_DO\_COMPUTADOR é incluída em um grupo de usuários que tem restrições de segurança, impostas pelas permissões do NTFS (sistema de arquivos do Windows Server 2003 que possui recursos de segurança mais avançados do que o sistema FAT ou FAT32, e que foi descrito no Capítulo 5), que designam o nível de acesso e o tipo de conteúdo disponível para os usuários públicos, via acesso anônimo. Com isso o usuário possui limitações sobre os recursos que ele pode acessar no servidor, sendo que estas limitações já atuam como um nível de segurança.

Se existem vários sites no seu servidor ou áreas no seu site que exigem privilégios de acesso diferentes, você pode criar várias contas para acesso anônimo, uma para cada área site, diretório ou arquivo.

Por exemplo, você pode querer medir o nível de acesso a diferentes áreas do seu site, utilizando para isso diferentes contas para o acesso anônimo a cada uma destas áreas.

O IIS usa a conta IUSR\_NOME\_DO\_COMPUTADOR da seguinte forma:

1. Quando uma solicitação é recebida, o IIS representa, isto é, acesso os recursos como se fosse o usuário representado pela conta IUSR\_NOME\_DO\_COMPUTADOR antes de executar qualquer código ou acessar qualquer arquivo. O IIS pode representar a conta IUSR\_NOME\_DO\_COMPUTADOR pois conhece o nome de usuário e a senha dessa conta, conforme veremos logo a seguir. Isso faz com que o usuário somente possa acessar os recursos para os quais a conta IUSR\_NOME\_DO\_COMPUTADOR tem permissão de acesso.
2. Antes de retornar uma página ao cliente, o IIS verifica as permissões dos arquivos e diretórios do NTFS para ver se a conta IUSR\_NOME\_DO\_COMPUTADOR tem permissão para acessar o arquivo. Neste ponto é que podemos limitar as áreas as quais o usuário que entra como acesso anônimo tem acesso. Basta configurar as permissões NTFS para que a conta associada ao acesso anônimo somente tenha acesso as áreas públicas do site.
3. Se o acesso for permitido, a autenticação é concluída e os recursos tornam-se disponíveis para o usuário.

4. Se o acesso não for permitido, o IIS tenta usar outro método de autenticação. Se nenhum método for selecionado, o IIS retorna uma mensagem de erro “HTTP 403 Acesso negado” ao navegador do cliente.

Na Figura 13.23, temos uma representação desta seqüência para o acesso anônimo.

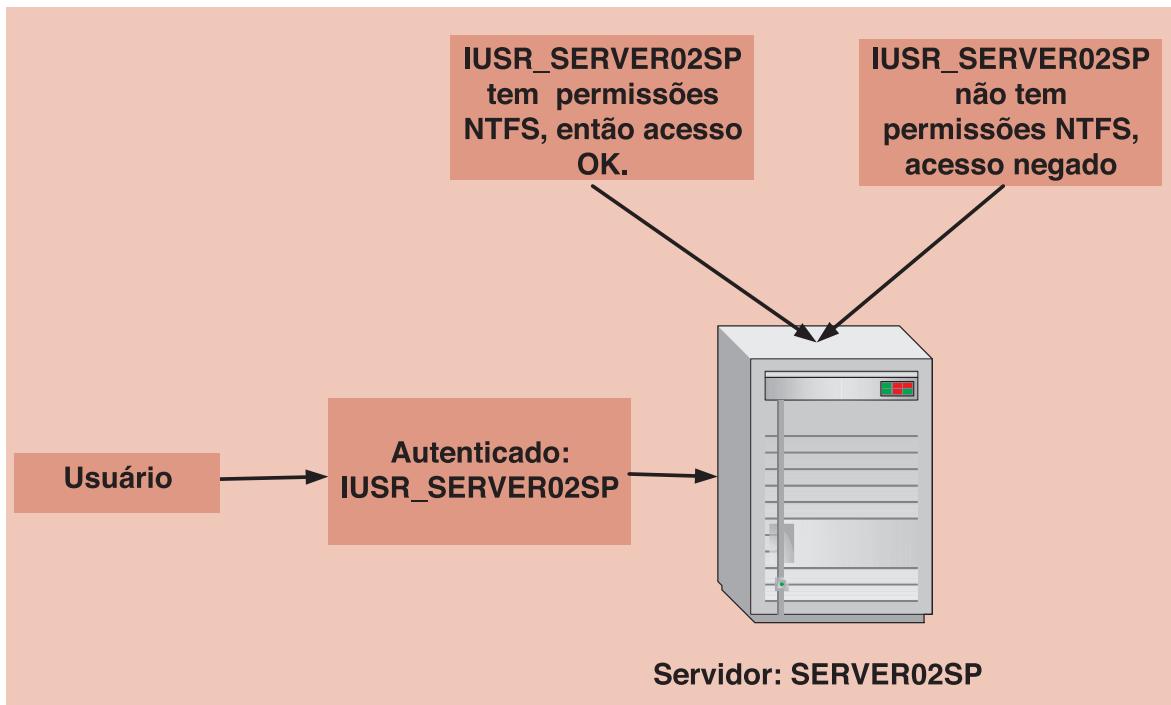


Figura 13.23 Acesso anônimo no IIS.

Considere as observações a seguir:

- ◆ Se a autenticação anônima for ativada, o IIS tentará sempre a autenticação usando-a primeiro, mesmo se outros métodos de autenticação forem ativados.
- ◆ Em alguns casos, o navegador solicitará ao usuário um nome de usuário e uma senha.

Você pode alterar a conta usada para a autenticação anônima no Snap-in do IIS, no nível de serviço do servidor Web ou para diretórios virtuais ou arquivos individuais, conforme veremos logo a seguir.

- ◆ A conta anônima deve ter o direito de usuário (right) de efetuar logon localmente. Se a conta não tiver a permissão “Efetuar logon localmente”, o IIS não poderá atender qualquer solicitação anônima. Ao instalarmos o IIS, automaticamente, a permissão “Efetuar logon localmente” é concedida à conta IUSR\_NOME\_DO\_COMPUTADOR.

Agora vamos aprender a configurar a conta para acesso anônimo, utilizada pelo IIS.

## Como definir a conta para acesso anônimo no IIS.

Para definir qual conta será utilizada para o acesso anônimo siga os seguintes passos:

1. Faça o logon como Administrador ou com uma conta com permissão de administrador.

**IMPORTANTE:** Não esqueça que a conta para acesso anônimo precisa da Right de fazer o logon localmente.

2. Abra o console Gerenciador dos Serviços de informações da Internet (IIS): Iniciar -> Ferramentas administrativas -> Gerenciador dos Serviços de informações da Internet (IIS).
3. Dê um clique duplo no nome do computador. No nosso exemplo o nome é srv-win2003. Clique no sinal de + ao lado da opção Sites da Web, para exibir as opções disponíveis.

Neste momento podemos configurar o acesso anônimo para todos os sites e aplicativos contidos no Servidor ou para cada site/aplicativo individualmente. Inclusive podemos configurar diferentes contas para ser utilizadas para o acesso anônimo em diferentes áreas do site.

No nosso exemplo, iremos configurar uma única conta para acesso anônimo para todo o site padrão. O procedimento é o mesmo quer seja para o site como um todo, para uma aplicação Web do site ou para uma pasta dentro da aplicação Web.

4. Clique com o botão direito do mouse sobre a opção Site da Web padrão. No menu de opções que surge dê um clique em Propriedades.
5. Será exibida a janela de propriedades do site padrão.
6. Dê um clique na guia Segurança de diretório. Serão exibidas as opções indicadas na Figura 13.24.

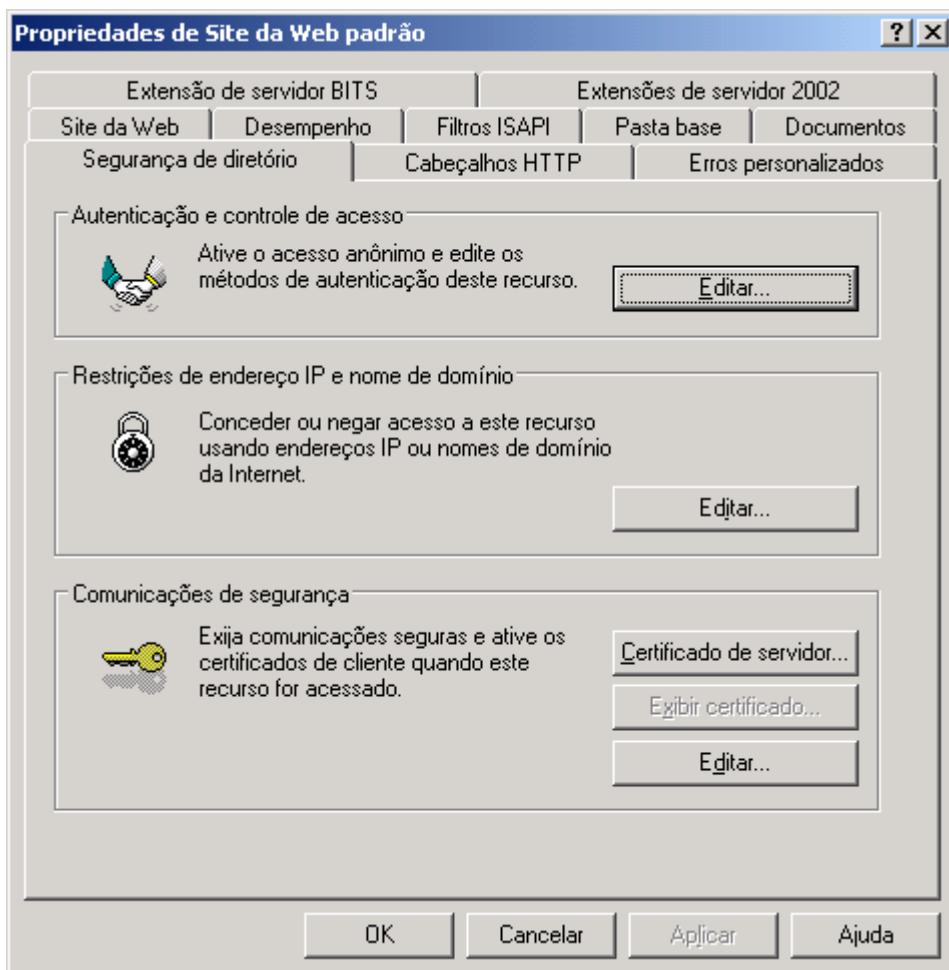


Figura 13.24 As opções da guia Segurança de diretório.

7. A primeira opção desta guia é Autenticação e Controle de acesso. Dê um clique no botão Editar..., ao lado desta opção. Surge a janela Métodos de autenticação, indicada na Figura 13.25.

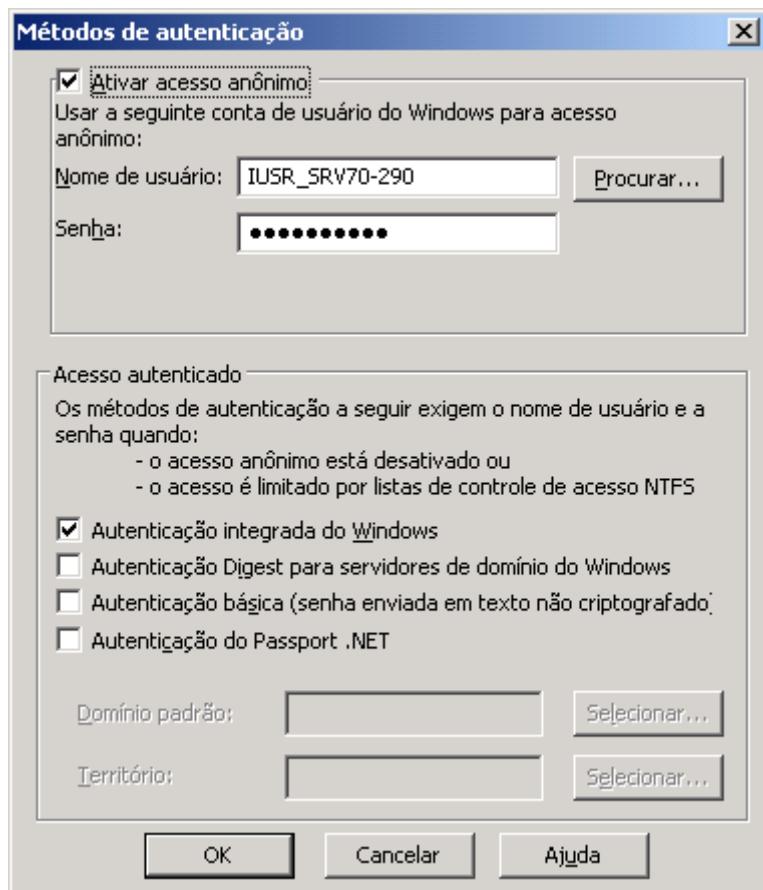


Figura 13.25 As opções para métodos de autenticação.

A primeira opção desta janela é Ativar acesso anônimo. Para que o acesso anônimo seja permitido, esta opção deve estar marcada.

8. Para definir a conta que será utilizada para o acesso anônimo, dê um clique no botão Procurar...
9. Será exibida a janela para selecionar usuário, já descrita em capítulos anteriores. Você utiliza esta janela para localizar a conta de usuário que será utilizada para o acesso anônimo. Se você souber o nome da conta pode digitá-lo diretamente na janela Selecionar usuário, no formato NomeDoComputador\NomeDaconta ou NomeDoDomínio\NomeDaConta. Se você não souber o nome da conta, utilize o botão Avançado para exibir uma lista com as contas disponíveis. Selecione a conta desejada e clique em OK.
10. Após ter configurado as informações para a conta de acesso anônimo, dê um clique em OK.
11. Você estará de volta à janela de métodos de autenticação, dê um clique em OK para fechá-la.
12. Você estará de volta à janela Propriedades do site da Web padrão, dê um clique em OK para fechá-la.
13. Você estará de volta ao console de gerenciamento do IIS. Feche-o.

## SUS – Software Update Services

### Introdução ao SUS

O SUS – Software Update Services é um serviço utilizado para automatizar o processo de download e instalação das correções do Windows, a partir do site Windows Update. No Windows Server 2003, em Português, este serviço é

denominado de Serviço de Atualizações Automáticas. Já há alguns anos, que a Microsoft disponibiliza o site Windows Update, através do qual você pode baixar e instalar atualizações e correções de segurança para as diferentes versões do Windows. Porém o usuário deve tomar a iniciativa de usar o comando Windows Update, para conectar o seu computador com o site do Windows Update, para fazer a instalação das últimas correções disponíveis. O SUS leva este processo um nível a frente. Você estala o SUS em um servidor da rede e pode configurar este servidor para baixar, automaticamente, as atualizações a partir do site Windows Update. Depois de baixadas para o servidor, estas atualizações poderão ser aplicadas, automaticamente, em todos os demais computadores da rede. Este processo tem inúmeras vantagens, as quais serão descritas neste capítulo.

O SUS é instalado como um site/aplicativo Web, baseado no IIS. Conforme você verá neste tópico, todo o processo de administração do SUS é feito via browser, através da página de administração do SUS.

O SUS é uma aplicação Cliente/Servidor. Você instala o SUS em um servidor baseado no IIS. No servidor você configura um agendamento para o download automático das atualizações, aprova as atualizações críticas de segurança e faz uma série de outras configurações. Nos clientes, você instala o software client do SUS, o qual se comunica com o servidor e baixa e instala, automaticamente, as atualizações disponíveis no servidor.

## Componentes do SUS:

Neste item farei uma breve descrição sobre os elementos que compõem o SUS, os quais permitem que seja montado uma infra-estrutura para download e instalação automática das atualizações do Windows. O SUS é formato, basicamente, pelos seguintes componentes:

1. O site do SUS rodando em um servidor com o IIS: Ao instalar o SUS será criado um site no servidor IIS, no qual estão todos os recursos necessários a administração e a configuração do SUS. Este é o componente de servidor do SUS. Este é o componente responsável por entrar em contato com o site Windows Update e por baixar as atualizações disponíveis. Você verá que é possível configurar um agendamento, para que o SUS verifique sobre a disponibilidade de novas atualizações no site Windows Update. Você aprenderá a instalar o SUS e a fazer as principais configurações disponíveis. Mostrarei que a interface de administração do SUS são simplesmente páginas hospedadas no IIS, as quais você acessa através do Internet Explorer.
2. O site de Administração do SUS: Esta é o componente de administração do SUS. A interface de administração do SUS nada mais é do que um conjunto de páginas, hospedadas em um site do IIS. Ao instalar o SUS, o site de administração é criado e configurado. Toda a administração do SUS é feita usando o navegador.
3. Atualizações Automáticas: Este é o componente cliente, na arquitetura Cliente/Servidor do SUS. O cliente é instalado em cada estação de trabalho e pode ser configurado para baixar as atualizações diretamente do site Windows Update ou de um servidor SUS. O cliente também pode ser configurado para buscar por atualizações dentro de um agendamento determinado. Você pode definir se as atualizações devem ser aplicadas automaticamente ou se deve ser apenas exibido um aviso sobre a disponibilidade das novas atualizações, de tal maneira que o usuário opte por iniciar ou não a instalação das novas atualizações.

**IMPORTANTE:** Algumas vezes pode acontecer de todos os serviços do SUS pararem de funcionar corretamente. As atualizações não são mais baixadas automaticamente, atualizações que já foram baixadas não são instaladas ou você não consegue se conectar com a página de administração do SUS. Nestas situações, a causa mais provável do problema é que o próprio IIS está com problemas. Quando isso ocorrer é recomendado que você pare e reinicialize todos os serviços relacionados ao IIS. Normalmente esta reinicialização dos serviços do IIS, faz com que o SUS normalize também.

4. Configurações das políticas de segurança: Este é um aspecto muito importante e que você deve conhecer muito bem para o exame. Por padrão, o cliente de Atualizações Automáticas, é configurado para baixar as atualizações a partir do site Windows Update. Você pode alterar estas configurações, para fazer com que o cliente de Atualizações Automáticas, baixe as atualizações a partir de um servidor com o SUS instalado. Estas configurações podem ser feitas via GPO (que é a maneira preferencial, a qual automatiza o processo de configuração), ou alterando, manualmente, a Registry de cada computador da rede. Mais adiante mostrarei qual a diretiva de GPO a ser alterada e qual a chave da Registry, caso você tenha optado por fazer as configurações do cliente via Registry.

## Instalando o SUS

O SUS não é incluído como parte do Windows Server 2003. O SUS é gratuito e pode ser copiado do site da Microsoft, a partir do seguinte endereço:

<http://www.microsoft.com/windowsserversystem/sus/default.mspx>

Antes de baixar e instalar o SUS é importante que você saiba que a partição onde o SUS será instalado e a partição do sistema, devem estar formatadas com o sistema de arquivos NTFS. Esta não é uma recomendação, mas sim um pré-requisito para que o SUS possa ser instalado.

A instalação do SUS faz com que os seguintes componentes sejam instalados no servidor:

- ◆ O serviço Software Update Synchronization Service, o qual é responsável por fazer o download das correções do site Windows Update para o servidor SUS
- ◆ Um site no IIS, o qual é utilizado para administração do SUS.
- ◆ Uma página para administração do SUS, a qual é utilizada para sincronização do servidor SUS e para aprovação das atualizações que foram baixadas, antes que estas sejam instaladas nos clientes.

Ao fazer o download do SUS, você irá copiar para o servidor o seguinte arquivo:

**SUS10SP1.exe**

Esta é a versão do SUS já com o SP1 do SUS, ou seja, já com um pacote de correções do SUS, em relação a primeira versão que foi lançada. Este arquivo tem 32,2 MB. A seguir descrevo os passos para instalação do SUS:

Para instalar o SUS, siga os passos indicados a seguir:

1. Faça um logon com uma conta com permissão de Administrador, em um servidor com o IIS já instalado.
2. Faça o download do SUS, usando o endereço descrito anteriormente.
3. Após ter feito o download deste arquivo, basta dar um clique duplo no arquivo SUS10SP1.exe para iniciar a instalação do SUS. Ao dar um clique duplo no arquivo SUS10SP1.exe, será aberto o assistente de instalação do SUS.
4. A primeira tela do assistente é apenas informativa. Clique em Next para seguir para a próxima etapa do assistente.

**IMPORTANTE:** No momento em que escrevo este capítulo (22-03-2004), o SUS está disponível somente nas versões em Inglês e Japonês. Um ponto importante a salientar é que o que está em Inglês é a interface de administração do SUS, mas isso não impede que você possa utilizá-lo para baixar atualizações para o Windows em outros idiomas, como por exemplo, Português do Brasil. Você verá mais adiante, que ao configurar o SUS, você define para quais idiomas (o termo técnico ao invés de Idioma seria Localidade) você quer que um servidor com o SUS baixe as atualizações. Por exemplo, se a sua empresa tem escritórios no Brasil, EUA e Itália, você pode configurar um único servidor SUS, para baixar atualizações para os três idiomas. O cliente de Atualizações Automáticas saberá identificar, automaticamente, as correções adequadas ao idioma da estação de trabalho. Ainda usando o exemplo da empresa que tem filiais no Brasil, EUA e Itália, cabe salientar que se você estiver usando um servidor SUS em cada localidade, você deve

- Na segunda etapa você deve aceitar o contrato de licença. Marque a opção “I accept the terms in the License Agreement” e clique em Next para seguir para a próxima etapa do assistente.
- Nesta etapa você deve optar por fazer uma instalação Típica (Typical) ou Personalizada (Custom), conforme indicado na Figura 13.26:

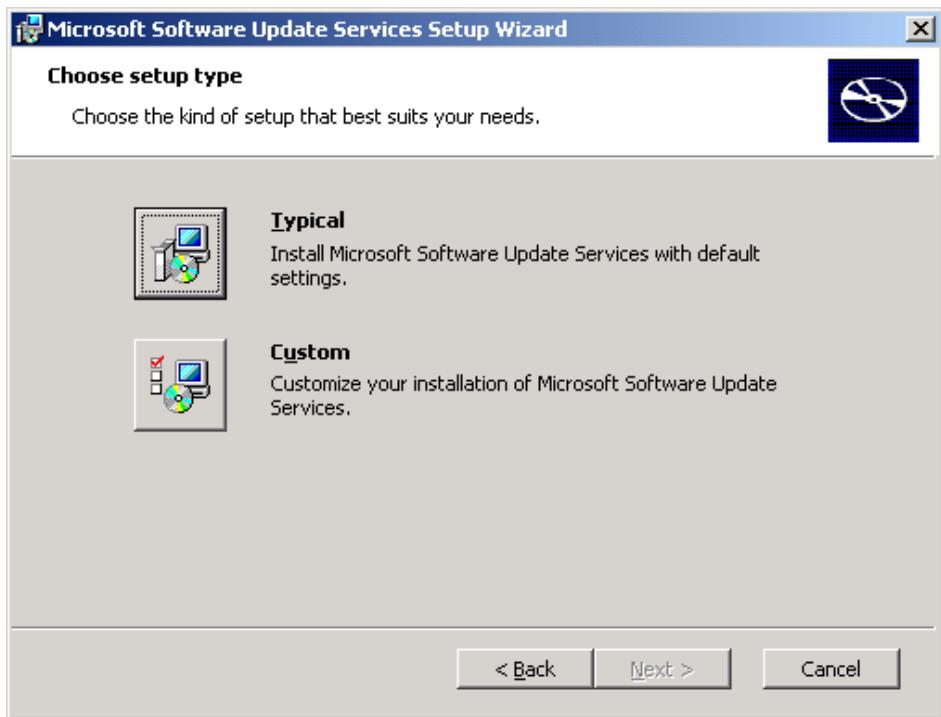


Figura 13.26 Definindo o tipo de instalação do SUS.

- Clique em Custom.
- Nesta etapa você define se o SUS deve baixar as atualizações para uma pasta local no servidor (por padrão é sugerida a pasta C:\SUS) ou se deve deixar as atualizações no site Windows Update e baixar apenas as informações sobre quais atualizações estão disponíveis. O mais usual é baixar as atualizações para o disco local do servidor. Os clientes então conectam-se com o servidor SUS da rede local e fazem a instalação a partir deste servidor. Certifique-se de que a opção Save the updates to this local folder esteja selecionada, conforme indicado na Figura 12.27.
- Clique em Next para seguir para a próxima etapa do assistente.
- Nesta etapa é que você define para qual ou quais idiomas é que devem ser baixadas as atualizações. Vou repetir o que foi colocado antes, devido a importância. A interface do SUS, por enquanto, está disponível apenas em Inglês e Japonês. Neste exemplo estou utilizando a interface em Inglês. Uma coisa é o idioma da interface de administração e outra, completamente separada é o idioma para os quais serão baixadas as atualizações. Nesta etapa é que você define para qual ou quais idiomas, o SUS irá baixar as atualizações a partir do site Windows Update. Você pode selecionar a opção English only, para baixar apenas as atualizações para o Windows em Inglês, ou você pode selecionar All available languages,

**configurar este servidor para baixar apenas as atualizações para a localidade. Por exemplo, o servidor da filial da Itália deve ser configurado para baixar apenas as atualizações para o idioma Italiano; o servidor da filial Brasileira, deve ser configurado para baixar apenas as atualizações para o idioma Português/Brasil e assim por diante. Este procedimento reduz o tráfego nos links de WAN e libera a banda disponível para outros serviços.**

**IMPORTANTE:** As atualizações que precisam, obrigatoriamente, ser aprovadas, antes de serem instaladas nos clientes, são as atualizações críticas de segurança. Pode ocorrer de ser publicada uma atualização da atualização. Ou em outras palavras, uma correção da correção. Nestas situações, você pode configurar o SUS para que ele aprove automaticamente, uma correção a uma correção que já foi aprovada previamente. Por exemplo, imagine que na segunda-feira você baixou uma correção crítica de segurança e usou o SUS para aprovar esta correção. Na sexta-feira, a equipe da Microsoft disponibiliza uma correção a esta correção baixada na segunda-feira. Você pode configurar o SUS para que baixe esta correção à correção e que a aprove, automaticamente, uma vez que ele é uma correção a uma correção já aprovada anteriormente.

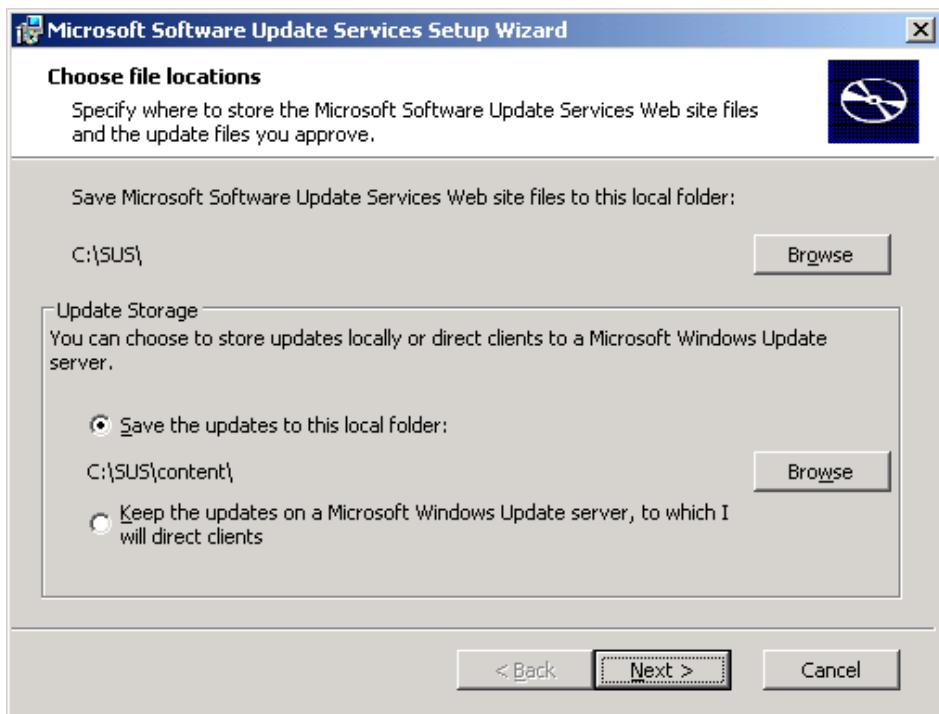


Figura 13.27 Baixando as atualizações para o servidor SUS.

**IMPORTANTE:** O SUS também pode ser instalado em um servidor com o Windows 2000 Server e com o IIS 5.0. Neste caso, durante a instalação, será executado o assistente conhecido como Lockdown Wizzard. Este assistente irá configurar o IIS para deixá-lo mais seguro, desativando serviços e portas que não sejam necessárias.

para baixar todas as atualizações disponíveis, em todos os idiomas. Conforme descrito anteriormente, esta não é uma boa opção. Você deve configurar o SUS para baixar as atualizações, somente para os idiomas que serão realmente utilizados. Por exemplo, se na rede onde o servidor SUS está sendo instalado, você tem computadores que utilizam o Windows em Inglês e outros que utilizam o Windows em Português, você deve configurar o SUS para baixar as atualizações apenas para estes dois idiomas. Para configurar quais as versões para as quais serão baixadas as atualizações, clique na opção Specific languages. O botão Choose Languages será habilitado, conforme indicado na Figura 13.28:

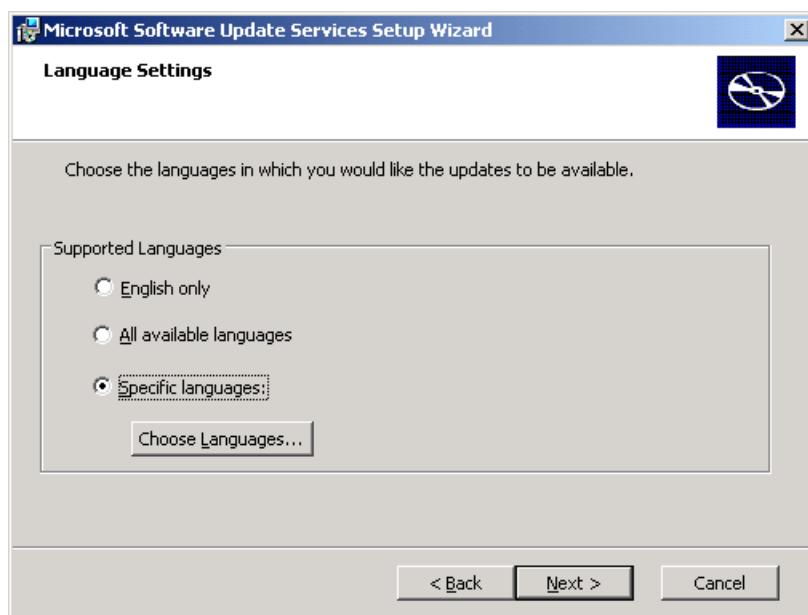


Figura 13.28 A opção Choose Languages.

11. Clique no botão Choose Languages.
12. Na janela que é exibida, deixe selecionados apenas os idiomas para os quais você deseja baixar as atualizações, conforme exemplo da Figura 13.29, onde deixei marcado apenas as opções English e Portuguese (Brazilian):

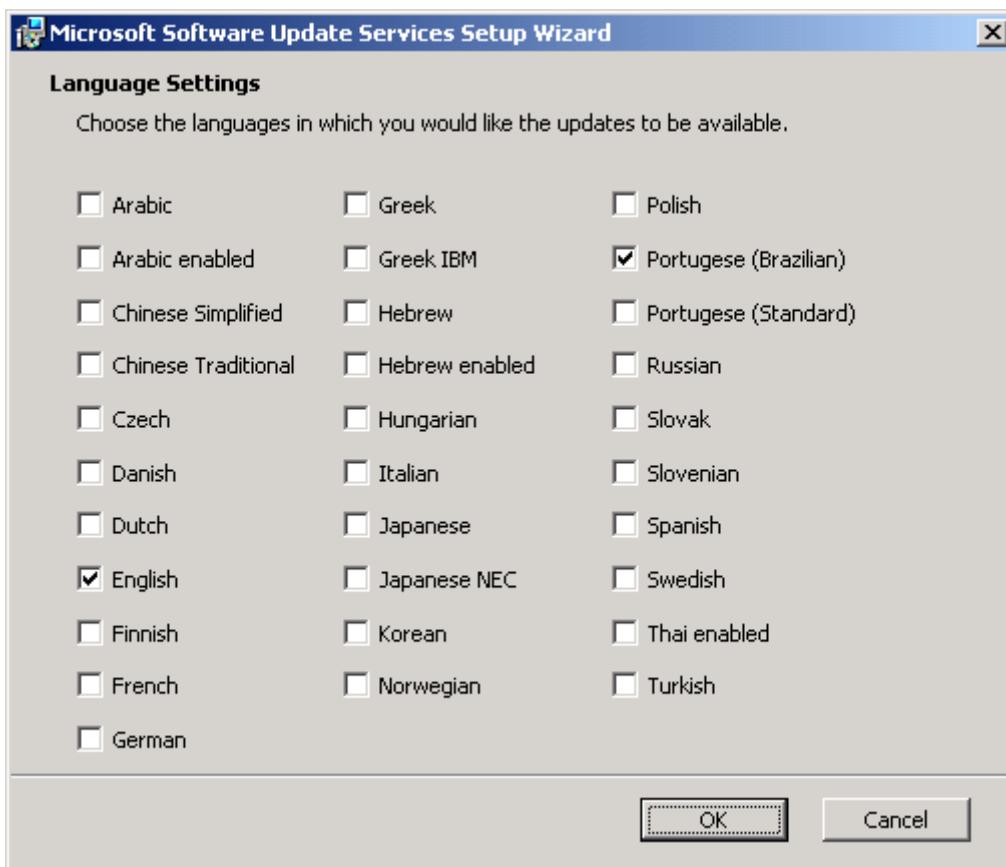
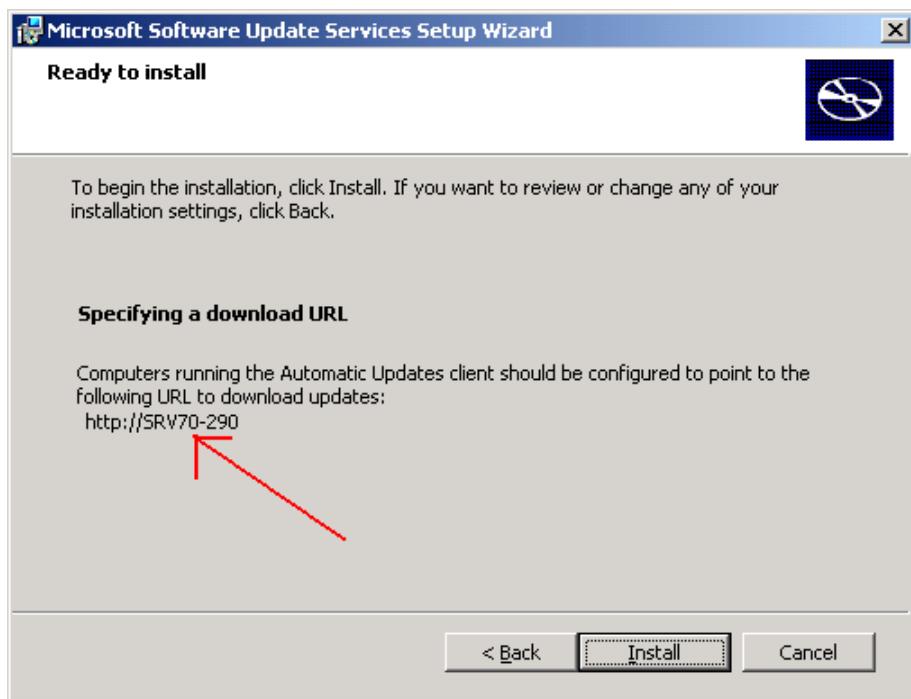


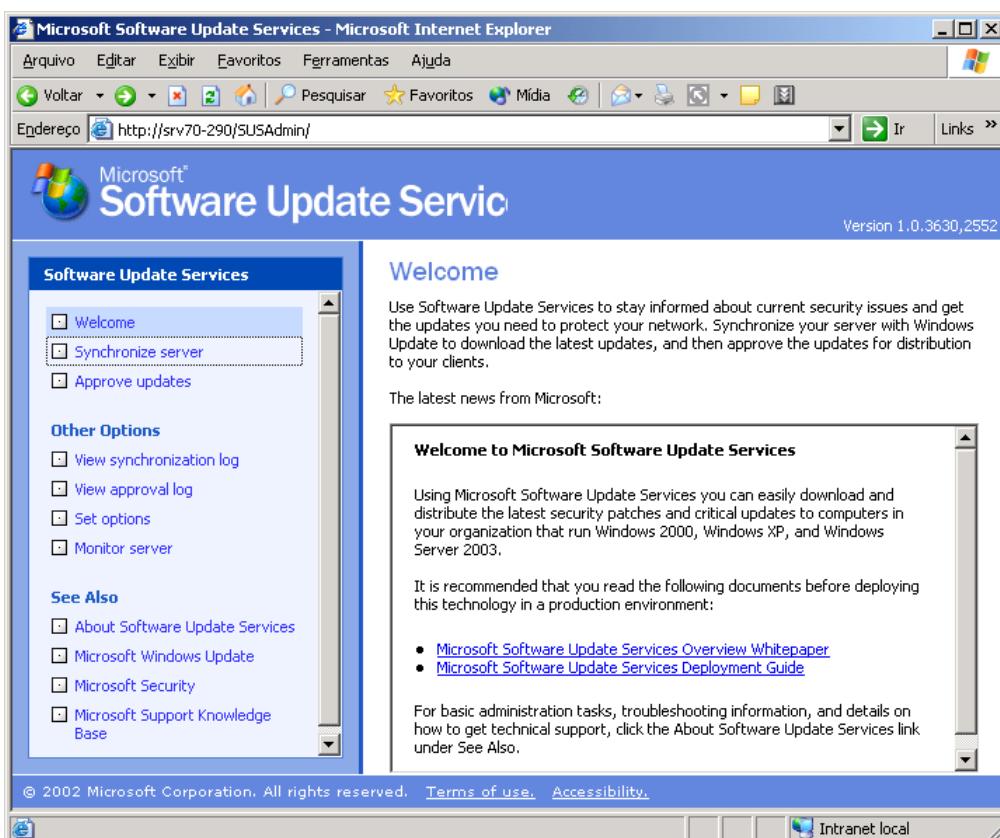
Figura 13.29 Selecionando os idiomas.

13. Após ter selecionado os idiomas clique em OK. Você estará de volta ao assistente de instalação do SUS.
14. Clique em Next para seguir para a próxima etapa do assistente.
15. Nesta etapa é que você define como deverão ser tratadas, novas versões de atualizações já previamente aprovadas. Você pode optar por aprovar automaticamente as novas versões de atualizações já previamente aprovadas (Automatically approve new versions of previously approved updates) ou pode definir que as novas versões de atualizações já previamente aprovadas, devam ser novamente aprovadas pelo Administrador (I will manually approve new versions of approved updates). Selecione a opção desejada e clique em Next para seguir para a próxima etapa do assistente.
16. Será exibida a tela final do assistente. Nesta tela tem uma informação muito importante. Nesta tela é informado o endereço que deve ser informado nos clientes (quer seja via Registry ou via GPO). Ou seja, é informada a URL com a qual os clientes devem se conectar, para baixar as atualizações disponíveis no SUS. Por padrão a URL é formada pelo nome do servidor. No exemplo da figura 13.30, estou instalando o SUS em um servidor cujo nome é SRV70-290. Com isso, a URL de conexão para os clientes é <http://SRV70-290>, conforme destacado na Figura 13.30.
17. Clique em Install para finalizar a instalação do SUS.
18. O assistente irá finalizar o processo de instalação e exibir uma mensagem informando que a instalação foi concluída com sucesso. Clique em Finish para fechar esta mensagem.



**Figura 13.30 A URL de conexão para os clientes.**

19. Após concluir a instalação, a página de administração do SUS será automaticamente carregada no Internet Explorer. Observe o endereço da página de administração, o qual é no seguinte formato: <http://nome-do-servidor/SUSAdmin>. No nosso exemplo, onde o SUS foi instalado no servidor SRV70-290, a página de administração do SUS é acessada no seguinte endereço: <http://srv70-290/SUSAdmin>, conforme indicado na Figura 13.31:



**Figura 13.31 O site de administração do SUS.**

20. Mantenha esta página aberta, pois iremos utilizá-la nos próximos tópicos.

Muito bem, o SUS foi instalado e está pronto para ser configurado e utilizado. Agora temos mais duas etapas a vencer:

- ◆ Aprender a administrar o SUS.
- ◆ Configurar os clientes para utilizar o SUS.

Estes são justamente os assuntos dos próximos tópicos.

## Administrando o SUS

Neste tópico, você acompanhará um exemplo prático, onde mostrarei as principais opções de configuração do SUS.

Exemplo: Para administrar o SUS, siga os passos indicados a seguir:

1. Faça o logon com uma conta com permissão de Administrador.
2. Abra o Internet Explorer e acesse o seguinte endereço, substituindo SRV70-290 pelo nome do servidor onde o SUS está instalado:  
**http://srv70-290/SUSAdmin**
3. Será aberta a página de administração do SUS. No painel da esquerda estão disponíveis links para as diversas categorias de opções de configuração, disponíveis no SUS. Na página inicial estão disponíveis links para um White Paper sobre o SUS e para um guia de implementação do SUS. Dê um conferida nestes documentos, vale realmente a pena.
4. No painel da esquerda, clique em Synchronize Server. Será carregada uma página, onde você tem duas opções, conforme indicado na Figura 13.32:

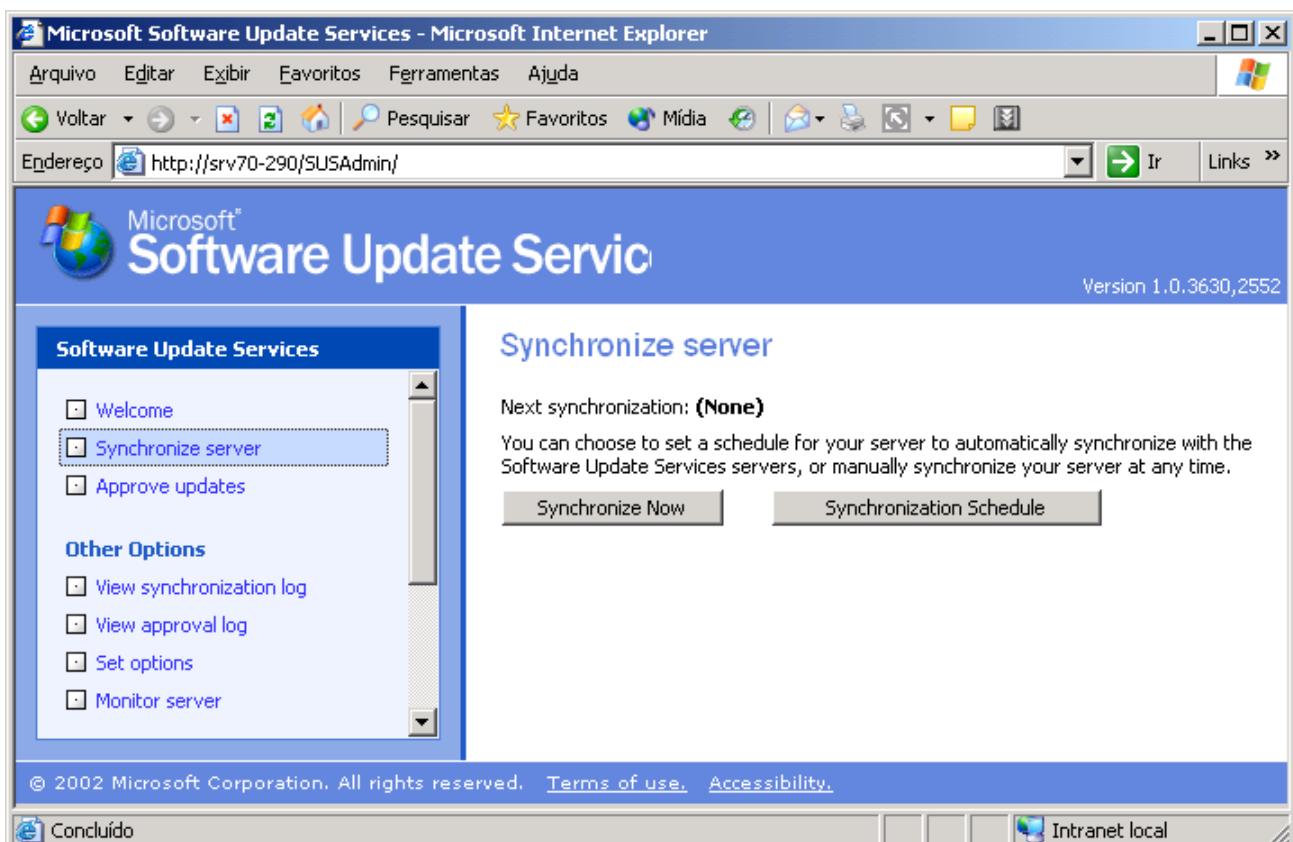


Figura 13.32 Opções de sincronização do SUS.

Você utiliza a opção Synchronize Now, para fazer com que o SUS se conecte imediatamente com o site do Windows Update e baixe as atualizações disponíveis. A opção Synchronization Schedule, é utilizada para criar um agendamento de sincronização. Ou seja, você define dias e horários em que o SUS irá se conectar com o site Windows Update e baixar as atualizações disponíveis. Ao clicar em Synchronization Schedule, será exibida a janela Indicada na Figura 13.33, na qual você pode definir um agendamento para o SUS. No exemplo da Figura 13:33 foi definida uma sincronização diária, as 00:00 hs.

5. Clique em Synchronize Now,
6. O SUS irá se conectar com o site Windows Update e baixar as atualizações disponíveis. A medida que vai baixando as atualizações, o SUS exibe uma barra indicando o percentual do processo que já foi concluído.

Ao finalizar a sincronização (a primeira sincronização pode demorar um bom tempo, uma vez que um grande número de atualizações será copiado a partir do site Windows Update), será exibida uma mensagem informando que o servidor foi sincronizado com sucesso e que agora você pode selecionar a aprovar as atualizações que foram baixadas. Esta mensagem está indicada na Figura 13.33:



Figura 13.33 Sincronização efetuada com sucesso.

7. Clique em OK para fechar esta mensagem.
8. A opção Aprove updates será automaticamente selecionada, no painel da esquerda. No painel da direita será exibida a lista de atualizações aguardando aprovação. Lembre-se de que as atualizações críticas não serão aplicadas aos clientes, até que não tenham sido aprovadas pelo administrador do SUS.
9. Para aprovar uma atualização, basta marcá-la e clicar em Approve, conforme indicado na Figura 13.35, onde duas atualizações foram marcadas para aprovação.
10. Selecione as atualizações a serem aprovadas e clique no botão Approve. Surge uma mensagem informando que você está aprovando uma nova lista de atualizações as quais estarão disponíveis para os clientes e que esta nova lista substituirá qualquer lista existente previamente. Clique em Sim para criar a nova lista de atualizações aprovadas e prontas para serem instaladas nos clientes.
11. Se alguma das atualizações exigir que você concorde com um Termo de serviços, será exibida uma mensagem solicitando que você aceite o termo de serviços. Clique em Accept para aceitar e aprovar a atualização. Ao final será exibida uma mensagem informando que uma nova lista foi criada. Clique em OK para fechar esta mensagem.
12. As atualizações já aparecem com o status de aprovado (Approved), conforme indicado na figura 13.34.

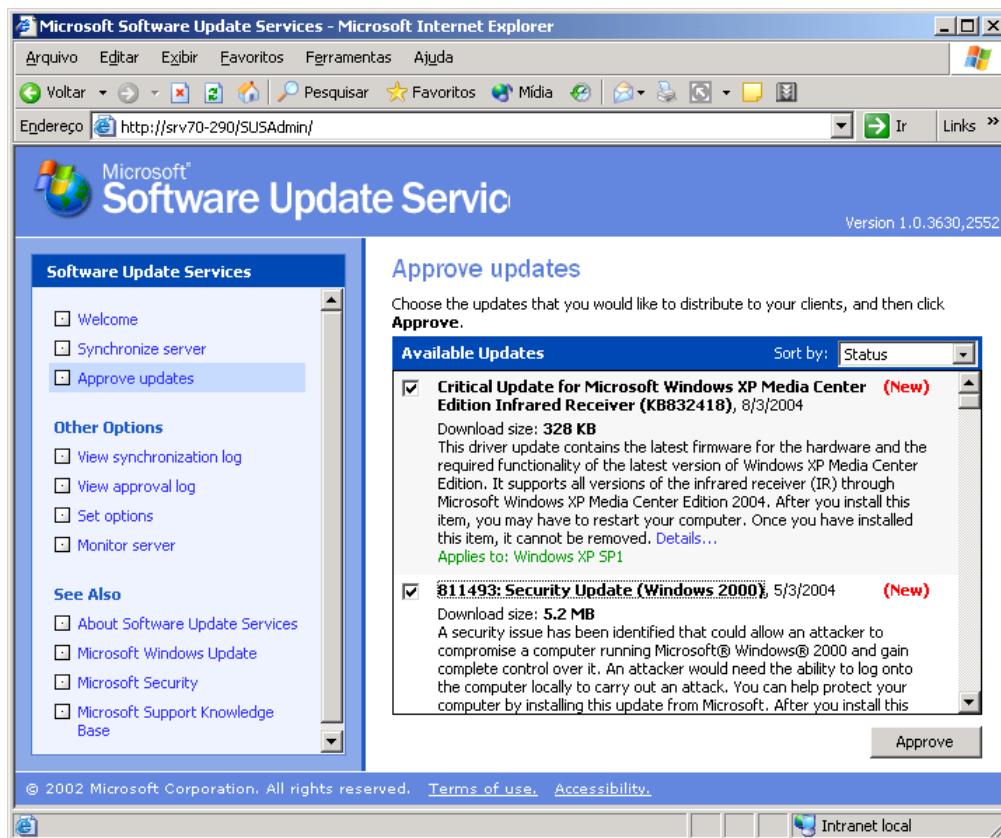


Figura 13.34 Aprovando atualizações críticas de segurança.

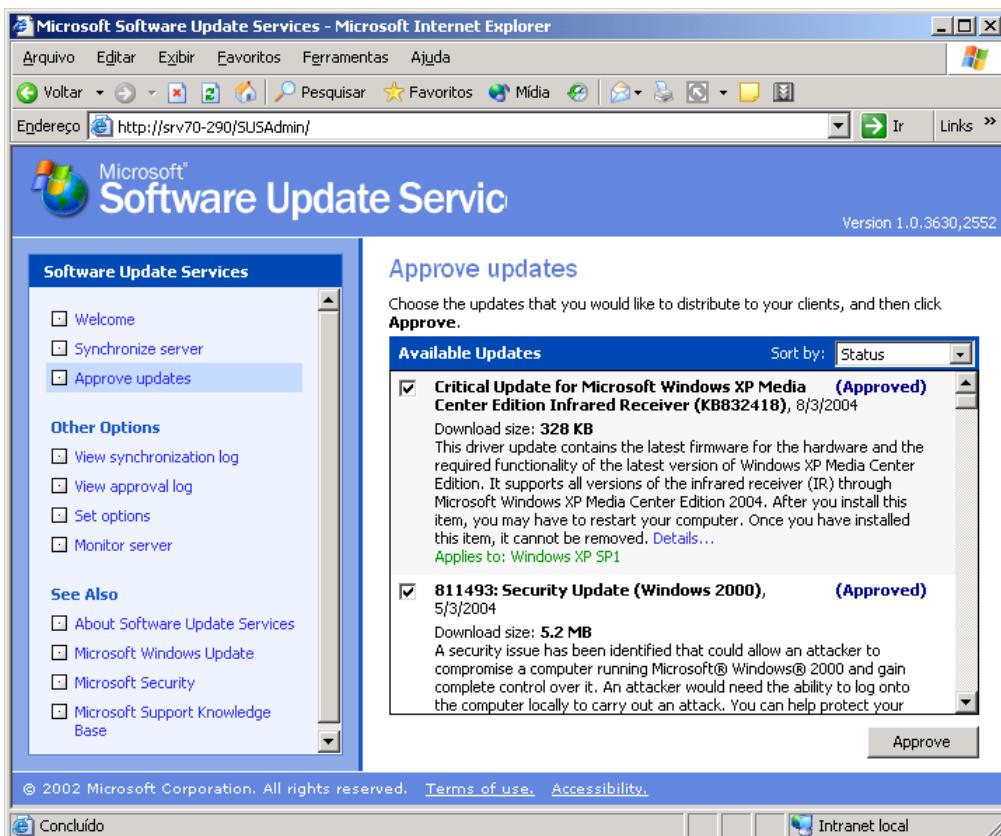


Figura 13.35 Atualizações já aprovadas.

13. No painel da esquerda, clique na opção View synchronization log. No painel da direita será exibido o log de eventos de sincronização do servidor SUS. Na listagem a seguir, apresento a parte inicial deste log:

\*\*\*\*\*

Manual Sync Started- segunda-feira, 22 de março de 2004 22:11:27 Successful

Updates Added:

Security Update, July 19, 2000 - q261255\_0F334C94167F1C095608F7B0599891EA83B56A0A.exe

Security Update, July 19, 2000 - q261255\_CECBAD4A43916313EC45E5DB5E7A8461E1A01E5F.exe

Q328676: Security Update (Outlook Express 5.5 SP2) -  
q328389\_3016A5C05107C80B472F83955BDD424027D051C3.exe

Q328676: Security Update (Outlook Express 5.5 SP2) -  
q328389\_825151815CDA30A1AF0B652FA17A10437C73CF82.exe

Security Update, February 14, 2002 (Internet Explorer 5.01) -  
VBS51NEN\_6679B4E5AD916D6462A3AB5B4C2B81C2867CA1E6.EXE

Security Update, February 14, 2002 (Internet Explorer 5.01) -  
VBS51NEN\_EA35DB61E858F2175BCF7DEDF0304C6DB48D8763.EXE

October 2003, Cumulative Patch for Internet Explorer 5.01 for Windows 2000 Service Pack 4  
(KB828750) - q828750\_2d9563d8fbe81b44f9c1ee21e858952.exe

.....

\*\*\*\*\*

14. No painel da esquerda, clique na opção View approval log. No painel da direita será exibido o log de eventos relacionados a aprovação de atualizações no servidor SUS. Na listagem a seguir, apresento a parte inicial deste log:

\*\*\*\*\*

Approved List Modified-terça-feira, 23 de março de 2004 19:40:02 Successful

Approved By: ABC\Administrador

List of Approved Updates:

811493: Security Update (Windows 2000)

Critical Update for Microsoft Windows XP Media Center Edition Infrared Receiver  
(KB832418)

List of UnApproved Updates:

Security Update for Microsoft Windows XP (KB328940)

329170: Security Update (Windows 2000)

329170: Security Update

October 2003, Cumulative Patch for Internet Explorer 5.5 Service Pack 2 (KB828750) -  
q828750\_f45f5a468a9cd3933305594418529bd.exe

October 2003, Cumulative Patch for Internet Explorer 5.5 Service Pack 2 (KB828750) -  
q828750\_e79d902ddfeaa3eee5913e2580f4dee.exe

Cumulative Security Update for Internet Explorer 5.5 SP2 (KB824145) -  
q824145\_81926bcee2daa2c6185379a6722bb05.exe

Cumulative Security Update for Internet Explorer 5.5 SP2 (KB824145) -  
q824145\_0e72e43b82edd2cdc3eb0dd92fd0273.exe

.....

\*\*\*\*\*

15. No painel da esquerda, clique em Set options. Esta opção nos dá acesso a uma série de configurações do servidor SUS. Nesta opção você pode definir se o servidor SUS se conecta diretamente à Internet ou através de um servidor Proxy, você define o nome que deve ser utilizado pelos clientes para se conectar com o servidor SUS, define se o servidor SUS irá baixar as atualizações diretamente do site Windows Update ou a partir de outro servidor SUS da empresa. Por exemplo, você pode ter um servidor SUS na matriz, sincronizando diretamente com o site Windows Update e configurar os servidores SUS das filiais, para sincronizar a partir do servidor SUS da matriz. Com isso as atualizações são baixadas uma única vez pela Internet, a partir do site Windows Update para o servidor SUS da matriz. Do servidor SUS da matriz, as atualizações são transferidas para os servidores SUS das filiais. Com isso você pode montar uma hierarquia de servidores SUS, com dois ou mais níveis. Outra opção importante que você pode definir nesta página é se as novas versões de atualizações já aprovadas serão automaticamente aprovadas ou se deverão ser aprovadas novamente. Por último você também pode definir um ou mais idiomas/localidades, para os quais serão baixadas atualizações.
16. Defina as configurações desejadas e clique no botão Apply para aplicar as alterações.
17. Muito bem, sobre as opções de administração do SUS é isso. Feche a página de administração do SUS.

## Configurar os clientes para utilizar o SUS.

Muito bem, já aprendemos a fazer o download e a instalar o SUS. A próxima etapa é aprender a configurar os clientes da rede, para que estes passem a baixar as atualizações a partir do servidor SUS. Para que os clientes possam utilizar o SUS eles devem ter o Cliente de Atualizações Automáticas (Automatic Updates Client) instalado. O Cliente de Atualizações Automáticas faz parte do Windows 2000, Windows Server 2003 ou Windows XP e é instalado, automaticamente, a primeira vez que você utilizar o Windows Update.

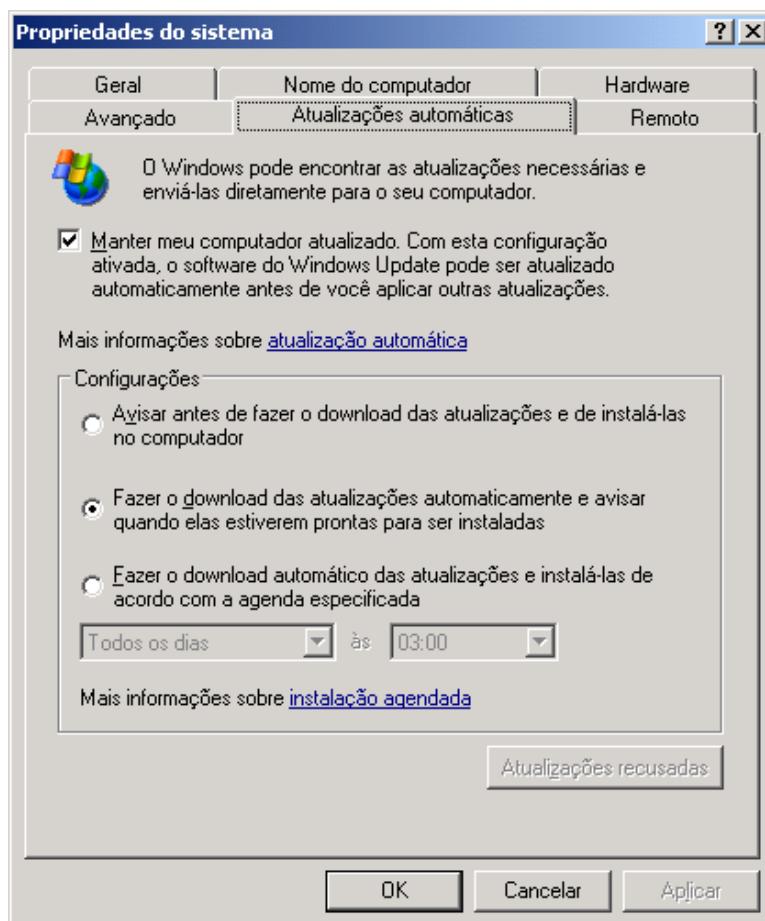


Figura 13.36 A guia Atualizações automáticas.

A configuração do cliente de atualizações automáticas é feita através da guia Atualizações automáticas, da janela de propriedades do Sistema (clique com o botão direito do mouse em Meu computador e, no menu que é exibido, clique em Propriedades). A janela Atualizações automáticas está indicada na Figura 13.36.

A seguir descrevo as opções disponíveis nesta guia:

- ◆ **Manter o meu computador atualizado:** Com esta configuração ativa, o software Windows Update pode ser atualizado automaticamente antes de você aplicar outras atualizações. É recomendado que você mantenha esta opção sempre marcada.
- ◆ **Avisar antes de fazer o download das atualizações e de instalá-las no computador:** Ao marcar esta opção, o Windows irá avisá-lo antes de fazer o download de qualquer atualização. O Windows irá avisá-lo novamente quando as atualizações estiverem prontas para serem instaladas.
- ◆ **Fazer o download das atualizações automaticamente e avisar quando elas estiverem prontas para serem instaladas:** Esta opção faz com que o Windows faça o download automaticamente das atualizações disponíveis. Após ter concluído o download, o Windows aviso o usuário para que este possa iniciar a instalação das atualizações que foram baixadas. Esta é a opção recomendada se você quer automatizar o processo de download, mas quer que o Windows notifique você antes de instalar as atualizações, dando a você a opção de instalá-las ou não.
- ◆ **Fazer o download automático das atualizações e instalá-las de acordo com a agenda especificada:** Esta opção permite que você defina um agendamento para a instalação das atualizações. O Winodwos fará o download automático das atualizações e irá isntalá-las de acordo com o agendamento configurado.

Após ter definido as configurações desejadas, clique em OK para aplicá-las. Muito bem, a guia Atualizações automáticas, apenas define de que maneira as atualizações serão baixadas e aplicadas. A questão agora é como fazer com que o cliente de atualizações automáticas baixe as atualizações a partir do servidor SUS e não diretamente do site Windows Update. Muito bem, existem duas maneiras de fazer isso: via GPO ou via Registry das estações de trabalho. A seguir mostro estas duas maneiras para configurar os clientes para utilizar o servidor SUS.

### Configurando os clientes via GPO:

Você pode utilizar o recurso de GPOs, descrito no Capítulo 9, para configurar os clientes para que utilizem o servidor SUS, ao invés de se conectar com o site Windows Update. Você deve acessar o seguinte grupo de GPOs: Configurações do computador -> Modelos administrativos -> Componentes do Windows – Windows Update, conforme ilustrado na figura 13.37.

Neste grupo estão disponíveis as seguintes polices:

- ◆ **Configurar atualizações automáticas:** Ao abrir esta police, serão exibidas as opções indicadas na Figura 13.38.

A police Configurar atualizações automáticas especifica se o computador irá receber atualizações de segurança e outros downloads importantes através do serviço de atualização automática do Windows.

Essa configuração permite especificar a ativação das atualizações automáticas no computador. Ao marcar a opção Ativado, você deve selecionar uma das opções a seguir, na lista Configurar atualização automática (observe que estas são exatamente as opções disponíveis na guia Atualizações automáticas):

**NOTA:** Se por algum motivo o cliente SUS não estiver instalado, você pode fazer o download a partir do seguinte endereço: <http://www.microsoft.com/windows2000/downloads/recommended/susclient/default.asp>

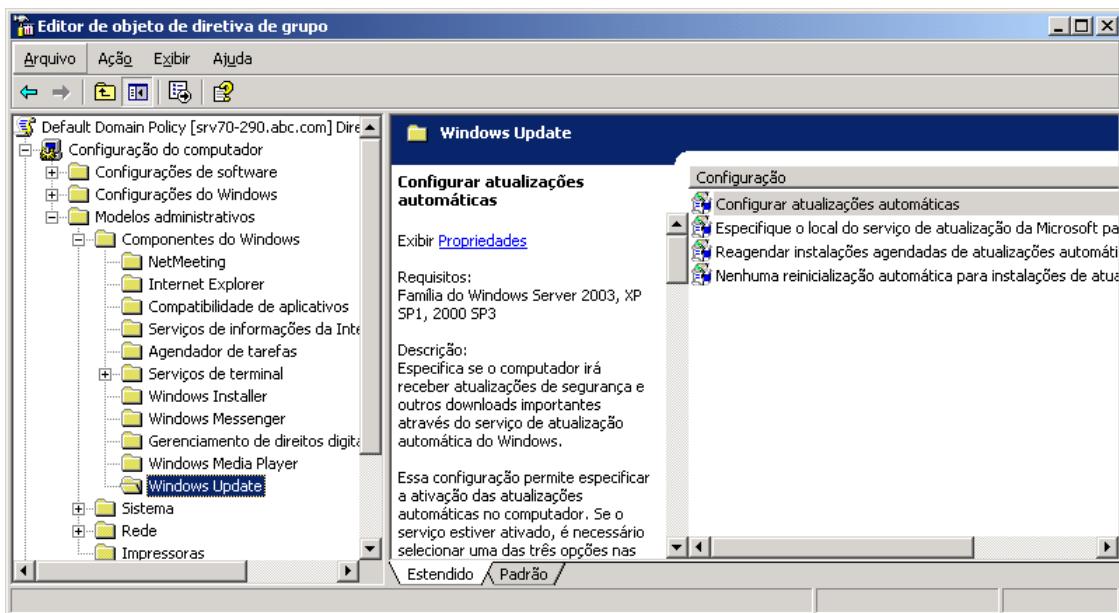


Figura 13.37 Opções de GPO relacionadas ao SUS.

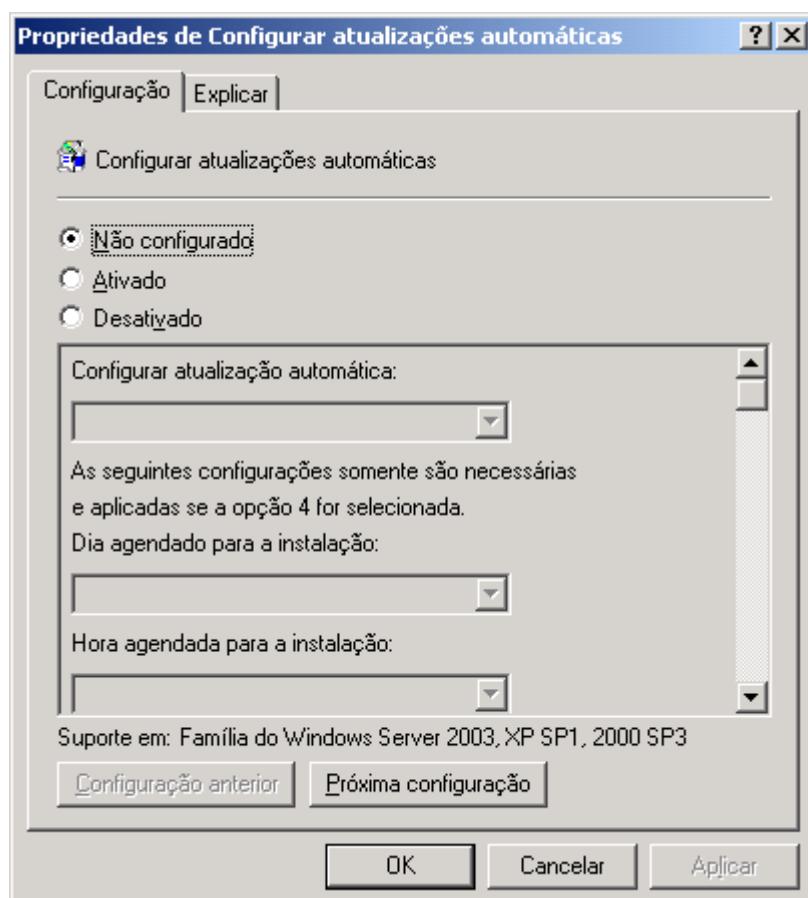


Figura 13.38 A police Configurar atualizações automáticas.

**2 - Avisar antes de fazer o download das atualizações e de instalá-las no computador:** Quando o Windows encontra atualizações que se aplicam ao computador, ele exibe um ícone na área de status com uma mensagem para fazer o download das atualizações. Clique no ícone ou na mensagem a fim de selecionar as atualizações cujo download você deseja fazer. Em seguida, o Windows fará o download das atualizações selecionadas em segundo plano. Quando o download estiver concluído, o ícone aparecerá novamente na área de status, avisando que as atualizações já estão disponíveis para serem instaladas. Clique no ícone ou na mensagem para selecionar as atualizações que deseja instalar.

**3 - (Configuração padrão) Fazer o download das atualizações automaticamente e avisar quando elas estiverem prontas para serem instaladas:** Com esta opção o Windows encontra atualizações que se aplicam ao computador e faz o download delas em segundo plano (o usuário não é avisado ou interrompido durante esse processo). Quando o download estiver concluído, o ícone aparecerá na área de status, avisando que as atualizações estão prontas para serem instaladas. Clique no ícone ou na mensagem para selecionar quais atualizações deseja instalar.

**4 - Fazer o download automático das atualizações e instalá-las no agendamento especificado abaixo:** Ao selecionar esta opção, você pode especificar o agendamento usando as demais opções disponíveis nesta diretiva. Se nenhum agendamento for especificado, o agendamento padrão para todas as instalações será todo dia às 15 horas. Se for necessário reiniciar o computador para concluir a instalação, o Windows irá reiniciá-lo automaticamente. (Se um usuário fizer logon no computador quando o Windows estiver pronto para reiniciar, o usuário será notificado e será fornecida a opção para reiniciar depois.)

Para usar essa configuração, clique em Ativado e selecione uma das opções (2, 3, ou 4). Caso tenha selecionado a opção 4, é possível configurar um agendamento recorrente (se não houver agendamento especificado, todas as instalações irão ocorrer todo dia às 15 horas).

Se o status estiver configurado como ‘Ativado’, o Windows reconhecerá quando o computador estiver on-line e usará sua conexão com a Internet para procurar por atualizações que se apliquem ao computador no site Windows Update.

Se o status estiver configurado como ‘Desativado’, deverão ser feitos o download e a instalação manual de qualquer atualização que esteja disponível no site Windows Update em <http://windowsupdate.microsoft.com>.

Se o status estiver definido como ‘Não configurado’, o uso das atualizações automáticas não será especificado pelo nível da diretiva de grupo. Porém, um administrador ainda pode configurar as atualizações automáticas através da guia Atualizações Automáticas, descrita anteriormente.

- ◆ **Especifique o local do serviço de atualização da Microsoft para a intranet:** Ao abrir esta police, serão exibidas as opções indicadas na Figura 13.39.

Esta é a police utilizada para especificar o servidor SUS que será utilizado pelos clientes. Ou seja, é nesta police que você informa o nome do servidor SUS a partir do qual os clientes irão copiar as atualizações disponíveis.

Essa configuração permite especificar um servidor na rede para funcionar como um serviço de atualização interno – servidor SUS. O cliente das atualizações automáticas procurará no serviço atualizações que se apliquem aos computadores da rede.

Para usar essa configuração, é necessário configurar dois valores de nome de servidor: o servidor a partir do qual o cliente das atualizações automáticas detecta e faz o download das atualizações, e o servidor para o qual as estações de trabalho atualizadas carregam as estatísticas. É possível configurar os dois valores para o mesmo servidor.

Se o status desta police estiver configurado como ‘Ativado’, o cliente das atualizações automáticas se conecta ao servidor SUS ao invés de se conectar com o site Windows Update, para procurar e fazer o download de atualizações. Ativar essa configuração significa que os usuários finais na organização não precisam atravessar um firewall para obter atualizações, assim como permite testar atualizações antes de implantá-las.

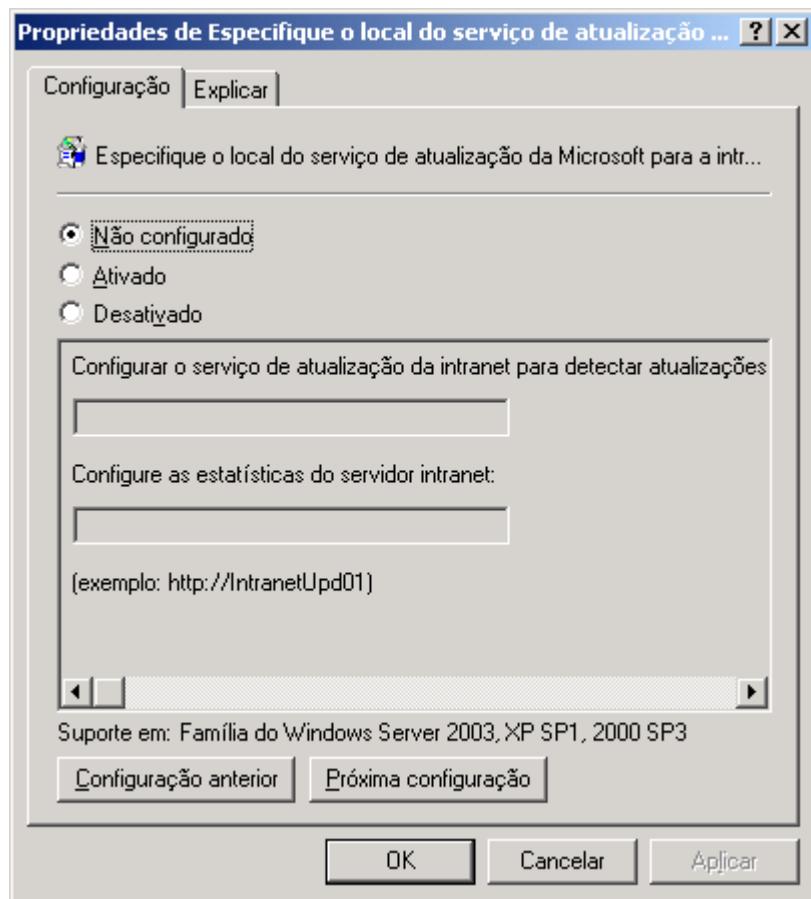


Figura 13.39 A police Especifique o local do serviço de atualização da Microsoft para a intranet.

Se o status estiver configurado como ‘Desativado’ ou ‘Não configurado’, e se as atualizações automáticas não forem desativadas pelas diretrivas ou preferências do usuário, o cliente das atualizações automáticas irá se conectar diretamente ao site Windows Update na Internet.

- ◆ **Reagendar instalações agendadas de atualizações automáticas:** Ao abrir esta police, serão exibidas as opções indicadas na Figura 13.40.

**IMPORTANTE: Se a diretiva “Configurar atualizações automáticas” estiver desativada, essa diretiva não terá efeito.**

Esta police é utilizada para especificar por quanto tempo as atualizações automáticas devem esperar, após a inicialização do sistema, para proceder com uma instalação agendada que tenha sido perdida anteriormente, isto é, que não tenha sido feita no horário agendado anteriormente.

Se o status estiver definido como Ativado, uma instalação agendada que não ocorreu anteriormente irá ocorrer após o número especificado de minutos nesta police, depois da inicialização do computador.

Se o status estiver definido como Desativado ou Não configurado, uma instalação agendada perdida irá ocorrer na próxima instalação agendada.

- ◆ **Nenhuma reinicialização automática para instalações de atualizações automáticas agendadas:** Ao abrir esta police, serão exibidas as opções indicadas na Figura 13.41.

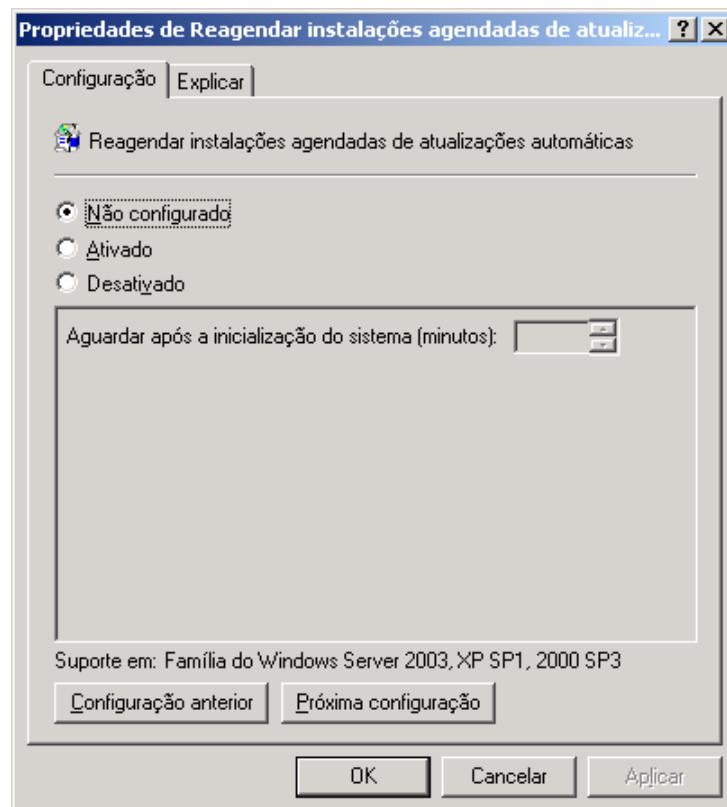


Figura 13.40 A police Reagendar instalações agendadas de atualizações automáticas.

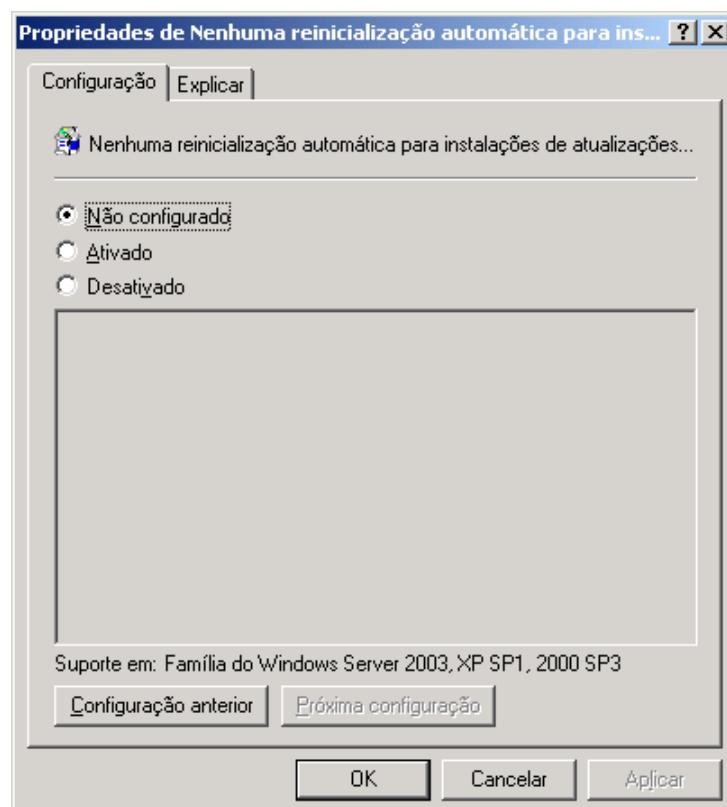


Figura 13.41 A police Nenhuma reinicialização automática para instalações de atualizações automáticas agendadas.

Esta police é utilizada para definir que, para a conclusão de uma instalação agendada, as atualizações automáticas aguardarão até que o computador seja reiniciado por qualquer usuário que tenha feito logon, em vez de fazer com que o computador seja reiniciado automaticamente.

Se o status for definido como ‘Ativado’, as atualizações automáticas não reiniciarão um computador automaticamente durante uma instalação agendada se um usuário tiver feito logon no computador. Em vez disso, as atualizações automáticas notificarão o usuário de que é necessário reiniciar o computador para concluir a instalação.

Se esta police for configurada como Desativado ou Não configurado, o cliente de atualizações automáticas irá notificar o usuário que o computador irá reiniciar, automaticamente, em cinco minutos, para que as atualizações recém instaladas possam ser aplicadas.

### Opções da Registry relacionadas com o SUS:

Existem, basicamente, duas chaves da registry relacionadas com o SUS. Estas chaves são úteis em uma situação onde o cliente de atualizações passa a não receber as atualizações, embora elas estejam disponíveis no SUS. Nestas situações, você deve acessar o seguinte caminho da Registry: HKEY\_LOCAL\_MACHINE\Software\Polices\Microsoft\Windows\WindowsUpdate e verificar o valor das chaves descritas a seguir:

- ◆ WUServer: Esta chave deve conter a URL que aponta para o servidor SUS, como por exemplo: <http://SRV70-290>
- ◆ WUStatusServer: Esta chave deve conter a URL do mesmo servidor SUS indicado na chave WUServer ou a URL de um servidor IIS, o qual é utilizado para gravação das estatísticas de sincronização.
- ◆ SubChave UseWUServer: Esta subchave deve sempre estar configurada com o valor: 00000001.

É isso.

## Conclusão

Neste capítulo você aprendeu a instalar e a fazer configurações básicas do IIS 6.0, que é o servidor Web da Microsoft. Você aprendeu a instalar o IIS, a criar pastas virtuais e a configurar os sites Web e de FTP do servidor IIS.

Você também aprendeu sobre uma das novidades do Windows Server 2003: Software Update Services –SUS.

O SUS – Software Update Services é um serviço utilizado para automatizar o processo de download e instalação das correções do Windows, a partir do site Windows Update. No Windows Server 2003, em Português, este serviço é denominado de Serviço de Atualizações Automáticas. Já há alguns anos, que a Microsoft disponibiliza o site Windows Update, através do qual você pode baixar e instalar atualizações e correções de segurança para as diferentes versões do Windows. Porém o usuário deve tomar a iniciativa de usar o comando Windows Update, para conectar o seu computador com o site do Windows Update, para fazer a instalação das últimas correções disponíveis. O SUS leva este processo

---

**IMPORTANTE:** Esta diretiva se aplica somente quando as atualizações automáticas estão configuradas para executar instalações agendadas de atualizações. Se a diretiva “Configurar atualizações automáticas” estiver desativada, esta diretiva não tem efeito algum.

---

**IMPORTANTE:** Com esta police ativada, o cliente de atualizações automáticas, não conseguirá detectar novas atualizações até que o computador tenha sido reinicializado.

---

**IMPORTANTE:** Esta police somente se aplica quando o cliente de atualizações automáticas estiver configurado para fazer atualizações agendadas. Se a police Configurar atualizações automáticas estiver desabilitadas, esta police não terá efeito prático.

---

um nível a frente. Você estala o SUS em um servidor da rede e pode configurar este servidor para baixar, automaticamente, as atualizações a partir do site Windows Update. Depois de baixadas para o servidor, estas atualizações poderão ser aplicadas, automaticamente, em todos os demais computadores da rede. Este processo tem inúmeras vantagens, as quais serão descritas neste capítulo.

O SUS é instalado como um site/aplicativo Web, baseado no IIS. O SUS é uma aplicação Cliente/Servidor. Você instala o SUS em um servidor baseado no IIS. No servidor você configura um agendamento para o download automático das atualizações, aprova as atualizações críticas de segurança e faz uma série de outras configurações. Nos clientes, você instala o software client do SUS, o qual se comunica com o servidor e baixa e instala, automaticamente, as atualizações disponíveis no servidor.

# Introdução

Neste capítulo eu apresento um resumo na forma de rápidos lembretes, sobre os principais pontos que você deve lembrar para o Exame 70-290. O objetivo é lembrar o amigo leitor sobre os pontos mais importantes, aqueles pontos que tem maior probabilidade de serem cobrados no exame. Em caso de dúvidas sobre um ou mais pontos citados, você deve voltar ao respectivo capítulo e revisar o conteúdo com mais detalhes. Não fique limitado ao conteúdo apresentado neste livro. Em caso de dúvidas, consulte a Ajuda do Windows Server 2003, a qual está bem completa, detalhada e organizada.

Este capítulo é indicado para uma leitura após você ter detalhadamente estudado os capítulos anteriores, para que você possa identificar quais pontos precisam de uma revisão final mais detalhada e de mais estudo. Eu recomendo também que você faça uma segunda leitura do livro e volte novamente a este resumo. Uma terceira leitura deste resumo é recomendada como um revisão final (juntamente com o simulado do próximo capítulo) para ser feita um ou dois dias antes do exame.

Para facilitar o acompanhamento, dividirei o resumo por assuntos, tais como Instalação, Active Directory, GPO, Administração de usuários, Administração de grupos, permissões de segurança, administração de impressoras e assim por diante. Tem alguns pontos que são de fundamental importância e devem ser revisados seguidamente, até que você tenha um entendimento completo e definitivo sobre o assunto em questão. Por exemplo, não tem como “encarar” este exame sem dominar, com firmeza, tópicos tais como os fundamentos sobre Active Directory, Backup e Restore, SUS, Administração de usuários e grupos, administração de discos e volumes e assim por diante.

Além do material contido neste manual, vou listar uma série de fontes de estudo da Internet, as quais podem ajudá-lo bastante para obter a aprovação neste exame. Não é meu objetivo “assustar” o candidato, mas é minha obrigação avisar que Exame 70-290 apresenta um nível de dificuldade um pouco maior do que os exames do MCSE-2000, tais como o 70-210 e 70-215. Por isso é preciso dedicação, estudo, experimentação. Eu recomendo que o candidato somente marque o exame quando estiver realmente convicto de que entendeu e domina os conceitos apresentados neste livro, juntamente com uma boa complementação nos endereços indicados neste capítulo. O exame 70-290 exige um bom entendimento sobre a administração dos principais recursos de uma rede baseada no Windows Server 2003 e no Active Directory.

Muito bem, vamos a apresentação do resumo para o exame e das dicas para mais sites com materiais de estudo e referência.

## Resumo para o exame 70-290.

A seguir apresento um resumo, no formato de citação dos tópicos principais, para o Exame 70-290. Os fatos serão apresentados, divididos por assunto, para facilitar a identificação das áreas onde o amigo leitor ainda possa estar com mais dúvidas e necessita dedicar um pouco mais de tempo.

CAPÍTULO

14

Resumo Final – O que você  
não pode esquecer para o  
Exame

# Redes Baseadas no Windows 2003 Server

O primeiro ponto que tem que ficar bem claro para candidato é o papel do Windows Server 2003 dentro da família Windows, onde estão disponíveis diferentes versões do Windows.

## Uma breve história “dos Windows”

Observe bem o título deste item – “dos Windows”. Não é um erro de português que o autor cometeu e que a equipe de revisão deixou passar. Com o termo “dos Windows” estou fazendo referência as inúmeras versões do Windows que foram lançadas na última década.

Vou apresentar um histórico destas versões, de tal maneira que fique claro onde o Windows Server 2003 se encaixa nesta história. Vou iniciar apresentando o histórico das versões do Windows utilizadas em estações de trabalho e nos computadores pessoais residenciais. Uma história que teve início com o nosso bom e velho MS-DOS.

## Os “Windows” para estações de trabalho e computadores de uso residencial:

Neste tópico vou mostrar a evolução que teve início com o MS-DOS e tem como seu mais novo representante o Windows XP (Home ou Professional). Uma nova versão do Windows, para estações de trabalho, já está sendo desenvolvida. Por enquanto ela tem o codinome de Longhorn e deverá ser lançada, provavelmente, em 2005. Considere o diagrama da Figura 14.1:

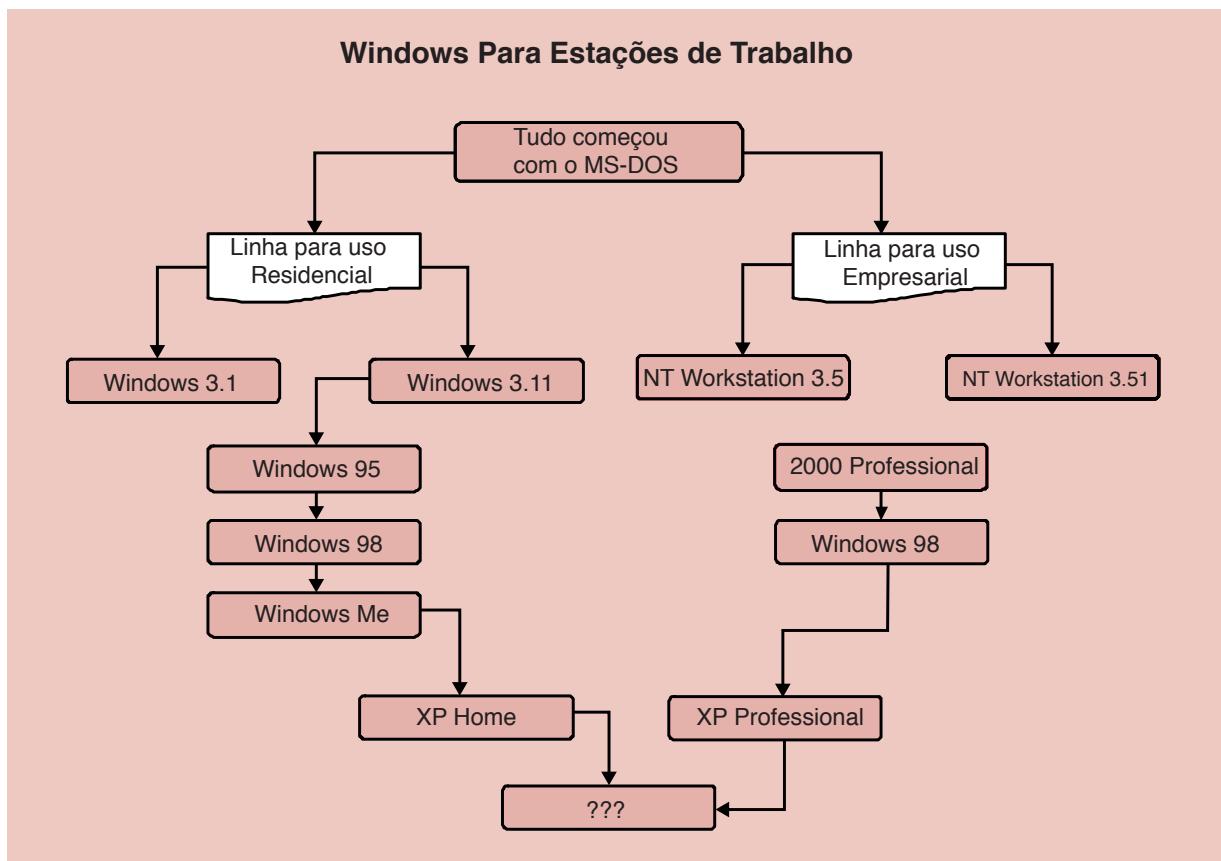


Figura 14.1 A Família Windows para estações de trabalho.

Farei alguns comentários sobre o diagrama da Figura 14.1.

O início de tudo foi o MS-DOS. Sem nenhuma dúvida, independentemente das qualidades/méritos do produto, foi o produto que transformou a Microsoft de uma empresa de garagem em uma empresa rumo a tornar-se a gigante dos dias atuais. Muita gente, inclusive este que escreve este texto, tem saudade de algumas das características do bom e velho MS-DOS. Para instalar programas, uma simplicidade: bastava copiar o diretório do programa de uma máquina para a outra e pronto. Uma interface a caractere, porém bastante rápida. Claro que “gastávamos” o teclado digitando comandos e mais comandos: dir, type, copy, etc.

Como sucessor do MS-DOS, porém ainda dependente do MS-DOS, surge o Windows. As versões iniciais do Windows pouco foram utilizadas no Brasil. Embora você possa não acreditar (ou não possa imaginar como era), existiu um Windows 1.0, um Windows 2.0 e assim por diante. A primeira versão a tornar-se popular no Brasil foi o Windows 3.1. O Sistema apresentava uma interface gráfica onde tínhamos novidades como ícones, atalhos e outros “enfeites” mais. Muitos classificavam o Windows 3.1 como sendo apenas um Ambiente Operacional e não um Sistema Operacional, por ser este dependente do MS-DOS para realizar uma série de tarefas básicas.

Com a disseminação das redes e a necessidade de compartilhamento de periféricos e de 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 for Workgroups, conforme o próprio nome sugere, 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. Uma revolução estava prestes a acontecer.

Em 25 de Agosto de 1995 deu-se a referida revolução: Foi 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 e tantos 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 (logo a seguir apresentarei o histórico das versões do Windows para Servidores, onde se encaixa o Windows Server 2003). Segundo recomendações da própria Microsoft o NT Workstation era indicado para uso empresarial, isto é, nas estações de trabalho das redes das empresas. O NT Workstation 3.5 e 3.51 tinham uma interface idêntica a do Windows 3.1/Windows 3.11 e também eram baseados na tecnologia de 16 bits.

Nesta época iniciava-se a confusão. Por que ter duas linhas diferentes do Windows? Drivers que funcionavam no Windows 3.1 ou 95 não funcionavam no NT. Instalar determinados dispositivos de Hardware no NT (Workstation ou Server) era um verdadeiro suplício. A linha Workstation, segundo a Microsoft, foi criada tendo como fundamentos, a criação de um sistema mais estável, com configurações de segurança mais avançadas e com suporte às tecnologias de rede existentes. Sem dúvida um sistema para uso em redes empresariais. Já para o usuário doméstico, a Microsoft não recomendava o uso do NT Workstation, principalmente pelo fato do NT precisar de Hardware mais potente do que o Windows 3.11 ou 95. Outro motivo é que muitos dispositivos de Hardware não tinham driver para NT. Além disso, muitos aplicativos que rodavam no Windows 3.11 ou 95 não rodavam no NT, principalmente jogos.

Neste momento a Microsoft já falava em unificar, quem sabe um dia, as duas linhas do Windows, porém este era uma promessa ainda distante. Uma nova versão do NT foi lançada: NT Workstation 4.0 e NT Server 4.0 (para servidores de rede). Esta era a versão do NT baseada na tecnologia de 32 Bits e com cara de Windows 95. Melhorias substanciais forma feitas em relação a versão anterior do NT. Neste momento muitas empresas começam a adotar o NT Workstation 4.0 como Sistema Operacional para as estações da rede. Embora o preço da licença do NT Workstation fosse um pouco mais caro, os benefícios em termos de estabilidade e segurança compensavam. Cabe aqui ressaltar que o NT Workstation 4.0 é muitíssimo mais estável do que o Windows 95, 98 ou Me.

**NOTA:** Para um curso completo sobre o Windows XP Home & Professional, consulte o meu livro: Windows XP Home & Professional Para Usuários e Administradores, Editora Axel Books.

Logo após o lançamento do NT 4.0 a Microsoft já começava a falar no lançamento do NT 5.0. Muita expectativa havia em relação a esta versão do NT. Porém uma série de fatores fez com que o lançamento do NT 5.0 fosse atrasando mais e mais. Na introdução do meu primeiro livro, “Série Curso Básico & Rápido Microsoft Windows 2000 Server”, eu escrevi o seguinte:

“Bem-vindo ao Windows 2000 Server. Sem a menor sombra de dúvidas o Sistema Operacional mais aguardado de toda a história da indústria da Informática. Nunca falou-se e até mesmo especulou-se tanto sobre um Sistema Operacional, como se fez a respeito do Windows 2000 Server. No início do projeto este era chamado de Windows NT Server 5.0. Após diversos atrasos e adiamentos, o sistema foi “rebatizado” para Windows 2000 Server. Finalmente a data oficial do lançamento está confirmada para o dia 17 de Fevereiro do ano 2000. O código final do produto foi enviado para produção no dia 15 de Dezembro de 1999, após diversas versões de avaliação. Atrasos e especulações a parte, o fato é que o Windows 2000 Server representa um grande esforço da Microsoft em melhorar o seu Sistema Operacional para servidores de rede. Inúmeros recursos novos foram acrescentados, além da melhoria dos recursos já existentes.”

Conforme descrito no parágrafo anterior, o que seria o NT 5.0, devido a sucessivos atrasos, foi lançado somente em Fevereiro de 2000, com o nome de Windows 2000. Neste meio tempo foi lançado o Windows 98, idêntico ao Windows 95 apenas com algumas melhorias e um número muito pequeno de novidades. O Windows 2000, a exemplo do NT 4.0 tem a versão para servidor – Windows 2000 Server e a versão para estação de trabalho – Windows 2000 Professional. 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 e muitas ainda estão em processo de migração.

Observe que neste momento ainda temos duas linhas bem distintas. Uma com o Windows 9x/Me e outra com o Windows 2000. 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.

Durante o ano de 2000 ainda foi lançado o Windows Me, que deveria ser o substituto do Windows 98. Como esta nova versão apresentava poucas diferenças, com apenas algumas inovações não muito significativas, o ritmo de adoção do Windows Me foi e continua um pouco lento. Acredito que o sucesso do Windows 2000 também colaborou para a adoção lenta do Windows Me. Principalmente nas empresas, a migração do Windows 98 foi para o Windows 2000 Professional ao invés do Windows Me, principalmente pela melhor estabilidade do Windows 2000 Professional e pelas configurações de segurança disponíveis no Windows 2000 Professional e não disponíveis no Windows 95/98/Me..

Finalmente, em Outubro de 2001 foi lançado o Windows XP. Segundo a Microsoft XP de “Experience”. O Windows XP, conforme visto na Figura 14.1, foi lançado em duas versões: Home e Professional. O Windows XP representa, agora sim, um passo 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, confiabilidade e segurança do Windows 2000.

Nos endereços a seguir, você encontra informações detalhadas sobre a história do Windows:

- ◆ <http://www.computerhope.com/history/windows.htm>
- ◆ <http://members.fortunecity.com/pcmuseum/windows.htm>
- ◆ <http://www.levenez.com/windows/history.html>
- ◆ [http://www.winsupersite.com/reviews/winserver2k3\\_gold1.asp](http://www.winsupersite.com/reviews/winserver2k3_gold1.asp)

## Os “Windows” para Servidores:

Neste tópico vou mostrar a evolução que teve início com as primeiras versões do Windows NT Server até a última versão do Windows para Servidores: Windows Server 2003.

Considere o diagrama da Figura 14.2:

### Windows Para Servidores de Rede

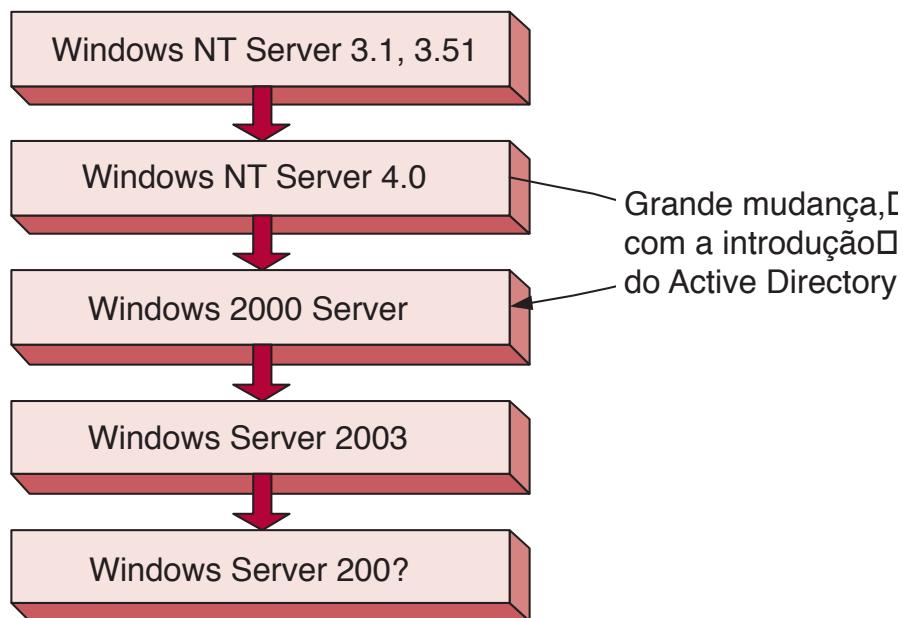


Figura 14.2 A Família Windows para servidores.

Farei alguns comentários sobre o diagrama da Figura 14.2.

A Microsoft entrou na “briga” dos servidores de rede no início dos anos 90, com o lançamento do NT Server. NT de New Tecnology. No início, na minha opinião, as versões do NT não tinham os mesmos recursos e nível de desempenho/segurança do que concorrentes mais antigos, tais como Novell e as versões do UNIX. 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.

Porém a realidade é que o NT Server teve uma boa aceitação. Até a versão 3.51 o NT tinha a mesma interface do Windows 3.11. A partir do NT Server 4.0, a interface era a do Windows 95. Com o NT Server 4.0, a participação da Microsoft no mercado de servidores realmente decolou. Muitas empresas passaram a adotar o NT Server 4.0 como Sistema Operacional para os seus servidores de rede.

Mas com tudo na vida tem dois lados, mais usuários significa mais exigências, ou seja, rapidamente as deficiências do NT Server 4.0 passaram a ser questionadas pelos usuários. A Microsoft em resposta começou a anunciar o NT 5.0, o qual conteria uma série de novos recursos para solucionar os problemas do NT 4.0. Porém o projeto do NT 5.0 começou a atrasar, conforme já descrito anteriormente (o que fez com que a concorrência começasse a chamar o NT 5.0 de “Vaporware”, em uma alusão a um sistema que não existe).

Finalmente em 17 de Fevereiro de 2000 a Microsoft lança a nova versão, agora “rebatizada” como Windows 2000 Server. A nova versão representou uma verdadeira revolução em relação ao NT Server 4.0. Basta citar o Active Direc-

tory para exemplificar esta revolução, esta verdadeira mudança de paradigma. Apesar das dúvidas e da aposta da concorrência de que não haveria uma aceitação do Windows 2000 Server, o fato é que este foi e continua sendo amplamente adotado por empresas do mundo inteiro.

Hoje, a maioria dos servidores Intel que rodam alguma versão do Windows, são baseados no Windows 2000 Server. Existem profissionais capacitados, farta literatura e fontes de referência na Internet e o Windows 2000 Server tem-se mostrado bastante estável e seguro.

Se o Windows 2000 Server está tão bom, então porque uma nova versão? Porque, como sempre, com a utilização por milhões de usuários, novas demandas e funcionalidades são solicitadas. Em resposta a estas demandas e necessidades de melhoria, a Microsoft apresenta o Windows Server 2003, lançado no dia 24 de Abril de 2003. Ou seja, posicionando o Windows Server 2003, podemos afirmar que ele é a versão mais recente, do Windows para Servidores de Rede.

E o futuro? Bem, ainda é cedo para especular. Mas provavelmente no início de 2006 saia uma nova versão do Windows para estações de trabalho, ou seja, o sucessor do Windows XP. E em 3 ou 4 anos, saia o sucessor do Windows Server 2003. Mas são apenas especulações que podem ou não se confirmar.

## Definindo exatamente o papel do Windows Server 2003

Neste item farei uma apresentação do Windows Server 2003. Os conceitos apresentados neste item, fornecem uma visão geral dos elementos que compõem uma rede baseada no Windows Server 2003.

O Windows Server 2003 é um sistema operacional para ser instalado em servidores de uma rede. Em uma rede de computadores temos, basicamente, dois tipos de equipamentos conectados (além dos equipamentos responsáveis pela conectividade da rede, tais como hubs, switchs, roteadores, etc):

- ◆ Estações de trabalho
- ◆ Servidores

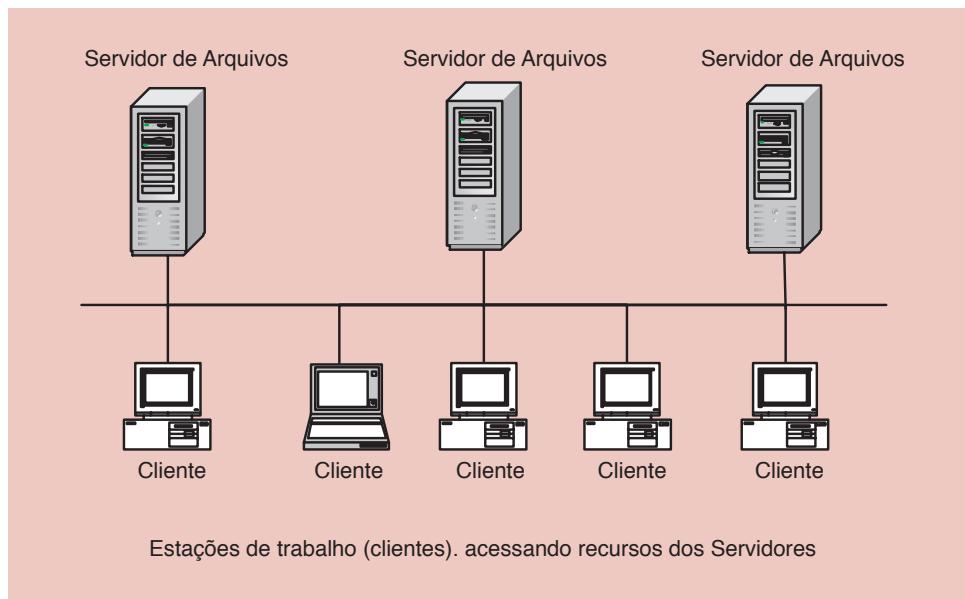
Como o próprio nome sugere, um Servidor fornece serviços para vários clientes. Por exemplo, podemos ter um servidor de arquivos onde ficam gravados arquivos, os quais podem ser acessados através da rede, por todos as estações da rede (estações de trabalho), as quais são conhecidas como Clientes. Outro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

Com base na explicação acima, podemos apresentar um outro conceito, que certamente a maioria dos leitores já conhece: O conceito da Arquitetura Cliente-Servidor. A Arquitetura Cliente-Servidor, de uma maneira simples, nada mais é do que uma rede 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.

Um exemplo típico, que com certeza utilizamos diariamente, é o acesso à Internet. Por exemplo, 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 dezenas ou até centenas de milhões de clientes acessando os mais variados recursos e serviços disponibilizados pelos servidores.

Na Figura 14.3, apresento um diagrama de exemplo de uma rede Cliente-servidor típica, onde serviços de Compartilhamento de arquivos e de Impressão são oferecidos por dois servidores com o Windows Server 2003 instalado , recursos estes que são acessados pelos Clientes da rede.



**Figura 14.3 Um exemplo simples de uma rede Cliente-servidor.**

Em uma rede de computadores (onde temos Servidores e Clientes, conforme descrito anteriormente), todos os computadores precisam “Falar a mesma língua”, para que possam ser trocadas informações entre os computadores da rede. Este “Falar a mesma língua”, em termos de redes, significa que todos os computadores de uma rede precisam ter o mesmo Protocolo de comunicação instalado e corretamente configurado.

Um protocolo de comunicação, nada mais é do que um conjunto de regras e normas para que os computadores possam trocar informações. Dois computadores que não possuem um protocolo em comum, não conseguirão trocar informações. É como um brasileiro que não sabe Chinês, tentando falar com um Chinês que não sabe Português. O diálogo (ou troca de informações) , fica simplesmente impossível.

Existem vários protocolos de comunicação entre computadores e outros dispositivos de uma rede. O Windows Server 2003 fornece suporte a uma série de protocolos, porém o mais utilizado é o TCP-IP – Transmission Control Protocol – Internet Protocol . Vários são os motivos que tornaram o TCP-IP, o protocolo mais adotado, e por isso mesmo o protocolo padrão do Windows Server 2003, isto é, o protocolo que é adicionado durante a instalação do Windows Server 2003. Um dos principais motivos para a ampla aceitação é que o TCP-IP é o protocolo utilizado na Internet, isto é, para que um computador possa ter acesso a Internet ele precisa ter o protocolo TCP-IP instalado e corretamente configurado. Outro motivo é a forte aceitação do Mercado em relação ao TCP-IP, uma vez que grande maioria dos Sistemas Operacionais adota o TCP-IP como protocolo padrão.

No diagrama da Figura 14.3 foram apresentados apenas exemplos de servidores baseados no Windows Server 2003 atuando nos serviços de compartilhamento de arquivos e de impressoras. Porém o Windows Server 2003 podem desempenhar diversos outros papéis, tais como:

- ◆ Servidor de Internet/Intranet, prestando serviços de hospedagem de sites (http), cópia de arquivos (ftp), envio de mensagens (SMTP), servidor de aplicativos Web, hospedando páginas ASP ou ASP.NET, etc. No Capítulo 13 você aprendeu um pouco mais sobre a utilização do IIS, que é o servidor Web disponibilizado com o Windows Server 2003.
- ◆ Controlador de domínio – DC (Domain Controller): Um servidor onde está instalado o Active Directory, que é o banco de dados onde ficam gravados as contas de usuários e as senhas dos usuários, contas dos computadores da rede, nome dos grupos de usuários e a lista de membros de cada grupo e uma série de outras informações necessárias ao funcionamento da rede. Um servidor com o Active Directory instalado é conhecido como DC – Domain Controller.
- ◆ Serviços de rede: Oferecendo serviços de resolução de nomes, tais como o DNS e WINS, serviço de configuração automática do protocolo TCP/IP (DHCP), roteamento e acesso remoto (RRAS) e assim por diante.
- ◆ Servidor de banco de dados: Um servidor com o Windows Server 2003 instalado e com o SQL Server 2000 (ou versão posterior) instalado. O SQL Server 2000 é o banco de dados para uso empresarial, com suporte a grande volume de acesso.
- ◆ Servidor de correio eletrônico e de ferramentas de colaboração: Um servidor como Windows Server 2003 instalado e com o Exchange 2000 (ou posterior) 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, uma aplicativo para aprovação de despesas de viagem. O funcionários que vai viajar preenche um formulário solicitando recursos para a viagem. O formulário é enviado, 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, Firewall, roteamento, etc. São muitas as funções que um servidor baseado no Windows Server 2003 pode exercer.

**DICA:** No Windows Server 2003 o protocolo TCP/IP é automaticamente adicionado durante a instalação do Sistema Operacional e não pode ser desinstalado. Esta é uma das novidades do Windows Server 2003. Fique atente a este ponto.

**DICA:** Lembre-se de que ao instalar o Windows Server 2003 não é possível, durante a instalação, já definir o servidor como um DC. Você deve instalar o Windows Server 2003. Após a instalação, você deve fazer o logon com uma conta com permissão de Administrador e executar o comando dcpromo. Ao executar este comando, será aberto o Assistente de Instalação do Active Directory, o qual será utilizado para instalar o Active Directory no servidor, tornando-o um DC.

**DICA:** Não esqueça que o tipo de registro utilizado, para localizar servidores de e-mail, via DNS é o registro do tipo MX.

Para resumir este item posso dizer o seguinte: “O Windows Server 2003 é um Sistema Operacional para uso em servidores de rede. Ele pode ser configurado para oferecer uma série de serviços aos clientes da rede. Possui novas funcionalidades e características em relação ao Windows 2000 Server.”

# O Protocolo TCP/IP

É muito importante que você volte a este tópico no Capítulo 1 e revise todos os itens sobre TCP/IP. Você deve conhecer os aspectos básicos do TCP/IP, tais como o conceito de Máscara de sub-rede e Default Gateway (Gateway Padrão). Revise todos os itens relacionados ao TCP/IP.

## O papel do Roteador em uma rede de computadores:

É importante que o candidato conheça o papel dos roteadores na ligação entre redes locais (LANs) para formar uma WAN. Mostrarei um exemplo básico de roteamento.

Mostrei anteriormente, no Capítulo 1, que a máscara de sub-rede é utilizada para determinar qual “parte” do endereço IP representa o número da Rede e qual parte representa o número da máquina dentro da rede. A máscara de sub-rede também foi utilizada na definição original das classes de endereço IP. Em cada classe existe um determinado número de redes possíveis e, em cada rede, um número máximo de máquinas. Com base na máscara de sub-rede o protocolo TCP/IP determina se o computador de origem e o de destino estão na mesma rede local. Com base em cálculos binários, o TCP/IP pode chegar a dois resultados distintos:

- ◆ O computador de origem e de destino estão na mesma rede local: Neste caso os dados são enviados para o barramento da rede local. Todos os computadores da rede recebem os dados. Ao receber os dados cada computador analisa o campo Número IP do destinatário. Se o IP do destinatário for igual ao IP do computador, os dados são capturados e processados pelo sistema, caso contrário são simplesmente descartados. Observe que com este procedimento, apenas o computador de destino é que efetivamente processa os dados para ele enviados, os demais computadores simplesmente descartam os dados.
- ◆ O computador de origem e de destino não estão na mesma rede local: Neste caso os dados são enviados o equipamento com o número IP configurado no parâmetro Default Gateway (Gateway Padrão). Ou seja, se após os cálculos baseados na máscara de sub-rede, o TCP/IP chegar a conclusão que o computador de destino e o computador de origem não fazem parte da mesma rede local, os dados são enviados para o Default Gateway, o qual será encarregado de encontrar um caminho para enviar os dados até o computador de destino. Esse “encontrar o caminho” é tecnicamente conhecido como Rotear os dados até o destino. O responsável por “Rotear” os dados é o equipamento que atua como Default Gateway o qual é conhecido como Roteador. Com isso fica fácil entender o papel do Roteador:

“É o responsável por encontrar um caminho entre a rede onde está o computador que enviou os dados e a rede onde está o computador que irá receber os dados.”

Quando ocorre um problema com o Roteador, tornando-o indisponível, você consegue se comunicar normalmente com os demais computadores da rede local, porém não conseguirá comunicação com outras redes de computadores, como por exemplo a Internet.

---

**DICA:** Para exibir as configurações do protocolo TCP/IP de um computador com o Windows Server 2003, você utiliza o comando ipconfig/all.

# Executar um teste de compatibilidade antes da instalação do Windows Server 2003

Antes de fazer a instalação do Windows Server 2003 é recomendável que você faça execute um teste de verificação de compatibilidade, para detectar se existe alguma incompatibilidade de Hardware ou de Software.

Se você for instalar o Windows Server 2003 em um servidor novo, basta ligar o servidor com o cd do Windows Server 2003 já no drive de CD. Em uma das primeiras telas do processo de instalação, será exibida uma opção para você executar um teste de compatibilidade. Você usa a opção Checar compatibilidade do sistema (Check System Compatibility), para iniciar um teste de compatibilidade, antes da instalação do Windows Server 2003.

## Itens a serem verificados e/ou considerados antes de iniciar a instalação:

Antes de iniciar a instalação do Windows Server 2003 você deve fazer uma espécie de inventário de alguns fatores. O primeiro deles é o teste de compatibilidade explicado anteriormente. Em seguida você deve verificar se o hardware atende os requisitos mínimos para o servidor onde será instalado o Windows Server 2003. Os requisitos mínimos dependem de uma série de fatores, tais como aplicações e serviços que serão executados no servidor, número de usuários simultâneos, volume de informações que será acessada e assim por diante.

Os requisitos mínimos de hardware foram apresentados no Capítulo 1. Mas lembre que estes são requisitos mínimos e não requisitos reais, que levam em conta a carga de trabalho a qual será submetida o servidor, uma vez que este seja colocado em operação.

Em seguida você deve decidir se será feita uma nova instalação ou se será feita a atualização de uma versão anterior do Windows já instalada, como o Windows 2000 Server ou o NT Server 4.0.

A vantagem de uma nova instalação é que você tem a certeza de partir com uma instalação sem problemas, sem arquivos corrompidos, sem comportamentos imprevistos e tantos outros problemas que podem surgir em uma instalação já existente. Ao fazer uma nova instalação é recomendado que você formate o Disco Rígido onde será feita a instalação (sempre lembrando de fazer um backup dos dados, se houver dados importantes no disco rígido que será formatado, pois este processo exclui toda a informação existente no disco rígido). Isso para o caso de você fazer uma nova instalação em um servidor já existente.

A desvantagem de fazer uma nova instalação é que todos os programas instalados e configurações serão perdidas. Você terá que reinstalar todos os programas e fazer as configurações novamente. Se você estiver fazendo a instalação de um novo servidor, esta é a única opção disponível.

Para servidores que já tem o Windows 2000 Server 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 vá fazer um upgrade, sempre é recomendável (eu diria até 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.

---

**DICA:** Você também pode executar o teste de compatibilidade, utilizando o comando `winnt32.exe`, da pasta `i386` do CD de instalação do Windows Server 2003, com a opção `/checkupgradeonly`, conforme exemplo a seguir: `winnt32/checkupgradeonly`

---

Você somente consegue fazer o upgrade para o Windows 2000 Server, das versões de servidor do Windows. Por exemplo, não é possível fazer um upgrade do Windows 2000 Professional ou do Windows XP Professional para o Windows Server 2003. Na Tabela 14.1, você tem uma relação dos caminhos de atualização de outras versões do Windows para o Windows Server 2003.

**Tabela 14.1 Caminhos para a atualização para o 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 Adv. Server    | Sim  |
| Windows 2000 Professional   | Não  |
| Windows XP Professional     | Não  |

Outra decisão que você deve tomar é se o servidor que está sendo instalado será um controlador de domínio ou um servidor para prestar outros serviços, como compartilhamento de arquivos, servidor Web, servidor de banco de dados e assim por diante. No caso de você estar fazendo uma atualização, é provável que o servidor continue a exercer as funções que estava exercendo antes.

Também é recomendado que você reuna as informações sobre as configurações de rede que serão utilizadas no servidor. Por exemplo:

- ◆ O servidor fará parte de um domínio ou de um Workgroup? (maiores detalhes sobre domínios e workgroups no Capítulo 2)
- ◆ Qual o nome do servidor? Sempre lembrando que não pode haver dois servidores com o mesmo nome, no mesmo domínio.
- ◆ Configurações do protocolo TCP/IP. Serão automáticas, obtidas a partir de um servidor DHCP? Ou serão configuradas manualmente. No caso de serem configuradas manualmente, você deve obter as seguintes informações com o administrador da rede: Número IP, máscara de sub-rede, número IP do Default Gateway, número IP de um ou mais servidores DNS, número IP de um ou mais servidores WINS (se existir servidores WINS na sua rede), nome de host e domínio DNS.

**NOTA: Para maiores detalhes sobre a instalação do Active Directory, domínios e a criação de Controladores de Domínio, consulte o Capítulo 2.**

Eu também poderia iniciar uma discussão sobre o sistema de arquivos que deve ser utilizado na partição onde o Windows Server 2003 será instalado. Estão disponíveis os sistemas de arquivo FAT32 e NTFS, os quais serão detalhadamente explicados no Capítulo 5. Porém são tantas as vantagens do sistema de arquivos NTFS, que nem vale a pena discutir. Servidor com o Windows Server 2003? Utilize NTFS. No Capítulo 5 você verá o porquê desta recomendação.

Antes de iniciar a instalação você também deve estar de posse do número de licença, o qual normalmente vem impresso em uma etiqueta colada na caixa do CD de instalação do Windows Server 2003.

## Modos de Licenciamento do Windows Server 2003

- ◆ Por Servidor: Esta forma de licenciamento é mais indicado para pequenas empresas, nas quais existe um único servidor com o Windows Server 2003 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 no servidor, este último usuário 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, independentemente 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 CALs, uma para cada estação de trabalho. O preço de uma CAL para este modo de licenciamento é maior do que para o Per Server, mas em compensação com uma única CAL, a estação de trabalho pode acessar recursos em qualquer servidor que esteja utilizando o licenciamento Per Device

## Active Directory – Conceitos, Estrutura Lógica e Física e Componentes

Neste tópico reapresentarei os conceitos sobre os principais elementos do Active Directory, focando nos elementos que você deve conhecer para o Exame 70-290.

### Entendendo o conceito de Diretórios e Workgroups

Nesta item mostrarei as diferenças entre uma rede baseada no modelo de Workgroup e uma rede baseada no modelo de diretórios.

Você entenderá porque uma rede baseada no conceito de Workgroup (Grupo de trabalho) somente é indicada para redes muito pequenas, entre cinco e dez usuários. E porque para redes maiores seria praticamente impossível administrar um modelo de redes baseado em Grupos de Trabalho ao invés de domínios.

### Domínios e Grupos de Trabalho (Workgroups):

Um rede baseada no Windows Server 2003 pode ser criada utilizando-se dois conceitos diferentes, dependendo da maneira com que os Servidores Windows Server 2003 são configurados. Os servidores podem ser configurados para fazerem parte de um Domínio ou de um Grupo de Trabalho, mais comumente chamado de Workgroup, termo que utilizarei de agora em diante.

## Entendendo o funcionamento de uma rede baseada no modelo de Workgroups:

Em uma rede baseada no modelo de Workgroups cada servidor é independente do outro. Em outras palavras, os servidores do Workgroup não compartilham uma lista de usuários, grupos, configurações de segurança, políticas, diretivas e outras informações. Cada servidor tem a sua própria lista de usuários e grupos, conforme indicado no diagrama da Figura 14.4:

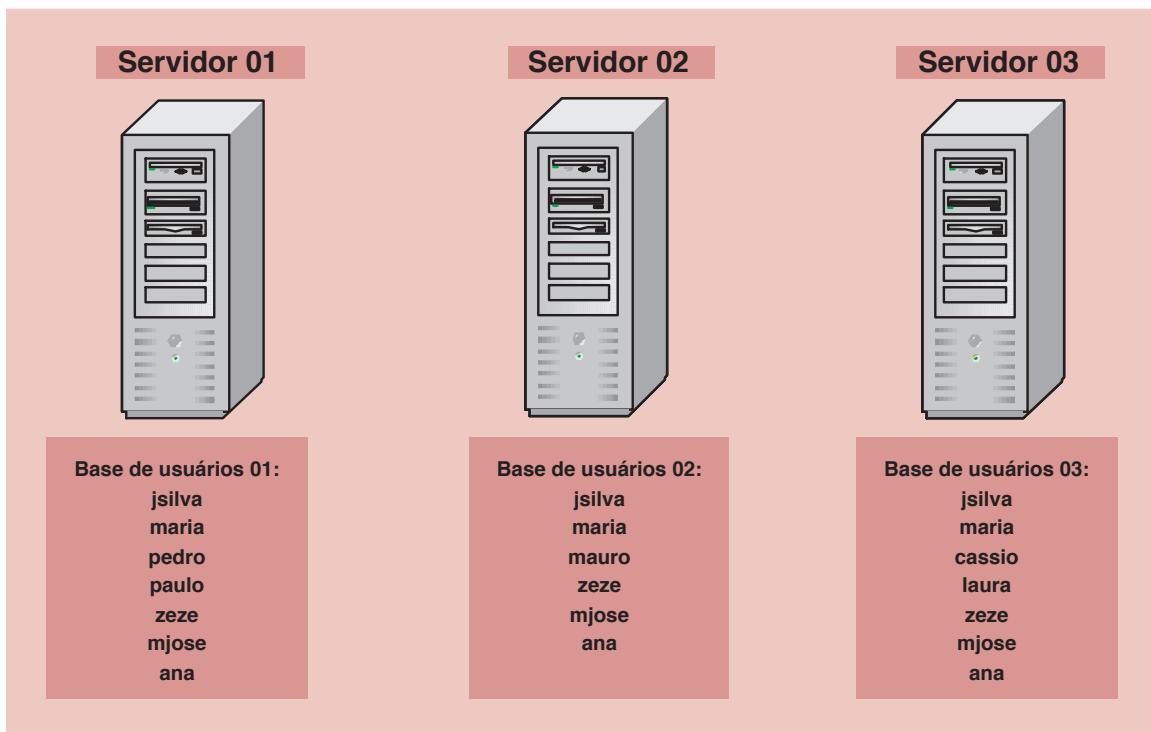


Figura 14.4 Uma rede baseada no conceito de Workgroup.

O diagrama demonstra uma rede baseada no modelo de Workgroup. Na rede de exemplo temos três servidores, onde cada servidor tem a sua própria base de usuários, senhas e grupos. Conforme pode ser visto no diagrama, as bases não estão sincronizadas, existem contas de usuários que foram criadas em um servidor mas não foram criadas nos demais. Por exemplo, a conta paulo somente existe no Servidor 01, a conta mauro só existe no Servidor 02 e a conta cassia só existe no servidor 03.

Agora imagine o usuário paulo, que está utilizando a sua estação de trabalho. Ele tenta acessar um recurso (por exemplo uma pasta compartilhada) no Servidor 01. Uma janela de logon é exibida. Ele fornece o seu nome de usuário e senha e o acesso (desde que ele tenha as devidas permissões) é liberado.

Agora este mesmo usuário – paulo, tenta acessar um recurso no Servidor 02. Novamente uma tela de logon é exibida e ele fornece o seu nome de usuário e senha. O acesso é negado, com uma mensagem de usuário inválido. E o usuário paulo fica sem entender o que está acontecendo. Orá, isso acontece porque o usuário paulo somente está cadastrado no Servidor 01; para o Servidor 02 e para o Servidor 03 é como se o usuário paulo não existisse (usuário inválido). Para que o usuário paulo possa acessar recursos dos servidores 02 e 03, o Administrador deveria criar uma conta chamada “paulo” nestes dois servidores.

Mas a “confusão” pode ser maior ainda. Imagine que o usuário paulo foi cadastrado pelo administrador com a conta paulo e senha: abc123de. Muito bem, o administrador fez o cadastro do usuário paulo nos três servidores: Servidor 01,

Servidor 02 e Servidor 03. Agora, cerca de 30 dias depois, o usuário paulo resolveu alterar a sua senha. Vamos supor que ele estava conectado ao Servidor 01, quando fez a alteração da sua senha para: xyz123kj. Agora o usuário paulo está na situação indicada a seguir:

| Servidor    | Usuário | Senha    |
|-------------|---------|----------|
| Servidor 01 | paulo   | abc123de |
| Servidor 02 | paulo   | abc123de |
| Servidor 03 | paulo   | xyz123kj |

Na concepção do usuário, a partir de agora vale a nova senha, independentemente do servidor que ele estiver acessando. Pois para o usuário interessa o recurso que ele está acessando, muitas vezes ele nem sequer tem noção de que o recurso está em um servidor e muito menos em qual servidor. Para o usuário não interessa se o recurso está no servidor 01, 02 ou outro servidor qualquer. Agora vamos ver o que acontece com o usuário paulo.

O usuário paulo, que está utilizando a sua estação de trabalho. Ele tenta acessar um recurso (por exemplo uma pasta compartilhada) no Servidor 01. Uma janela de logon é exibida. Ele fornece o seu nome de usuário e a nova senha e o acesso (desde que ele tenha as devidas permissões) é liberado.

Agora este mesmo usuário – paulo, tenta acessar um recurso no Servidor 02. Novamente uma tela de logon é exibida e ele fornece o seu nome de usuário e a nova senha e a surpresa: O acesso é negado, com uma mensagem de falha na autenticação. Aí o usuário fica pensando: mas como é possível, eu recém troquei a senha. Ele trocou a senha no Servidor 01. Para os demais servidores continua valendo a senha antiga. A única maneira de ele conseguir alterar a senha é fazendo o logon com a senha antiga e alterando para a nova senha, em todos os servidores da rede. Agora imagine o problema em uma rede de grandes proporções, com dezenas de servidores e milhares de funcionários. Fica fácil concluir que o modelo de Workgroup ficaria insustentável, impossível de ser implementado na prática.

Eu somente recomendaria modelo de Workgroup para redes pequenas, com um único servidor e com um número de, no máximo, 10 usuários.

## Entendendo o funcionamento de uma rede baseada no conceito de Diretório – Domínio:

Agora vou apresentar o modelo de rede baseado em um diretório. Vamos iniciar considerando o diagrama da Figura 14.5:

No modelo baseado em diretório, nos temos uma base de usuários única, ou seja, todos os servidores da rede compartilham a mesma base de usuários. O que acontece, na prática, não é que existe uma única base, armazenada em um determinado servidor, e todos os demais servidores acessam esta base. Não, não é isso. O que ocorre na prática, é que todos os servidores do domínio, configurados como DCs – Domain Controllers, contém uma cópia da base de informações do diretório (do Active Directory, no caso do Windows 2000 Server e Windows Server 2003). Alterações efetuadas em um dos servidores são repassadas para os demais servidores da rede, para que todos fiquem com uma cópia idêntica da base de dados do diretório. Esta sincronização entre os servidores do domínio é conhecida como Replicação do Active Directory.

O que caracteriza uma rede baseada em diretório é o fato de todos os servidores terem acesso a mesma base de dados, ou seja, todos compartilham o mesmo diretório, as mesmas informações sobre usuários, grupos, servidores e recursos e as mesmas políticas e diretivas de segurança. Mais adiante será apresentado o conceito de domínio,

floresta, relação de confiança, etc. Estes são outros elementos relacionados com o diretório e que permitem a criação de redes de grande extensão geográfica, como por exemplo redes de uma grande empresa com escritórios no mundo inteiro (Microsoft).

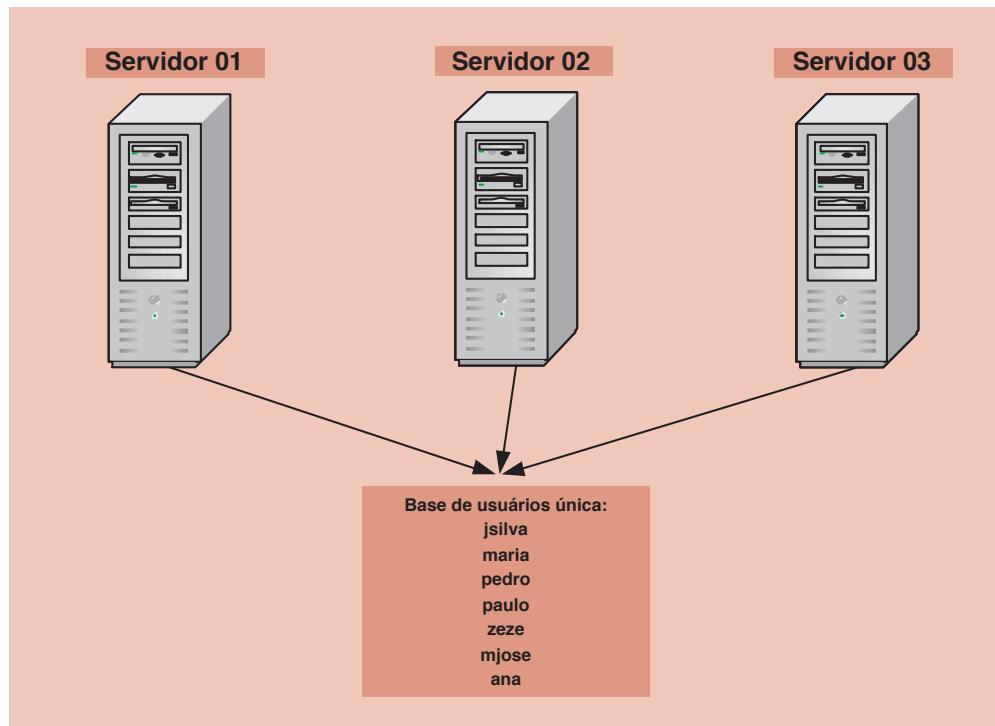


Figura 14.5 Uma rede baseada no conceito de Diretório - Domínio.

No modelo baseado em diretório, a vida do Administrador fica bem mais fácil. Vamos supor que o usuário paulo queira acessar um recurso em um dos servidores da rede. Sem problemas, qualquer servidor tem uma cópia da base de dados do diretório. Com isso a conta do usuário paulo estará disponível em qualquer servidor. Com isso ele poderá acessar recursos em qualquer um destes servidores. Há, mas se o usuário paulo alterar a sua senha. Isso será feito na cópia do banco de dados do diretório de um dos servidores. Correto? Correto, porém em pouco tempo esta alteração será replicada para todos os demais servidores e a senha do usuário paulo estará sincronizada em todos os servidores.

O modelo baseado em diretórios (e no conceito de domínios, florestas, etc) é bem mais fácil para administrar e permite a implementação de redes de grandes proporções, tanto geográficas quanto em números de usuários. Na empresa onde eu trabalho, temos uma rede baseada no Active Directory. A rede se estende por todos os estados do território nacional e tem cerca de 22.000 usuários. Uma rede e tanto. Seria literalmente impossível manter uma rede destas proporções sem utilizar o modelo baseado em diretórios.

## Domínios, Árvores de domínios e Unidades Organizacionais – Conceitos.

Agora que você já conhece bem a diferença entre um modelo de rede baseada em Workgroup e outro de rede baseada em diretórios, é hora de avançar um pouco mais e nós aproximar da terminologia do Active Directory. Neste item vou apresentar o conceito de diretório. Não um conceito formal, apresentado no Capítulo 2, mas sim o conceito de diretório que é utilizado em redes baseadas no Active Directory e no Windows Server 2003 (ou Windows 2000 Server).

No Windows Server 2003 (e também no Windows 2000 Server), o conjunto de servidores, estações de trabalho, bem como as informações do diretório é que formam uma unidade conhecida como Domínio. Todos os servidores

que contém uma cópia da base de dados do Active Directory, fazem parte do domínio. As estações de trabalho podem ser configuradas para fazer parte do domínio. No caso de estações de trabalho com o NT Workstation 4.0, Windows 2000 Professional ou Windows XP Professional, cada estação de trabalho que faz parte do domínio, tem uma conta de computador criada no domínio. A conta de computador tem o mesmo nome do computador. Por exemplo, a estação de trabalho micro-cont-001, tem uma conta de computador, na base de dados do Active Directory, com o nome de micro-cont-001.

Um domínio pode também ser definido com um limite administrativo e de segurança. Ele é um limite administrativo, pois as contas de Administrador tem permissões de acesso em todos os recursos do domínio, mas não em recursos de outros domínios. Ele é um limite de segurança porque cada domínio tem definições de políticas de segurança que se aplicam as contas de usuários e demais recursos dentro de domínio e não a outros domínios. Ou seja, diferentes domínios podem ter diferentes políticas e configurações de segurança. Por exemplo, no domínio A, posso ter uma política de segurança que define um tamanho mínimo de senha como 8 caracteres. Esta política será válida para todas as contas de usuário do domínio A. Um segundo domínio B, pode ter uma política de segurança diferente, a qual define um tamanho mínimo de senha de 12 caracteres. Esta política será válida para todas as contas de usuários do domínio B.

Um Domínio é simplesmente um agrupamento lógico de contas e recursos, os quais compartilham políticas de segurança. As informações sobre os diversos elementos do domínio (contas de usuários, contas de computador, grupos de usuários, políticas de segurança, etc), estão contidas no banco de dados do Active Directory.

Em um domínio baseado no Active Directory e no Windows Server 2003 é possível ter dois tipos de servidores Windows Server 2003:

- ◆ Controladores de Domínio (DC – Domain Controllers)
- ◆ Servidores Membro (Member Servers).

Falarei um pouco mais sobre Controladores de Domínio e Servidores Membro no final deste tópico.

A criação de contas de usuários, grupos de usuários e outros elementos do Active Directory, bem como alterações nas contas de usuários, nas políticas de segurança e em outros elementos do Active Directory, podem ser feitas em qualquer um dos Controladores de Domínio. Uma alteração feita em um DC será automaticamente repassadas (o termo técnico é “replicada”) para os demais Controladores de Domínio. Por isso se você cria uma conta para o usuário jsilva e cadastrá uma senha para este usuário, essa conta passa a ser válida em todo o domínio, sendo que o usuário jsilva pode receber permissões para acessar recursos e serviços em qualquer servidor do Domínio, seja em um Controlador de Domínio ou em um Servidor Membro.

Por isso que o Domínio transmite a idéia de um agrupamento lógico de Contas de Usuários e Grupos, bem como de políticas de segurança, uma vez que todo o Domínio compartilha a mesma lista de Usuários, Grupos e políticas de segurança. A criação de domínios facilita enormemente a administração de uma rede baseada no Windows Server 2003, sendo altamente recomendada para qualquer rede de maior porte seja criada com base em um ou mais domínios (dependendo do porte da rede).

---

**IMPORTANTE:** Computadores com o Windows 95/98/Me não tem conta de computador no domínio. Computadores com o Windows XP Home não podem ser configurados para fazer parte de um domínio baseado no Active Directory.

---

**IMPORTANTE:** Lembre que configurações de políticas de senha são aplicadas a nível de domínio. Por exemplo, você define a política que a conta deve ser bloqueada, após três tentativas de logon sem sucesso, dentro de uma hora, a nível de domínio. Não é possível, por exemplo, configurar diferentes políticas de senha, dentro do mesmo domínio. Você deve conhecer bem quais as políticas que são aplicadas ao domínio como um todo e quais podem ser aplicadas a nível de Unidade Organizacional, dentro do domínio.

---

Em um Domínio todos os Controladores de Domínio, compartilham uma lista de usuários, grupos e políticas de segurança, além de algumas outras características que falarei no tópico sobre o Active Directory. Além disso alterações feitas em um dos Controladores de Domínio, são automaticamente replicadas para os demais. DCs

Os DCs também são responsáveis por fazer a autenticação dos usuários na rede. Por exemplo, vamos supor que o usuário jsilva trabalha em uma estação de trabalho com o Windows XP Professional instalado. Esta estação foi configurada para fazer parte do domínio. Quando o usuário jsilva liga a estação de trabalho e o Windows é inicializado, é apresentada a tela de logon para que ele forneça o seu nome de usuário e senha. O Windows precisa verificar se o nome de usuário e senha estão corretos. A Windows tenta localizar um DC na rede. É no DC que a verificação é feita, comparando as informações digitadas pelo usuário, com as informações da base de dados do Active Directory. Se as informações estão OK o logon é liberado, o usuário é autenticado e a área de trabalho do Windows é exibida. A partir deste momento, toda vez que o usuário tentar acessar um recurso do domínio, será apresentada a sua autenticação, com base nas informações de logon apresentadas, para provar a identidade do usuário para a rede. Isso evita que o usuário tenha que entrar com o seu logon e senha cada vez que for acessar um recurso em um servidor diferente (que é justamente o que acontece no modelo baseado em Workgroup, conforme descrito anteriormente).

Como os Servidores Membro não possuem uma cópia da lista de usuários e grupos, estes não efetuam a autenticação dos clientes e também não armazenam informações sobre as políticas de segurança para o Domínio – as quais também são conhecidas por GPO – Group Policies Objects.

Quando os servidores Windows Server 2003 são configurados para trabalhar com um Workgroup, não existe o conceito de domínio e nem de Controlador de Domínio. Cada servidor mantém uma lista separada para contas de usuários, grupos e políticas de segurança, conforme descrito anteriormente. Com isso se um usuário precisa acessar recursos em três servidores, por exemplo, será necessário criar uma conta para esse usuário nos três servidores diferentes. Um Workgroup somente é recomendado para redes extremamente pequenas, normalmente com um único servidor Windows Server 2003 e não mais do que 10 estações clientes, conforme descrito anteriormente.

## Active Directory

Lembro de já ter escrito a seguinte frase, em um dos capítulos deste livro:

“O Active Directory é, sem dúvidas, a mudança mais significativa incluída no Windows 2000 Server e que também faz parte do Windows Server 2003.”

Mas de uma maneira simples, o que é o Active Directory ?

“O Active Directory é o serviço de diretórios do Windows Server 2003. Um Serviço de Diretórios é um serviço de rede, o qual identifica todos os recursos disponíveis em uma rede, mantendo informações sobre estes dispositivos (contas de usuários,

**IMPORTANTE: Nos Servidores Membros podem ser criadas contas de usuários e grupos, as quais somente serão válidas no Servidor Membro onde foram criadas. Estas contas são chamadas de contas locais. Embora isso seja tecnicamente possível, essa é uma prática não recomendada, uma vez que este procedimento dificulta enormemente a administração de um Domínio. Você pode atribuir permissões para os Recursos de um Servidor Membro, à contas de Usuários e Grupos do domínio, sem a necessidade de criar esses usuários ou grupos localmente. Por exemplo, um usuário jsilva, que pertence ao domínio, pode receber permissões de acesso em uma pasta compartilhada de um Servidor Membro. Com isso você pode concluir que um Servidor Membro, é um servidor que embora não mantenha uma cópia da lista de usuários e grupos do Active Directory, este tem acesso a essa lista. Com isso que podem ser atribuídas permissões nos recursos do Servidor Membro (tais como pastas compartilhadas, impressoras, etc ) para as contas e grupos do Domínio.**

**IMPORTANTE: Estações de trabalho com o Windows XP Home, não podem ser configuradas para fazer parte de um domínio. Estações de trabalho com o Windows 95/98/ Me podem ser configuradas para fazer parte de um domínio. Para ter**

grupos, computadores, recursos, políticas de segurança, etc) em um banco de dados e torna estes recursos disponíveis para usuários e aplicações.”

Pode parecer que o Active Directory é, na verdade um banco de dados. Mas não é só isso. Além do banco de dados com informações sobre os elementos (teoricamente conhecidos como objetos) que compõem o domínio, o Active Directory também disponibiliza uma série de serviços que executam as seguintes funções:

- ◆ Replicação entre os Controladores de domínio.
- ◆ Autenticação
- ◆ Pesquisa de objetos na base de dados
- ◆ Interface de programação para acesso aos objetos do diretório

Pela descrição formal, é possível inferir que o Active Directory é um serviço de rede, no qual ficam armazenadas informações sobre dados dos usuários, impressoras, servidores, grupos de usuários, computadores e políticas de segurança. Cada um desses elementos são conhecidos como objetos.

O Active Directory além de armazenar uma série de informações sobre os objetos disponíveis no domínio (contas de usuários, grupos de usuários, servidores, computadores, etc), torna fácil para o administrador localizar e fazer alterações nos objetos existentes, bem como criar novos objetos ou excluir objetos que não sejam mais necessários. Em resumo, com o conjunto de serviços oferecidos pelo Active Directory, a administração da rede fica bem mais fácil.

Os recursos de segurança são integrados com o Active Directory, através do mecanismo de logon e autenticação. Todo usuário tem que fazer o logon (informar o seu nome de usuário e senha), para ter acesso aos recursos da rede. Durante o logon o Active Directory verifica se as informações fornecidas pelo usuário estão corretas e então libera o acesso aos recursos para os quais o usuário tem permissão de acesso.

Os recursos disponíveis através do Active Directory , são organizados de uma maneira hierárquica, através do uso de Domínios. Uma rede na qual o Active Directory está instalado, pode ser formada por um ou mais Domínios. Com a utilização do Active Directory um usuário somente precisa estar cadastrado em um único Domínio, sendo que este usuário pode receber permissões para acessar recursos em qualquer um dos Domínios, que compõem a árvore de domínios da empresa.

A utilização do Active Directory simplifica em muito a administração, pois fornece um local centralizado, através do qual todos os recursos da rede podem ser administrados. Todos os Controladores de Domínio (DCs), possuem o Active Directory instalado. A Maneira de criar um domínio é instalar o Active Directory em um Member Server e informar que este é o primeiro Controlador de Domínio. Depois de criado o domínio (a parte prática da criação de domínios será vista na parte final do capítulo.) você pode criar DCs adicionais, simplesmente instalando o Active Directory outros servidores.

O Active Directory utiliza o DNS (Domain Name System) como serviço de nomeação de servidores e recursos e de resolução de nomes. Por isso um dos pré-requisitos para que o Active Directory possa ser instalado e funcionar perfeitamente é que o DNS deve estar instalado e corretamente configurado.

O Agrupamento de objetos em um ou mais Domínios permite que a rede de computadores reflita a organização da sua empresa. Para que um usuário cadastrado em um domínio, possa receber permissões para acessar recursos em outros domínios, o Windows Server 2003 cria e mantém relações de confiança entre os diversos domínios. As relações de confiança são bidirecionais e transitivas. Isso significa se o Domínio A confia no Domínio B, o qual por sua vez confia em um Domínio C, então o Domínio A também confia no Domínio C. Isso é bastante diferente do que

acesso a maioria dos recursos do Active Directory, também é preciso instalar o Active Directory Client, nas estações de trabalho com o Windows 95/98/Me. Uma estação de trabalho com o NT Workstation 4.0 também pode ser configurada para fazer parte de um domínio baseado no Active Directory e no Windows Server 2003.

acontecia até o NT Server 4.0, uma vez que as relações de confiança tinham que ser criadas e mantidas pelos administradores dos domínios, uma a uma. Era um trabalho e tanto, o que dificultava a implementação de relações de confiança em uma rede com muitos domínios.

Todo Domínio possui as seguintes características:

- ◆ Todos os objetos de uma rede (contas de usuários, grupos, impressoras, políticas de segurança, etc) fazem parte de um único domínio. Cada domínio somente armazena informações sobre os objetos do próprio domínio.
- ◆ Cada domínio possui suas próprias políticas de segurança.

## Árvore de domínios:

Quando existem diversos domínios relacionados através de relações de confiança, criadas e mantidas automaticamente pelo Active Directory, temos uma Árvore de domínios. Uma árvore nada mais é do que um agrupamento ou arranjo hierárquico de um ou mais domínios do Windows Server 2003, os quais “compartilham um espaço de nome.”

Vou explicar em detalhes o que significa a expressão “compartilham um espaço de nome”. Primeiramente observe a Figura 14.6:

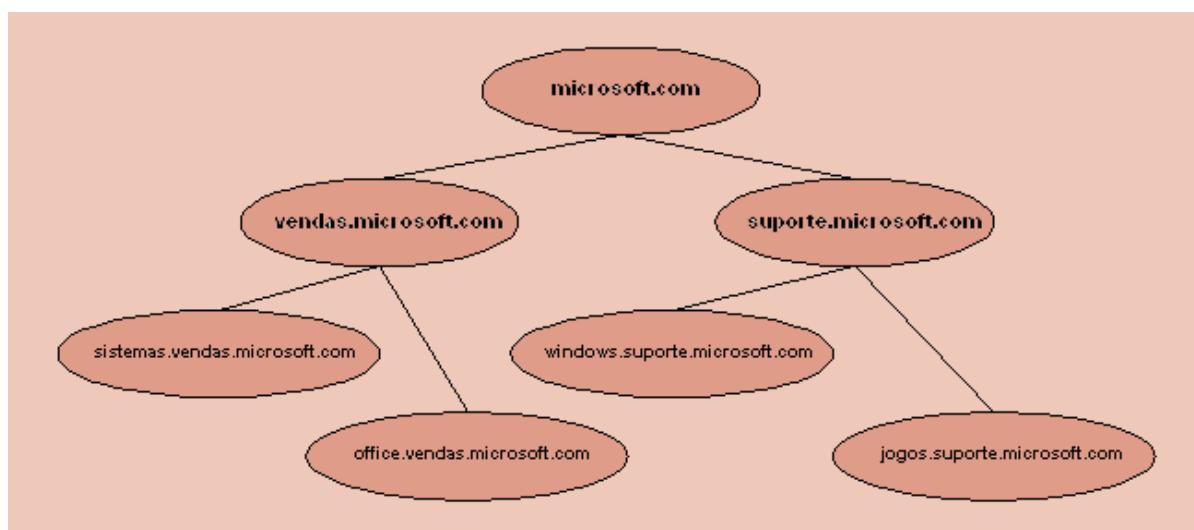


Figura 14.6 Todos os domínios de uma árvore compartilham um espaço de nomes em comum.

Observe que é exibida uma árvore com 7 domínios. Mas o que significa mesmo “compartilham um espaço de nome”?

Observe que o domínio inicial, também conhecido como domínio pai ou domínio root, é microsoft.com. Os domínios seguintes são: vendas.microsoft.com e suporte.microsoft.com. Quando é formada uma hierarquia de domínios, compartilhar um espaço de nomes, significa que os nomes dos objetos filho (de segundo nível, por exemplo: vendas.microsoft.com e suporte.microsoft.com), contém o nome do objeto pai (microsoft.com). Por exemplo, vendas.microsoft.com contém microsoft.com. Descendo mais ainda na hierarquia, você pode observar que este fato

**Novidade: No Windows Server 2003, o assistente de instalação do Active Directory é capaz de instalar e configurar o DNS, caso ele não encontre um servidor DNS adequadamente configurado na rede. Esta não chega a ser exatamente uma novidade. O que ocorre na prática, é que o assistente de instalação do Active Directory, no Windows Server 2003, consegue na maioria das vezes configurar o DNS corretamente, o que não ocorria no Windows 2000 Server.**

continua verdadeiro. Por exemplo o objeto filho sistemas.vendas.microsoft.com contém o nome do objeto Pai vendas.microsoft.com.

Com isso uma árvore de diretórios deste tipo forma um espaço de nomes contínuo, onde o nome do objeto filho sempre contém o nome do objeto pai.

## Unidades Organizacionais

Você pode ainda dividir um Domínio em “Unidades Organizacionais”. Uma Unidade Organizacional é uma divisão lógica do domínio, a qual pode ser utilizada para organizar os objetos de um determinado domínio em um agrupamento lógico para efeitos de administração. Isso resolve uma série de problemas que existiam em redes baseadas no NT Server 4.0.

No Windows NT Server 4.0 se um usuário fosse adicionado ao grupo Administradores (grupo com poderes totais sobre qualquer recurso do domínio), ele poderia executar qualquer ação em qualquer servidor do domínio. Com a utilização de Unidades Organizacionais, é possível restringir os direitos administrativos apenas a nível da Unidade Organizacional, sem que com isso o usuário tenha poderes sobre todos os demais objetos do Domínio.

Cada domínio pode implementar a sua hierarquia de Unidades Organizacionais, independentemente dos demais domínios, isto é, os diversos domínios que formam uma árvore, não precisam ter a mesma estrutura hierárquica de unidades organizacionais.

No exemplo da Figura 2.4, o domínio vendas.microsoft.com, poderia ter uma estrutura hierárquica de Unidades Organizacionais, projetada para atender as necessidades do domínio vendas. Essa estrutura poderia ser completamente diferente da estrutura do domínio suporte.microsoft.com, a qual será projetada para atender as necessidades do domínio suporte. Com isso tem-se uma flexibilidade bastante grande, de tal forma que a árvore de domínios e a organização dos domínios em uma hierarquia de Unidades Organizacionais, possa atender perfeitamente as necessidades da empresa. A utilização de Unidades Organizacionais não é obrigatória, porém altamente recomendada, conforme mostrarei em alguns exemplos mais adiante.

Utilize Unidades Organizacionais quando:

- ◆ Você quiser representar a estrutura e organização da sua companhia em um domínio. Sem a utilização de Unidades Organizacionais, todas as contas de usuários são mantidas e exibidas em uma única lista, independente da localização, departamento ou função do usuário.
- ◆ Você quiser delegar tarefas administrativas sem para isso ter que dar poderes administrativos em todo o Domínio. Com o uso de Unidades Organizacionais, você pode dar permissões para um usuário somente a nível da Unidade Organizacional.
- ◆ Quiser facilitar e melhor acomodar alterações na estrutura da sua companhia. Por exemplo, é muito mais fácil mover contas de usuários entre Unidades Organizacionais do que entre domínios, embora no Windows Server 2003 seja bem mais fácil mover uma conta de um domínio para outro, do que era no Windows 2000 Server.

## Conhecendo os principais Objetos do Active Directory

Até aqui apresentei os conceitos básicos sobre diretórios, domínios, unidades organizacionais e árvores de diretórios. A partir deste item passarei a descrever os objetos que fazem parte do Active Directory. Na seqüência falarei sobre os serviços que dão suporte ao Active Directory, tais como os serviços de replicação e o conceito de relações de confiança entre diretórios.

## Contas de usuários

Todo usuário que quer ter acesso aos recursos dos computadores do domínio (pastas compartilhadas, impressoras compartilhadas, etc) deve ser cadastrado no Active Directory. Cadastrar o usuário, significa criar uma conta de usuário e uma senha. Ao cadastrar um usuário, outras informações tais como seção, nome completo, endereço, telefone, etc, podem ser cadastradas, conforme vimos, em detalhes, no Capítulo 4.

Uma conta de usuário é um objeto do Active Directory, o qual contém diversas informações sobre o usuário, conforme descrito anteriormente. É importante salientar que a conta somente precisa ser criada uma vez, em um dos Controladores de domínio. Uma vez criada, a conta será replicada para todos os demais DCs do domínio.

Embora seja tecnicamente possível a criação de usuários e grupos locais, nos Servidores Membros e nas estações de trabalho, esta prática não é recomendada. Quando você trabalha em um domínio, o ideal é que contas de usuários e grupos sejam criadas somente no domínio, isto é, nos DCs.

Algumas recomendações e observações sobre contas de usuários:

- ◆ Todo usuário que acessa a rede deve ter a sua própria conta. Não é recomendado que dois ou mais usuários compartilhem a mesma conta. A conta é a identidade do usuário para a rede. Por exemplo, quando o usuário jsilva faz o logon no domínio, a sua conta é a sua identidade para o sistema. Todas as ações realizadas pelo usuário estão associadas a sua conta. O Windows Server 2003 tem um sistema de auditoria de segurança, no qual o Administrador pode configurar quais ações devem ser registradas no Log de auditoria. Por exemplo, o administrador pode definir que toda tentativa de alterar um determinado arquivo seja registrada no log de auditoria. Se o usuário jsilva tentar alterar o referido arquivo, ficará registrado no log de auditoria que o usuário jsilva, no dia tal, hora tal, tentou alterar o arquivo tal. Se dois ou mais usuários estão compartilhando a mesma conta, fica difícil identificar qual o usuário que estava logado no momento. Para o sistema é o jsilva. Agora quem dos diversos usuários que utilizam a conta jsilva é que estava logado e tentou alterar o referido arquivo? Fica difícil saber. Por isso a recomendação para que cada usuário seja cadastrado e tenha a sua própria conta e senha.
- ◆ Com base nas contas de usuários e grupos, o administrador pode habilitar ou negar permissões de acesso aos recursos da rede. Por exemplo, o administrador pode restringir o acesso a pastas e arquivos compartilhados na rede, definindo quais usuários podem ter acesso e qual o nível de acesso de cada usuário – leitura, leitura e alteração, exclusão e assim por diante. Mais um bom motivo para que cada usuário tenha a sua própria conta e senha.

Outro detalhe que você deve observar, é a utilização de um padrão para o nome das contas de usuários. Você deve estabelecer um padrão para a criação de nomes,

**IMPORTANTE:** Você também pode criar contas nos servidores membros e nas estações de trabalho com Windows 2000 Professional ou Windows XP Professional. As contas criadas nestes computadores são ditas contas locais, ou seja, somente existem no computador onde foram criadas. Vamos imaginar que você está trabalhando em uma estação de trabalho com o Windows XP Professional instalado. Esta estação foi configurada para fazer parte do domínio abc.com.br. Como a estação de trabalho faz parte do domínio, você terá acesso a lista de usuários e grupos do domínio. Com isso você poderá, por exemplo, atribuir permissão de acesso para um usuário do domínio (ou um grupo de usuários) em uma pasta compartilhada na sua estação de trabalho. Nesta mesma estação você também poderá criar contas de usuários e grupos locais, os quais ficam gravados na base de usuários local e só existe neste computador. Estes usuários e grupos (criados localmente), somente podem receber permissões de acesso para os recursos do computador onde foram criados. Você não conseguirá atribuir permissão de acesso em uma pasta compartilhada no servidor, para um usuário local da sua estação de trabalho.

pois não podem existir dois usuários com o mesmo nome de logon dentro do mesmo Domínio. Por exemplo se existir no mesmo Domínio, dois “José da Silva” e os dois resolverem utilizar como logon “jsilva”, somente o primeiro conseguirá, o segundo terá que se conformar em escolher um outro nome de logon. Para isso é importante que seja definido um padrão e no caso de nomes iguais deve ser definido uma maneira de diferenciá-los. Por exemplo poderíamos usar como padrão a primeira letra do nome e o último sobrenome. No caso de nomes iguais, acrescenta-se números. No nosso exemplo o primeiro José da Silva cadastrado ficaria como jsilva, já o segundo a ser cadastrado ficaria como jsilva1. Caso no futuro tivéssemos mais um José da Silva dentro da mesma Unidade Organizacional, este seria o jsilva2 e assim por diante.

Quando for criar nomes de logon para os usuários, leve em consideração os seguintes detalhes:

- ◆ Nomes de Usuários do Domínio devem ser únicos dentro do Domínio.
- ◆ Podem ter no máximo 20 caracteres.
- ◆ Os seguintes caracteres não podem ser utilizados: “/ \ : ; [ ] | = , + \* ? < >

Sempre que você for cadastrar um usuário também deve ser cadastrada uma senha para o usuário. Conforme mostrarei no Capítulo 4, o administrador pode especificar um número mínimo de caracteres aceito para a senha. O número máximo de caracteres da senha é 128.

## Contas de Computador

Estações de trabalho que rodam o Windows NT Workstation 4.0, Windows 2000 Professional ou Windows XP Professional e que fazem parte do domínio, devem ter uma conta de computador no Active Directory. Servidores, quer sejam Member Servers ou DCs, rodando Windows NT Server 4.0, Windows 2000 Server ou Windows Server 2003, também tem contas de computador no Active Directory.

A conta de computador pode ser criada antes da instalação do computador ser adicionado ao domínio ou no momento em que o computador é configurado para fazer parte do domínio. A conta do computador deve ter o mesmo nome do computador na rede. Por exemplo, um computador com o nome de microxp01, terá uma conta no Active Directory, com o nome: microxp01.

Para que um usuário possa fazer o logon no domínio é preciso que a sua conta de usuário esteja ativa e que não esteja bloqueada. Além disso, a conta do computador onde o usuário faz o logon, também deve estar ativa no domínio.

## Grupos de usuários

Um grupo de usuários é uma coleção de contas de usuários. Por exemplo, podemos criar um grupo chamado Contabilidade, do qual farão parte todos os usuários do departamento de Contabilidade (todas as contas de usuários dos funcionários do departamento de Contabilidade).

**IMPORTANTE:** O Administrador pode utilizar o recurso de GPOs – Group Policies Objects para impedir que os usuários possam criar contas de usuários e grupos locais, em suas estações de trabalho. O assunto GPOs é abordado, em detalhes, no Capítulo 18 do Livro: Windows Server 2003 – Curso Completo, 1568 páginas.

**IMPORTANTE:** Para as senhas, o Windows Server 2003 distingue letras maiúsculas de minúsculas. Por exemplo a senha “Abc123” é diferente da senha “abc123”.

**IMPORTANTE:** Conheça bem as políticas relacionadas as senhas de contas, as quais foram descritas, detalhadamente, no Capítulo 4 e para as quais apresentarei um resumo mais adiante.

**IMPORTANTE:** Computadores rodando Windows 95/98/Me, mesmo tendo acesso a lista de usuários e grupos do domínio, não terão contas de computador criadas no Active Directory. Computadores rodando o Windows XP Home, não podem ser configurados para fazer parte de um domínio.

A principal função dos grupos de usuários é facilitar a administração e a atribuição de permissões para acesso a recursos, tais como: pastas compartilhadas, impressoras remotas, serviços diversos, etc.

Ao invés de dar permissões individualmente, para cada um dos usuários que necessitam acessar um determinado recurso, você cria um grupo, inclui os usuários no grupo e atribui permissões para o grupo. Para que um usuário tenha permissão ao recurso, basta incluir o usuário no grupo, pois todos os usuários de um determinado grupo, herdam as permissões dos grupos aos quais o usuário pertence.

Quando um usuário troca de seção, por exemplo, basta trocar o usuário de grupo. Vamos supor que o usuário jsilva trabalha na seção de contabilidade e pertence ao grupo Contabilidade. Com isso ele tem acesso a todos os recursos para os quais o grupo Contabilidade tem acesso. Ao ser transferido para a seção de Marketing, basta retirar o usuário jsilva do grupo Contabilidade e adicioná-lo ao grupo Marketing. Com isso o jsilva deixa de ter as permissões atribuídas ao grupo Contabilidade e passa a ter as mesmas permissões que tem o grupo Marketing. Este exemplo simples já consegue demonstrar o quanto a utilização de grupos pode facilitar a administração de atribuição de permissões.

Vamos analisar mais um exemplo. Suponha que exista um sistema chamado SEAT, para o qual somente um número restrito de usuários deve ter acesso, sendo que são usuários de diferentes seções. A maneira mais simples de definir as permissões de acesso ao sistema SEAT é criar um grupo chamado Seat e dar permissões para esse grupo. Assim cada usuário que precisar acessar o sistema SEAT, deve ser incluído no grupo Seat. Quando o usuário não deve mais ter acesso ao sistema SEAT, basta removê-lo do grupo Seat. Simples, fácil e muito prático.

Na Figura 14.6 apresento uma ilustração para o conceito de Grupo de usuários. O Grupo Contabilidade possui direito para um recurso compartilhado, o qual pode ser acessado através da rede. Todos os usuários que pertencem ao grupo contabilidade, também possuem permissão para o recurso compartilhado, uma vez que os usuários de um grupo, herdam as permissões do grupo.

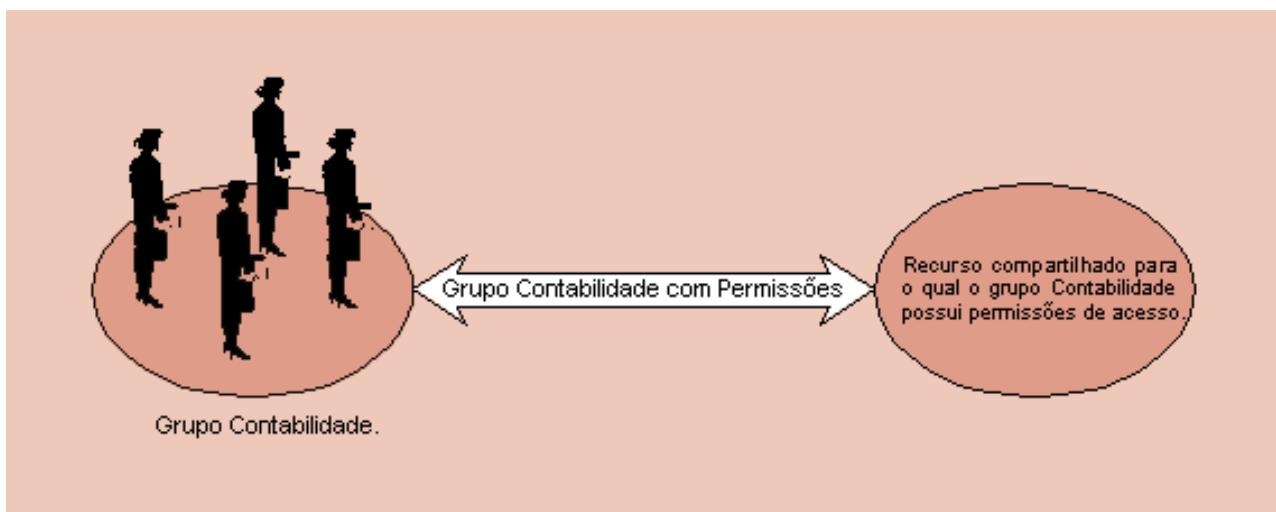


Figura 14.6 O Usuário herda as permissões do grupo.

Quando estiver trabalhando com grupos de usuários, considere os fatos a seguir:

- ◆ Grupos são uma coleção de contas de usuários.
- ◆ Os membros de um grupo, herdam as permissões atribuídas ao grupo.
- ◆ Os usuários podem ser membros de vários grupos
- ◆ Grupos podem ser membros de outros grupos.
- ◆ Contas de computadores podem ser membros de um grupo (novidade do Windows Server 2003).

Agora vou falar sobre os tipos de grupos existentes no Windows Server 2003. Os grupos são classificados de acordo com diferentes critérios, tais como: tipo, escopo e visibilidade.

Podemos ter dois tipos de grupos no Windows Server 2003 : Grupos de segurança ( Security Groups) e Grupos de distribuição (Distribution Groups).

#### Classificação dos grupos quanto ao tipo:

- ◆ Grupos de segurança: Normalmente utilizado para atribuir permissões de acesso aos recursos da rede. Por exemplo, ao criar um grupo Contabilidade, o qual conterá todas as contas dos funcionários do departamento de contabilidade, o qual será utilizado para atribuir permissões de acesso a uma pasta compartilhada, devo criar este grupo como sendo do tipo Grupo de segurança. Um grupo de segurança também pode ser utilizado como um grupo de distribuição, embora essa não seja uma situação muito comum. Esses grupos, assim como as contas de usuários são armazenados no Banco de dados do Active Directory.
- ◆ Grupos de distribuição: São utilizados para funções não relacionadas com segurança ( atribuição de permissões) . Normalmente são utilizados em conjunto com servidores de e-mail, tais como o Exchange 2000, para o envio de e-mail para um grupo de usuários. Uma das utilizações típicas para um Grupo de distribuição é o envio de mensagens de e-mail para um grupo de usuários de uma só vez. Somente programas que foram programados para trabalhar com o Active Directory, poderão utilizar Grupos de distribuição (como é o caso do Exchange 2000 citado anteriormente). Provavelmente as novas versões dos principais sistemas de correio eletrônico estarão habilitadas para trabalhar com o Active Directory. Não é possível utilizar grupos de distribuição para funções relacionadas com segurança.

#### Classificação dos grupos quanto ao Escopo:

Quando criamos um grupo de usuários, devemos selecionar um tipo (descrito anteriormente) e um escopo. O Escopo permite que o grupo seja utilizado de diferentes maneiras para a atribuição de permissões. O escopo de um grupo, determina em partes do domínio ou de uma floresta de domínios, o grupo é visível, ou seja, pode ser utilizado para receber permissões de acesso aos recursos da rede.

Existem três escopos para grupos de usuários, conforme descrito a seguir: Universal, Global e Local do domínio. Vamos apresentar as diversas características e usos de cada tipo de grupo.

#### Grupos universais (Universal group):

Como o próprio nome sugere são grupos que podem ser utilizados em qualquer parte de um domínio ou da árvore de domínios e podem conter como membros, grupos e usuários de quaisquer domínios. Em resumo:

**IMPORTANTE:** Para o exame é fundamental importância que você conheça, bem, os diferentes tipos e escopos de grupo de usuários, disponíveis no Windows Server 2003. Também é importante que você saiba quais objetos podem ser membros de cada tipo de grupo e quando utilizar cada tipo. Estes conceitos serão salientados em alguns estudos de caso, mais adiante, neste resumo.

**IMPORTANTE:** Não esqueça que não é possível atribuir permissões de acesso, quer seja permissões de compartilhamento, permissões NTFS ou permissões de impressão, para grupos do tipo Grupo de Distribuição. Só é permitido atribuir permissões de acesso para grupos do tipo Grupo de Segurança. Não esqueça deste detalhe.

**IMPORTANTE:** É possível converter um grupo do tipo Segurança para distribuição e vice-versa. Para tal é preciso que o domínio esteja, pelo menos, no modo Windows 2000 Nativo. Para domínios que ainda estejam no modo Windows 2000 Mixed, esta conversão não será possível. Mais adiante falarei sobre Modos de um Domínio e Modos de uma Árvore de Domínios. Este é outro detalhe que você não deve esquecer, de jeito nenhum.

- ◆ Pode conter: Contas de usuários, outros grupos universais, e grupos globais de qualquer domínio.
- ◆ Pode ser membro de: Grupos locais do domínio ou grupos universais de qualquer domínio.
- ◆ Pode receber permissões para recursos localizados em qualquer domínio.

Conforme detalharei mais adiante, um domínio baseado no Active Directory pode estar em diferentes modos (Windows 2000 Nativo, Misto ou Windows Server 2003). Para cada modo existem diferentes possibilidades em relação aos grupos Universais:

- ◆ Quando o nível de funcionalidade do Domínio está configurado como Windows 2000 Nativo ou Windows Server 2003, os seguintes elementos podem ser incluídos como membros de um grupo universal: Usuários, grupos Globais e grupos Universais de qualquer domínio da floresta.
- ◆ Quando o nível de funcionalidade do Domínio está configurado como Windows 2000 Misto, não é possível criar grupos Universais. Este é outro detalhe de grande importância, ou seja, não é possível o uso de grupos Universais, quando o modo do domínio for Modo Misto. Não esqueça, de jeito nenhum, deste detalhe.
- ◆ Quando o nível de funcionalidade do Domínio está configurado como Windows 2000 Nativo ou Windows Server 2003, um grupo Universal pode ser colocado como membro de um outro grupo Universal e permissões podem ser atribuídas em qualquer domínio.
- ◆ Um grupo pode ser convertido de Universal para Global ou de Universal para Local do domínio. Nos dois casos esta conversão somente pode ser feita se o grupo Universal não tiver como um de seus membros, outro grupo Universal.

### **Quando devemos utilizar grupos universais:**

Quando você deseja consolidar diversos grupos globais. Você pode fazer isso criando um grupo Universal e adicionando os diversos grupos globais como membros do grupo Universal.

### **Grupo global:**

Um grupo Global é “global” quanto aos locais onde ele pode receber permissões de acesso, ou seja, um grupo Global pode receber permissões de acesso em recursos (pastas compartilhadas, impressoras, etc) de qualquer domínio. Em resumo, considere as afirmações a seguir:

- ◆ Pode conter: Contas de usuários e grupos globais do mesmo domínio, ou seja, somente pode conter membros do domínio no qual o grupo é criado.
- ◆ Pode ser membro de: Grupos universais e Grupos locais do domínio, de qualquer domínio.

### **Grupos globais do mesmo domínio.**

- ◆ Pode receber permissões para recursos localizados em qualquer domínio.

Conforme detalharei mais adiante, um domínio baseado no Active Directory pode estar em diferentes modos (Windows 2000 Nativo, Misto ou Windows Server 2003). Para cada modo existem diferentes possibilidades em relação aos grupos Globais:

- ◆ Quando o nível de funcionalidade do Domínio está configurado como Windows 2000 Nativo ou Windows Server 2003, os seguintes elementos podem ser incluídos como membros de um grupo Global: contas de usuários e grupos globais do mesmo domínio. Por exemplo, se você cria um grupo global chamado WebUsers, no domínio abc.com.br, este grupo poderá conter como membros, grupos globais do domínio abc.com.br e usuários do domínio abc.com.br

- ◆ Quando o nível de funcionalidade do Domínio está configurado como Windows 2000 Misto, somente contas de usuários do próprio domínio é que podem ser membros de um grupo Global.

Por exemplo, se você cria um grupo global chamado WebUsers, no domínio abc.com.br e este domínio está no modo Misto, então somente contas de usuários do domínio abc.com.br é que poderão ser membros do grupo WebUsers.

- ◆ Um grupo pode ser convertido de Global para Universal, desde que o grupo Global não seja membro de nenhum outro grupo Global.

#### **Quando devemos utilizar grupos globais:**

Os grupos Globais devem ser utilizados para o gerenciamento dos objetos que sofrem alterações constantemente, quase que diariamente, tais como contas de usuários e de computadores. As alterações feitas em um grupo Global são replicadas somente dentro do domínio onde foi criado o grupo Global e não através de toda a árvore de domínios. Com isso o volume de replicação é reduzido, o que permite a utilização de grupos Globais para a administração de objetos que mudam freqüentemente.

#### **Grupos locais do domínio (Domain local group):**

São grupos que somente podem receber permissões para os recursos do domínio onde foram criados, porém podem ter como membros, grupos e usuários de outros domínios. Em resumo:

- ◆ Pode conter membros de qualquer domínio.
- ◆ Somente pode receber permissões para o domínio no qual o grupo foi criado.
- ◆ Pode conter: Contas de usuários, grupos universais e grupos globais de qualquer domínio.

#### **Outros grupos Locais do próprio domínio.**

- ◆ Pode ser membro de: Grupos locais do próprio domínio.

Conforme detalharei mais adiante, um domínio baseado no Active Directory pode estar em diferentes modos (Windows 2000 Nativo, Misto ou Windows Server 2003). Para cada modo existem diferentes possibilidades em relação aos grupos Globais:

- ◆ Quando o nível de funcionalidade do Domínio está configurado como Windows 2000 Nativo ou Windows Server 2003, os seguintes elementos podem ser incluídos como membros de um grupo Local: contas de usuários, grupos universais e grupos globais de qualquer domínio. Outros grupos locais do próprio domínio.
- ◆ Um grupo pode ser convertido de Local para Universal, desde que o grupo não tenha como seu membro um outro grupo Local.

#### **Quando devemos utilizar grupos Locais:**

Os grupos Locais são utilizados para atribuir permissões de acesso aos recursos da rede. Conforme discutirei mais adiante, a Microsoft recomenda uma estratégia baseada nos seguintes passos:

#### **Criar as contas de usuários.**

- ◆ Adicionar as contas de usuários a grupos Globais (confere com o que foi dito anteriormente, onde falei que os grupos Globais são utilizados para gerenciar os objetos do dia-a-dia, tais como contas de usuários).
- ◆ Adicione os grupos globais ou Universais (se for o caso) como membros dos grupos Locais.
- ◆ Atribua permissões de acesso para os grupos Locais.

# Atribuição de permissões em múltiplos domínios – estudos de caso.

Neste tópico vou analisar um exemplo de uma rede onde existe uma árvore de domínios, ou seja, vários domínios formando uma árvore de domínios. Com base no diagrama apresentado na Figura 14.7, apresento alguns estudos de caso logo em seguida.

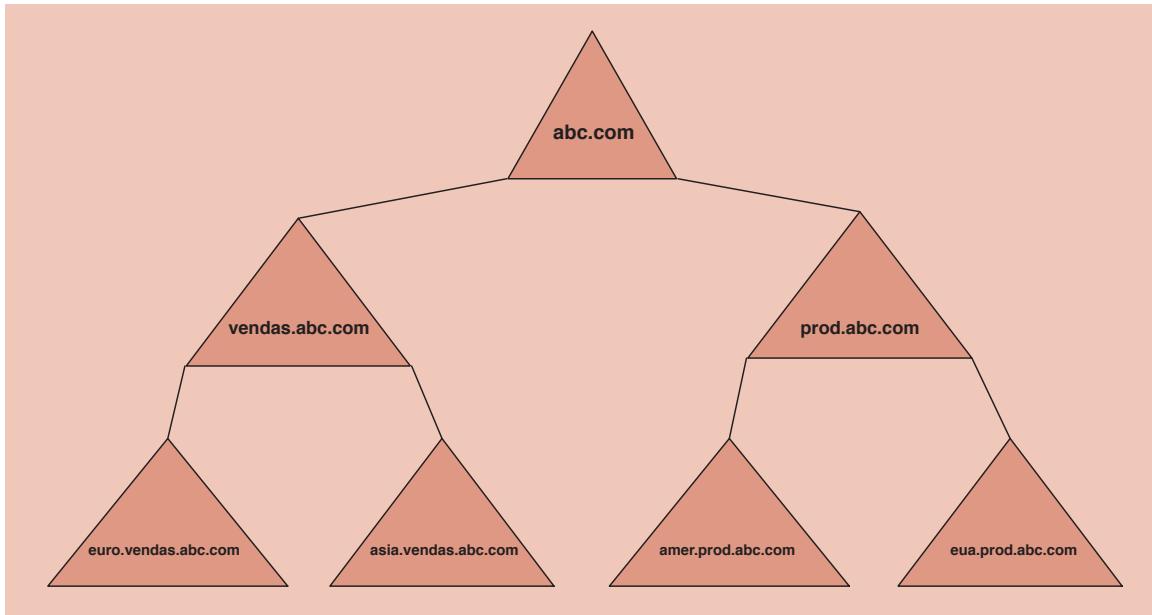


Figura 14.7 Uma árvore de domínios.

## Uma árvore com sete domínios:

No diagrama proposto na Figura 14.7, é exibida uma árvore com sete domínios. O domínio principal, também conhecido como domínio root tem o nome DNS: abc.com. Um domínio tem normalmente dois nomes:

- ◆ O nome DNS, que é o nome completo, no padrão do DNS. No nosso exemplo temos os domínios: abc.com, vendas.abc.com, prod.abc.com e assim por diante.
- ◆ O nome NETBIOS do domínio, que normalmente é a primeira parte do nome DNS. No nosso exemplo temos os domínios: ABC, VENDAS, PROD, EURO e assim por diante.

Observe que a árvore forma um espaço contínuo de nomes, conforme descrito anteriormente. Cada domínio filho contém o nome completo do domínio pai. Veja a descrição a seguir:

Domínio root – principal:

**abc . com**

Domínios de segundo nível, “filhos” do abc.com – contém abc.com no nome:

**vendas . abc . com**

**prod . abc . com**

Domínios de terceiro nível, “filhos” dos domínios de segundo nível – contém o nome do domínio de segundo nível:

**Filhos do vendas . abc . com:**

euro.vendas.abc.com

asia.vendas.abc.com

Filhos do prod.abc.com:

amer.prod.abc.com

eua.prod.abc.com

Neste exemplo temos uma árvore com sete domínios. Este é um exemplo de árvore de domínios perfeitamente possível de ser implementada com o uso do Windows Server 2003 e do Active Directory. Nesta árvore o primeiro domínio a ser instalado deve ser o domínio root: abc.com. Em seguida um dos domínios filhos, por exemplo vendas.abc.com e assim por diante.

## Um pouco sobre nomenclaturas de objetos no domínio, LDAP e caminhos UNC:

O Active Directory além de uma base de dados e um conjunto de serviços, também interage e depende de vários outros serviços e padrões para o seu completo funcionamento. Já citamos anteriormente que o DNS é o serviço de resolução de nomes no qual se baseia o Active Directory. O Active Directory foi projetado baseado em padrões de diretórios, definidos por entidades internacionais de padronização.

Entidades internacionais tais como a International Telecommunication Union (ITU), International Organization for Standardization (ISSO) e o Internet Engineering Task Force (IETF) trabalham em conjunto ou em colaboração para definir uma série de padrões que dão suporte a serviços de diretórios.

Um padrão de uso genérico é o X.500. Este padrão apesar de sua grande abrangência é bastante complexo e acabou por não ser adotado na sua íntegra como um padrão de mercado para a criação de serviços de diretórios. Um padrão mais “light” e que efetivamente tornou-se um padrão de mercado é o LDAP – Lightweight Directory Access Protocol. O protocolo LDAP fornece mecanismos de acesso aos objetos do Active Directory, de tal maneira que qualquer programa ou sistema habilitado ao padrão LDAP, seja capaz de acessar as informações do Active Directory, desde que devidamente identificado e tendo as devidas permissões. No início do capítulo, quando falei sobre diretórios, múltiplas senhas e afirmei que a visão de futuro da Microsoft é uma empresa onde todos os sistemas sejam integrados com o Active Directory, eu estava pensando no padrão LDAP. Com o uso deste padrão, é possível desenvolver sistemas integrados com o Active Directory.

O padrão LDAP define um sistema de nomeação hierárquico, através do qual é possível referenciar qualquer objeto do Active Directory. Você deve estar pensando que o LDAP e o DNS estão sendo utilizados para a mesma função. Não é exatamente isso. Sem entrar nas especificações técnicas de cada protocolo, arrisco a fazer as seguintes colocações:

- ◆ O DNS é o sistema de resolução de nomes utilizado pelos clientes para localizar recursos na rede, tais como o nome de um servidor ou uma pasta compartilhada em um servidor.
- ◆ O LDAP é um padrão para acesso e referência aos objetos do Active Directory. Com base neste padrão é possível criar APIs (Application Program Interfaces) que facilitam a criação de aplicações integradas ao Active Directory.

Um nome LDAP é formado pelo caminho completo do objeto, partindo do domínio raiz, até chegar ao objeto referenciado. Nesta nomenclatura hierárquica são utilizados algumas abreviaturas, conforme descrito a seguir:

- ◆ **CN:** common name: por exemplo, o nome da conta de um usuário, grupo ou computador.
- ◆ **OU:** faz referência a uma unidade organizacional.
- ◆ **DC:** um componente de domínio. Normalmente o nome de um domínio.

- ◆ **O:** Nome da organização. Normalmente representado pelo nome do domínio Root.
- ◆ **C: Country:** Identificação de país. Não é normalmente utilizado.

Para entender como é formado um nome LDAP, é melhor analisarmos alguns exemplos. Considere os exemplos a seguir:

- ◆ CN=jsilva,OU=contabilidade,DC=vendas,DC=abc.com -> Este nome representa o usuário jsilva, cuja conta está contida na unidade organizacional contabilidade, no domínio vendas.abc.com (observe que juntamos os dois componentes de domínio).]
- ◆ CN=maria,OU=auditoria,OU=financias,DC=euro,DC=vendas,DC=abc.com -> Este nome representa o usuário maria, cuja conta está contida na unidade organizacional auditoria, a qual está contida dentro da unidade organizacional financias do domínio euro.vendas.abc.com.

Conforme já descrito anteriormente, os nomes LDAP e o protocolo LDAP são importantes para quem pretende desenvolver aplicações integradas com o Active Directory. Para efeitos de localização de recursos e identificação de objetos da rede, interessa mais o nome DNS e a nomenclatura de objetos do domínio, conforme descreverei logo a seguir.

A nomenclatura para localização de recursos em um servidor segue o padrão UNC Universal Naming Convention. Neste padrão um recurso é identificado pelo nome do servidor, separado do nome do recurso por uma barra. Considere os exemplos a seguir:

**\server01.vendas.abc.com\documentos**

Este é o caminho para uma pasta compartilhada com o nome de compartilhamento “documentos”, no servidor server01 do domínio vendas.abc.com. Ao invés do nome DNS do servidor também poderia ser utilizado o número IP do servidor, como no exemplo a seguir:

**\10.10.20.5\documentos**

Outro exemplo:

**\pr-server.prod.abc.com\laser01**

Este é o caminho para uma impressora compartilhada com o nome de compartilhamento “laser01”, no servidor pr-server do domínio prod.abc.com. Ao invés do nome DNS do servidor também poderia ser utilizado o número IP do servidor, como no exemplo a seguir:

**\10.10.30.5\laser01**

Outro ponto que convém ser abordado neste momento é a nomenclatura simplificada de identificação dos usuários. Considere o exemplo a seguir:

**vendas.abc.com\jsilva**

Este nome faz referência ao usuário jsilva do domínio vendas.abc.com. Outra forma de referência seria utilizar apenas o nome NETBIOS do domínio, ao invés do nome DNS completo, como no exemplo a seguir:

**VENDAS\jsilva**

O padrão é NomeDoDomínio\NomeDoObjeto

---

**NOTA:** Você utilizará nomes no padrão UNC em diversos exemplos práticos, ao longo dos demais capítulos deste livro.

---

## Estudo de caso 01: Exemplo de uso de Grupos Universais:

Para este primeiro estudo de caso vamos imaginar a árvore de domínios indicada na Figura 14.8, onde todos os domínios estão no modo Windows Server 2003, o que implica que é possível a utilização de grupos Universais.

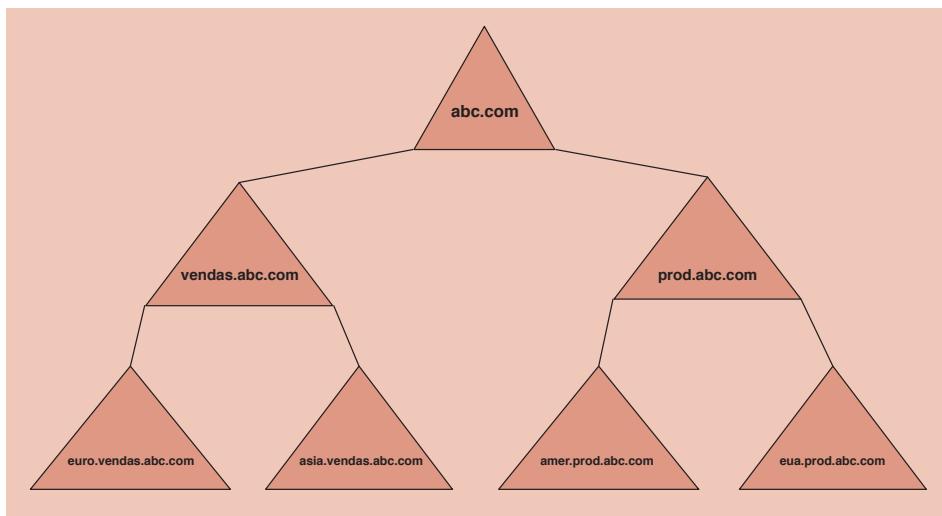


Figura 14.8 Uso de grupos Universais.

Neste exemplo, existe uma aplicação Web no servidor srv01.abc.com. Esta aplicação exige que o usuário seja autenticado antes de ter acesso a aplicação. Esta exigência é para que possa ser registrado no log do servidor, as ações realizadas por cada usuário. Em cada domínio, apenas alguns usuários, de diferentes seções, deverão ter permissão de acesso a esta aplicação. Qual a solução recomendada para simplificar a administração deste sistema de permissões de acesso?

Solução proposta: Este é um exemplo típico para o uso de uma combinação de Grupos Universais e Grupos Globais. Como os domínios estão no modo Windows Server 2003, é possível a criação de Grupos Universais (o que também seria possível se os domínios estivessem no modo Windows 2000 Nativo). Em cada domínio você cria um grupo Global. É aconselhável que o nome do grupo seja descritivo do seu objetivo. Você adiciona os usuários que devem ter acesso a aplicação Web, como membros do grupo Global do seu respectivo domínio. No domínio abc.com você cria um grupo Universal e, adiciona como membros deste grupo, o grupo global de cada domínio, grupos estes criados anteriormente e aos quais foram adicionados os usuários que devem ter acesso a aplicação Web. No servidor srv01.abc.com você atribui as permissões necessárias ao grupo Universal criado no domínio abc.com (do qual são membros os respectivos grupos globais de cada domínio).

Ao atribuir as permissões necessárias ao grupo universal do domínio abc.com, os grupos globais que são membros deste grupo irão herdar as mesmas permissões, as quais serão herdadas pelos membros do grupo. Observe que o efeito de atribuir a permissão ao grupo universal no domínio abc.com é que esta permissão propaga-se até os usuários em seus respectivos domínios.

**IMPORTANTE:** Esta nomenclatura também pode ser utilizada para referencia contas locais em um Member Server ou em uma estação de trabalho. Por exemplo, para fazer referência a conta Administrador, do Member Server srv01, você utiliza a seguinte nomenclatura: srv01\ Administrador.

Agora que já apresentei os aspectos básicos de nomeação de objetos e recursos no Active Directory, é hora de apresentar alguns estudos de casos, para que você possa entender, na prática, os escopos de grupos (Universal, Global e Local) e como é feita a utilização de grupos para simplificar o processo de atribuição de permissões de acesso aos recursos da rede.

Dando nome aos grupos e dividindo a solução em etapas, poderíamos descrever a solução proposta da seguinte maneira:

- ◆ Criar um grupo global em cada um dos domínios, conforme sugestão a seguir:

| Domínio             | Nome do Grupo Global                 |
|---------------------|--------------------------------------|
| abc.com             | G-Glob-abc-com-AcessoWeb             |
| vendas.abc.com      | G-Glob-vendas-abc-com-AcessoWeb      |
| euro.vendas.abc.com | G-Glob-euro-vendas-abc-com-AcessoWeb |
| asia.vendas.abc.com | G-Glob-asia-vendas-abc-com-AcessoWeb |
| prod.abc.com        | G-Glob-prod-abc-com-AcessoWeb        |
| amer.prod.abc.com   | G-Glob-prod-amer-abc-com-AcessoWeb   |
| eua.prod.abc.com    | G-Glob-prod-eua-abc-com-AcessoWeb    |

- ◆ Em cada domínio você inclui os usuários que devem ter acesso à aplicação Web, ao grupo global do respectivo domínio, criado no passo anterior.
- ◆ Crio um grupo Universal no domínio abc.com:  
Domínio Nome do Grupo Universal  
abc.com G-Univ-abc-com-AcessoWeb
- ◆ Incluo os grupos globais criados na primeira etapa como membros do grupo Universal:
- ◆ Membros do grupo G-Univ-abc-com-AcessoWeb:  
*G-Glob-abc-com-AcessoWeb  
G-Glob-vendas-abc-com-AcessoWeb  
G-Glob-euro-vendas-abc-com-AcessoWeb  
G-Glob-asia-vendas-abc-com-AcessoWeb  
G-Glob-prod-abc-com-AcessoWeb  
G-Glob-prod-amer-abc-com-AcessoWeb  
G-Glob-prod-eua-abc-com-AcessoWeb*
- ◆ Pronto, está implementada a solução para definição das permissões de acesso a aplicação Web no servidor srv01.abc.com. Com esta solução, sempre que um usuário precisar de acesso à aplicação Web, basta incluí-lo no grupo global do seu respectivo domínio. Se o usuário não deve mais ter acesso à aplicação, basta retirá-lo do respectivo grupo global. Observe que a administração das permissões fica bem simplificada. É uma simples questão de incluir ou retirar o usuário de um determinado grupo.

**NOTA:** Estas são apenas sugestões de nomes. Eu procurei utilizar nomes que identificassem que o grupo é do tipo Global, a qual domínio ele pertence e qual a sua finalidade.

## Estudo de caso 02: Analisando o escopo de grupos em relação a membros e permissões de acesso:

Para este estudo de caso vou continuar considerando a árvore de domínios da Figura 14.8. Vamos colocar algumas questões para análise:

Questão 01: Vamos supor que você crie um grupo Global chamado AcessoFinanç, no domínio vendas.abc.com. Considere os itens a seguir:

*O grupo AcessoFinança pode ter usuários e grupos de que domínio(os) como membros do grupo?*

Como o grupo AcessoFinança é Global e foi criado no domínio vendas.abc.com, ele somente pode conter como membros, usuários e outros grupos globais do próprio domínio vendas.abc.com. Esta é uma das características dos grupos Globais, ou seja, somente podem conter como membros, usuários e outros grupos globais do seu próprio domínio.

*Em qual ou quais domínios o grupo AcessoFinança pode receber permissões de acesso?*

Um grupo Global pode receber permissões de acesso a recursos em qualquer domínio na árvore de domínios. Normalmente para atribuir permissões a um grupo Global, em outro domínio, basta colocar o grupo Global como membro de um grupo Local do domínio de destino (onde está localizado o recurso) e atribuir permissão para o grupo Local. Este é o procedimento recomendado pela Microsoft. Por exemplo, vamos supor que o grupo global AcessoFinança, do domínio vendas.abc.com, precise de acesso a uma pasta compartilhada em um servidor do domínio prod.abc.com. O processo recomendado pela Microsoft é incluir o grupo global AcessoFinança, do domínio vendas.abc.com, como membro de um grupo local do domínio prod.abc.com e atribuir as permissões necessárias para este grupo local. Com isso o grupo global herda as permissões e todos os usuários do grupo Global também herdam as permissões.

Questão 02: Vamos supor que você crie um grupo Local chamado UsuáriosMemo, no domínio vendas.abc.com. Considere os itens a seguir:

*O grupo UsuáriosMemo pode ter usuários e grupos de que domínio(os) como membros do grupo?*

Como o grupo UsuáriosMemo é Local, ele pode ter como membros, usuários e grupos do seu próprio domínio e também usuários e grupos de outros domínios. Por exemplo, posso incluir um grupo global do domínio prod.abc.com, como membro de um grupo local do domínio vendas.abc.com.

*Em qual ou quais domínios o grupo UsuáriosMemo pode receber permissões de acesso?*

Como o grupo é Local ele somente pode receber permissões de acesso a recursos localizados em servidores do seu próprio domínio, ou seja, a recursos localizados em servidores do domínio vendas.abc.com, onde o grupo UsuáriosMemo foi criado.

Questão 03: Vamos supor que você crie um grupo Universal chamado AcessoWeb, no domínio abc.com. Considere os itens a seguir:

*O grupo AcessoWeb pode ter usuários e grupos de que domínio(os) como membros do grupo?*

De qualquer domínio, pois ele é um grupo Universal.

*Em qual ou quais domínios o grupo Acesso Web pode receber permissões de acesso?*

Em qualquer domínio, pois ele é um grupo Universal.

Agora é chegado o momento de analisar mais alguns elementos que formam a infra-estrutura que permite o funcionamento do Active Directory. Vou falar um pouco mais sobre Unidades organizacionais. Na seqüência falarei sobre Relações de confiança e florestas.

## Entendendo as Unidades organizacionais.

O conceito de Unidade organizacional foi introduzido no Windows 2000 Server, juntamente com o Active Directory e veio para solucionar um problema sério de Administração existente no Windows NT Server 4.0.

Com o NT Server 4.0, não havia como atribuir permissões de acesso apenas a uma parte do domínio. Ou você atribuía permissões de Administrador no domínio inteiro ou não tinha como atribuir permissões de administrador para um

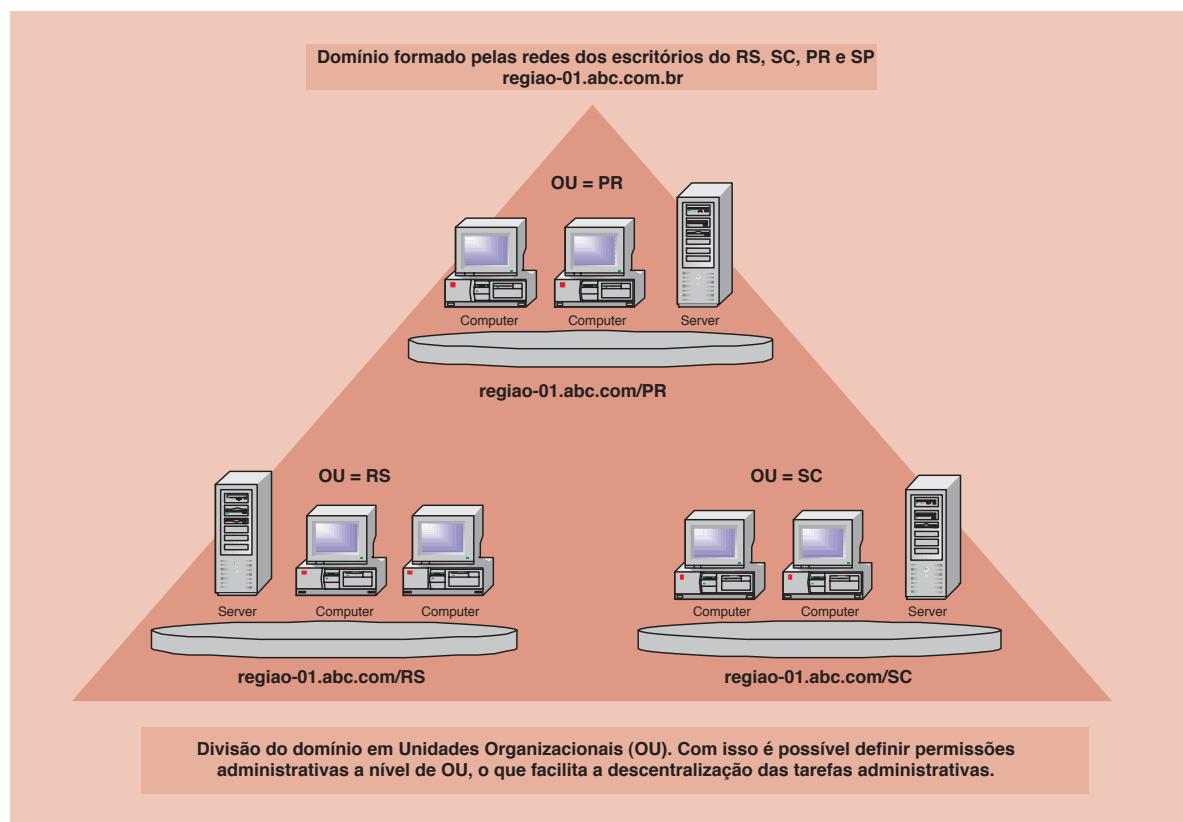
usuário. Imagine uma empresa que tem uma rede, com filiais em todos os estados brasileiros. Por questões de simplicidade vamos supor que a rede é composta de seis domínios, sendo que em cada domínio estão as filiais de 4 ou mais estados. Vamos supor que um dos domínios seja composto pelas redes das filiais do RS, SC, PR e SP. Com o NT Server 4.0, você não teria como definir que um usuário tivesse permissões de Administrador somente nos servidores da filial do RS. Uma vez que você atribuía permissões de Administrador, o usuário teria estas permissões em todos os recursos do domínio. No nosso exemplo, o usuário seria Administrador nos servidores das filiais do RS, SC, PR e SP, ou seja, em todos os servidores do domínio.

Esta situação gerava inconvenientes (e noites de sono perdidas) muito sérios. Era comum a situação onde um domínio tinha 10 ou mais contas de usuários com permissão de Administrador. Ora, eram 10 ou mais contas com permissões total em todos os servidores do domínio. Nada bom.

Com a disponibilidade de Unidades Organizacionais, a partir do Windows 2000 Server, este problema foi minimizado. Agora você pode criar, dentro do domínio, várias Unidades organizacionais. Em seguida você desloca para dentro de cada unidade organizacional, as contas de usuários e computadores, de acordo com critérios geográficos ou funcionais. Em seguida você pode delegar tarefas administrativas a nível de Unidade organizacional (OU – Organizational Unit).

Vamos considerar o exemplo anterior, onde tínhamos um domínio formado pelas redes das filiais do RS, SC, PR e SP. Neste exemplo, o Administrador do domínio poderia criar quatro unidades organizacionais:

RS  
SC  
PR  
SP



**Figura 14.9 Divisão de um domínio em OUs.**

Em seguida ele move as contas de usuários e computadores e contas de grupos para as respectivas OUs. O último passo é atribuir permissões de administração em cada OU. Por exemplo, para o Administrador da filial do RS, seriam delegadas permissões de administração na OU RS, para o Administrador da filial de SC, seriam delegadas permissões de administração na OU SC e assim por diante. O diagrama da Figura 14.9 ilustra a divisão de um domínio em OUs.

No diagrama está representada a divisão do domínio regiao-01.abc.com.br em OUs. Dentro de uma OU é possível criar outras OUs. Por exemplo, dentro da Unidade Organizacional RS, o administrador poderia criar outras unidades organizacionais, tais como: Usuários, Grupos e Computadores. Em seguida, todas as contas de usuários da filial do RS, seriam deslocadas para a OU Usuários, dentro da OU RS; todas as contas dos computadores da filial do RS seriam deslocadas para a OU Computadores, dentro da OU RS e assim por diante.

Observem que, basicamente, a utilização de OUs facilita a descentralização das tarefas administrativas, através da delegação de tarefas para porções específicas de um domínio. A utilização de OUs também desempenha um papel importante no gerenciamento das políticas de segurança, através do uso de Group Policies Objects (GPOs). Para um estudo completo de GPOs, consulte o Capítulo 18 do livro Windows Server 2003 – Curso Completo, 1568 páginas.

## Relações de confiança e florestas.

É através do uso de relações de confiança entre domínios, que é possível que um usuário de um domínio possa fazer o logon com sua conta de usuário e senha, mesmo utilizando um computador de um outro domínio. Por exemplo, o usuário jsilva está cadastrado no domínio A e viaja para a filial da empresa, a qual pertence ao domínio B. O usuário jsilva está utilizando um computador que faz parte do domínio B. Durante o processo de logon ele informa o seu nome de usuário, senha e seleciona o domínio no qual ele quer fazer o logon (no exemplo o domínio A) e consegue fazer o logon normalmente.

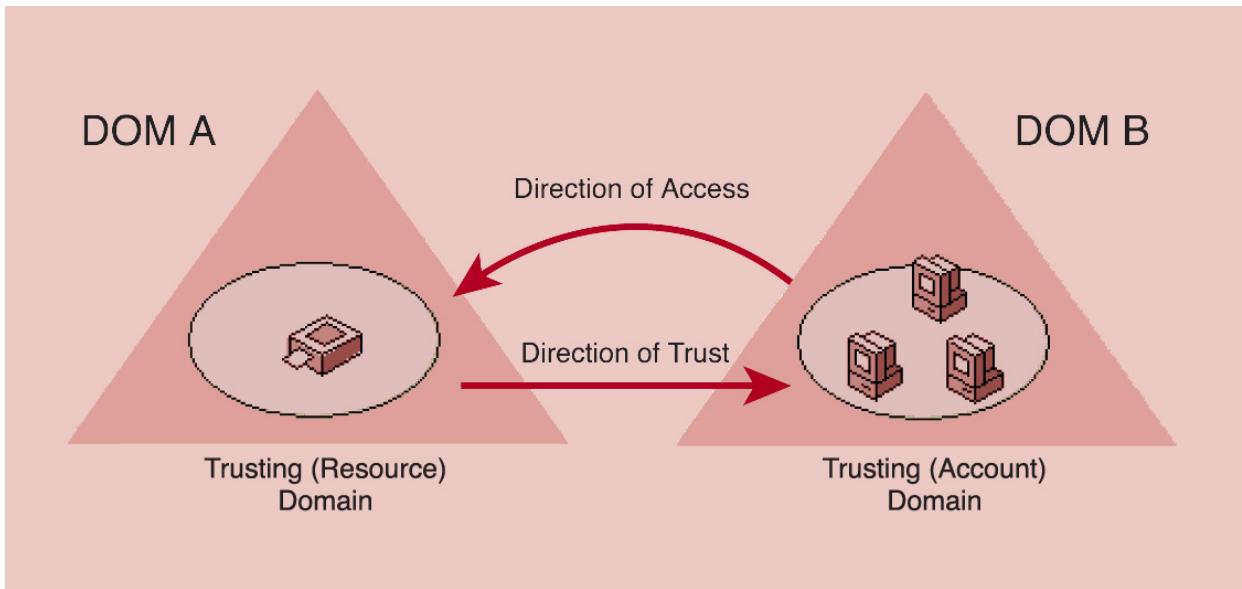
Como foi possível ao domínio B (mais especificamente a um DC do domínio B), verificar as credenciais do usuário (logon e senha) e permitir o logon? Isso foi possível graças ao mecanismo de relações de confiança existente no Windows Server 2003, o qual é muito semelhante ao que existe no Windows 2000 Server, porém completamente diferente do que acontecia no Windows NT Server 4.0. Neste item apresentarei em mais detalhes, o mecanismo de relações de confiança entre domínios no Windows Server 2003.

## Como eram as relações de confiança na época do NT Server 4.0?

As relações de confiança no NT Server 4.0 são definidas por três características principais:

- ◆ São unilaterais: Se o domínio A confia no domínio B, isso não significa que o domínio B confia no domínio A automaticamente. Para que haja essa confiança recíproca é preciso criar duas relações de confiança: uma para definir que o domínio A confia no domínio B e outra para definir que o domínio B confia no domínio A. A Figura 14.10, da ajuda do Windows Server 2003, ilustra este conceito:

Neste exemplo do Dom A confia no Dom B. Isso significa que as contas do Dom B são “visíveis” no Dom A, ou seja, é possível atribuir permissões de acesso para as contas do Dom B, em recursos do Dom A. O contrário não é verdadeiro, ou seja, não é possível atribuir permissões de acesso para as contas do Dom A, em recursos do domínio B. Para que isso fosse possível teria que ser criada mais uma relação de confiança, agora com o Dom B “confiando” nas contas do Dom A. Isso tudo acontece porque as relações de confiança no NT Server 4.0 são unilaterais.



**Figura 14.10 Relação de confiança unilateral.**

- ◆ Não são transitivas: Se o Dom A confia no Dom B e o Dom B confia no domínio C, isso não implica que o Dom A também confia no Dom C. Para que o Dom A confie no Dom C, uma relação de confiança entre os dois domínios tem que ser manualmente criada pelo Administrador.
- ◆ Devem ser criadas manualmente pelos Administradores: As relações de confiança não são criadas automaticamente e devem ser criadas pelos Administradores de cada domínio. O processo é bem trabalhoso. Para que o Dom A possa confiar no Dom B, primeiro o Administrador do Dom B tem que fazer uma configuração “dizendo” que ele aceita que o Dom A confie no Dom B. O próximo passo é o Administrador do Dom A estabelecer a relação de confiança com o Dom B. Para que o Dom B também possa confiar no Dom A, todo o processo (só que na direção inversa) tem que ser repetido.

Para uma rede com 10 domínios, para que todos possam confiar em todos os outros, são necessárias 90 relações de confiança. O número de relações de confiança, com base no número de domínios, pode ser calculada pela fórmula a seguir:

$$n * (n - 1)$$

onde n é o número de domínios.

Para 10 domínios teremos:

$$10 * (10 - 1)$$

$$10 * 9$$

$$90$$

A Figura 14.11, obtida do Resource Kit do Windows 2000 Server, mostra como seria uma árvore de domínios no NT Server 4.0, onde foram implementadas relações de confianças entre todos os domínios:

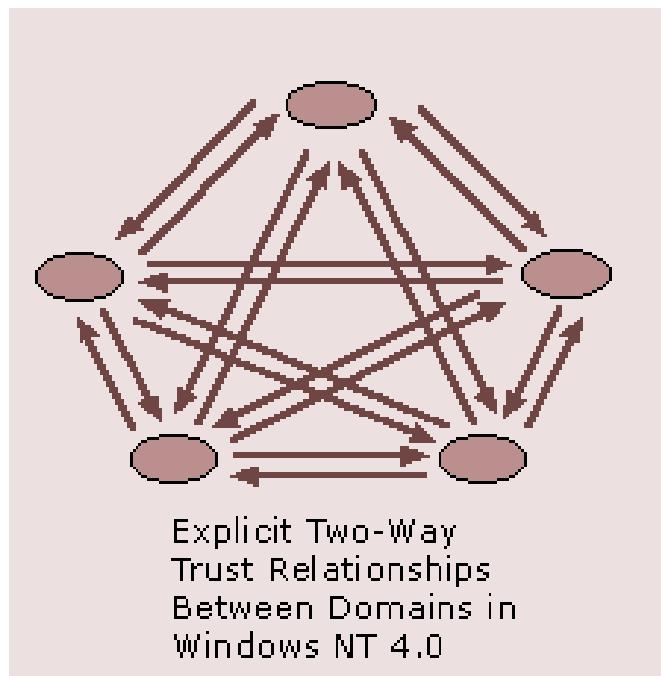


Figura 14.11 Relações de confiança unidirecionais, não transitivas do NT Server 4.0.

## E como são as relações de confiança no Windows Server 2003?

No Windows Server 2003 (bem como no Windows 2000 Server) as relações de confiança são criadas automaticamente entre os domínios de uma árvore de domínios. As relações são bi-direcionais, ou seja, se o Dom A confia no Dom A, isso significa que o Dom B também confia no Dom A. As relações de confiança são transitivas, ou seja se o Dom A confia no Dom B, o qual confia no Dom C, então o dom A também confia no Dom C e vice-versa. A Figura 14.12 ilustra as relações de confiança no Windows Server 2003.

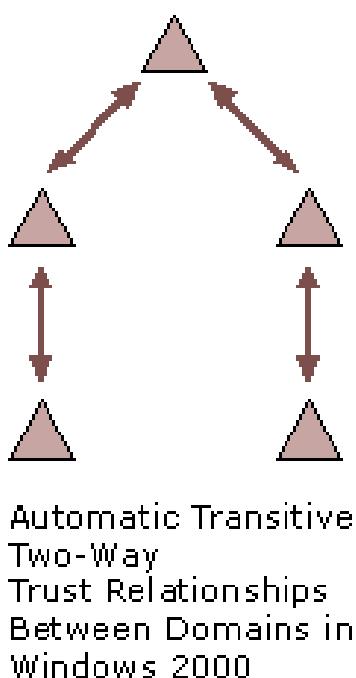


Figura 14.12 Relações de confiança bi-direcionais e transitivas do Windows Server 2003.

## **Outros tipos de relações de confiança:**

As relações de confiança criadas automaticamente, entre os domínios de uma árvore no Windows Server 2003, apresentam as características descritas anteriormente: Automaticamente criadas, bi-direcionais e transitivas.

Porém existem situações em que pode ser necessária a criação de outros tipos de relações de confiança. Por exemplo, pode ser necessária a criação de uma relação de confiança entre um dos domínios da sua rede, com um domínio baseado no Windows NT Server da rede de um fornecedor ou parceiro de negócio. Ou pode ser necessária a criação de uma relação de confiança entre um domínio da sua rede (baseado no Windows Server 2003) com um domínio da rede de outra empresa, também baseado no Windows Server 2003. Neste caso você teria que criar uma relação de confiança com um domínio em outra árvore de domínios. A seguir vou analisar e exemplificar os tipos de relações de confiança que existem.

### **Tipos padrão de relações de confiança:**

Existem dois tipos padrão de relação de confiança, conforme descrito a seguir:

- ◆ Transitiva bi-direcional entre um Domínio pai e um Domínio filho: Quando o Administrador cria um domínio filho, uma relação de confiança bi-direcional e transitiva é criada, automaticamente, pelo assistente de instalação do Active Directory. Por exemplo, se você tem um domínio root chamado abc.com e cria um domínio filho chamado vendas.abc.com, o assistente de instalação do Active Directory, automaticamente cria durante a criação do domínio vendas.abc.com, uma relação de confiança bi-direcional e transitiva entre os domínios abc.com e vendas.abc.com.
- ◆ Transitiva bi-direcional entre uma árvore de domínios e o domínio root de uma floresta: Você pode juntar várias árvores de domínios para formar um floresta. Este tipo de relação de confiança é automaticamente criado, quando você cria um novo domínio em uma floresta já existente. A relação é estabelecida.

### **Outros tipos de relações de confiança:**

Existem outros tipos padrão de relação de confiança, conforme descrito a seguir:

Externa, não transitiva, unidirecional ou bi-direcional: Este tipo de relacionamento é criado com um domínio externo, baseado no Windows NT Server 4.0 ou com um domínio baseado no Windows Server 2003 ou Windows 2000 Server, localizado em outra floresta. Se o domínio for baseado no NT Server 4.0 a relação será unidirecional, caso contrário será bi-direcional.

O exemplo da Figura 4.13 ilustra bem as situações onde pode ser criada uma relação de confiança deste tipo.

- ◆ Realm, transitiva ou não transitiva, unidirecional ou bi-direcional: Este tipo de relação é criado entre um domínio baseado no Windows Server 2003 e outros domínios, também baseados no protocolo Kerberos, como por exemplo o UNIX. O protocolo Kerberos é um padrão de fato que fornece, dentre outros, serviços de autenticação em um domínio do Windows 2000 Server ou Windows Server 2003. Outros sistemas operacionais também utilizam o Kerberos. Este tipo de relacionamento poderia ser utilizado, por exemplo, para que as contas de um domínio baseado no UNIX, pudessem receber permissões de acesso em recursos de um domínio baseado no Windows Server 2003.
- ◆ Entre florestas, transitiva, unidirecional ou bi-direcional: Este tipo de relacionamento é criado entre os domínios root de duas florestas. Pode ser do tipo unidirecional ou bi-direcional. Se for do tipo bi-direcional, os usuários de uma floresta podem acessar recursos nos domínios da outra floresta e vice-versa. Um exemplo prático de uso deste tipo de relação de confiança seria quando é feita a fusão de duas empresas e você precisa permitir que os usuários de uma empresa possam acessar recursos nos servidores da rede da outra empresa e vice-versa.

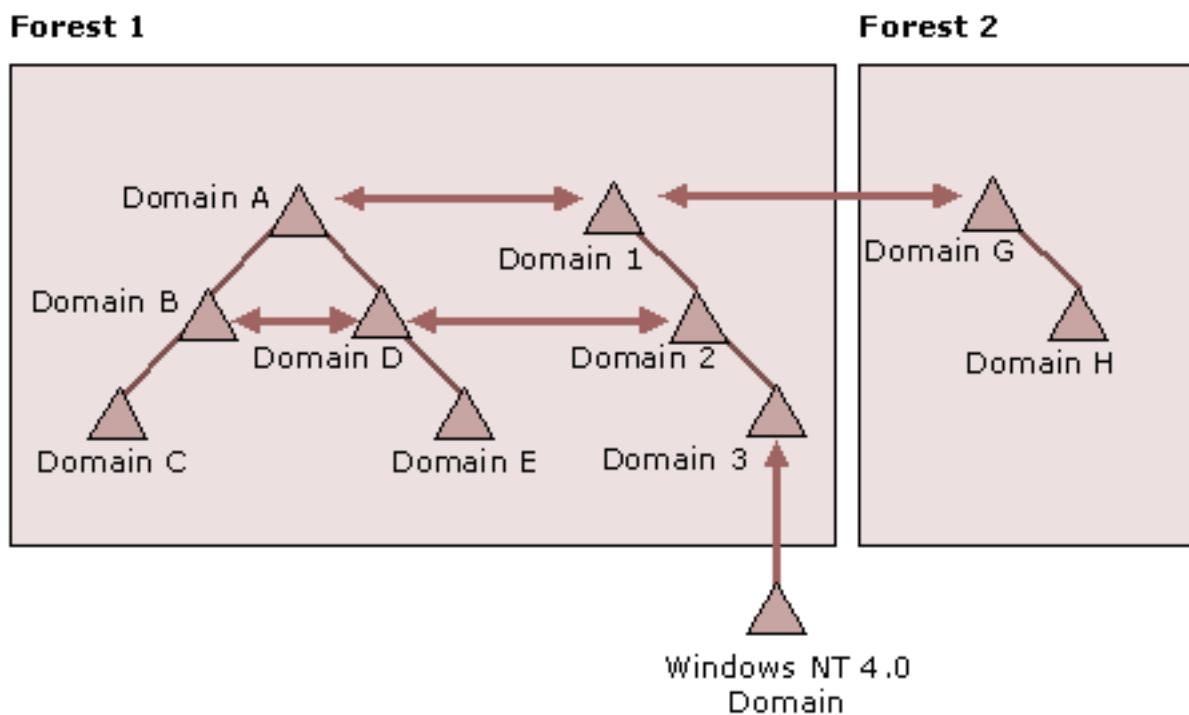


Figura 4.13 Relações de confiança externas – unidirecional ou bi-direcional.

- ◆ Shortcut, transitiva, unidirecional ou bi-direcional: Este tipo de relação de confiança é utilizado para melhorar o tempo de logon entre dois domínios, em uma floresta. Considere o exemplo da Figura 4.14:

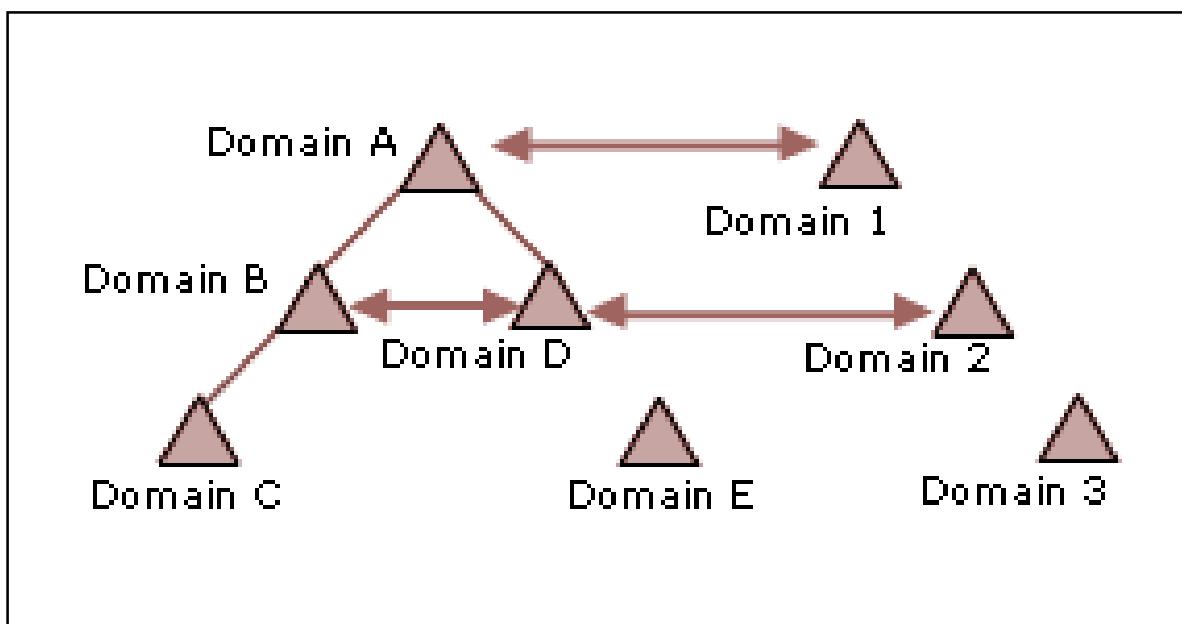


Figura 414 Relações de confiança do tipo Shortcut (atalho).

Neste exemplo foram criadas três relações de confiança do tipo Shortcut:

- ◆ Entre os domínios B e D.
- ◆ Entre os domínios A e 1.

- ◆ Entre os domínios D e 2.

O principal objetivo deste tipo de relação de confiança é otimizar os tempos de logon. No exemplo da Figura 2.13, vou analisar o que acontece quando um usuário do Dom B precisa acessar um recurso no Dom D. O primeiro passo é autenticar o usuário. Se não houver a relação do tipo Shortcut entre B e D, o Windows Server 2003 precisa percorrer o caminho de relações de confiança na árvore (De B para A e da A para D), para poder autenticar o usuário do domínio D. Já com a relação do tipo shortcut entre B e D, existe um caminho direto entre estes dois domínios, o que diminui o tempo de logon/autenticação. Quanto mais afastados (quanto maior o caminho e o número de relações de confiança a ser percorrido), mais será reduzido o tempo de logon entre os domínios, se o Administrador criar uma relação de confiança do tipo Shortcut.

## Servidores de Catálogo Global (Global Catalogs)

Pelo que foi visto até aqui, é possível perceber que o Active Directory no Windows Server 2003 é bastante flexível, permitindo que usuários de um domínio acessem recursos em servidores de outro domínio ou até mesmo outra floresta, sem ter que entrar novamente com o seu login e senha. Para que isso seja possível, o Active Directory mantém uma base com algumas informações sobre objetos de todos os domínios. Esta base de informações é mantida em Controladores de Domínio (DCs), configurados para atuar como Servidores de Catálogo Global (Global Catalog Servers). Nem todo DC é um Global Catalog, mas para ser Global Catalog tem que ser um DC, não pode ser um Member Server. Neste item vou apresentar informações detalhadas sobre os Servidores de Catálogo Global.

**IMPORTANTE:** Só faz sentido criar este tipo de relação de confiança, se for comum usuários de um domínio acessarem recursos do outro domínio e se o tempo de logon estiver apresentando tempos muito elevados.

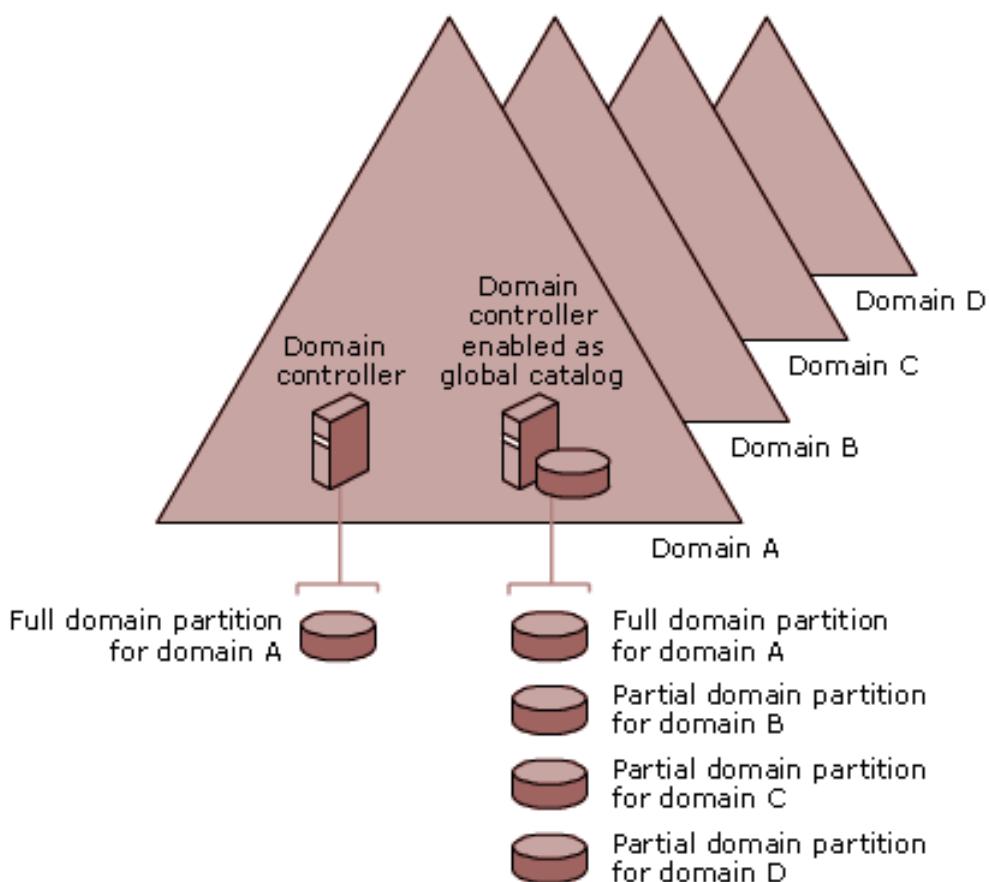


Figura 4.15 Informações armazenadas em um Servidor de Catálogo Global.

Um Servidor de Catálogo Global armazena uma cópia de todos os objetos do Active Directory, de todos os domínios em uma ou mais árvores de domínios de uma floresta. No Servidor de Catálogo Global fica uma cópia completa de todos os objetos do próprio domínio do servidor e uma cópia parcial de todos os objetos dos demais domínios. Esta estrutura é indicada na Figura 14.15:

Observe que um servidor que é DC mas não está configurado como Servidor de Catálogo Global, contém uma cópia completa de todos os objetos do seu domínio, mas não tem cópia de objetos de outros domínios. Já um DC habilitado como Servidor de Catálogo Global, tem, além da cópia completa dos objetos do seu próprio domínio, cópias parciais de todos os objetos dos demais domínios. Quando se fala em cópias parciais, significa que o Servidor de Catálogo Global mantém cópia de todos os objetos, mas não de todos os atributos de um objeto de outro domínio. Por exemplo, o Servidor de Catálogo Global tem cópia de todos os usuários de outros domínios, mas para cada usuário apenas alguns atributos (nome, senha, etc) são armazenados no Catálogo Global e não todos os atributos.

Os atributos de cada objeto que são copiados para o Catálogo Global são aqueles atributos mais utilizados para a realização de pesquisas no Active Directory. Por exemplo nome do usuário, nome de compartilhamento e tipo da impressora e assim por diante. A definição de quais atributos são armazenados no Catálogo Global e quais não são é feita no Schema. Conforme mostrarei mais adiante o Schema é como se fosse (na prática eu considero que é) a definição da estrutura do banco de dados do Active Directory. Falarei mais sobre Schema no próximo item.

Ao armazenar os atributos mais utilizados no Catálogo Global, o Windows Server 2003 aumenta o desempenho das pesquisas no Active Directory. Se não houvesse um Catálogo Global, as pesquisas teriam que percorrer todo o caminho da rede, da origem, até encontrar um servidor (um DC) no domínio de destino e os resultados percorrer o caminho inverso. Em redes maiores, com mais domínios, isso representaria um sério problema de desempenho, além de gerar um excessivo tráfego de rede. Evidentemente que a manutenção do Catálogo Global atualizado em todos os Servidores de Catálogo Global, gera tráfego de replicação, mas o resultado final é um ganho de performance e redução do tráfego de rede, em comparação se não existisse o Catálogo Global.

Quando um domínio é criado, com a instalação do primeiro DC do domínio, este DC é automaticamente configurado com Servidor de Catálogo Global. Os próximos DCs do domínio não serão automaticamente configurados como Servidor de Catálogo Global, mas você poderá configurá-los posteriormente.

## Principais funções desempenhadas por um Servidor de Catálogo Global:

Um Servidor de Catálogo Global desempenha importantes funções, dentre as quais podemos destacar as indicadas a seguir:

- ◆ **Pesquisa de objetos no Active Directory:** Com o uso de Servidor de Catálogo Global, o usuário é capaz de pesquisar objetos em todos os domínios de uma floresta. A velocidade das pesquisas melhora bastante, uma vez que a pesquisa é feita no Servidor de Catálogo Global mais próximo do usuário, no seu próprio domínio e não no servidor de destino ou no caso de uma pesquisa genérica (por exemplo, pesquisar silva no campo Sobrenome dos objetos usuários) em todos os servidores de todos os domínios.
- ◆ **Fornece autenticação para nomes de usuários de outro domínio:** O Catálogo Global é utilizado para a resolução de nomes de usuários (ou de outros objetos do Active Directory), quando o DC que autenticou o usuário não tem informações sobre a referida conta. Por exemplo, se o usuário jsilva do domínio vendas.abc.com precisa fazer o logon como jsilva@vendas.abc.com em um computador pertencente ao domínio prod.abc.com, o DC do domínio prod.abc.com não será capaz de localizar o usuário jsilva@vendas.abc.com (pois o DC do domínio prod.abc.com tem informações somente sobre os usuários do seu próprio domínio e não dos demais domínios. Estas informações estão nos Servidores de Catálogo Global). O DC no domínio prod.abc.com irá contatar um Servidor de Catálogo Global para poder completar o processo de logon do usuário jsilva@abc.com, com sucesso.

- ◆ **Disponibiliza informações sobre os membros dos grupos universais, em um ambiente com múltiplos domínios:** As informações sobre os membros dos grupos locais são armazenadas apenas no domínio onde o grupo é criado. Por isso que um grupo local somente pode receber permissões de acesso aos recursos do domínio onde o grupo foi criado. Já as informações sobre os membros dos grupos Universais são armazenadas somente nos Servidor de Catálogo Global. Por isso que recomenda-se que sejam inseridos como membros dos grupos Universais, apenas outros grupos e não usuários individualmente. Se forem inseridos usuários individualmente, cada vez que um usuário for adicionado ou excluído de um grupo universal, todas as informações do grupo Universal serão replicadas entre todos os Servidor de Catálogo Global da floresta. Por exemplo, quando um usuário que pertence a um grupo universal faz o logon em um domínio configurado para o modo Windows 2000 Nativo ou Windows Server 2003, o Catálogo Global fornece informações sobre a quais grupos universais a conta do usuário pertence.

Existe uma exceção à esta regra, que é quando a conta do usuário pertence ao grupo Administradores do Domínio (Domain Admins). Neste caso, o usuário conseguirá fazer o logon, mesmo que um Servidor de Catálogo Global não esteja disponível e mesmo que seja o seu primeiro logon no computador.

- ◆ **Validação de referências a objetos em uma floresta:** O Catálogo Global é utilizado pelos DCs para validar referências a objetos de outros domínios de uma floresta. Quando um DC trata com um objeto onde um dos seus atributos contém referências a um objeto em outro domínio, esta referência é validada pelo Catálogo Global. Mais uma vez é importante salientar o papel dos Servidores de Catálogo Global em melhorar o desempenho do Active Directory. Nesta situação, se não existisse o Catálogo Global, a validação da referência ao objeto teria que ser feito por um DC do domínio do objeto referenciado. Só nestas situações (muito comuns na utilização diária da rede), imagine quanto tráfego de validação seria gerado através dos links de WAN da rede. Sem contar também a demora adicional até que a validação fosse feita através da rede, no domínio de destino e a resposta retornasse.

## Replicação de informações entre os Servidor de Catálogo Global:

Conforme descrito anteriormente, o Catálogo Global contém informações completas sobre todos os objetos do seu domínio e informações parciais sobre todos os objetos dos demais domínios. Alterações são efetuadas diariamente em diversos objetos da rede. Por exemplo, usuários são renomeados, novos grupos criados, usuários são adicionados ou retirados de grupos e assim por diante.

Todas estas alterações tem que ser replicadas entre os vários Servidores de Catálogo Global de todos os domínios, para que estes estejam sempre atualizados. A estrutura

**IMPORTANTE:** Se não estiver disponível um Servidor de Catálogo Global, o computador no qual o usuário fez o logon irá utilizar as informações armazenadas no cache do computador, caso o usuário já tenha feito um logon anterior neste computador. Se for o primeiro logon do usuário neste computador e não estiver disponível um Servidor de Catálogo Global, o usuário não conseguirá fazer o logon no domínio. Ele conseguirá fazer o logon apenas localmente no computador, usando uma das contas locais ao invés de uma conta do domínio.

**IMPORTANTE:** Quando a rede é formada por um único domínio, não é necessário que os usuários obtenham informações sobre os grupos Universais durante o logon, a partir de um Servidor de Catálogo Global. Isso acontece porque quando existe um único domínio, o Active Directory é capaz de detectar que não existem outros domínios e que não é necessária uma pesquisa no Catálogo Global (uma vez que a pesquisa pode ser feita no próprio DC que está autenticando o usuário)

de replicação do Catálogo Global é criada e gerenciada automaticamente por um processo do Active Directory, conhecido como Knowledge Consistency Checker (KCC). O KCC é responsável por determinar a melhor “topologia” de replicação do Global Catalog, de tal maneira que a rede não seja sobrecarregada com tráfego excessivo devido à replicação.

Algumas considerações devem ser feitas em relação a replicação dos grupos Universais. Os grupos Universais e informações sobre os seus membros estão contidas somente no Catálogo Global, conforme descrito anteriormente. Grupos Globais e Locais são também listados no Catálogo Global, porém no Catálogo Global não são armazenadas informações sobre os membros dos grupos Globais e Locais. Com isso o tamanho do Catálogo Global é reduzido, bem como o tráfego de replicação associado com a atualização do Catálogo Global. Para recursos e objetos que sofrerão alterações constantes, é aconselhável que você utilize grupos Globais e Locais para a definição de permissões, pois com isso você reduzirá o tráfego de replicação, comparativamente se você utilizasse grupos Universais. Como as informações sobre os membros dos grupos Universais são armazenadas no Catálogo Global, sempre que houver uma alteração na lista de membros de um grupo Universal, será necessário replicar esta informação para todos os Servidores de Catálogo Global de todos os domínios. Isso justifica a recomendação feita anteriormente, de somente adicionar grupos como membros de grupos Universais e não usuários.

## O Schema do Active Directory.

A definição de todos os objetos do Active Directory e demais informações está contida no que é conhecido como Schema do Active Directory. O Active Directory utiliza um modelo de banco de dados hierárquico, diferente do Modelo Relacional de Dados com o qual estamos mais habituados. Mas, me permitam esta analogia, o Schema é como se fosse (na verdade é) a definição da estrutura do banco de dados do Active Directory. Por exemplo, a definição do objeto usuário, quais atributos tem este objeto, o tipo de cada atributo e demais informações sobre o objeto usuário, estão todas contidas no Schema. A definição de cada objeto, de cada atributo, está contida no Schema.

O Schema contém a definição para todos os objetos do Active Directory. Quando você cria um novo objeto, as informações fornecidas são validadas com base nas definições contidas no Schema, antes que o objeto seja salvo na base de dados do Active Directory. Por exemplo, se você preencheu um atributo do tipo número, com valores de texto, o Active Directory não irá gravar o objeto no Active Directory e uma mensagem de erro será exibida.

O Schema é feito de objetos, classes e atributos. O Schema definido por padrão com o Active Directory, contém um número de classes e atributos, os quais atendem as necessidades da maioria das empresas. Porém o Schema pode ser modificado, o Administrador pode modificar as classes existentes ou adicionar novas classes ou atributos. Qualquer alteração no Schema deve ser cuidadosamente planejada, pois alterações feitas no Schema afetam toda a árvore de domínios. Todos os domínios de uma árvore tem que utilizar o mesmo Schema, ou seja, não podem ser utilizados diferentes esquemas para os diferentes domínios de uma árvore de domínios.

## Como os objetos do Active Directory são definidos no Schema:

No Schema, uma classe de objetos representa uma categoria de objetos do Active Directory, como por exemplo contas de usuários, contas de computadores, impressoras ou pastas compartilhadas publicadas no Active Directory e assim por diante. Na definição de cada classe de objetos do Active Directory, está contida uma lista de atributos que podem ser utilizadas para descrever um objeto da referida classe. Por exemplo, um objeto usuário contém atributos de nome, senha, validade da conta, descrição, etc. Quando um novo usuário é criado no Active Directory, o usuário torna-se uma nova instância da classe User do Schema e as informações que você digita sobre o usuário, tornam-se instâncias dos atributos definidos na classe user.

## Como o Schema é armazenado no Active Directory:

Cada floresta pode conter um único Schema, ou seja, o Schema tem que ser único ao longo de todos os domínios de uma floresta. O Schema é armazenado nas partições de schema do Active Directory. A partição de schema do Active Directory, bem como a partição de definição do Active Directory, são replicadas para todos os DCs da floresta. Porém um único DC controla a estrutura do Schema, DC este conhecido como Schema Master. Ou seja, somente no DC configurado como Schema Master é que o Administrador poderá fazer alterações no Schema.

## Cache do Schema.

Cada DC mantém uma cópia do Schema na memória do servidor (bem como uma cópia em disco), para melhorar a performance das operações relacionadas ao Schema, tais como validação de novos objetos. A versão armazenada no Cache do servidor é automaticamente atualizada (em intervalos de tempos definidos) cada vez que o Schema é atualizado (o que não ocorre com frequência, na verdade é muito raro fazer alterações no Schema).

## Níveis de funcionalidade de um domínio.

É comum a rede da empresa “conviver” com diferentes versões do Windows. Isso aconteceu na migração do NT Server 4.0 para o Windows 2000 Server, onde durante um bom tempo ainda existiam (na prática sabemos que ainda existem) servidores com o NT Server 4.0 em utilização na rede.

O Windows Server 2003 (a exemplo do que acontecia com o Windows 2000 Server), tem diferentes níveis de funcionalidade, com base nos tipos de DCs instalados na rede. Neste tópico vou descrever os níveis de funcionalidade disponíveis e as diferentes funcionalidades que estão disponíveis em cada nível de funcionalidade.

Com o Windows Server 2003 foi introduzido o nível de funcionalidade da floresta, o que não existia com o Windows 2000 Server.

O nível de funcionalidade do domínio determina quais características estão ou não disponíveis.

Existem quatro níveis de funcionalidade no Windows Server 2003: Windows 2000 mixed, Windows 2000 native, Windows Server 2003 interim, and Windows Server 2003.

Por padrão é selecionado o nível de funcionalidade Windows 2000 mixed. Muitos dos recursos mais avançados, tais como grupos Universais, somente estão disponíveis nos demais níveis de funcionalidade: Windows 2000 native, Windows Server 2003 interim ou Windows Server 2003.

O nível de funcionalidade da floresta é uma novidade do Windows Server 2003. Existem três níveis de funcionalidade da floresta disponíveis: Windows 2000, Windows Server 2003 interim, and Windows Server 2003. Por padrão é selecionado o nível Windows 2000. Muitas das novidades do Windows Server 2003 em relação ao Active Directory somente estão disponíveis nos níveis mais avançados: Windows Server 2003 interim ou Windows Server 2003.

Para que o nível de funcionalidade da floresta seja configurado para Windows Server 2003, todos os DCs de todos os domínios devem estar com o Windows Server 2003 instalado. Somente neste nível é que estarão disponíveis todos os recursos do Active Directory, incluindo a maioria das novidades introduzidas com o Windows Server 2003.

O que define se é possível ou não utilizar um determinado nível de funcionalidade é a existência ou não de DCs com versões anteriores do Windows, tais como o Windows 2000 Server e o Windows NT Server 4.0.

A seguir descrevo quais as versões do Windows que podem ser utilizadas nos DCs, para cada um dos modos de funcionalidade de domínio:

- ◆ **Windows 2000 mixed:** Suporta DCs com o Windows NT Server 4.0, Windows 2000 Server ou Windows Server 2003. Neste nível de funcionalidade não é possível a utilização de grupos Universais.
- ◆ **Windows 2000 native:** Suporta DCs com o Windows 2000 Server ou com o Windows 2003 Server. Neste nível de funcionalidade são suportados grupos Universais.
- ◆ **Windows Server 2003 interim:** Suporta DCs com o NT Server 4.0 ou com o Windows Server 2003. Este nível de funcionalidade é utilizado quando você está em processo de migração de uma rede baseada no Windows NT Server 4.0 para o Windows Server 2003.
- ◆ **Windows Server 2003:** Somente DCs com o Windows Server 2003. Este é o nível onde estão disponíveis todos os recursos e novidades do Active Directory.

Muito bem, já vimos um bocado de teoria sobre o Active Directory. Nos próximos tópicos você aprenderá a instalar o Active Directory, transformando um Member Server em DC e também aprenderá sobre as modificações introduzidas pela instalação do Active Directory.

---

**IMPORTANTE:** Quando você altera de um modo de funcionalidade para o outro, não será mais possível criar DCs com versões não suportadas do Windows. Por exemplo, quando você passa do modo Windows 2000 mixed para o modo Windows 2000 Native, não será mais possível inserir DCs com o NT Server 4.0 e nem será voltar para o nível de funcionalidade anterior.

---

## Preparação para a instalação do Active Directory.

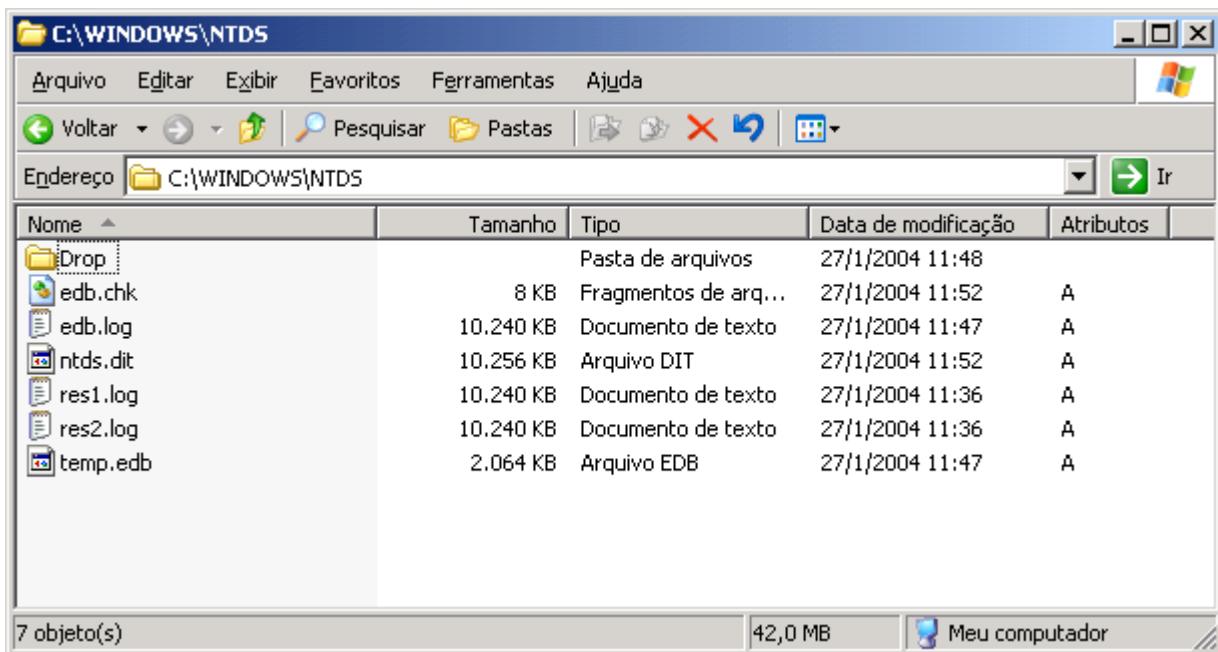
Para que o Active Directory possa ser instalado, transformando um Member Server em Controlador de Domínio, dois pré-requisitos básicos devem ser atendidos:

- ◆ Um volume formatado com NTFS
- ◆ Um servidor DNS padrão Windows 2000 Server ou Superior

O volume NTFS é necessário para gravar os arquivos da base de dados do Active Directory. Se não houver um volume com NTFS, o assistente de instalação do Active Directory será cancelado. Coloco esta recomendação apenas para deixar registrada esta exigência, mas é muito pouco provável que alguém utilize FAT ou FAT 32 em partições de um servidor. No Capítulo 5 falarei sobre as diferenças entre os sistemas de arquivo FAT/FAT 32 e NTFS. Você verá que, principalmente, em relação a segurança, a única escolha recomendada é NTFS.

## Modificações feitas com a instalação do Active Directory.

A primeira e mais óbvia modificação é o fato do servidor ter sido promovido de Member Server para Controlador de Domínio (Domain Controller -DC). Também foram criadas as pastas NTDS e SYSVOL, dentro da pasta onde o Windows Server 2003 está instalado. Na pasta NTDS são gravados os arquivos com a base de dados do Active Directory e com o log de transações desta base de dados. Na Figura 14.16 estão indicados os arquivos que são criados na pasta NTDS:



**Figura 14.16 A pasta NTDS.**

Também é criada a pasta SYSVOL e, dentro desta pasta, uma estrutura de outras pastas que dão suporte a uma série de atividades do Active Directory, tais como scripts de logon, aplicações de Políticas de segurança e assim por diante.

Além destas alterações, novas ferramentas de administração são instaladas. Estas novas ferramentas estão disponíveis no menu Ferramentas Administrativas, do menu Iniciar. A seguir descrevo, brevemente, as novas ferramentas administrativas que são instaladas quando o Active Directory é instalado:

- ◆ Domínios e relações de confiança do Active Directory: Este console é utilizado para o gerenciamento das relações de confiança entre os domínios (relações que são criadas explicitamente pelo Administrador e não as relações de confiança criadas automaticamente pelo Windows Server 2003), para configurar o nível de funcionalidade do domínio (conforme descreverei mais adiante) e para gerenciar o sufixo que é utilizado pelas contas dos usuários. Por exemplo, o usuário jsilva, do domínio abc.com, pode fazer o logon como usuário jsilva@abc.com. Onde abc.com é o sufixo deste usuário.
- ◆ Serviços e sites do Active Directory: Este console é utilizado para gerenciar a replicação de dados do Active Directory. Com este console você cria sites e links entre sites, para implementar uma política de replicação otimizada.
- ◆ Usuários e computadores do Active Directory: Este é um dos consoles mais utilizados pelo Administrador. Com este console é possível gerenciar contas de usuários e grupos de usuários, criar unidades organizacionais e mover usuários e grupos para dentro de uma unidade organizacional. Utilizaremos bastante este console no Capítulo 4 e nos demais capítulos do livro.
- ◆ Diretiva de segurança do controlador de domínio: Este console é utilizado para administrar as políticas de segurança que serão aplicadas ao controlador de domínio com o qual o console está conectado, normalmente o servidor local. As políticas definidas com este console não terão efeito em todo o domínio, mas somente no servidor onde foram configuradas.

**NOTA:** Para um estudo completo sobre GPOs, consulte o Capítulo 18 do livro Windows Server 2003 – Curso Completo, 1568 páginas, de minha autoria, publicado pela Axcel Books.

- ◆ **Diretiva de segurança do domínio:** Este console é utilizado para configurar as políticas de segurança que serão aplicados em todos os servidores e estações de trabalho do domínio.

No exemplo do item anterior, quando deixamos a cargo do assistente a instalação do DNS, foi instalado e configurado o DNS no próprio DC. Com isso mais uma modificação foi feita (a instalação do DNS) e mais um console está disponível, que é o console de administração do DNS: Iniciar -> Ferramentas Administrativas -> DNS.

Neste exemplo foi criada uma zona direta no DNS, com o mesmo nome do domínio, ou seja: abc.com, conforme indicado na Figura 14.17. Este fato ressalta bem a dependência entre o DNS e o Active Directory. O nome do domínio é também o nome da zona DNS direta.

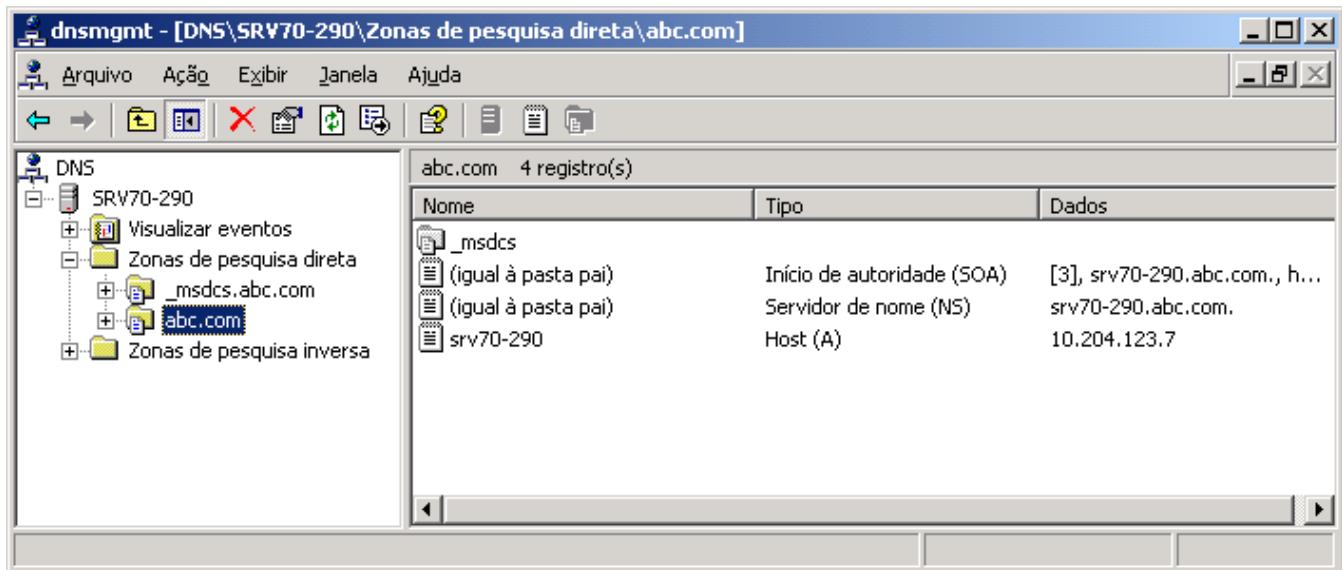


Figura 14.17 A zona DNS direta abc.com.

Outras mudanças, menos visíveis também são feitas com a instalação do Active Directory. Novos contadores são disponibilizados no console de monitoração de desempenho (Capítulo 11), uma nova opção é adicionada no menu de inicialização avançada (Capítulo 12) e assim por diante.

**NOTA:** No Capítulo 16 do livro Windows Server 2003 – Curso Completo, 1568 páginas você aprende todos os detalhes sobre o DNS, sobre zonas diretas e inversas. Estes tópicos não são abordados neste livro, pois não fazem parte do programa oficial do Exame 70-290.

## Dicas de sites com mais material de estudo sobre o Active Directory:

- ◆ <http://www.microsoft.com/technet/treeview/default.asp?url=/technet/columns/profwin/pw0503.asp>
- ◆ <http://www.microsoft.com/windowsserver2003/techinfo/overview/adam.mspx>
- ◆ <http://www.microsoft.com/windowsserver2003/evaluation/whyupgrade/nt4/nt4domtoad.mspx>
- ◆ <http://www.microsoft.com/windowsserver2003/techinfo/overview/activedirectory.mspx>

- ◆ <http://www.microsoft.com/windowsserver2003/evaluation/overview/technologies/activedirectory.mspx>
- ◆ <http://www.microsoft.com/technet/treeview/default.asp?url=/technet/columns/profwin/pw0303.asp>
- ◆ <http://support.microsoft.com/default.aspx?scid=kb;en-us;325363>
- ◆ <http://support.microsoft.com/default.aspx?scid=kb;en-us;816313>
- ◆ <http://support.microsoft.com/default.aspx?scid=kb;en-us;324803>
- ◆ <http://support.microsoft.com/default.aspx?scid=kb;en-us;814595>
- ◆ <http://support.microsoft.com/default.aspx?scid=kb;en-us;326214>
- ◆ <http://support.microsoft.com/default.aspx?scid=kb;en-us;816101>
- ◆ <http://support.microsoft.com/default.aspx?scid=kb;en-us;324753>
- ◆ <http://support.microsoft.com/default.aspx?scid=kb;en-us;325872>
- ◆ <http://support.microsoft.com/default.aspx?scid=kb;en-us;816099>
- ◆ <http://support.microsoft.com/default.aspx?scid=kb;en-us;324745>
- ◆ <http://support.microsoft.com/default.aspx?scid=kb;en-us;322672>
- ◆ <http://support.microsoft.com/default.aspx?scid=kb;en-us;325356>
- ◆ <http://support.microsoft.com/default.aspx?scid=kb;en-us;814589>
- ◆ <http://support.microsoft.com/default.aspx?scid=kb;en-us;811509>

## Administração de contas de usuários e grupos do Active Directory.

Neste tópico do resumo, você irá revisar os seguintes conceitos:

- ◆ O conceito de contas de usuários, contas de computadores e grupos de usuários.
- ◆ Criação e administração de contas de usuários e de computadores.
- ◆ Criação e administração de grupos de usuários.
- ◆ Criação e administração de Unidades Organizacionais.
- ◆ O modelo de permissões do Windows Server 2003.
- ◆ Ferramentas para executar outras tarefas no Active Directory.

Quando você trabalha na rede da empresa, o Windows Server 2003 precisa de uma maneira para poder identificar quem é o usuário logado e quais ações ele está realizando. O Windows Server 2003 também precisa identificar cada usuário para liberar ou não o acesso a recursos protegidos por permissões de acesso. Por exemplo, suponha que você tem uma pasta compartilhada chamada Docs, no servidor SRV01. Nesta pasta o Administrador configurou as permissões de acesso, de tal maneira que somente o usuário José da Silva, logon jsilva, possa acessar esta pasta. O Windows Server 2003 precisa saber quem é o usuário que está “tentando” acessar a pasta. Se for o José da Silva, o Windows Server 2003 libera o acesso, caso contrário o acesso é negado.

O Windows Server 2003 identifica cada usuário pelas informações de logon – nome e senha. Quem informações são essas? Um nome com o qual o usuário foi cadastrado na rede e a respectiva senha. Por exemplo, o nosso usuário José da Silva poderia ser cadastrado como jsilva, já a Maria Aparecida poderia ser cadastrada como mariaap, e assim por diante. Ou seja, o primeiro passo para que um usuário possa ter acesso aos recursos da rede é cadastrar o usuário. Cadastrar o usuário significa criar uma conta de usuário e um senha no Active Directory. Na primeira parte deste tópico você revisará os conceitos sobre contas de usuários. Inicialmente apresentarei alguns detalhes teóricos sobre contas de usuário e após a teoria, mostrarei a parte prática, ou seja, como criar e administrar contas de usuários.

Uma vez entendido o conceito de usuários, você aprenderá sobre grupos de usuários. Mostarei que existem diferentes tipos de grupo e com diferentes escopos de utilização. No Capítulo 2 fiz uma discussão teórica (de fundamental

importância para a eficiente administração das permissões de acesso aos recursos) sobre as estratégias de utilização de grupos de usuários, para atribuição de permissões aos recursos da rede: pastas e impressoras compartilhadas, aplicativos Web, bancos de dados e assim por diante. Neste capítulo você aprenderá a parte prática de criação de grupos. No Capítulo 6 você aprendeu a implementar, na prática, a estratégia explicada no Capítulo 2.

Entendidos os conceitos de contas de usuários e grupos de usuários, é hora de revisar mais alguns itens sobre unidades organizacionais. Vou mostrar o que é uma Unidade organizacional, como ela difere de um domínio, quando usar Unidades Organizacionais e quando utilizar domínios. Também mostrarei a parte prática de criação e administração de Unidades Organizacionais, bem como operações de mover contas de usuários e grupos de uma unidade organizacional para outra.

**IMPORTANTE:** O tópico sobre permissões NTFS, permissões de compartilhamento e atribuição de permissões usando grupos é de fundamental importância para o exame. Você deve conhecer estes tópicos, em detalhes.

## Contas de usuários

Quando você trabalha em uma rede de computadores, segurança é um dos itens de maior importância. O Administrador deve ser capaz de permitir que cada usuário somente tenha acesso aos recursos – sejam eles arquivos, impressoras ou serviços – os quais sejam necessários para a realização do seu trabalho. Por exemplo, um usuário que trabalha no departamento de bagagem não deve ser capaz de acessar informações sobre salários contidas nos arquivos de um Computador do departamento de Recursos Humanos.

No Capítulo 1 você aprendeu sobre redes de computadores e os diferentes papéis que o Windows Server 2003 pode desempenhar em uma rede. Mostrei que, em uma configuração típica, o Windows Server 2003 pode estar configurado como um servidor de arquivos, onde existem pastas compartilhadas que os usuários acessam através da rede.

No Capítulo 2 você aprendeu sobre o conceito de Domínio. Quando você cria um domínio, os servidores e também as estações de trabalho dos usuários, devem ser configuradas para fazer parte do domínio. Quando um usuário liga a sua estação de trabalho (quer ele esteja configurada com o Windows 95/98/Me, 2000, NT Workstation ou XP Profissional), o Windows é inicializado e em seguida é apresentada a tela de logon no domínio, conforme indicado na Figura 14.18, onde temos o exemplo do usuário jsilva fazendo o logon no domínio ABC.



Figura 14.18 A tela de logon no domínio.

As informações sobre as contas de usuários e grupos ficam gravadas na base de dados do Active Directory, nos servidores configurados como DCs do domínio. Quando o usuário liga a sua estação de trabalho e digita o seu nome de usuário e senha, estas informações são repassadas para um DC do domínio, onde as informações são verificadas. Se o nome de usuário existir, a senha estiver correta e a conta do usuário não estiver bloqueada, o logon será liberado e a área de trabalho do Windows será carregada. Uma vez que o usuário fez o logon no domínio, ele passou a estar identificado, ou seja, todas as ações que o usuário executar estarão associadas com a sua conta de usuário. Por exemplo, se o usuário jsilva fizer o logon no domínio ABC e tentar acessar um arquivo para o qual ele não tem permissão, ficará registrado nos logs de auditoria do servidor as seguintes informações (isso se o administrador configurou a auditoria de acesso a pastas e arquivos, conforme mostrarei no Capítulo 10):

- ◆ Identificação do usuário – no exemplo jsilva.
- ◆ Data e hora da tentativa de acesso.
- ◆ Nome do arquivo e/ou pasta que o usuário tentou acessar.

Em um domínio, além de servidores configurados como DCs, você pode ter servidores configurados como Member Servers. Um member server não tem o Active Directory instalado e, portanto, não tem uma cópia de toda a lista de usuários e grupos do domínio e nem das demais informações contidas no Active Directory. Um member server normalmente é um servidor que desempenha um papel específico, tal como servidor de arquivos, servidor de impressão, servidor de acesso remoto, servidor Web e assim por diante.

Como o servidor faz parte do domínio (member server), as contas de usuários e grupos do domínio podem receber permissões para acessar os recursos disponibilizados pelo member server. Um detalhe interessante é que é possível criar uma lista de usuários e grupos de usuários no próprio member server. Estas contas somente são válidas para o logon localmente no servidor onde foram criadas e são conhecidas como contas locais.

Por exemplo, ao instalar o Windows Server 2003 em um member server, automaticamente é criada a conta Administrador, com permissões de administrador em todos os recursos do member server. **IMPORTANTE:** As contas e grupos locais, criados em um member server, somente podem receber permissões de acesso aos recursos do servidor onde foram criadas, já que estas contas não são “visíveis” em outro servidor que não o próprio onde foram criadas. Embora seja possível criar contas e grupos locais, esta não é uma prática recomendada. Sempre que possível você deve utilizar as contas e grupos do domínio. Uma exceção é a conta local Administrador, a qual é criada automaticamente com a instalação do Windows Server 2003. Esta conta tem permissões totais em todos os recursos do servidor. Um procedimento normalmente adotado é definir a mesma senha para todas as contas Administrador de todos os member servers do domínio. Normalmente esta senha é de conhecimento apenas dos administradores do domínio. A conta local Administrador pode ser utilizada para fazer configurações no servidor quando, por algum motivo, não for possível fazer o logon no domínio.

Contas criadas em um DC são chamadas de “Domain User Accounts” (Contas de Usuários do Domínio). Essas contas permitem que o usuário faça o logon em qualquer computador do domínio e receba permissões para acessar recursos em qualquer computador do domínio.

Contas criadas em um Servidor Membro são chamadas de “Local User Accounts” (Contas de Usuários Locais). Essas contas somente permitem que o usuário faça o logon e receba permissões para acessar recursos do servidor onde a conta foi criada. Sempre que possível evite criar Contas Locais em servidores que fazem parte de um domínio. Utilizar as contas do Domínio, as quais ficam armazenadas no Active Directory, torna a administração bem mais fácil.

---

**IMPORTANTE:** Observe que a conta do usuário é utilizada como a sua identidade na rede.

---

---

**IMPORTANTE:** Uma conta pode ser criada em um DC – situação em que a conta é válida e reconhecida em todo o domínio; ou a conta pode ser criada em um member server – situação em que a conta somente é válida e reconhecida no member server onde ela foi criada.

---

Quando é exibida a tela de logon em um member server, o usuário pode escolher entre fornecer uma conta e senha do domínio ou uma conta e senha local. Na lista Log on to o usuário seleciona o nome do domínio no qual ele quer fazer o logon ou o nome do servidor local, para fazer o logon com uma conta local. A criação e administração de contas de usuários e grupos locais é feita utilizando-se o console Gerenciamento do Computador (Computer Management), descrito no Capítulo 7. As etapas para a criação e administração de contas e grupos locais são semelhantes as etapas para a criação e administração de contas do Active Directory.

No Windows Server 2003, é possível limitar os recursos aos quais cada usuário tem acesso, através do uso de permissões de acesso . Por exemplo, o administrador pode definir uma lista de usuários com acesso a uma pasta compartilhada, podendo definir, inclusive, níveis de acesso diferentes. Um determinado grupo tem acesso completo (leitura, gravação e exclusão), já um segundo tem acesso mais restrito (leitura e gravação) e um terceiro grupo tem acesso ainda mais restrito (leitura). Para que seja possível atribuir permissões, cada usuário deve ser cadastrado no domínio. Cadastrar o usuário significa criar uma “Conta de Usuário”. Com uma conta o usuário pode efetuar o logon e receber permissões para acessar os mais variados recursos disponibilizados na rede.

Reunindo esta história toda, cada usuário deve ser cadastrado. Cadastrar o usuário significa criar uma conta de usuário no Active Directory (veja exemplos práticos mais adiante). Uma vez que a conta foi criada, o usuário pode utilizá-la para fazer o logon em qualquer computador da rede. Antes de partir para a parte prática, apresentarei mais algumas recomendações e detalhes relacionados com contas de usuários:

## Observações sobre o nome das contas de usuários

Quando o administrador cria nomes de logon para os usuários, devem ser levados em consideração os seguintes fatos:

- ◆ O nome de logon deve ser único no domínio. Veja o exemplo do item anterior, onde mostrei que não seria possível criar dois usuários com nome de logon jsilva, no mesmo domínio.
- ◆ O nome de logon também não pode ser igual ao nome de um grupo do domínio. Por exemplo, se já existe um grupo chamado Contabilidade, você não poderá criar uma conta de usuário com o campo nome de logon preenchido como Contabilidade.
- ◆ O nome de logon pode conter espaços em branco e pontos, porém não pode ser formado somente por espaços e pontos. É conveniente evitar o uso de espaços em branco, pois contas com espaços em branco no nome, terão que ser escritas entre aspas, quando você utiliza scripts para administração do Windows Server 2003.
- ◆ Podem ter no máximo 20 caracteres.
- ◆ Os seguintes caracteres não podem ser utilizados: “ / \ : ; [ ] | = , + \* ? < >
- ◆ O Windows Server 2003 não diferencia entre maiúsculas e minúsculas para o nome de logon. Por exemplo, para o Windows Server 2003 jsilva, JSILVA ou Jsilva representa o mesmo usuário.

## Questões relacionadas com a definição da senha do usuário

Sempre que você for cadastrar um usuário também deve ser cadastrada uma senha para ele. No Windows 2000 Server, por padrão, era aceito que o administrador definisse uma senha em branco. Caso fosse necessário, o administrador poderia definir um número mínimo de caracteres para as senhas dos usuários. No Windows Server 2003, a preocupação com a segurança está presente desde o momento da instalação. No Windows Server 2003.

No Windows Server 2003, por padrão, são definidas as seguintes políticas de segurança em relação as senhas de usuários:

- ◆ Quando o usuário vai trocar a senha, não pode ser utilizada uma senha igual as 24 últimas (haja criatividade para inventar senhas).
- ◆ A senha expira (isto é, deve ser alterada) a cada 42 dias.
- ◆ O tempo mínimo de vida de senha é um dia. Ou seja, você trocou a senha hoje, não poderá trocá-lo novamente daqui a uma ou duas horas, somente após um dia.
- ◆ Tamanho mínimo de sete caracteres.
- ◆ A opção “A senha deve atender critérios de complexidade (Password must meet complexity requirements) é habilitada por padrão”.
- ◆ A senha não pode conter parte ou todo o nome da conta. Por exemplo, se o nome da conta for jsilva, a senha não poderá conter a sílaba “sil” ou a palavra “silva”.
- ◆ Ter pelo menos seis caracteres. O número mínimo de caracteres pode ser aumentado, configurando-se as políticas de segurança para senhas, conforme mostrarei mais adiante.
- ◆ Deve conter caracteres de pelo menos três dos quatro grupos a seguir: letras maiúsculas de A até Z, letras minúsculas de a até z, dígitos de 0 a 9 ou caracteres especiais (:, !, @, #, \$, %, etc.).

---

**IMPORTANTE:** Com a opção A senha deve atender critérios de complexidade (Password must meet complexity requirements) é habilitada por padrão, uma série de requisitos devem ser atendidos para que a senha seja aceita.

---

Estes requisitos de complexidade são verificados quando a senha é criada pela primeira vez, durante o cadastramento do usuário e toda vez que a senha for alterada. Com os requisitos de complexidade habilitados, as senhas a seguir seriam válidas:

**AbCsenha1**

**AbcSenha#**

**Abc123**

**Abc ; ; senha**

Já as senhas a seguir não seriam válidas:

- ◆ **abcsenha123:** (contém somente caracteres de dois dos quatro grupos: letras minúsculas e números).
- ◆ **abc;senha:** (contém somente caracteres de dois dos quatro grupos: letras minúsculas e caracteres especiais).

---

**IMPORTANTE:** Para as senhas, o Windows Server 2003 distingue letras maiúsculas de minúsculas. Por exemplo a senha “Abc123” é diferente da senha “abc123”.

---

---

**IMPORTANTE:** O grupo Oper. de contas é criado automaticamente durante a instalação do Active Directory. Membros deste grupo podem realizar tarefas relacionadas a criação e administração de contas de usuários no domínio.

---

## Opções padrão do console Usuários e Computadores do Active Directory:

- ◆ **Builtin:** Nesta opção estão os chamados grupos Builtin, ou seja, aqueles grupos criados automaticamente quando o Active Directory é instalado. Estes grupos são utilizados para funções de administração do domínio. Por exemplo, os membros do grupo Administradores (Administrators) tem permissões administrativas em todo o domínio, já membros do grupo Oper. de contas (Account Operators) tem permissões para criar e administrar contas de usuários no domínio e assim por diante. Os grupos que ficam nesta opção são grupos Locais do domínio. Mais adiante neste capítulo, descreverei as diferenças entre grupos Locais, Globais e Universais.

- ◆ **Computers (Computadores):** Nesta opção ficam as contas de todos os computadores do domínio, a não ser que tenham sido criadas outras unidades organizacionais e contas tenham sido movidas para estas unidades organizacionais. É importante lembrar que somente computadores com o Windows NT 4.0, Windows 2000, Windows Server 2003 ou Windows XP Professional, possuem conta de computador. Computadores com o Windows 95/98/Me não tem contas de computador no domínio.
- ◆ **Domain Controllers (Controladores de domínio):** Nesta opção ficam as contas de computadores dos DCs do domínio.
- ◆ **ForeignSecurityPrincipals:** Nesta opção ficam objetos relacionados a relações de confiança criadas manualmente pelo administrador.
- ◆ **Users:** Nesta opção ficam as contas que foram criadas automaticamente pelo Active Directory, bem como os grupos Globais criados automaticamente. Um exemplo de conta criada automaticamente é a conta Administrador (Administrator), a qual tem permissões de administrador em todos os recursos de todos os servidores do domínio. Por padrão é nesta opção que criamos novas contas de usuários. Conforme mostrarei mais adiante você também pode criar novas unidades organizacionais e criar contas de usuários dentro destas unidades organizacionais, o que também será visto neste capítulo.

## Opcões de configuração durante a criação de uma nova conta de usuário:

- ◆ **O usuário deve alterar a senha no próximo logon :** Se esta opção estiver marcada, a primeira vez que o usuário fizer o logon, será solicitado que ele altere a sua senha. Esta opção é utilizada para que o usuário possa colocar uma senha que somente ele conhece. Quando o usuário é cadastrado, a senha é digitada pelo Administrador, o qual fica sabendo a senha do usuário. No próximo logon o usuário é obrigado a alterar a senha de tal maneira que somente ele saiba qual a senha está definida para a sua conta.
- ◆ **O usuário não pode alterar a senha:** Se esta opção estiver marcada, a senha somente pode ser alterada pelo Administrador. Normalmente utilizada para empregados temporários e para estagiários. Para as contas utilizadas pelos funcionários da empresa, esta opção normalmente é desabilitada.
- ◆ **A senha nunca expira:** Ao marcar esta opção, independente das políticas de segurança do domínio, o usuário nunca precisará trocar a sua senha. Caso contrário de tempos em tempos (conforme configurado nas políticas de segurança do domínio ), o usuário deve trocar a senha.
- ◆ **Conta desativada:** O Administrador marca esta opção para desativar/bloquear a conta de um usuário. Usuários com a conta bloqueada não podem mais efetuar logon e, consequentemente, não podem mais acessar recursos da rede. Esta opção normalmente é utilizada para desativar, temporariamente, a conta de empregados que estão em férias. Quando o empregado retorna ao serviço, o Administrador libera a sua conta, simplesmente desmarcando esta opção. Não é possível fazer o logon enquanto a conta estiver Desativada. Contas desativadas são exibidas com um X vermelho, na listagem de contas do Active Directory. Desativada é diferente de bloqueada. Uma conta é bloqueada, quando o usuário erra a senha, um determinado número de vezes, dentro de um determinado período, conforme configurado nas políticas de conta do domínio. Contas bloqueadas não são exibidas com o X vermelho, somente contas Desativadas é que são exibidas com o X vermelho.

## Configurando opções importantes da conta do usuário

A seguir descrevo opções importantes de configuração das contas de usuários do Active Directory, opções estas que você deve conhecer para o exame.

Na lista Opções da conta, o administrador pode configurar uma série de opções, descritas a seguir:

- ◆ **O usuário deve alterar a senha no próximo logon:** Se esta opção estiver marcada, a próxima vez que o usuário fizer o logon, será solicitado que ele altere a sua senha. Esta opção é utilizada para que o usuário possa colocar uma senha que somente ele conhece. Quando o usuário é cadastrado, a senha é digitada pelo Administrador, o qual fica sabendo a senha do usuário. No próximo logon o usuário é obrigado a alterar a senha de tal maneira que somente ele saiba qual a senha está definida para a sua conta.
- ◆ **O usuário não pode alterar a senha:** Se esta opção estiver marcada, a senha somente pode ser alterada pelo Administrador. Normalmente utilizada para empregados temporários e para estagiários. Para as contas utilizadas pelos funcionários da empresa, esta opção normalmente é desabilitada.
- ◆ **A senha nunca expira:** Ao marcar esta opção, independente das políticas de segurança do domínio, o usuário nunca precisará trocar a sua senha. Caso contrário de tempos em tempos (conforme configurado nas políticas de segurança do domínio ), o usuário deve trocar a senha.
- ◆ **Gravar senha c/ criptografia reversível:** Esta opção somente deve ser marcada se o usuário precisa fazer o logon no domínio, a partir de estações de trabalho padrão Apple/Macintosh.
- ◆ **Conta desativada:** O Administrador marca esta opção para desativar a conta de um usuário. Usuários com a conta desativada não podem mais efetuar o logon no domínio e, consequentemente, não podem mais acessar recursos da rede. Esta opção normalmente é utilizada para desativar, temporariamente, a conta de empregados que estão em férias. Quando o empregado retorna ao serviço, o Administrador libera a sua conta, simplesmente desmarcando esta opção.
- ◆ **Cartão inteligente necess. p/ logon interativo:** Se esta opção estiver marcada, o usuário somente poderá fazer o logon se estiver utilizando um Smart card. O uso de Smart card aumenta bastante a segurança no logon, uma vez que mesmo de posse da senha do usuário, outra pessoa não conseguirá fazer o logon se não tiver também o Smart card do usuário. É um nível de segurança adicional. Um dos fatores que impedem (ou estão atrasando) o uso em larga escala de Smart card é o custo dos leitores de Smart card.. Quando esta opção for utilizada, a senha da conta do usuário é automaticamente e aleatoriamente criada pelo Windows Server 2003, usando requisitos de complexidade e a opção Password never expires (A senha nunca expira) é selecionada.
- ◆ **Conta sensível à segurança não pode ser deleg.:** Esta é uma opção que deve ser utilizada com muito cuidado, pois pode gerar problemas em relação à segurança. Com esta opção marcada, um hacker poderia tentar fazer se passar por um serviço válido para executar em nome da conta. Com isso o “falso serviço” teria todas as permissões atribuídas a conta. Já imaginou se isso acontecesse com a conta Administrador? O falso serviço simplesmente teria permissões totais em todo o domínio, ou seja, um verdadeiro desastre.

**IMPORTANTE: A opção A conta está bloqueada: Por padrão, é definido no domínio, um número máximo de tentativas de logon sem sucesso que o usuário pode fazer, dentro de um período de tempo. Se este limite for ultrapassado, a conta será bloqueada automaticamente. Por exemplo, pode ser definido que se o usuário fizer três tentativas de logon sem sucesso, dentro de 20 minutos, a conta fique bloqueada por 24 horas. Ou também é possível definir que, uma vez bloqueada, a conta somente possa ser desbloqueada pelo administrador. Estas configurações fazem parte das diretrizes de segurança do domínio e serão explicadas mais adiante. Quando uma conta está bloqueada, a opção Conta bloqueada aparece habilitada e marcada. Para desbloquear a conta, basta que o administrador desmarque esta opção. O Administrador não pode bloquear uma conta. Ele pode desativar a conta, conforme veremos mais adiante, mas a única maneira de bloquear uma conta é o usuário fazer o número definido de tentativas de logon sem sucesso, dentro do período configurado no domínio.**

- ◆ **Use tipos de criptografia DES p/ esta conta:** Habilita suporte para o tipo de criptografia conhecido como DES, o qual suporta diversos níveis de criptografia, incluindo MPPE Standard (40-bit), MPPE Standard (56-bit), MPPE Strong (128-bit) IPSec DES (40-bit), Ipsec 56-bit DES e IPsec Triple DES (3DES).
- ◆ **Não exige pré-autenticação Kerberos:** O Kerberos é um protocolo de autenticação. Ao marcar esta opção você permite que a conta seja autenticada por servidores utilizando diferentes versões e implementações do protocolo Kerberos.

## Criando e utilizando uma conta modelo.

As contas de usuários de uma mesma seção, normalmente, compartilham algumas propriedades em comum. Por exemplo, todas as contas dos funcionários da seção de contabilidade (ou a maioria das contas), terá campos em comum, tais como número de telefone, escritório, grupos aos quais a conta pertence e assim por diante.

Nestas situações, é indicado que você crie uma conta modelo. Por exemplo, você poderia criar uma conta chamada Modelo\_Contabilidade. Ao criar a conta modelo contabilidade, você define as propriedades que serão comuns a todas as contas da seção de contabilidade. Depois você pode usar este modelo, para criar novas contas. As novas contas já irão vir com as propriedades da conta modelo e você só precisará definir as propriedades que são diferentes para cada conta, tais como senha e nome de logon. A vantagem do uso de um modelo de conta é que a criação de novas contas é facilitada e você consegue manter um padrão, para as propriedades que são comuns a todas as contas. A desvantagem é que não é mantido um vínculo entre as contas criadas a partir de um modelo e o respectivo modelo. Por exemplo, se você alterar a conta modelo, as contas que foram criadas a partir do modelo, não irão ser atualizadas com as alterações feitas na conta modelo. Talvez em uma próxima versão do Windows, tenhamos este mecanismo de herança implementado.

Para criar uma conta modelo você usa os passos descritos nos exemplos práticos anteriores, ou seja, a conta modelo é uma conta normal, como qualquer outra.

**IMPORTANTE:** Como a conta modelo será usada para a criação de novas contas, a partir dela, a conta modelo deve estar com a opção Conta desativada, marcada. Isso porque a conta modelo não deve ser usada para fazer o logon no domínio. Por isso, para impedir que a conta possa ser usada para fazer o logon no domínio, é que você deve marcar a opção Conta desativada.

A seguir descrevo quais propriedades, uma nova conta herda da conta modelo:

- ◆ **Guia Geral:** Nenhuma propriedade é herdada do modelo.
- ◆ **Guia Endereço:** Todas as propriedades são herdadas, com exceção do campo Rua.
- ◆ **Guia Conta:** Todas as propriedades são herdadas, com exceção dos campos Nome de logon do usuário e Nome de logon do usuário (anterior ao Windows 2000).

**IMPORTANTE:** O Administrador também pode definir se a conta nunca expira (Nunca) ou se a conta deve expirar em um determinada data. Expirar significa que a partir da data de expiração, não será mais possível utilizar a conta que expirou para fazer o logon no domínio, a não ser que o administrador acesse as propriedades da conta e defina uma nova data de expiração. Um exemplo prático onde você utiliza esta opção é para contas utilizadas por estagiários ou empregados temporários. Vamos supor que você contrata os estagiários por períodos definidos. Com isso você pode cadastrar o estagiário e já configurar esta conta para que expire na data de encerramento do estágio. Com isso exatamente no dia e hora do encerramento do estágio a conta será desativada. Agora vamos supor que um novo estagiário tenha sido contratado para substituir o que saiu. Basta ativar novamente a conta e renomeá-la. Informe a conta renomeada para o novo estagiário. Com isso não é preciso reconfigurar as permissões de acesso, uma vez que a conta é a mesma (apenas foi renomeada), o estagiário que chega tem exatamente as mesmas permissões de acesso do que o que saiu. O que faz sentido, já que ele está substituindo o anterior.

- ◆ **Guia Perfil:** Todas as propriedades são copiadas, porém são adaptadas para refletir o nome de logon do usuário que está sendo criado. Por exemplo, se a Pasta base do modelo está em: \\servidor\profiles\modelocont, e está sendo criado um usuário chamado jsilva2, a pasta base do usuário que está sendo criado, será: \\servidor\profiles\jsilva2.
- ◆ **Guia Telefones:** Nenhuma propriedade é copiada.
- ◆ **Guia Organização:** Todas as propriedades são copiadas, com exceção do campo Título.
- ◆ **Guia Membro de:** Todas as informações são copiadas, ou seja, a nova conta, criada a partir de um modelo, pertencerá exatamente aos mesmos grupos aos quais pertence a conta modelo.
- ◆ **Guias Discagem, Ambiente, Sessões, Controle remoto, Perfil de serviços de terminal e COM+:** Nenhuma informação é copiada destas guias, do modelo para a nova conta que está sendo criada.

## Comandos para trabalhar com contas de usuários.

Além da interface gráfica, usando o console Usuários e computadores do Active Directory, o Administrador tem acesso a uma série de comandos, os quais estão diretamente relacionados com a criação, edição e administração de contas de usuários, bem como a Administração do Active Directory. Estes comandos, normalmente, são utilizados em scripts, para executar uma série de tarefas repetitivas, em um grande número de contas no Active Directory.

---

**IMPORTANTE:** Você não precisa conhecer a sintaxe detalhada de cada comando. Para o exame, o que você precisa conhecer é em que situação cada comando é utilizado. Por exemplo, falou em importar informações de contas de usuários ou de grupos, que estão em um arquivo do tipo Delimitado por Vírgula, você tem que lembrar na hora que é o comando CSVDE que é utilizado para fazer esta importação. Você não precisa decorar a sintaxe e todas as opções de cada comando, apenas saber para que é utilizado cada comando.

---

A seguir descrevo os principais comandos relacionados ao gerenciamento de contas de usuários e ao gerenciamento do Active Directory.

### O comando CSVDE:

Este comando é utilizado para importar e exportar dados do e para o Active Directory usando arquivos que armazenam dados no formato de valores separados por vírgula (CSV). Você também pode oferecer suporte a operações em lotes no padrão do formato de arquivo CSV. Um arquivo no formato CSV, apresenta um registro em cada linha e os campos de cada registro são separados por vírgula.

### O comando DSADD:

Este comando é utilizado para adicionar tipos específicos de objetos ao Active Directory, tais como usuários, grupos, etc. A seguir descrevo as diferentes opções do comando DSADD

**IMPORTANTE:** Quando você cria uma nova conta, a partir de um modelo, a nova conta pertencerá aos mesmos grupos aos quais pertence a conta modelo. Com isso, a nova conta, herdará as permissões de acesso, que forem atribuídas a estes grupos. Porém, permissões que tenham sido atribuídas diretamente a conta modelo, não serão herdadas pela nova conta, criada a partir da conta modelo. Fique atento a este detalhe, pois ele pode ser a diferença entre acertar e errar uma ou mais questões no exame. Você também deve lembrar que as configurações para acesso, via Terminal Services, não são herdadas por uma nova conta, criada a partir de uma conta modelo. É isso.

---

- ◆ **dsadd computer:** É utilizado para adicionar um único computador ao diretório.
- ◆ **dsadd group:** Este comando é utilizado para adicionar um único grupo ao diretório.
- ◆ **dsadd ou:** Este comando é utilizado para adicionar uma única unidade organizacional ao diretório.
- ◆ **dsadd user:** Adiciona um usuário único ao diretório.

## dsget user

Este comando é utilizado para exibir as várias propriedades de um usuário no diretório. Esse comando dispõe de duas variações. A primeira permite exibir as propriedades de vários usuários. A segunda permite exibir as informações de participação em um grupo de um usuário único.

## Outros comandos disponíveis:

A seguir apresenta uma lista de outros comandos disponíveis. Você encontra informações detalhadas sobre estes comandos, na Ajuda do Windows Server 2003, digitando o nome do comando, no campo de pesquisa da Ajuda.

- ◆ **dsmod:** É utilizado para modificar atributos selecionados de um objeto existente no Active directory. Por exemplo, pode ser utilizado para modificar informações sobre um usuário, grupo ou unidade organizacional do Active Directory.
- ◆ **dsquery:** É utilizado para localizar objetos no Active Directory, de acordo com um ou mais critérios de pesquisa, especificados.
- ◆ **dsmove:** É utilizado para mover um objeto de seu local atual para um novo local pai.
- ◆ **dsrm:** É utilizado para remover um objeto, a subárvore completa abaixo de um objeto no diretório, ou ambos.

## O conceito de Profiles

O Windows Server 2003 (a exemplo do que ocorre no Windows 2000 e no Windows XP), mantém configurações de ambiente separadas para cada usuário. Por exemplo, o usuário jsilva faz o logon e cria um ícone na área de trabalho. Este ícone não será exibido na área de trabalho de outros usuários, quando estes fizerem o logon no computador. O Windows também mantém diversas outras configurações separadamente para cada usuário, como por exemplo: papel de parede, opções do menu iniciar, configurações do Internet Explorer e do Outlook Express, associação de extensões de arquivos, configurações da barra de tarefas e assim por diante. A pasta Meus documentos também é individualizada para cada usuário. O Windows Server 2003 mantém estas configurações separadamente para cada usuário, através de uma estrutura de pastas e subpastas, dentro da pasta C:\Documents and settings. Dentro desta pasta o Windows Server 2003 cria uma pasta para cada usuário, pasta esta com o nome de logon do usuário.

Por exemplo, todas as configurações do usuário jsilvap são gravadas e mantidas em uma estrutura de subpastas, dentro de C:\Documents and settings\jsilvap; todas as configurações do usuário pedro2 são gravadas e mantidas em uma estrutura de subpastas, dentro de C:\Documents and settings\paulo2 e assim por diante.

Este conjunto de configurações, que define o ambiente de trabalho de cada usuário, é conhecido como Profile do usuário (User Profile). Quando você trabalha em um ambiente de rede, baseado em um domínio do Windows 2000 Server ou do Windows Server 2003, é possível salvar as configurações da Profile de cada usuário em pastas em um servidor da rede. Este tipo de Profile é conhecido como Roaming Profile (eu me arriscaria a traduzir como Profile Viajante).

O Roaming significa que a Profile acompanha (viaja com) o usuário através da rede. Ou seja, independente da estação de trabalho que o usuário estiver utilizando, ele receberá as configurações de sua Profile, as quais serão carregadas a

partir da rede. Com a combinação do recurso de User Profiles com a distribuição de Software via GPO (assunto abordado em detalhes no Capítulo 18 do livro: Windows Server 2003 – Curso Completo, 1568 páginas), é possível fazer com que os programas e as configurações “sigam” o usuário através da rede, ou seja, em qualquer estação de trabalho que o usuário faça o logon, ele terá a mesma área de trabalho, com o mesmo conjunto de ícones, atalhos e programas. Neste tópico você aprenderá sobre Profiles.

## Vantagens de se utilizar Profiles:

- ◆ Vários usuários podem utilizar o mesmo computador, sem que as configurações feitas por um dos usuários, afetem o ambiente de trabalho dos demais usuários. Quando o usuário faz o logon ele recebe exatamente o mesmo ambiente de trabalho que ele deixou, quando fez o último log off.
- ◆ User profiles podem ser gravadas em uma pasta compartilhada em um servidor, de tal maneira que as configurações “sigam” o usuário através da rede. Esta opção está disponíveis para computadores rodando o Windows NT, Windows 2000, Windows XP ou Windows Server 2003. Não está disponível para o Windows 95/98/Me. O uso de User Profiles é uma ferramenta de grande auxílio para o administrador, principalmente para a padronização do ambiente de trabalho dos usuários. O administrador pode utilizar o conceito de User Profiles para executar, dentre outras, as seguintes configurações:
- ◆ Criar uma profile padrão e distribuir esta profile para um grupo de usuários da rede. Esta opção é útil para usuários que devam ter acesso restrito as opções de personalização do windows. Por exemplo, posso usar uma profile para definir, automaticamente, os ícones da área de trabalho para um grupo de usuários.
- ◆ Você pode criar as chamadas “Mandatory user profile”. Este tipo de profile não permite que o usuário faça alterações nas configurações definidas na profile. O usuário até consegue alterar o seu ambiente de trabalho, mas no momento em que for feito o log off, as alterações não serão salvas. Ao fazer o próximo logon, o usuário receberá as configurações definidas na profile, sem as alterações que ele fez, mas que não foram salvas. As configurações são copiadas para o computador do usuário cada vez que este faz o logon. Quando o usuário faz alterações, estas são feitas na sua cópia local da profile. Ao fazer o logoff, estas alterações não são repassadas para a profile que está gravada no servidor. No próximo logon é esta profile que está no servidor (sem alterações) que é novamente copiada para a estação de trabalho do usuário, sobrescrevendo as alterações que por ventura ele tenha feito. O resultado prático é que sempre que o logon é feito, são carregadas as configurações definidas na profile do tipo Mandatory, armazenada no servidor e para a qual somente o Administrador tem permissão para fazer alterações.

## Tipos de User Profile:

- ◆ **Local user profile (profile de usuário – local):** Este tipo de profile é criada a primeira vez que o usuário faz o logon em um computador com o Windows NT 4.0 (Server ou Workstation), com o Windows 2000 (Server ou Professional), com o Windows XP (Home ou Professional) ou com o Windows Server 2003. A profile é criada dentro de uma pasta com o mesmo nome do usuário, em C:\Documents and settings. Por exemplo, a primeira vez que o usuário jsilva fizer o logon no computador, a sua profile será criada em C:\Documents and settings\jsilva. Dentro de jsilva serão criadas diversas pastas onde estão as configurações do usuário jsilva. Um profile local é específica para o computador onde ela foi criada. Por exemplo, se o usuário jsilva faz o logon no computador micro01 e faz

**IMPORTANTE:** Não esqueça, de jeito nenhum, que para tornar uma Profile Mandatory é só renomear o arquivo Ntuser.dat para Ntuser.man.

alterações em sua profile local, estas alterações não estarão presentes quando ele fizer o logon no micro02. Cada micro tem a sua própria profile local para o usuário jsilva.

- ◆ **Roaming user profile:** Este tipo de profile é criada pelo administrador e depois armazenada em um servidor. Por exemplo, o administrador faz o logon em uma estação de trabalho e faz as configurações padrão para a profile. Vamos supor que o administrador fez o logon com a conta Administrator (Administrador). A sua profile será armazenada em C:\Documents and settings\Administrator. Se for uma conta do domínio, o nome do domínio é anexado ao nome da conta por um ponto. Por exemplo, a profile para o usuário Administrator, do domínio ABC, seria gravada na pasta C:\Documents and settings\zAdministrator.Abc, do computador onde o administrador fez o logon. O administrador faz as alterações necessárias. Estas são salvas na sua profile local. Em seguida o administrador pode fazer uma cópia desta profile padrão para o servidor. Por exemplo, pode ser criada uma pasta compartilhada chamada Profiles, no servidor srv01. Neste caso o caminho para esta pasta seria: \\srv01\profiles. Dentro da pasta profiles pode ser criada uma pasta para cada usuário, por exemplo: \\srv01\profiles\jsilva, \\srv01\profiles\maria, \\srv01\profiles\Pedro e assim por diante. Para copiar a profile da sua máquina local para a rede, basta que o administrador copie todo o conteúdo da pasta C:\Documents and settings\Administrator para a pasta de cada usuário. Depois o administrador deve definir as permissões de acesso em cada profile criada no compartilhamento profiles. Por exemplo, na pasta \\srv01\profiles\jsilva, somente o usuário jsilva deve ter permissão de acesso, na pasta \\srv01\profiles\maria, somente o usuário maria deve ter permissão de acesso e assim por diante. O passo final, para que o usuário possa utilizar esta profile armazenada no servidor, é informar nas propriedades da conta do usuário, o caminho para a respectiva profile. Isso é feito na guia Perfil, das propriedades da conta do usuário. Por exemplo, nas propriedades da conta do usuário jsilva o administrador informa o caminho \\srv01\profiles\jsilva, nas propriedades da conta do usuário maria o administrador informa o caminho \\srv01\profiles\maria e por aí vai. Feito isso, sempre que o usuário fizer alterações em suas configurações do ambiente de trabalho do Windows, estas alterações serão salvas na profile armazenada no servidor. Por exemplo, quando o usuário jsilva faz alterações nas configurações do ambiente de trabalho, estas alterações são salvas em \\srv01\profiles\jsilva. Quando o usuário jsilva fizer o logon em uma outra estação de trabalho da rede (diferente da estação na qual ele fez as alterações), as suas configurações serão carregadas (durante o logon), a partir de \\srv01\profiles\jsilva, em qualquer computador do domínio, onde o usuário faça o logon. Com isso as alterações que ele fez em uma estação de trabalho, estarão disponíveis em quaisquer estação da rede na qual ele fizer o logon, pois estas configurações são copiada a partir do servidor e “seguem” (viajam com – Roaming) o usuário em qualquer estação de trabalho na qual ele fizer o logon. Combinando o uso de Roaming Profiles com GPOs (Capítulo 18 do livro: Windows Server 2003 – Curso Completo, 1568 páginas), é possível que o ambiente de trabalho do usuário “siga o usuário” através da rede.

- ◆ **Mandatory user profile:** Este tipo de profile é uma profile do tipo somente leitura. As alterações feitas pelo usuário não serão salvas na profile. Quando o usuário fizer o logon, ele obtém sempre o mesmo ambiente de trabalho, independente das alterações que ele fez durante o seu último logon (alterações estas que são abandonadas). Este tipo de profile não permite que o usuário faça alterações nas configurações definidas na profile. O usuário até consegue alterar o seu ambiente de trabalho, mas no momento em que ele fizer o log off, as alterações não serão salvas. Ao fazer o próximo logon, o usuário receberá as configurações definidas na profile que está no servidor, sem as alterações que ele fez, mas que não foram salvas. As configurações são copiadas para o computador do usuário cada vez que este faz o logon. Quando o usuário faz alterações, estas são feitas na sua cópia local da profile. Ao fazer o log off, estas alterações não são repassadas

**IMPORTANTE:** Ao informar o caminho da profile, ao invés de usar diretamente o nome de logon do usuário, você pode utilizar a variável %username%. Desta maneira, o próprio Windows, ao salvar as alterações nas propriedades da conta do usuário, substitui %username% pelo nome de logon do usuário. O uso da variável %username% é recomendada, pois evita problemas

para a profile que está gravada no servidor. No próximo logon é esta profile que está no servidor (sem alterações) que é novamente copiada para a estação de trabalho do usuário, sobrescrevendo as alterações que por ventura ele tenha feito. O resultado prático é que sempre que o logon é feito, são carregadas as configurações definidas na profile do tipo Mandatory, armazenada no servidor e para a qual somente o Administrador tem permissão para fazer alterações. Este tipo de profile é utilizado para manter ambientes altamente padronizados, onde os usuários não devem poder fazer alterações nas configurações do seu ambiente de trabalho. Somente o administrador pode fazer alterações na profile do tipo Mandatory, armazenada no servidor. Na prática, a maioria das configurações de uma profile estão em um arquivo chamada NTUser.dat. Para tornar uma profile do tipo Mandatory, basta renomear este arquivo para NTUser.man. Não esqueça deste detalhe.

**com erros de digitação. Desta forma, você informa o caminho da profile dos usuários, usando o seguinte formato: \\srv01\profiles\%username%, neste caso supondo que as profiles são armazenadas em uma pasta compartilhada como profiles, no servidor srv01.**

- ◆ **Temporary user profile:** Uma profile temporária será criada sempre que algum erro ocorrer durante o logon do usuário, erro este que impeça que uma profile seja carregada, quer seja uma profile local, quer seja uma profile carregada a partir de um servidor. Alterações feitas nesta profile temporária (enquanto o usuário está logado) serão descartadas quando o usuário fizer o log off.

## Entendendo o conteúdo de uma User profile

Neste item descreverei em detalhes as configurações e o conteúdo que é salvo em um profile de usuário. Conforme descrito anteriormente, todas as informações de configuração contidas na Profile do usuário são gravadas em um conjunto de arquivos e pastas dentro de uma pasta com o nome de logon de usuário, no caminho C:\Documents and settings. Por exemplo, as configurações da profile local para o usuário jsilva são gravadas em um conjunto de arquivos e pastas dentro de C:\Documents and settings\jsilva.

Dentro da pasta onde fica a profile de cada usuário, existem uma série de subpastas. Por exemplo, dentro da pasta C:\Documents and settings\Administrator existem diversas outras pastas, conforme indicado na Figura 14.19. Cada uma tem uma função específica.

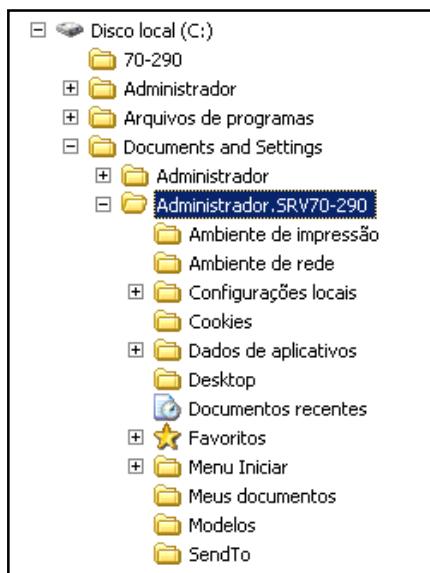


Figura 14.19 Subpastas da profile de usuário.

**IMPORTANTE: A primeira vez que o usuário faz o logon em um computador, o Windows Server 2003 (ou Windows 2000 ou NT 4 ou XP) cria a profile do usuário, baseada na profile Default User (C:\Documents and settings\Default User). Se você quiser que determinados itens, tais como atalhos, estejam presentes para todos os novos usuários que fizerem o logon em um computador, você deve acrescentar estes itens à profile Default User. A maioria das configurações da profile estão contidas no arquivo NTUser.dat. Por exemplo, para o usuário jsilva as configurações estão no arquivo**

A seguir descrevo o conteúdo destas pastas:

- ◆ **Application Data (Dados de Aplicativo):** Nesta pasta ficam configurações dos programas utilizados no computador. Por exemplo, configurações do Outlook Express, do Office, tais como modelos e dicionários personalizados criados pelo usuário e assim por diante.
- ◆ **Cookies:** Informações do usuário referentes a sites que ele visitou. Por exemplo, existem sites no qual você deve fazer um cadastro para fazer compras. A maioria dos sites de livrarias on-line, por exemplo, exige o cadastro. Você faz o cadastro e preenche um formulário. Algumas destas informações são gravadas em pequenos arquivos conhecidos como Cookies. Futuramente, quando você visita o site novamente, você é surpreendido com uma mensagem Bem vindo fulano de tal. Mas como é que o site sabe que você é o fulano de tal? Ele leu as informações no Cookie que ele havia gravado anteriormente. Os cookies gravados pelos diversos sites que você visita ficam gravados na pasta Cookies, dentro da profile do usuário.
- ◆ **Desktop:** Esta pasta contém os atalhos, arquivos, pastas e demais itens que são exibidos na área de trabalho do usuário.
- ◆ **Favoritos:** Contém a estrutura de Favoritos do Internet Explorer.
- ◆ **Configurações locais:** Configurações de aplicativos locais, o histórico de navegação na Internet e arquivos temporários. Estas informações “viajam” com o usuário, isto é, acompanham o usuário pela rede quando este está utilizando Roaming Profiles.
- ◆ **Meus documentos:** Esta é a pasta padrão para gravação dos arquivos de dados do usuário. Por exemplo, quando você executa o comando Arquivo -> Salvar, no Word, por padrão é selecionada a pasta Meus documentos.
- ◆ **Documentos Recentes:** Contém atalhos para os documentos recentemente utilizados pelo usuário. Estes atalhos facilitam a abertura de documentos e pastas que o usuário está utilizando seguidamente.
- ◆ **Ambiente de rede:** Contém atalhos para os itens contidos na opção Meus locais de rede.
- ◆ **Ambiente de impressão:** Atalhos para as impressoras instaladas pelo usuário.
- ◆ **SendTo:** Contém atalhos para os itens que aparecem quando você clica com o botão direito do mouse em um arquivo ou pasta e seleciona o comando Enviar para. Por exemplo, se você quer que apareça no menu Enviar para o nome de uma pasta onde você faz cópias de Backup, basta adicionar um atalho para esta pasta, dentro da pasta SendTo, na profile do usuário.
- ◆ **Menu Iniciar:** Esta pasta contém uma subpasta chamada Programas. Esta subpasta contém todos os itens do menu Todos os programas.
- ◆ **Modelos:** Arquivos de modelos do Office, utilizados pelo usuário.
- ◆ **A profile do usuário também contém o arquivo NTUser.dat:** O arquivo NTUser.dat contém a parte das configurações que são armazenadas na Registry do sistema (para mais detalhes sobre a Registry consulte o Capítulo 12). Enquanto o usuário está logado e faz alterações em suas configurações, estas são feitas diretamente na Registry (mais especificamente na chave HKEY\_CURRENT\_USER). Quando o usuário faz o log off, o Windows grava as alterações feitas pelo usuário no arquivo NTUser.dat. Com isso na próxima vez que o usuário fizer o logon, o Windows lê as configurações a partir do arquivo NTUser.dat e carrega-as novamente na Registry. O efeito prático é que as alterações são mantidas e o usuário recebe o mesmo ambiente de trabalho de quando ele fez o log off pela última vez.

C:\Documents and settings\jsilva\NTUser.dat. As configurações do menu Todos os programas (All programs) são copiadas da profile All Users (C:\Documents and settings\All Users\Start Menu\ Programs. Ou seja, os atalhos que estão dentro desta pasta, automaticamente serão copiados para a nova profile que é criada, a primeira vez que o usuário faz o logon no computador.

## A pasta All Users

Dentro da pasta Documents and Settings, existe uma profile chamada All Users. As configurações desta pasta definem itens do menu programas e atalhos da área de trabalho, os quais estarão disponíveis para qualquer usuário que fizer o logon no computador. Por exemplo, se você quer que um atalho para uma determinada pasta seja exibida na área de trabalho, independentemente do usuário logado. É só colocar este atalho na pasta Desktop da profile All Users. Quando o usuário faz o logon, o Windows utiliza as configurações da profile do próprio usuário, mas os atalhos da área de trabalho, do menu Todos os programas e da barra de tarefas da profile All Users.

A profile All Users contém atalhos para os chamados programas comuns, ou seja, programas que estão disponíveis para todos os usuários que fizerem o logon no computador. Os atalhos para programas individuais ou privativos, ou seja, somente disponíveis para um determinado usuário, são gravados na profile do respectivo usuário.

A seguir descrevo quais as configurações que são gravadas na profile de cada usuário e, portanto, são individualizadas para cada usuário que faz o logon no computador.

- ◆ Configurações feitas no Windows Explorer, tais como Opções de pasta, de visualização e assim por diante.
- ◆ Arquivos da pasta Meus documentos. A pasta Meus documentos é individualizada para cada usuário.
- ◆ Minhas figuras: Esta pasta fica dentro da pasta Meus documentos e é a pasta padrão para gravação de figuras. Por exemplo, quando você usa o comando Arquivo -> Salvar no Paint Brush, por padrão já vem selecionada a pasta Minhas figuras.
- ◆ Favoritos do Internet Explorar. A lista de favoritas também é individual, ou seja, fica gravada na profile de cada usuário.
- ◆ Drives de rede mapeados via script de logon ou manualmente mapeados pelo usuário.
- ◆ Informações da pasta Meus locais de rede, a qual contém atalhos para outros computadores e recursos da rede.
- ◆ Os itens da área de trabalho.
- ◆ Configurações do vídeo.
- ◆ Configurações de aplicativos (tais como Office, Outlook Express, Internet Explorer, etc.)
- ◆ Configurações de impressoras.
- ◆ Conexões de rede.
- ◆ Configurações feitas através das opções do Painel de controle

**IMPORTANTE:** Por padrão algumas pastas da profile do usuário são marcadas como pastas ocultas e não serão exibidas no Windows Explorer, a não ser que você configure o Windows para exibir pastas e arquivos ocultos. Por padrão as seguintes pastas são ocultas: Ambiente de rede, Ambiente de impressão, Configurações locais, Arquivos recentes e Modelos. Para exibir os arquivos e pastas ocultas abra o Windows Explorer, selecione o comando Ferramentas -> Opções de pasta, clique na guia Exibir e marque a opção Exibir pastas e arquivos ocultos. Clique em OK.

**IMPORTANTE:** Em um computador com o Windows Server 2003, somente usuários com permissão de administrador terão permissão para modificar a pasta All Users. Neste caso, se você deseja instalar um programa cujo atalho deve estar disponíveis para todos os usuários do computador, você deve estar logado com uma conta com permissão de administrador, para fazer a instalação do programa. Se a instalação for feita com uma conta que não tem permissão de administrador, o atalho será criado somente na profile da conta logada. Quando outros usuários fizerem o logon, o respectivo atalho não estará disponível. Este é um dos erros mais comuns e que geram muitas chamadas do suporte. Do outro lado da linha o usuário diz: "O Programa X não está instalado na minha máquina". Na verdade o programa X está instalado, o que acontece é que não foi criado o atalho para o programa. [www.juliobattisti.com.br](http://www.juliobattisti.com.br)

# Menu Acessórios

Outros programas instalados e que tenham sido programados para manter configurações separadas para cada usuário e salvar estas configurações na profile do usuário. Os programas que tem o logo do Windows Server 2003, ou seja, aprovados para uso no Windows Server 2003, devem ser capazes de gravar configurações separadas para cada usuário.

Atalhos colocados como favoritos na documentação do Windows Server 2003, também são individualizados por usuário.

## Opções de configuração da guia Perfil, das propriedades de uma conta de usuário:

Na guia Perfil você pode informar mais algumas configurações, conforme descrito a seguir:

- ◆ **Script de logon:** Neste campo você informa o nome do script de logon (normalmente um arquivo .bat ou .cmd), que será executado quando o usuário fizer o logon. O script de logon normalmente é um arquivo .bat e deve ser gravado em uma pasta específica nos controladores de domínio. Em todo DC do domínio existe um compartilhamento chamado Netlogon. É neste compartilhamento que deve ser gravado um ou mais arquivos que serão utilizados como script de logon. O próximo passo é informar, no campo Script de logon, o nome do script associado com a conta do usuário. Durante o logon, o Windows Server 2003 procura, no compartilhamento Netlogon, do DC que está autenticando o usuário, um arquivo com o nome informado no campo Script de logon. Se o arquivo for encontrado e for um arquivo com comandos válidos, os comando serão executados. Neste script devem ser colocados comandos que devem ser executados automaticamente quando o usuário faz o logon, como por exemplo comandos para mapear unidades de rede, atulizar o anti-vírus e assim por diante. O conteúdo do compartilhamento Netlogon é replcado, automaticamente, pelo Active Directory, entre todos os DCs do domínio.
- ◆ **Pasta base (Home folder) :** Neste grupo o administrador pode informar um caminho local, como por exemplo c:\documentos ou um drive de rede por exemploX:, associado com o caminho \\srv01\home\jsilva. O conceito de pasta base pode ser utilizado para consolidar os arquivos de dados dos usuários em um ou mais servidor da rede. Isso traz muitas vantagens, sendo a principal delas a possibilidade de fazer o backup dos dados dos usuários de uma maneira centralizada. Ao invés de gravar os dados no próprio computador, o usuário pode salvá-los em sua pasta base, diretamente no servidor. A grande vantagem é que o usuário terá acesso a esta pasta em qualquer computador da rede onde ele fizer o logon e não apenas no seu próprio computador. A desvantagem é que se o usuário estiver sem acesso a rede, ele perderá acesso a estes dados (este problema pode ser minimizado com o uso de Pastas Off-line, conforme mostrei no Capítulo 6). Para montar uma estrutura de pastas base, o administrador deve reservar espaço em um volume em um dos servidores da rede. Em seguida ele cria uma pasta, por exemplo ele pode criar uma pasta chamada homeusers. Dentro desta pasta o administrador cria uma subpasta para cada usuário que irá utilizar uma pasta base. Por exemplo, ele cria uma subpasta jsilva, a qual será a pasta base da conta de logon jsilva, cria uma subpasta maria, a qual será a pasta base da conta de logon maria e assim por diante. Cada pasta individual é compartilhada, com o nome de compartilhamento igual ao nome de logon. Por exemplo, a pasta jsilva é compartilhada como jsilva, a pasta maria é compartilhada como maria e assim por diante. Com isso o caminha da pasta base dos usuários jsila e maria fica conforme exemplo a seguir:

**\\srv01\homeusers\jsilva**

**\\srv01\homeusers\maria**

O próximo passo é definir as permissões de acesso em cada pasta. Por padrão deve ser definido que apenas o próprio usuário deve ter permissão de acesso a sua pasta base. Dependendo das políticas de segurança da empresa, pode ser

necessário definir permissão de acesso também para o grupo Administradores do domínio. Criada a estrutura de pastas em um dos servidores da rede, agora é só informar no campo Conectar, a letra do drive que será associado a pasta base do usuário. No campo “a”, o administrador informa o caminho de rede para a pasta base do usuário. No exemplo da Figura 14.20 está sendo associado o drive X, com a pasta base \\srv01\homeusers\jsilva. Neste exemplo, toda vez que o usuário jsilva fizer o logon, em qualquer computador da rede, será disponibilizado um drive X:, o qual está associado com o caminho \\srv01\homeusers\jsilva.

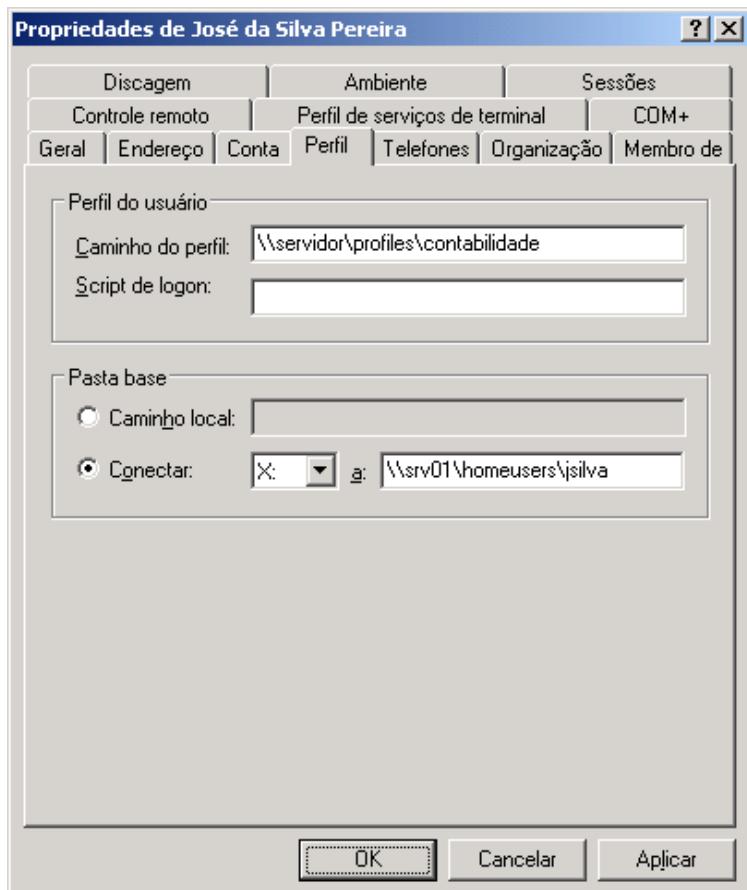


Figura 14.20 Informando o caminho da pasta base e da profile do usuário.

Ao salvar as alterações, o Windows Server 2003 substitui %username% pelo nome de logon do usuário, o que reduz erros devido a erros de digitação no nome de logon do usuário.

## Mais algumas observações sobre contas de usuários:

**IMPORTANTÍSSIMO:** Por que nomes iguais não significam contas iguais?

Esta é uma questão fundamental e um erro comum que Administradores com pouca experiência podem cometer. Me explico melhor. Quando você cria uma conta de usuário (quer seja uma conta local quer seja uma conta no domínio), você atribui um nome de logon para a conta, por exemplo: jsilva. Além do nome, o Windows Server 2003 cria um SID – Security Identifier (Identificador de segurança) para cada objeto do Active Directory. Para o Windows Server 2003 o que vale, na prática, é o SID do objeto. Agora imagine que você criou o usuário

---

**IMPORTANTE:** Ao invés de informar o nome do usuário, no caminho da pasta base, você pode utilizar a variável %username%, conforme exemplo a seguir:  
\\srv01\homeusers\%username%

jsilva, incluiu ele em diversos grupos e atribuiu permissões de acesso para este usuário. Internamente, o que o Windows Server 2003 usa para identificar o usuário jsilva é o SID associado a conta jsilva. O erro que muitos administradores cometem é o seguinte:

Vamos supor que, por engano, a conta jsilva foi excluída. Você pode raciocinar assim: não tem problema, é só criar a conta jsilva novamente, definir a mesma senha e incluí-la nos mesmos grupos de antes que automaticamente a conta jsilva terá todas as permissões de acesso que tinha antes. Certo? Nada disso, absolutamente errado. Ao excluir a conta e criá-la novamente, um novo SID será gerado para a conta jsilva. Embora o nome de logon seja o mesmo, para o Windows Server 2003 é como se fossem contas completamente diferentes. Porém, nos recursos da rede, está a permissão de acesso para o SID antigo. Por isso que a nova conta, mesmo com o mesmo nome, não consegue acessar os recursos que a antiga acessava, pois são SIDs diferentes. Na prática o que tem que ser feito é excluir a conta jsilva das listas de permissão de todos os recursos e incluí-la novamente, para que seja utilizado o novo SID. Veja que é um trabalho e tanto, mas existem motivos relacionados à segurança, para que seja utilizado um SID associado com cada objeto do Active Directory, conforme descreverei na parte de segurança, mais adiante.

Então não esqueça: Ao excluir uma conta e criá-la novamente, com o mesmo nome e a mesma senha, para o Windows Server 2003 não é a mesma conta, porque um novo SID foi gerado quando a conta é criada novamente. Por exemplo, se você havia criptografado uma pasta com a conta antiga, a nova conta, mesmo tendo o mesmo nome e a mesma senha, não conseguirá descriptografar esta pasta, porque para o Windows é uma conta diferente, porque o SID interno é diferente.

Outra situação que pode acontecer é simplesmente o usuário esquecer a senha da sua conta. Situação que é comum em ambientes de redes com múltiplos diretórios, o que é sinônimo de múltiplas senhas para lembrar, conforme descrito no Capítulo 2. Quando o usuário esquece a senha, o administrador pode definir uma nova senha para a conta do usuário. O administrador deve definir a nova senha, informá-la ao usuário usando os procedimentos definidos nas políticas de segurança da empresa e deve configurar a conta do usuário para que seja solicitada a troca da senha no primeiro logon. Esta última opção é importante para que o usuário possa trocar a sua senha, de tal maneira que somente ele saiba a senha de sua conta (e de preferência não esqueça mais).

## Built-in Groups.

Quando um domínio é criado (com a instalação do Active Directory no primeiro DC do domínio), uma série de grupos são criados. Estes grupos podem ser acessados usando o console Usuários e computadores do Active Directory. Na opção Built-in são exibidos os grupos locais do domínio, criados automaticamente durante a criação do domínio, conforme indicado na Figura 14.21:

**IMPORTANTE:** Desabilitar é diferente de bloquear. Uma conta é bloqueada, automaticamente, quando o usuário tenta fazer o logon sem sucesso (por exemplo, digitou a senha incorretamente), um determinado número de vezes (por padrão três vezes) dentro de um período determinado (por padrão uma hora). Nesta situação o Active Directory bloqueia a conta automaticamente. O administrador pode acessar as propriedades de uma conta bloqueada, clicar na guia Conta e desmarcar a opção A conta está bloqueada, para desbloquear a conta. Por padrão a conta será desbloqueada, automaticamente, dentro de 24 horas, caso o administrador não a tenha desbloqueado manualmente.

**Usuários e computadores do Active Directory**

| Builtin 16 objetos                      |                                    |  |
|---|------------------------------------|--|
| Nome                                    | Tipo                               | Descrição  |
| Acesso compatível com versões ant...    | Grupo de segurança - Domínio local | Um grupo compatível com versões anteriores que permite o a...    |
| Administradores                         | Grupo de segurança - Domínio local | Os administradores têm acesso completo e irrestrito ao comp...   |
| Convidados                              | Grupo de segurança - Domínio local | Por padrão, os convidados têm o mesmo acesso como membro...      |
| Criadores de confiança de floresta d... | Grupo de segurança - Domínio local | Membros deste grupo podem criar relações de confiança de e...    |
| Duplicadores                            | Grupo de segurança - Domínio local | Permite a duplicação de arquivos em um domínio                   |
| Grupo de acesso de autorização Win...   | Grupo de segurança - Domínio local | Membros deste grupo têm acesso ao atributo calculado token...    |
| Operadores de configuração de rede      | Grupo de segurança - Domínio local | Membros do grupo podem ter alguns privilégios administrativo...  |
| Operadores de cópia                     | Grupo de segurança - Domínio local | Os operadores de cópia podem substituir as restrições de seq...  |
| Oper. de contas                         | Grupo de segurança - Domínio local | Os membros podem administrar contas de usuários e grupos i...    |
| Oper. de impressão                      | Grupo de segurança - Domínio local | Os membros podem administrar impressoras do domínio              |
| Oper. de servidores                     | Grupo de segurança - Domínio local | Os membros podem administrar servidores do domínio               |
| Servidores de licenças do Terminal S... | Grupo de segurança - Domínio local | Servidores de licenças do Terminal Server                        |
| Usuários                                | Grupo de segurança - Domínio local | Os usuários são impedidos de fazer alterações acidentais ou i... |
| Usuários da área de trabalho remota     | Grupo de segurança - Domínio local | Os membros deste grupo têm direito a fazer logon remotamente     |
| Usuários de log de desempenho           | Grupo de segurança - Domínio local | Membros deste grupo têm acesso remoto para agendar logs i...     |
| Usuários de monitor de desempenho       | Grupo de segurança - Domínio local | Membros deste grupo têm acesso remoto para monitorar este...     |

Figura 14.21 Grupos locais do domínio, criados automaticamente.

Outros grupos também são criados automaticamente. Estes grupos ficam na opção Users. Nesta opção são criados grupos Locais, Globais e universais, conforme indicado na Figura 14.22:

**Usuários e computadores do Active Directory**

| Users 16 objetos               |                                    |   |
|--------------------------------|------------------------------------|---|
| Nome                           | Tipo                               | Descrição   |
| Administração de empresa       | Grupo de segurança - Universal     | Administradores designados da empresa                                     |
| Administrador                  | Usuário                            | Conta interna para a administração do computador/domínio                  |
| Administradores de esquemas    | Grupo de segurança - Universal     | Administradores designados do esquema                                     |
| Admins. do domínio             | Grupo de segurança - Global        | Administradores designados do domínio                                     |
| Computadores do domínio        | Grupo de segurança - Global        | Todas as estações de trabalho e servidores incluídos no domínio           |
| Controladores de domínio       | Grupo de segurança - Global        | Todos os controladores de domínio no domínio                              |
| Convidado                      | Usuário                            | Conta interna para acesso como convidado ao computador/domínio            |
| Convidados domínio             | Grupo de segurança - Global        | Todos os convidados do domínio  |
| DnsAdmins                      | Grupo de segurança - Domínio local | Grupo de administradores DNS  |
| DnsUpdateProxy                 | Grupo de segurança - Global        | Os clientes DNS que possuem permissão para executar atualizações di...    |
| Editores de certificados       | Grupo de segurança - Domínio local | Os membros deste grupo têm direito a publicar certificados no Active C... |
| José da Silva Pereira          | Usuário                            | Funcionários da seção de Contabilidade                                    |
| Maria José da Silva            | Usuário                            |   |
| Proprietários criadores de ... | Grupo de segurança - Global        | Membros desse grupo podem modificar a diretiva de grupo do domínio        |
| Servidores RAS e IAS           | Grupo de segurança - Domínio local | Os servidores neste grupo podem acessar propriedades de acesso ren...     |
| Usuários do domínio            | Grupo de segurança - Global        | Todos os usuários do domínio  |

Figura 14.22 Grupos locais, globais e universais, criados automaticamente na opção Users.

A seguir descrevo os diversos grupos que são criados automaticamente pelo Active Directory, os chamados Built-in groups.

Grupos locais criados na opção Built-in:

- ◆ **Account Operators (Operadores de conta):** Membros deste grupo podem criar, modificar e excluir contas de usuários, grupos e computadores localizadas nas opções Users e Computers e também localizadas em Unidades organizacionais do domínio. A exceção são as contas de DCs localizadas na opção Domain Controllers, para as quais somente membros do grupo Administradores tem permissão. Membros do grupo Account Operators não poderão modificar a conta Administrator (Administrador) e nem o grupo Domain Admins (Admins. do Domínio). Também não tem permissão para modificar as contas que pertencem ao grupo Domain Admins. Observe que o objetivo é impedir que membros deste grupo possam se incluir no grupo Admins. ou modificar uma conta que já está neste grupo (por exemplo alterando a senha de uma destas contas), para poder fazer o logon com permissão de administrador. Os membros deste grupo podem fazer o logon local nos DCs do domínio e também tem permissão para desligar estes servidores. Membros deste grupo tem um nível de permissão elevado, principalmente pelo fato de poder alterar contas de usuários, por isso o administrador deve ter cuidado ao adicionar membros a este grupo. Por padrão os membros deste grupo também tem os seguintes direitos de usuário: Allow log on locally; Shut down the system.
- ◆ **Administrators (Administradores):** Podem tudo dentro do domínio. Membros deste grupo tem controle e permissão total, em todos os DCs do domínio. Por padrão, o grupo Domain Admins (Adminis. do Domínio) e o grupo Enterprise Admins (“maravilhosamente” traduzido como Administradores de empresa), são membros do grupo local Administrators. A conta Administrator (Administrador) também é membro deste grupo, por padrão. Por padrão os membros deste grupo também tem os seguintes direitos de usuário: Access this computer from the network; Adjust memory quotas for a process; Back up files and directories; Bypass traverse checking; Change the system time; Create a pagefile; Debug programs; Enable computer and user accounts to be trusted for delegation; Force a shutdown from a remote system; Increase scheduling priority; Load and unload device drivers; Allow log on locally; Manage auditing and security log; Modify firmware environment values; Profile single process; Profile system performance; Remove computer from docking station; Restore files and directories; Shut down the system; Take ownership of files or other objects. Como os membros deste grupo tem controle total em todos os DCs do domínio, seja cuidadoso e somente adicione novos membros a este grupo quando realmente for necessário.
- ◆ **Backup Operators (Operadores de Cópia):** Os membros deste grupo podem fazer o backup de pastas e arquivos, mesmo que não tenham permissão de acesso (permisões NTFS – Capítulo 6) as pastas e arquivos. Isso permite que a administração das cópias de segurança (backup) seja realizada centralizadamente, sem que tenha que ser atribuída permissão de acesso para o administrador do backup, em todos os recursos que fazem parte do backup. Por padrão este grupo não tem nenhum membro. O administrador deverá adicionar membros a este grupo. Por padrão os membros deste grupo também tem os seguintes direitos de usuário: Back up files and directories; Allow log on locally; Restore files and directories; Shut down the system
- ◆ **Guests (Convidados):** Por padrão, o grupo Domain Guests (Convidados do Domínio) e a conta Guest (Convidado) são membros deste grupo. Por padrão nenhum direito de usuário é atribuído a este grupo.
- ◆ **Incoming Forest Trust Builders (Criadores de confiança de floresta de entrada):** Membros deste grupo tem permissão para criar relações de confiança one-way (unilateral) com domínio root de outras florestas. Por

**IMPORTANTE:** Os direitos de usuários são uma série especial de permissões (tais como fazer o logon localmente, desligar o servidor, incluir um computador no domínio e assim por diante), as quais são atribuídas a grupos e usuários. O administrador pode atribuir diferentes direitos para grupos e usuários.

exemplo, membros deste grupo, pertencente a um domínio da floresta A, podem criar uma relação de confiança one-way (unilateral) com um domínio pertencente a uma floresta X, de tal maneira que as contas do domínio na floresta A, podem receber permissões de acesso aos recursos do domínio na floresta X, ou seja, o domínio na floresta X, passou a confiar nas contas do domínio da floresta A. Este grupo, por padrão, não tem nenhum membro e também não tem nenhum direito de usuário atribuído ao grupo.

- ◆ **Network Configuration Operators (Operadores de Configurações de Rede):** Membros deste grupo podem fazer alterações nas configurações do TCP/IP nos DCs do domínio e também podem usar o comando ipconfig/renew e o comando ipconfig/release. Por padrão este grupo não tem nenhum membro e nenhum direito de usuário é atribuído a este grupo.
- ◆ **Performance Monitor Users (Usuários do monitor de Desempenho):** Membros deste grupo tem permissão para usar o Console de Desempenho para monitorar os contadores de desempenho dos DCs, tanto localmente quanto a partir de uma estação de trabalho da rede. Estas permissões, por padrão, são atribuídas a este grupo e aos grupos Administrators (Administradores) e Performance Log Users (Usuários dos log de desempenho). Por padrão este grupo não tem nenhum membro e nenhum direito de usuário é atribuído a este grupo.
- ◆ **Performance Log Users (Usuários dos log de desempenho):** Membros deste grupo tem permissão para usar o Console de Desempenho para monitorar os contadores e logs de desempenho, bem como alertas de desempenho nos DCs, tanto localmente quanto a partir de uma estação de trabalho da rede. Estas permissões, por padrão, são atribuídas a este grupo e aos grupos Administrators (Administradores) e Performance Log Users (Usuários de log de desempenho). Por padrão este grupo não tem nenhum membro e nenhum direito de usuário é atribuído a este grupo.
- ◆ **Pre-Windows 2000 Compatible Access (Acesso compatível com versões anteriores ao Windows 2000):** Membros deste grupo tem permissão de acesso de leitura (Read) em todos os objetos do tipo usuários e grupos do domínio. Este grupo é disponibilizado por questões de compatibilidade com estações de trabalho rodando o Windows NT 4.0 ou versão anterior. Por padrão, o objeto Everyone (Todos) é membro deste grupo. Somente adicione usuários a este grupo, se eles estiverem utilizando uma estação de trabalho com o NT 4.0 ou versão anterior. Por padrão os membros deste grupo também tem os seguintes direitos de usuário: Access this computer from the network; Bypass traverse checking.
- ◆ **Print Operators (Oper. de Impressão):** Membros deste grupo tem permissão para gerenciar, criar, compartilhar e excluir impressoras conectadas em DCs do domínio. Eles também tem permissão para gerenciar impressoras que foram publicadas no Active Directory (No Capítulo 7 você aprenderá a publicar e a pesquisar impressoras no Active Directory). Os membros deste grupo também tem permissão para fazer o logon localmente e para desligar os DCs do domínio. Por padrão este grupo não tem nenhum membro. Por padrão os membros deste grupo também tem os seguintes direitos de usuário: Allow log on locally; Shut down the system..
- ◆ **Remote Desktop (Usuários da área de trabalho remota):** Membros deste grupo tem permissão para fazer o logon remotamente nos DCs do domínio. É a mesma funcionalidade de desktop remoto, introduzida inicialmente no Windows XP. Você aprendeu a utilizar esta funcionalidade no Capítulo 12. Por padrão este grupo não tem nenhum membro e nenhum direito de usuário é atribuído a este grupo.
- ◆ **Replicator (Duplicadores):** Este grupo dá suporte as funcionalidades de replicação do Active Directory e é utilizado pelo serviço de replicação de arquivos que roda nos DCs do domínio. Não adicione usuários a este grupo. Por padrão este grupo não tem nenhum membro e nenhum direito de usuário é atribuído a este grupo.

**IMPORTANTE:** Não esqueça que, para que um usuário possa fazer o logon via Terminal Services, sendo um usuário sem privilégios de administrador, este usuário deve pertencer ao grupo Usuários da área de trabalho remota. Por exemplo, se um usuário estiver tendo permissão negada para acessar um servidor, via Terminal Services, a solução é induzir a conta deste usuário, no grupo Usuários da área de trabalho remota.

- ◆ **Server Operators (Operadores de Servidores):** Os membros deste grupo podem realizar uma série de operações nos DCs do domínio, tais como: logar localmente, criar e deletar compartilhamentos, inicializar e parar serviços, fazer o backup e o restore de arquivos, formatar um disco rígido e desligar o servidor. Por padrão este grupo não tem nenhum membro. Por padrão os membros deste grupo também tem os seguintes direitos de usuário: Back up files and directories; Change the system time; Force shutdown from a remote system; Allow log on locally; Restore files and directories; Shut down the system.
- ◆ **Users (Usuários):** Os membros deste grupo tem permissão para executar as tarefas mais comuns do dia-a-dia, tais como: executar programas, usar impressoras locais e da rede e bloquear o servidor. Por padrão os seguintes grupos são membros deste grupo: Domain Users (Usuários do domínio), Authenticated Users (Usuários autenticados) e Interactive (Interativo – este é um grupo especial interno do Windows Server 2003, o qual não é exibido no console Active Directory Users and Computers). Com isso qualquer conta do domínio fará parte deste grupo. Por padrão nenhum direito de usuário é atribuído a este grupo.

A seguir descrevo os grupos que são criados, automaticamente, na opção Users. Nesta opção são criados grupos locais, globais e universais, dependendo do modo de funcionalidade do domínio.

Grupos criados na opção Users:

- ◆ **Cert Publishers (Editores de certificados):** Grupo local. Membros deste grupo tem permissões para publicar certificados para contas de usuários e computadores. Por padrão este grupo não tem nenhum membro e nenhum direito de usuário é atribuído ao grupo.
- ◆ **DnsAdmins (em Português o nome também é DnsAdmins):** Grupo local. Este grupo somente é criado quando o DNS é instalado no servidor. Membros deste grupo tem acesso administrativo ao servidor DNS, ou seja, podem executar quaisquer ações nas configurações do servidor DNS. Por padrão este grupo não tem nenhum membro e nenhum direito de usuário é atribuído ao grupo.
- ◆ **DnsUpdateProxy (em Português o nome também é DnsUpdateProxy):** Grupo global. Este grupo somente é criado quando o DNS é instalado no servidor. Membros deste grupo são clientes DNS que podem fazer atualizações dinâmicas em nome de outros clientes, como por exemplo um servidor DHCP. Por padrão este grupo não tem nenhum membro e nenhum direito de usuário é atribuído ao grupo.
- ◆ **Domain Admins (Administradores do domínio):** Grupo global. Membros deste grupo tem controle total nos recursos do domínio. Por padrão, este grupo é membro do grupo local Administrators (Administradores) em todos os DCs, em todas as estações de trabalho e em todos os member servers do domínio. Esta inclusão é feita, automaticamente, quando a estação de trabalho ou o member server é configurado para fazer parte do domínio. Por padrão a conta Administrator (Administrador) faz parte deste grupo. Tenha cuidado ao incluir uma nova conta neste grupo, pois você dará “poderes” totais a esta conta. Por padrão os membros deste grupo também tem os seguintes direitos de usuário: Access this computer from the network; Adjust memory quotas for a process; Back up files and directories; Bypass traverse checking; Change the system time; Create a pagefile; Debug programs; Enable computer and user accounts to be trusted for delegation; Force a shutdown from a remote system; Increase scheduling priority; Load and unload device drivers; Allow log on locally; Manage auditing and security log; Modify firmware environment values; Profile

---

**NOTA: No Capítulo 16, do livro Windows Server 2003 – Curso Completo, 1568 páginas, quando você estudar o DNS e o DHCP em detalhes, você encontra uma descrição detalhada desta interação entre o DNS e o DHCP.**

---

single process; Profile system performance; Remove computer from docking station; Restore files and directories; Shut down the system; Take ownership of files or other objects.

- ◆ **Domain Computers (Computadores do domínio):** Grupo Global. Este grupo contém as contas de todas as estações de trabalho e servidores (member servers) que fazem parte do domínio. Por padrão, qualquer conta de computador criada no domínio, fará parte deste grupo. Por padrão nenhum direito de usuário é atribuído ao grupo.
- ◆ **Domain Controllers (Controladores de domínio):** Grupo Global. Este grupo contém as contas de todos os DCs do domínio. Por padrão nenhum direito de usuário é atribuído ao grupo.
- ◆ **Domain Guests (Convidados domínio):** Grupo Global. Este grupo contém a conta Convidado como seu único membro. Por padrão nenhum direito de usuário é atribuído ao grupo.
- ◆ **Domain Users (Usuários do domínio):** Grupo Global. Este grupo contém todos os usuários do domínio. Quando uma nova conta de usuário é criada, ela é automaticamente adicionada a este grupo. Este grupo pode ser utilizado para representar todos os usuários do domínio. Por exemplo, se você quer que todos os usuários do domínio tenham acesso de leitura aos arquivos de uma pasta compartilhada, basta dar permissão de leitura para este grupo. Por padrão nenhum direito de usuário é atribuído ao grupo.
- ◆ **Enterprise Admins (Administração de empresa – este grupo somente é exibido no domínio root de uma árvore de domínios):** Grupo Universal se o modo de funcionalidade do domínio aceita grupos Universais, caso contrário será um grupo Global. Membros deste grupo tem controle total em todos os domínios de uma floresta. Por padrão este grupo é membro do grupo Administrators (Administradores) em todos os DCs da floresta. Por padrão a conta Administrator (Administrador) é membro deste grupo. Existem determinadas operações que somente podem ser realizadas por membros deste grupo, como por exemplo autorizar um servidor DHCP no Active Directory (não esqueça deste importante detalhe). Por padrão, os membros deste grupo também tem os seguintes direitos de usuário: Access this computer from the network; Adjust memory quotas for a process; Back up files and directories; Bypass traverse checking; Change the system time; Create a pagefile; Debug programs; Enable computer and user accounts to be trusted for delegation; Force shutdown from a remote system; Increase scheduling priority; Load and unload device drivers; Allow log on locally; Manage auditing and security log; Modify firmware environment values; Profile single process; Profile system performance; Remove computer from docking station; Restore files and directories; Shut down the system; Take ownership of files or other objects.
- ◆ **Group Policy Creator Owners (Proprietários criadores de diretiva de grupo):** Grupo global. Membros deste grupo podem modificar as políticas de segurança (GPOs) do domínio. Por padrão a conta Administrator (Administrador) é membro deste grupo. . Por padrão nenhum direito de usuário é atribuído ao grupo.
- ◆ **IIS\_WPG (somente está disponível quando o IIS é instalado no servidor. Para detalhes sobre o IIS consulte o Capítulo 13):** Este grupo representa o processo de execução do IIS 6.0. Por padrão não tem nenhum membro e nenhum direito de usuário é atribuído a este grupo.
- ◆ **RAS and IAS Servers:** Servidores que são membros deste grupo tem permissão para acessar as propriedades de acesso remoto dos usuários. Por padrão nenhum direito é atribuído a este grupo.
- ◆ **Schema Admins (Administradores de esquemas – somente é exibido no domínio root):** Membros deste grupo podem modificar o esquema do Active Directory. Conforme vimos no Capítulo 2, o esquema é a definição da estrutura de dados do Active Directory. Por padrão a conta Administrator (Administrador) é membro deste grupo. Muito cuidado ao adicionar contas a este grupo, pois modificação indevidas no esquema podem causar verdadeiros desastres em todos os domínios da sua rede. Por padrão nenhum direito é atribuído a este grupo.

## Delegando tarefas administrativas a nível de OU:

Conforme descrito nos Capítulo 1 e 2 e “reforçado no capítulo 4”, uma das grandes vantagens/utilizações das OUs, é justamente a possibilidade de descentralizar tarefas administrativas, com a possibilidade de delegar permissões para determinados usuários executarem tarefas específicas, apenas nos objetos (usuários, grupos e computadores), contidos dentro de uma determinada OU.

Por exemplo, imagine uma rede onde temos um domínio chamado regiaosul.com.br. Neste domínio temos três redes locais, uma em Curitiba, outra em Florianópolis e outra em Porto Alegre. Você pode montar uma estrutura de tal maneira que apenas um grupo restrito (talvez um ou dois usuários), tenham poderes de Administrador em todo o domínio, isto é, somente um ou dois usuários pertençam ao grupo Admins. do domínio.

Em seguida você pode criar três unidades organizacionais, por exemplo: Curitiba, Florianópolis e Porto Alegre. O próximo passo é mover as contas de usuários, computadores e grupos da rede de Curitiba, para dentro da OU Curitiba; mover as contas de usuários, computadores e grupos da rede de Florianópolis para a OU Florianópolis e, por fim, mover as contas de usuários, computadores e grupos da rede de Porto Alegre para a OU Porto Alegre.

Agora você pode descentralizar algumas tarefas administrativas, dando permissões para que um ou mais usuários possam executar algumas tarefas administrativas nas contas de usuários, grupos e computadores da própria OU. Por exemplo, você pode criar um grupo chamada Administradores da OU Curitiba, dentro da OU Curitiba. Em seguida você pode delegar tarefas para este grupo, em relação a OU Curitiba. Por exemplo, você pode permitir que os membros do grupo Administradores da OU Curitiba, possam criar novas contas de usuários e editar as contas já existentes somente dentro da OU Curitiba. O mesmo pode ser feito em relação as demais OUs do domínio.

Observe que o com o uso de OUs, na prática, é possível descentralizar uma série de tarefas administrativas, delegando tarefas para que um administrador da própria OU, execute as tarefas mais comuns do dia-a-dia, tais como administração de contas de usuários e de recursos compartilhados, dentro dos recursos da própria OU. No Capítulo 4 você encontra um exemplo prático, de como delegar permissões a nível de OU.

## Propriedades e Permissões de Segurança em Unidades Organizacionais.

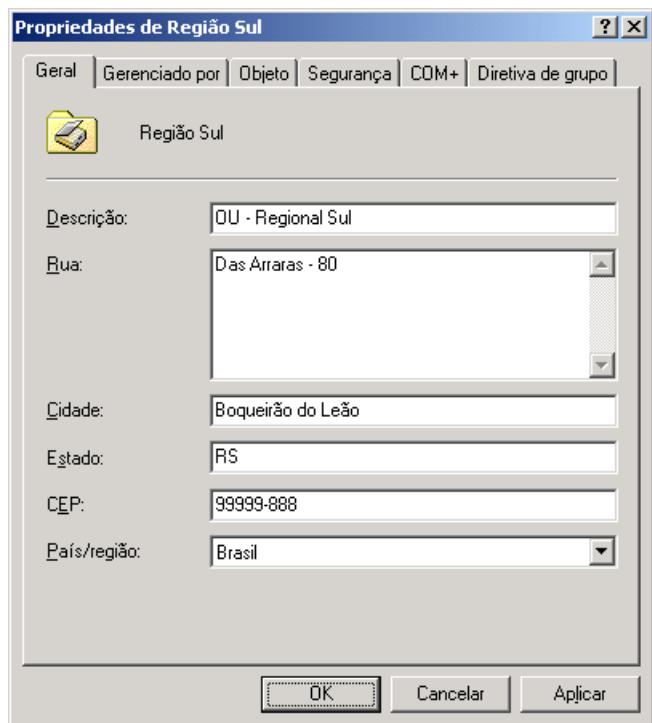
Todos os objetos do Active Directory (usuários, grupos, computadores, Unidades Organizacionais e assim por diante) tem um conjunto de propriedades e uma lista de permissões associadas. Neste item mostrarei as principais propriedades de uma OU e as configurações de segurança associadas.

---

**DICA:** Para que todas as opções da janela de propriedades de um objeto do Active Directory estejam disponíveis, você deve fazer com que as opções avançadas sejam exibidas. Para tal basta usar o comando Exibir -> Recursos avançados, no console Usuários e Computadores do Active Directory. Execute este comando antes de seguir adiante.

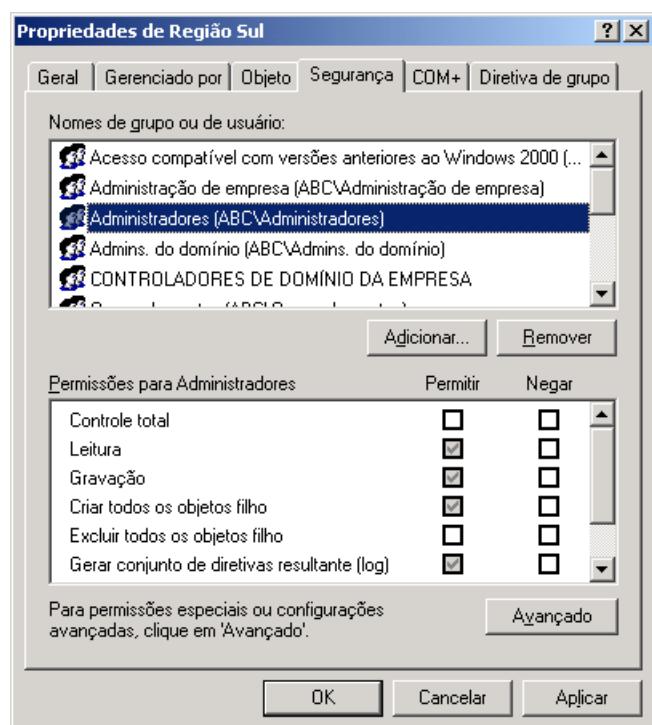
---

Para acessar as propriedades de uma OU, basta abrir o console Usuários e Computadores do Active Directory, localizar a OU desejada, clicar com o botão direito na OU e, no menu de opções que é exibido, clicar em Propriedades. Será exibida a janela de Propriedades da OU, com a guia Geral selecionada por padrão, conforme indicado na Figura 14.23:



**Figura 14.23 A janela de propriedades da OU.**

Na guia Geral são exibidas informações sobre a OU, tais como Cidade, país, etc. Na guia Gerenciado por você pode selecionar um usuários que será o contato e o responsável pelo gerenciamento da OU. Normalmente é o usuário que recebeu permissões para gerenciar os objetos da OU, através do uso do assistente para Delegação de controle, descrito anteriormente. Clique na guia Segurança. Será exibida uma lista de usuários e grupos, com permissões de acesso a OU e aos objetos da OU. Este é uma lista de permissão de segurança igual a tantas outras utilizadas no Windows Server 2003, como por exemplo uma lista de permissões NTFS de acesso a pastas e arquivos (Capítulo 6), conforme exemplo da Figura 14.24:



**Figura 14.24 Permissões básicas de segurança para a OU.**

Além das permissões básicas, tais como Controle total, Leitura, Gravação, Criar todos os objetos filho e Excluir todos os objetos filho, você pode definir permissões bem mais refinadas. Para isso clique no botão Avançado. Será exibida a janela de Configurações de controle de acesso. Para definir uma grande variedade de permissões para um determinado usuário ou grupo, clique no respectivo usuário ou grupo para selecioná-lo e em seguida clique no botão Exibir/editar... Será aberta a janela Entrada de permissão, na qual você tem um grande número de permissões, conforme indicado na Figura 14.25:

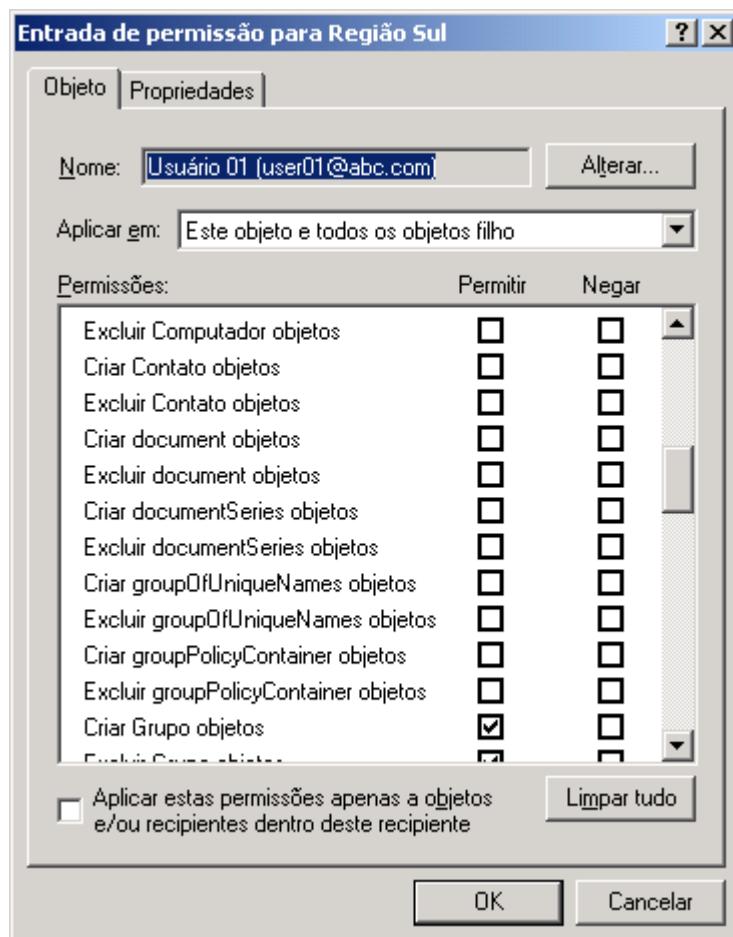


Figura 14.25 Diversas permissões de segurança para a OU.

Na lista aplicar em você ainda pode selecionar um determinado tipo de objeto. Ao selecionar um tipo de objeto, serão exibidas apenas as permissões relacionadas ao tipo de objeto selecionado. Após ter definido as permissões desejadas clique em OK. Você estará de volta à janela de Configurações de controle de acesso. Clique em OK para fechá-la. Você estará de volta à janela de propriedades da OU, com a guia Segurança selecionada. Clique em OK para fechá-la.

## Contas de computadores

Todos os computadores que executam o Windows NT, o Windows 2000, o Windows XP ou um servidor que executa Windows Server 2003 que se associa a um domínio têm uma conta de computador. Semelhantes a contas de usuário, as contas de computador fornecem um meio de autenticar e auditar o acesso do computador à rede e aos recursos de domínio. Cada conta de computador deve ser exclusiva, isto é, não podem haver duas contas, com o mesmo nome, no mesmo domínio.

As contas de usuário e computador são adicionadas, desabilitadas, redefinidas e excluídas usando o console Usuários e computadores do Active Directory. Uma conta de computador também pode ser criada quando você inclui um computador em um domínio. Uma conta de computador é mais um tipo de objeto, armazenado no Active Directory. Quando um administrador configura uma estação de trabalho, para fazer parte de um domínio, será criada no Active Directory, uma conta para o computador que está ingressando no domínio. O nome da conta terá o mesmo nome do computador.

Todo computador que faz parte de um domínio (com exceção de computadores com o Windows 95/98/Me), tem uma conta de computador criada no Active Directory. Além da conta é criada também uma senha, porém esta senha é gerada, automaticamente, pelo Active Directory. Esta senha também é alterada, periodicamente, pelo Active Directory.

Ao instalar o Windows Server 2003 em um servidor ou em uma estação de trabalho, o padrão é que o computador seja configurado para fazer parte de um Workgroup. Para que o computador faça parte de um domínio, baseado no Active Directory, você deve executar os seguintes passos:

- ◆ Criar uma conta de computador, com o mesmo nome do computador.
- ◆ Configurar o computador para fazer parte do domínio.
- ◆ NDComputador: É Obrigatório. Especifica o nome distinto do computador a ser adicionado. Se o nome distinto for omitido, ele será retirado da entrada padrão (stdin).

## Políticas de Senha para o Domínio

Ao criar um domínio, com a instalação do Active Directory no primeiro DC do domínio, por padrão são definidas algumas políticas de segurança relacionadas com as senhas dos usuários. Por exemplo, por padrão é definido que a senha deve ter no mínimo 7 caracteres e que deve ser trocada a cada 42 dias, dentre outras definições. O administrador do sistema pode alterar estas políticas de segurança, para adequá-las as necessidades da sua rede.

As políticas de segurança são definidas para o domínio como um todo, ou seja, uma vez definidas elas passam a valer em todo o domínio. Aliás esta é um das características determinantes de um domínio, ou seja, o compartilhamento de um conjunto único de políticas de segurança.

Neste item você aprenderá a configurar as políticas de segurança relacionadas com a senha do usuário. Estas políticas estão divididas em três grupos, conforme descrito a seguir:

- ◆ **Password Policy (Políticas de Senha):** Estas políticas definem as características que as senhas devem ter. Por exemplo: qual o número mínimo de caracteres, devem ser trocadas de quantos em quantos dias, devem ou não atender a critérios de complexidade e assim por diante.

**IMPORTANTE:** Computadores executando Windows 95 e Windows 98 não têm recursos de segurança avançados e não têm contas de computador atribuídas a eles.

**IMPORTANTE:** Quando o nível funcional de domínio foi definido como Windows Server 2003, um novo atributo `lastLogonTimestamp` é usado para rastrear o último horário de logon de uma conta de usuário ou computador. Este atributo é replicado no domínio e pode fornecer informações importantes sobre o histórico de um usuário ou computador.

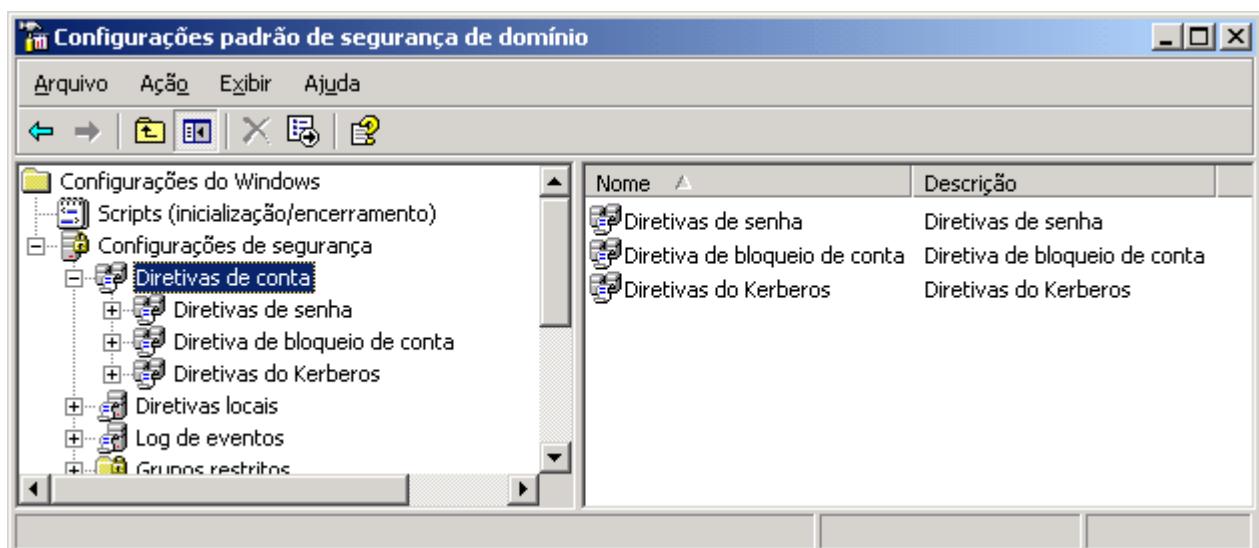
**IMPORTANTE:** Você pode criar uma conta de computador, usando o comando `dsadd computer`. A forma mais simples deste comando, está descrita a seguir: `dsadd computer NDComputador`

**DICA:** Outro comando que pode ser utilizado para criar uma conta de computador é o comando `NETDOM`, o qual está contido no arquivo `Support.cab`, da pasta `Support\Tools`, do CD de instalação do Windows Server 2003.

- ◆ **Account Lockout Policy (Políticas para Bloqueio de Senha):** Estas políticas definem quando uma conta será bloqueada, com base em um número de tentativas de logon sem sucesso. Por exemplo, o administrador pode definir que se o usuário tentar fazer três logons sem sucesso (por exemplo digitando uma senha incorreta para a sua conta) dentro do período de uma hora, que a conta seja bloqueada. Estas políticas são utilizadas para evitar que um usuário mal intencionado tente sucessivamente fazer o logon, usando diferentes senhas, em uma tentativa de “adivinar” a senha do usuário.
- ◆ **Kerberos Policy (Políticas do Kerberos):** O Kerberos é um protocolo de autenticação utilizado por muitos sistemas operacionais, como por exemplo o Windows 2000 Server, Windows Server 2003 e muitas versões do UNIX. É um protocolo padrão e muito utilizado. Existem algumas políticas de segurança relacionadas ao protocolo Kerberos que podem ser definidas pelo administrador.

Estas políticas são configuradas usando o console Diretiva de segurança de domínio, o qual é acessado Iniciar -> Ferramentas Administrativas.

Ao abrir o console Diretiva de segurança de domínio serão exibidas diversas opções de configurações de políticas de segurança do domínio. Clique no sinal de +, ao lado da opção configurações de segurança. Serão exibidas várias opções. A primeira opção, no painel da esquerda, é: Diretivas de conta. Ao clicar no sinal de + ao lado desta opção, são exibidas as opções Diretivas de senha, Diretivas de bloqueio de conta e Diretivas do Kerberos, conforme indicado na Figura 14.26:



**Figura 14.26 As opções de diretivas de contas do domínio.**

Ao clicar em uma das opções, por exemplo Diretivas de senha, as diversas diretivas da opção selecionada serão exibida no painel da direita, conforme indicado na Figura 14.27:

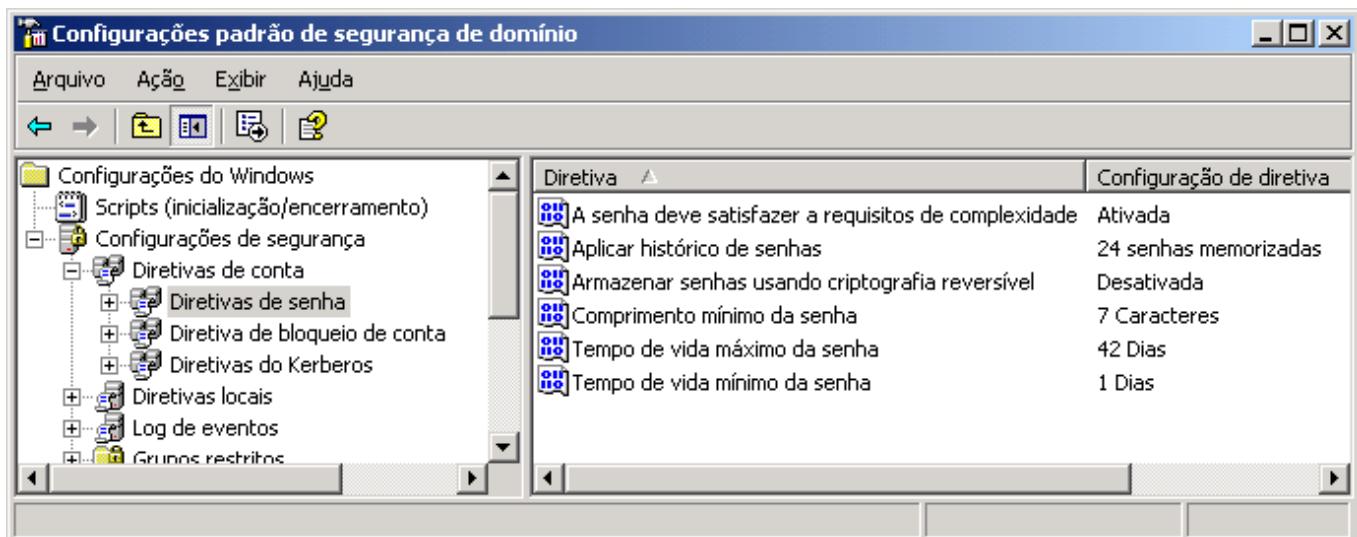


Figura 14.27 Diretivas da opção Diretivas de senha.

Para alterar uma diretiva basta dar um clique duplo na respectiva diretiva. Por exemplo, dê um clique duplo na diretiva Tempo de vida máximo da senha. Por padrão é definido o valor de 42 dias para esta diretiva. Ao dar um clique duplo nesta diretiva será aberta uma janela onde são exibidas as configurações atuais da diretiva e onde você pode fazer as alterações necessárias, conforme exemplo da Figura 14.27 onde são exibidas as configurações da diretiva Tempo de vida máximo de senha:

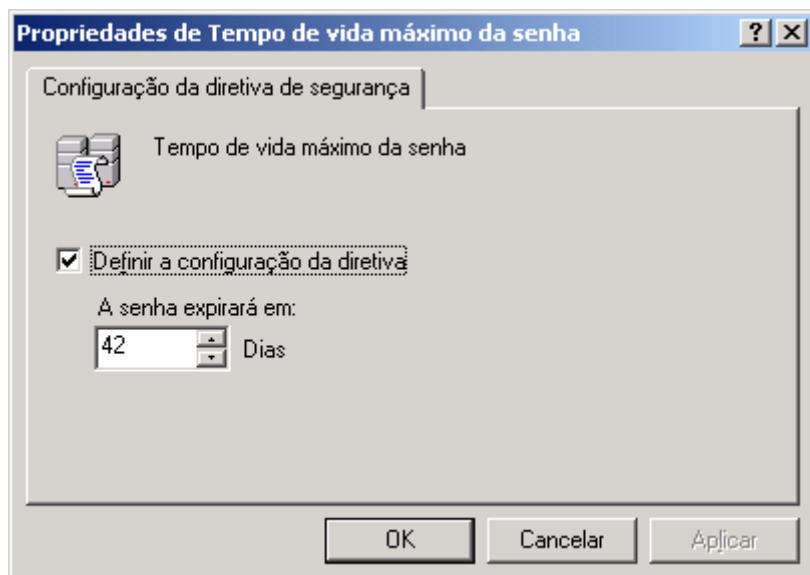


Figura 14.28 Configurando os valores da diretiva Tempo de vida máximo de senha.

Após ter definido as configurações desejadas é só clicar em OK. Observe a opção Definir a configuração da diretiva. Você pode desabilitar uma diretiva, fazendo com que ela deixe de ser aplicada, simplesmente desmarcando esta opção.

A seguir descrevo as diretivas dos grupos Diretivas de senha e Diretivas de bloqueio de senha. Estas são as diretivas cobradas no Exame 70-290.

## **Descrição das diretivas do grupo Diretivas de senha: No Windows Server 2003, por padrão, são definidas as seguintes políticas de segurança em relação as senhas de usuários:**

Quando o usuário vai trocar a senha, não pode ser utilizada uma senha igual as 24 últimas (haja criatividade para inventar senhas).

- ◆ A senha expira (isto é, deve ser alterada) a cada 42 dias.
- ◆ O tempo mínimo de vida de senha é um dia. Ou seja, você trocou a senha hoje, não poderá trocá-lo novamente daqui a uma ou duas horas, somente após um dia.
- ◆ Tamanho mínimo de sete caracteres.
- ◆ A opção “A senha deve atender critérios de complexidade (Password must meet complexity requirements) é habilitada por padrão”.

Com a opção A senha deve atender critérios de complexidade (Password must meet complexity requirements) habilitada por padrão, uma série de requisitos devem ser atendidos para que a senha seja aceita. A seguir descrevo estes critérios:

- ◆ A senha não pode conter parte ou todo o nome da conta. Por exemplo, se o nome da conta for jsilva, a senha não poderá conter a sílaba “sil” ou a palavra “silva”.
- ◆ Ter pelo menos seis caracteres. O número mínimo de caracteres pode ser aumentado, configurando-se as políticas de segurança para senhas, conforme mostrarei mais adiante.
- ◆ Deve conter caracteres de pelo menos três dos quatro grupos a seguir: letras maiúsculas de A até Z, letras minúsculas de a até z, dígitos de 0 a 9 ou caracteres especiais (:, !, @, #, \$, %, etc.).

Estes requisitos de complexidade são verificados quando a senha é criada pela primeira vez, durante o cadastramento do usuário e toda vez que a senha for alterada. Com estes requisitos definidos, as senhas a seguir seriam válidas:

**AbCsenha1**

**AbcSenha#**

**Abc123**

**Abc ; ; senha**

Já as senhas a seguir não seriam válidas:

- ◆ **abcsenha123:** (contém somente caracteres de dois dos quatro grupos: letras minúsculas e números).
- ◆ **abc;senha:** (contém somente caracteres de dois dos quatro grupos: letras minúsculas e caracteres especiais).

Todas estas configurações de senha são definidas pelas diretivas de segurança do grupo Diretivas de senha, as quais estão descritas a seguir:

- ◆ **Aplicar histórico de senhas:** Nesta diretiva o administrador informa o número de senhas que serão gravadas no histórico de senhas do usuário. Por exemplo, se esta diretiva estiver definida com um valor 5, significa que ao trocar a senha, o usuário não poderá utilizar uma das últimas cinco senhas que ele utilizou. Esta diretiva é utilizada para evitar que o usuário possa repetir sempre as mesmas senhas. Por padrão ela tem o seu valor definido como 24, ou seja, ao trocar a senha, o usuário não poderá utilizar uma senha igual a uma das últimas 24 que ele utilizou.
- ◆ **Tempo de vida máximo da senha:** Esta diretiva define um tempo máximo de duração da senha. Uma vez transcorrido este período o usuário é obrigado a alterar a senha. Esta diretiva aceita valores na faixa entre 1 e

---

**IMPORTANTE : Para as senhas, o Windows Server 2003 distingue letras maiúsculas de minúsculas. Por exemplo a senha “Abc123” é diferente da senha “abc123”.**

---

999. Se você definir um valor 0 para este diretiva, equivale a definir que as senhas nunca expiram (embora não seja nada recomendado definir que as senhas nunca expiram). Se o valor desta diretiva for definido na faixa entre 1 e 999, o valor da diretiva Minimum password age (Tempo de vida mínimo da senha), deve ser menor do que o valor definido na diretiva Maximum password age (Tempo de vida máximo da senha). Em outras palavras, o tempo mínimo de vida deve ser menor do que o tempo máximo, o que faz sentido evidentemente. O valor padrão para esta diretiva é de 42 dias. É recomendado um valor entre 30 e 45 dias para esta diretiva.

- ◆ **Tempo de vida mínimo da senha:** Esta diretiva define o tempo mínimo, em dias, pelo qual a senha deve ser utilizada, antes que ele possa ser novamente alterada. Por exemplo, se esta diretiva estiver definida com um valor igual a 5 e o usuário alterar a sua senha hoje, significa que ele somente poderá alterar novamente esta senha daqui a cinco dias. Este diretiva, conforme descrito anteriormente, deve ser utilizada em conjunto com a diretiva Enfore password history (Aplicar histórico de senhas), para efetivamente forçar que seja mantido um histórico de senhas e que o usuário não possa utilizar uma senha igual as últimas x senhas, sendo o valor x definido na diretiva Enfore password history (Aplicar histórico de senhas). O valor desta diretiva pode estar na faixa de 1 a 998. Um valor 0 significa que não existe tempo de vida mínimo da senha, ou seja, o usuário pode alterar a senha a qualquer momento e repetidamente. Por padrão é definido o valor 1 nos DCs e 0 nos member servers. Uma regra normalmente utilizada é definir esta diretiva com um valor correspondente a um terço do valor definido na diretiva Maximum password age (Tempo de vida máximo da senha).
- ◆ **Comprimento mínimo da senha:** Esta diretiva define o número mínimo de caracteres que deve ter a senha. Você pode definir um valor entre 1 e 14. Para definir que não é exigido um comprimento mínimo, defina esta diretiva com o valor 0. Por padrão é definido o valor 7 nos DCs e 0 nos member servers.
- ◆ **A senha deve satisfazer a requisitos de complexidade:** Esta diretiva é habilitada por padrão. Com isso, uma série de requisitos devem ser atendidos para que a senha seja aceita, conforme descrevi anteriormente.
- ◆ **Armazenar senhas usando criptografia reversa:** Esta diretiva somente deve ser habilitada quando houver aplicações que necessitam deste padrão de senhas. Mais especificamente são aplicações que precisam conhecer a senha do usuário por questões de autenticação. Esta diretiva, em termos de segurança, é muito semelhante a armazenar a senha como texto sem criptografia, ou seja, não é recomendada em termos de segurança e somente deve ser habilitada quando realmente houver necessidade por questões de compatibilidade com algum sistema de aplicação crítica para a empresa. Esta diretiva é requerida também em algumas situações específicas, por exemplo, quando é utilizado o protocolo CHAP para autenticação através do RRAS ou do IAS. Também é requerida quando for usada a autenticação do tipo Digest Authentication com o IIS. Por padrão esta diretiva está desabilitada.

**NOTA:** O valor de 24 para este diretiva é o padrão em DCs do domínio. Em member servers o valor padrão é zero, ou seja, sem histórico de senha. Para que esta diretiva tenha efeito, ele deve ser utilizada em conjunto com a diretiva Minimum password age (Tempo de vida mínimo da senha). Se não houver um tempo mínimo de vida para a senha, o usuário poderia trocar a senha 24 vezes no mesmo dia. Com isso ele poderia simplesmente continuar utilizando sempre a mesma senha.

## Descrição das diretivas do grupo Diretivas de bloqueio de conta

- ◆ **Límite de bloqueio de conta:** Esta diretiva define o número de tentativas de logon sem sucesso que serão necessárias para que a conta seja bloqueada. Este número de tentativas deve ocorrer dentro do período definido pela diretiva Zerar contador de bloqueios de conta após. Vamos supor que a diretiva Límite de bloqueio de conta esteja definida com o valor três e que a diretiva Zerar contador de bloqueios de conta após esteja definida com o valor 60 minutos. Isso significa que se o usuário fizer três tentativas de logon sem sucesso, dentro de uma hora, a sua conta será bloqueada. Esta diretiva pode ter um valor entre 1 e 999. Um valor igual a 0 significa sem bloqueio, ou seja, o usuário poderá fazer quantas tentativas quiser, que a conta não será bloqueada.
- ◆ **Zerar contador de bloqueios de conta após:** Esta diretiva define o período dentro do qual as tentativas de logon sem sucesso devem ser feitas para que a conta seja bloqueada. Por exemplo, vamos imaginar que esta diretiva estiver definida como 60 minutos e o usuário tenha feito duas tentativas de logon sem sucesso. Se ele fizer mais uma tentativa nos próximos sessenta minutos, a conta será bloqueada. Se transcorrer 60 minutos sem nenhuma tentativa sem sucesso, o contador será zerado. Esta diretiva pode conter valores na faixa de 1 a 99999 minutos. Esta diretiva somente pode ser habilitada quando a diretiva Límite de bloqueio de conta, estiver habilitada.
- ◆ **Duração do bloqueio de conta:** Esta diretiva define o tempo, em minutos, pelo qual a conta permanecerá bloqueada, uma vez que tenha sido bloqueada por sucessivas tentativas de logon sem sucesso. O valor pode variar de 1 a 99999. Um valor 0 significa que a conta não será desbloqueada automaticamente. Com esta configuração o Administrador terá que desbloquear a conta do usuário. Esta diretiva somente terá efeito quando a diretiva Límite de bloqueio de conta tiver sido definida.

**IMPORTANTE:** A seguir descrevo as diretivas deste grupo, as quais são utilizadas para definir quando uma conta deve ser bloqueada, após sucessivas tentativas de logon sem sucesso. Conheça bem estas diretivas, pois elas são um ponto importante para o Exame 70-290.

**IMPORTANTE:** Tentativas de desbloqueio de estações de trabalho e member servers, sem sucesso, também contam para o número de tentativas sem sucesso.

## Gerenciamento de discos e Volumes no Windows Server 2003

Existem alguns conceitos, termos e definições que você precisa conhecer sobre o gerenciamento de discos e volumes, no Windows Server 2003. Por exemplo, é fundamental que você saiba a diferença entre um Disco físico e um Volume lógico. Neste tópico vou apresentar uma revisão sobre os diversos termos relacionados com o gerenciamento de discos e volumes no Windows Server 2003.

### Disco Físico

Chamamos de Disco Físico, a cada HD (antigamente mais conhecido por Winchester) instalado no computador. O primeiro HD instalado é denominado de Disco 0, o Segundo HD é chamado de Disco 1 e assim por diante. Um disco físico pode ser configurado como Disco Básico ou Disco Dinâmico. Mais adiante você entenderá 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. Você aprenderá o conceito de disco dinâmico e básico, bem como as ações práticas relacionadas, neste capítulo.
- ◆ Em servidores, onde é utilizada uma placa da RAID por hardware, pode acontecer de um conjunto de três ou mais discos físicos, que fazem parte do RAID, “aparecerem” para o Windows Server 2003 como um único disco. Por exemplo, pode acontecer de você ter cinco discos de 50 GB formando o RAID, e estes discos aparecerem como um único disco físico, de 160 GB (eu não errei na soma não, quando estudarmos RAID, você entenderá o porquê 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. Por exemplo, você pode criar o C: com 40 GB, onde será instalado o Windows Server 2003 e os aplicativos, pode criar um D: com 20 GB, onde serão gravados arquivos de log do Sistema Operacional, o banco de dados do Active Directory e arquivos de log de outros serviços, como por exemplo os arquivos de Log de Transações do SQL Server 2000 e, finalmente, um E:, com os 20 GB restantes, onde serão gravados arquivos dos usuários. Observe que neste exemplo temos um disco físico (Disco 0), o qual foi dividido em três Volumes Lógicos (C:, D: e E:).

A definição oficial de volume, contida na Ajuda do Windows Server 2003 é a seguinte:

“Volume é uma área de armazenamento em um disco rígido (disco físico). Um volume é formatado usando um sistema de arquivos, tais como FAT ou NTFS, e tem uma letra de unidade atribuída a ele. Você pode visualizar o conteúdo de um volume clicando em seu ícone no Windows Explorer ou em Meu computador. Um único disco rígido pode ter vários volumes, que também podem abranger vários discos”.

A última parte da definição é que pode parecer um pouco esquisita: “...que podem abranger vários discos”. Você verá, neste capítulo, que determinados tipos de volumes, podem ocupar áreas em dois ou mais discos.

## 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 (a exemplo do que acontece no Windows 2000 Server) é possível optar entre dois tipos de armazenamento: Armazenamento básico ou o Armazenamento dinâmico. A seguir descreverei estes dois tipos de armazenamento em detalhes.

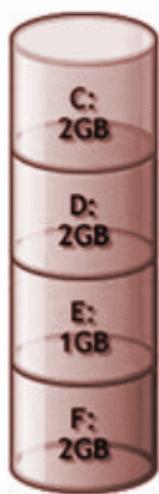
### Armazenamento básico

É o tipo de armazenamento que vem sendo utilizado desde a época do bom e velho (talvez não tão bom) MS-DOS. É utilizado por sistemas como o Windows 95, Windows 98, Windows NT Server 4.0 e Windows NT Workstation 4.0. 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. 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 prática se comportam como se fossem dois discos de 2GB independentes. Em um disco com armazenamento básico, é possível ter Partições primárias, partições estendidas e Drivers lógicos. Mostrarei mais detalhes sobre estes elementos, bem como exemplos de utilização de cada um deles.

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 partição marcada como ativa. Um disco básico pode conter no máximo quatro partições primárias. Considere o exemplo da Figura 14.29, onde um disco de 7 GB foi dividido em quatro partições primárias. Três de 2 GB e uma de 1GB. Observe que para cada partição primária é atribuída uma letra de unidade: C; D; e assim por diante.

**NOTA:** Utilizarei a palavra **disco** como sendo sinônimo de um **disco rígido**, ou seja, um **disco físico**. Então sempre que você encontrar uma referência a **disco**, entenda como sendo um **disco rígido** e não um **disquete** ou outro tipo de mídia. Também é importante salientar que uso a palavra **disco** em referência ao **disco físico**, o qual pode ser dividido em várias partições (no caso de armazenamento básico) ou vários volumes (no caso de armazenamento dinâmico).

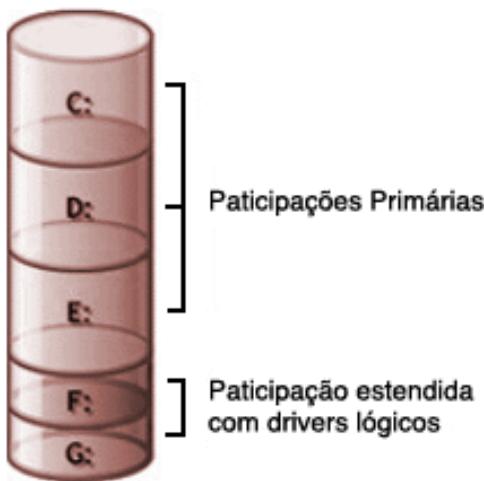


**Figura 14.29** No máximo podem ser criadas quatro partições primárias em um disco básico.

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 um drive lógico. Deve ser atribuída uma letra para cada drive lógico e este deve ser formatado com um sistema de arquivos – FAT, FAT32, NTFS ou NTFS 5 (nova versão do NTFS disponível a partir do Windows 2000). Com o uso de uma partição estendida e drivers lógicos, é possível superar o limite de quatro unidades por disco, que é imposto quando se utiliza apenas partições primárias.

Considere o exemplo da Figura 14.30, onde é exibido um disco com três partições primárias (C:, D: e E:), e um volume estendido, no qual foram criados dois drivers lógicos (F: e G:).

**IMPORTANTE:** É importante salientar que um disco somente pode ser configurado para um tipo de armazenamento. Não é possível, por exemplo, ter uma parte do disco configurada como armazenamento básico e o restante como armazenamento dinâmico.



**Figura 14.30 Utilizando partições estendidas.**

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 Partição de 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 do Sistema e a Partição de boot, estão na mesma partição, tipicamente no drive C:

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 do Sistema:** Contém os arquivos necessários para o boot do Windows Server 2003.
- ◆ **Partição de boot:** Contém os arquivos do Windows Server 2003, tipicamente em uma pasta WINNT ou WINDOWS.
- ◆ **Volume set:** Para criar um Volume set é usado o espaço de duas ou mais partições, no mesmo disco ou em discos diferentes, de tal forma que estas partições apareçam, para o Windows Server 2003 como uma única unidade. Por exemplo posso combinar uma partição de 1 GB com outra de 4 GB, para formar uma unidade de 5 GB. Posso aumentar o tamanho de um Volume set (operação chamada de estender o Volume set), porém não posso reduzir 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. Posso juntar partições de tamanhos diferentes. Um Volume set não pode conter a Partição do sistema, nem a Partição de boot.
- ◆ **Stripe set:** Para criar um Stripe set combina-se espaços iguais de dois ou mais discos. Não podem ser utilizadas duas partições do mesmo disco. Posso utilizar 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 do 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 do 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 (2 GB 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.

**IMPORTANTE:** Não esqueça que a partição do sistema e a partição de boot, não pode ser uma partição do tipo Volume set, Stripe set sem paridade ou Stripe Set com Paridade (RAID-5). Ou de uma maneira mais simples, as partições do sistema e de boot, somente podem ser do tipo partição simples ou do tipo Mirror set (Raid-1).

## 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 disco dinâmico, diretamente, sem perda de dados. Existem diferentes tipos de volumes. O tipo de volume a ser utilizado, é determinado por fatores tais 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 de comprometimento de um disco ou volume.

Em discos de volume dinâmico 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 criado usando duas ou mais partes de um mesmo disco dinâmico. Não fornece nenhum 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 do 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 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 – Raid-1):** 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 10 GB você precisará de um espaço adicional de 10 GB em outro disco rígido. Ou seja, para 10 Gb de informações você utiliza 20 GB, sendo os 10 GB adicionais para o espelhamento.
- ◆ **Striped Volume:** Podem ser combinadas áreas de espaço livre de até 32 discos. Não apresenta 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 Striped volume, 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 reconstituída a partir das informações de paridade, contida nos demais discos. O disco defeituoso pode ser substituído e a informação nele contida pode ser recriada a partir da informação de paridade gravada 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 à falhas restringe-se a falha de um dos discos do volume, se dois discos falharem ao mesmo tempo, não será possível recuperar os dados

Existem mais alguns detalhes importantes que devem ser conhecidos:

## Reativando discos que ainda não foram completamente reconhecidos pelo Windows Server 2003.

Pode acontecer de após o administrador ter instalado, fisicamente o disco e inicializado o servidor, de o disco ter sido reconhecido no Setup do computador, porém ainda não estar disponível para uso no Windows Server 2003. Nestas situações o disco pode apresentar diferentes Status, dependendo de o disco já estar sendo utilizado em outro servidor, de estar ou não formatado, de fazer ou não parte de um volume set ou de um volume RAID-5 e assim por diante. No próximo exemplo mostrarei uma situação onde dois novos discos foram instalados no servidor. O Windows Server 2003 reconheceu a presença destes discos, porém marcou-os com o Status Foreign (Externo). Este status, normalmente, indica discos que estavam sendo utilizados em outros computadores e foram instalados no servidor no qual você está trabalhando. No exemplo a seguir mostrarei como tornar estes discos disponíveis para o Windows Server 2003. Você irá, primeiro, importar os discos.

Exemplo: Para tornar disponíveis discos com o status Foreign (Externo), siga os passos indicados a seguir:

1. Faça o logon como Administrador ou com uma conta com permissões de administrador.
2. Abra o console Gerenciamento do computador.
3. Clique na opção Gerenciamento de disco.

---

**NOTA:** Dispositivos de armazenamento removíveis, com um Zip drive, somente suportam armazenamento básico e somente podem ter partições primárias. Além disso uma partição primária deste tipo de dispositivo, não pode ser marcada como ativa, para que seja possível dar o boot a partir desta partição.

---

**IMPORTANTE:** É muito importante lembrar, que o armazenamento dinâmico somente é suportado pelo Windows 2000 (Professional e Server e também pelo Windows XP) e pelo Windows Server 2003, sendo que discos dinâmicos não serão reconhecidos por outros sistemas operacionais como o Windows NT Server 4.0, Windows 95, Windows 98 e Windows NT Workstation 4.0.

---

- Em alguns instantes são exibidos os discos disponíveis no computador. No exemplo da Figura 14.31 são exibidos dois discos com o status Foreign (Externo). Neste exemplo você irá importar estes discos e depois irá excluir os volumes (ou volume) neles existentes.

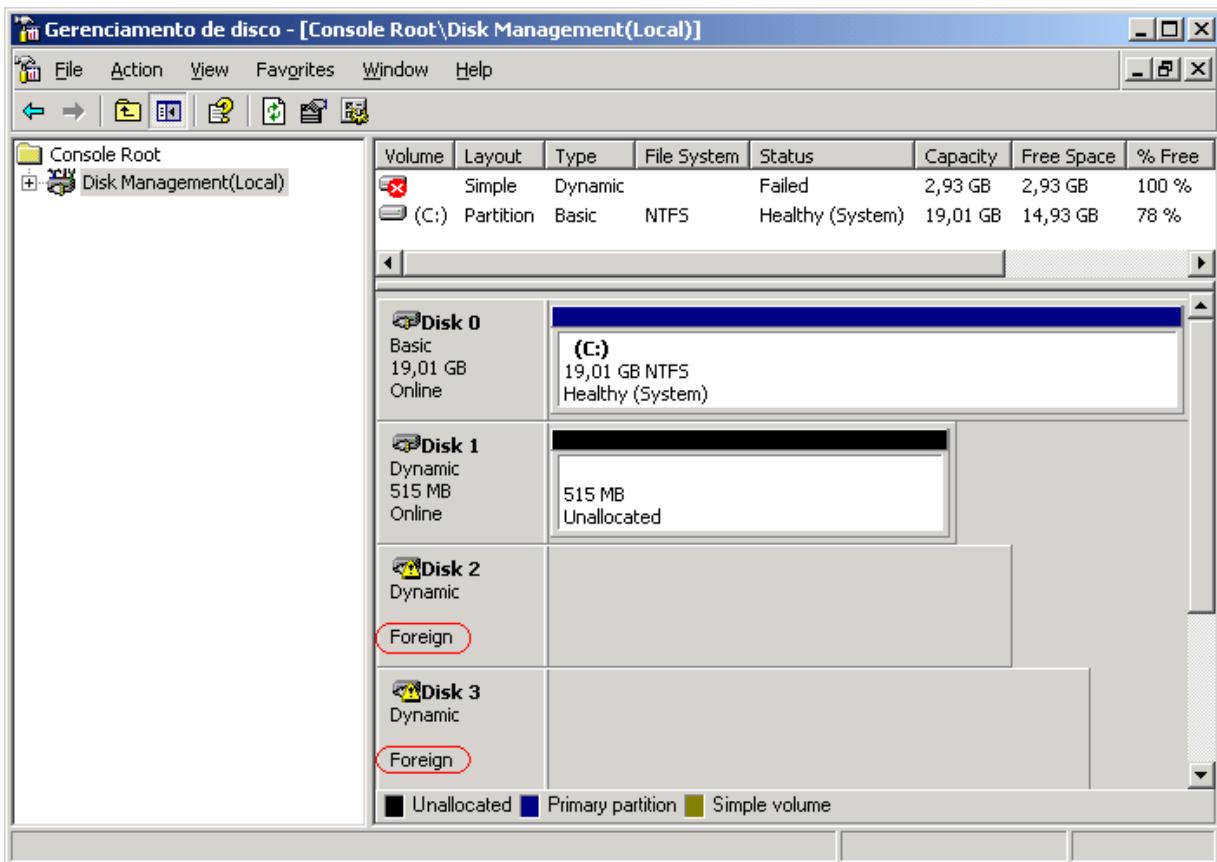


Figura 14.31 Discos com o status Foreign.

Observe que o Disco 2 e o Disco 3 estão com o status Foreign (Externo). O Windows Server 2003 numera os discos a partir do zero. No servidor da Figura 5.6 existem 4 discos instalados (Disco 0, Disco 1, Disco 2 e Disco 3). Você irá importar os discos 2 e 3, os quais estão com o status Foreign (Externo).

- Clique com o botão direito do mouse próximo ao ponto de exclamação, ao lado de Disco 2. No menu de opções que é exibido clique na opção Importar discos externos.
- Será exibida a janela Importar discos externos. Nesta janela já vem selecionado o disco no qual você clicou com o botão direito do mouse, conforme indicado na Figura 14.32. Se você clicar no botão Discos, será exibido o disco no qual você clicou com o botão direito do mouse. Nesta janela somente pode ser selecionado um disco por vez, ou seja, não é possível importar mais de um disco ao mesmo tempo.
- Clique em OK e pronto, o disco será importado. Observe que o disco que você acabou de importar já está disponível para uso.
- Agora clique com o botão direito do mouse no outro disco a ser importado. Selecione o comando Importar discos externos...

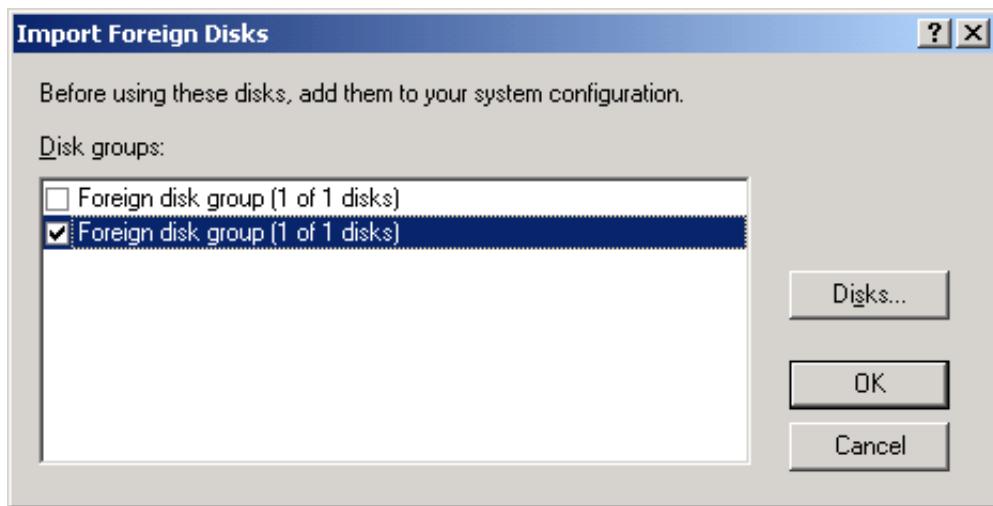


Figura 14.32 Discos com o status Externo.

9. A janela Importar discos externos será exibida. Clique em OK. Se houver algum volume que possa ser utilizado no Windows Server 2003, disponível no disco que está sendo importado, será exibida a janela Foreign Disk Volumes (Volumes do disco externo).
10. Clique em OK para fechar esta janela.
11. Pronto, o disco foi importado e está disponível para uso, conforme indicado na Figura 14.33, onde não existe mais nenhum disco com o status Foreign (externo). Todos os discos estão com o status Online. Observe que no último disco que foi importado (Disco 3) existe um volume simples (formado por duas porções do disco, uma de 2 GB e outra de 512 MB e um espaço não alocado de 1,51 GB).

|                                  |  |                                  |                                 |                        |
|----------------------------------|--|----------------------------------|---------------------------------|------------------------|
| Disk 0                           | (C:)<br>19,01 GB NTFS<br>Healthy (System)  |                                  |                                 |                        |
| Disk 1                           | 515 MB<br>Unallocated  |                                  |                                 |                        |
| Disk 2                           | 1,19 GB<br>Unallocated   |                                  |                                 |                        |
| Disk 3                           | <table border="1"> <tr> <td>Dados<br/>2,00 GB NTFS<br/>Healthy</td> <td>Dados<br/>512 MB NTFS<br/>Healthy</td> <td>1,51 GB<br/>Unallocated</td> </tr> </table> | Dados<br>2,00 GB NTFS<br>Healthy | Dados<br>512 MB NTFS<br>Healthy | 1,51 GB<br>Unallocated |
| Dados<br>2,00 GB NTFS<br>Healthy | Dados<br>512 MB NTFS<br>Healthy  | 1,51 GB<br>Unallocated           |                                 |                        |

Figura 14.33 Volumes existentes no disco que foi importado.

A seguir apresenta uma descrição de cada um dos possíveis Status que podem ser exibidos para um disco, no console Gerenciamento de disco.

#### Status Externo:

O status Externo ocorre quando você move um disco dinâmico de um computador que esteja executando o Windows 2000, Windows XP Professional, ou a família de sistemas operacionais Windows Server 2003 para o computador local. O status Externo também pode ocorrer em computadores executando o Windows XP Home Edition que estejam configurados como multi boot, com outro sistema operacional que use discos dinâmicos (como o Windows 2000 Professional ou o Windows XP Professional). Não há suporte para discos dinâmicos no Windows XP Home Edition ou em notebooks. Um ícone de aviso é exibido nos discos que exibem o status Externo.

Para acessar os dados no disco, você deve adicionar o disco à configuração de sistema do computador. Para adicionar um disco à configuração de sistema do computador, importe o disco externo (conforme descrito no exemplo anterior). Todos os volumes existentes no disco externo se tornam visíveis e acessíveis quando você importa o disco.

Em alguns casos, um disco que foi previamente conectado ao sistema pode exibir o status Externo. Os dados de configuração dos discos dinâmicos são armazenados em todos os discos dinâmicos. Portanto, as informações sobre quais discos pertencem ao sistema se perdem quando todos os discos dinâmicos falham.

#### Status Inicializando:

O status Inicializando é um status temporário que ocorre quando você converte um disco básico em dinâmico. Quando a inicialização termina, o status do disco é alterado para On-line.

#### Status Faltando:

O status Faltando ocorre quando um disco dinâmico é corrompido, desligado ou desconectado. Em vez de ser exibido na coluna de status, o status Faltando é exibido como nome de disco. Após reconectar ou ligar o disco ausente, abra o console Gerenciamento de disco, clique com o botão direito do mouse no disco ausente e, em seguida, clique em Reativar disco. Se houver mais de um disco faltando no grupo, o Gerenciamento de disco tentará reativar todos os discos.

#### Status Não inicializado:

O status Não inicializado ocorre quando um disco não contém uma assinatura válida. Depois que você instala um novo disco, o Windows XP Professional ou a família de sistemas operacionais Windows Server 2003 deve gravar um registro de inicialização principal (MBR) ou uma tabela de partição GUID (GPT) para que seja possível criar partições no disco. Quando você iniciar o Gerenciamento de disco pela primeira vez após a instalação de um novo disco, será exibido um assistente que fornece uma lista dos novos discos detectados. Se você cancelar o assistente antes que a assinatura de disco seja gravada, o status do disco permanecerá como Não inicializado até que você clique com o botão direito do mouse no disco e, em seguida, clique em Inicializar disco. O status do disco se altera brevemente para Inicializando e, em seguida, para On-line.

---

**IMPORTANTE:** No entanto, você não poderá acessar dados no disco se estiver executando o Windows XP Home Edition. Para usar o disco no Windows XP Home Edition, é necessário convertê-lo em disco básico, o que destrói todos os dados contidos nele. Também é importante salientar, que computadores móveis, como Notebooks, não tem suporta a discos dinâmicos.

---

**IMPORTANTE:** Não converta um disco dinâmico em básico, a menos que você tenha certeza de que não precisará mais dos dados contidos nesse disco. A conversão de um disco dinâmico em básico destruirá todos os dados do disco.

---

### **Status On-line:**

O status On-line ocorre quando um disco básico ou dinâmico pode ser acessado e aparenta não ter nenhum problema. Este é o status normal de um disco. Não é necessária nenhuma ação do usuário.

### **Status On-line (erros):**

O status On-line (erros) ocorre quando os erros de E/S (entrada e saída) são detectados em uma região de um disco dinâmico. Um ícone de aviso é exibido no disco dinâmico com erros.

Se os erros de E/S forem temporários, (por exemplo, devido a um fio solto que já esteja no lugar) o disco retornará para o status On-line quando você reativá-lo.

### **Status Off-line:**

O status Off-line ocorre quando um disco dinâmico não pode ser acessado. O disco dinâmico pode estar corrompido ou temporariamente não disponível. Um ícone de erro é exibido no disco dinâmico off-line.

Se o status do disco for Off-line e o nome do disco for alterado para Faltando, é sinal de que o disco estava recentemente disponível no sistema, mas não pode mais ser localizado ou identificado. O disco ausente pode estar corrompido, desligado ou desconectado.

### **Colocando um disco que está off-line e ausente novamente on-line:**

Repare qualquer disco, controlador ou problema de cabo e certifique-se de que o disco físico está ligado, conectado à fonte de energia e instalado no computador. No Gerenciamento de disco, clique com o botão direito do mouse no disco e, em seguida, clique em Reativar disco para colocar o disco novamente on-line.

Se o status do disco permanecer Off-line, o nome do disco continuar como Faltando e você determinar que o disco está com um problema que não pode ser reparado, remova o disco do sistema (usando o comando Remover disco). Entretanto, antes de remover o disco, exclua todos os volumes (ou espelhos) do disco. Você pode salvar todos os volumes espelhados do disco removendo o espelho, em vez de remover todo o volume. A exclusão de um volume destruirá os dados do volume. Portanto, você deve remover um disco somente se estiver absolutamente certo de que o disco está definitivamente danificado ou inutilizado.

### **Colocando um disco que está off-line e ainda é chamado de Disco nº (não ausente) novamente on-line:**

No Gerenciamento de disco, clique com o botão direito do mouse no disco e, em seguida, clique em Reativar disco para colocar o disco novamente on-line. Se o status do disco continuar Off-line, verifique os cabos e o controlador do disco, e certifique-se de que o disco físico está íntegro. Corrija quaisquer problemas e tente reativar o disco novamente. Se a reativação do disco tiver êxito, todos os volumes do disco retornarão automaticamente ao status Íntegro.

### **Status Ilegível:**

O status Ilegível ocorre quando um disco básico ou dinâmico não pode ser acessado. O disco pode estar com uma falha de hardware, corrompido ou com erros de E/S. A cópia do banco de dados de configuração de disco do sistema pertencente ao disco pode estar corrompida. Um ícone de erro é exibido nos discos que exibem o status Ilegível.

Os discos podem exibir o status Ilegível enquanto estão girando ou quando o Gerenciamento de disco está examinando novamente todos os discos do sistema. Em alguns casos, um disco ilegível apresenta falha e não pode ser recuperado. Nos discos dinâmicos, o status Ilegível é geralmente provocado por danos e erros de E/S em parte do disco, e não por falhas no disco inteiro. Você pode examinar novamente os discos (clique em Ação e, em seguida, clique em Examinar discos novamente) ou reiniciar o computador para ver se o status do disco foi alterado.

## Convertendo um disco de Armazenamento básico para Armazenamento dinâmico

É possível converter um disco de Armazenamento básico para Armazenamento dinâmico, sem perda de dados. Para efetuar a conversão para Armazenamento dinâmico, deve haver pelo menos 1 MB de espaço não alocado, no disco a ser convertido, para que a conversão possa ser feita com sucesso. O console de Gerenciamento de disco, automaticamente reserva este espaço ao criar partições ou volumes em um disco. Porém discos com partições ou volumes criados por outros sistemas operacionais, podem não ter este espaço não alocado, disponível. Um disco com Armazenamento dinâmico não terá partições ou drivers lógicos, ao invés disso o disco é dividido em volumes, conforme detalhado no início deste capítulo.

Quando você converte um disco de Armazenamento básico para Armazenamento dinâmico, o Windows Server 2003 efetua o mapeamento das partições existentes para os tipos de volume indicados na Tabela 14.1.

Tabela 14.1 Conversão de armazenamento básico para dinâmico.

| Disco Básico            | Disco Dinâmico  |
|-------------------------|---|
| Partição do sistema     | Volume simples  |
| Partição do boot        | Volume simples  |
| Partição primária       | Volume simples  |
| Partição estendida      | Um volume simples para cada drive lógico e qualquer espaço não alocado restante |
| Drive lógico            | Volume simples  |
| Volume set              | Spanned volume  |
| Stripe set              | Striped volume  |
| Disk mirror             | Mirrored volume   |
| Stripe set com paridade | Volume RAID-5   |

**IMPORTANTE:** Discos dinâmicos são reconhecidos apenas pelo Windows 2000 (Server e Professional), Windows XP Professional e Windows Server 2003. O Windows XP Home, versões anteriores do Windows (95/98/Me, NT 4.0) não reconhecem discos dinâmicos. Também não é possível utilizar discos dinâmicos em computadores portáteis, tais como Notebooks, independentemente da versão do Windows.

**IMPORTANTE:** Converter um disco de Armazenamento dinâmico de volta para Armazenamento básico diretamente, não é possível, sem perda de dados. Primeiro você deve excluir todos os volumes existentes no disco de Armazenamento dinâmico, para depois revertê-lo para armazenamento básico. Porém isso causa a perda de toda a informação armazenada no disco, a qual deve ser restaurada a partir de uma cópia de segurança (backup).

**IMPORTANTE:** Se um disco básico possui parte de uma partição que se estende por mais de um disco (Volume set, Stripe set, Disk mirror ou Stripe set com paridade), todos os discos que contém as partes da partição devem ser convertidos ao mesmo tempo. Todos os discos devem conter, pelo menos, 1 MB de espaço não alocado, caso contrário a conversão irá falhar. Este espaço de 1 MB pode existir mesmo que não seja visível no Snap-in de Gerenciamento de disco, conforme descrito anteriormente.

Caso programas instalados no disco a ser atualizado, estejam abertos, estes devem ser fechados antes que a atualização possa ser feita.

As partições de boot e do sistema somente são convertidas após uma reinicialização do computador. Todas as outras partições serão atualizadas imediatamente.

## Restabelecendo um volume do tipo Mirror (Espelhado – Raid-1):

Pode acontecer de um dos discos onde está o espelhamento apresentar falhas. Por exemplo, uma falha física que compromete todo o disco. Neste caso existem alguns passos que devem ser efetuados para que o Mirror (Espelhamento) possa ser restabelecido, conforme descrito a seguir.

Passos para restabelecer um espelhamento:

1. Quebrar o espelhamento. Para isso basta acessar o console de Gerenciamento de discos, clicar com o botão direito do mouse em uma das partes do espelhamento (de preferência na parte que está no disco bom, sem problemas). No menu que é exibido clique em Quebrar o Volume espelhado...
2. Surge uma mensagem avisando que se o espelhamento for quebrado não haverá mais tolerância a falhas, conforme indicado na Figura 14.34:

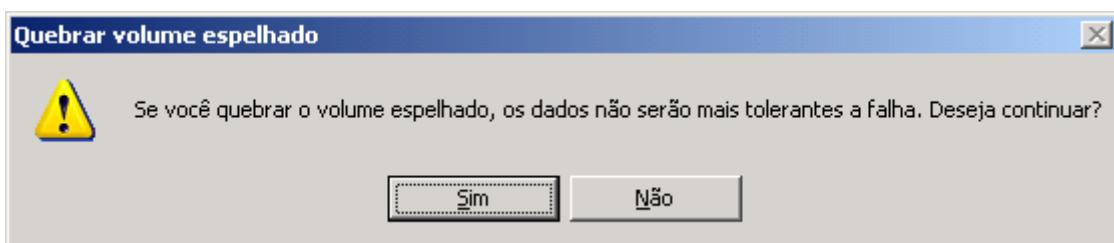


Figura 14.34 Confirmando a quebra do espelhamento.

3. Clique em Sim para confirmar a quebra do espelhamento.
4. Desligue o servidor e substitua o disco com defeito.
5. Reinicialize o servidor e faça o espelhamento novamente, usando espaço não alocado no novo disco. Pronto, o espelhamento será restabelecido e novamente haverá tolerância à falhas, no caso de falha de um dos discos.

## Restabelecendo um volume do tipo RAID-5:

Pode acontecer de um dos discos onde compõem um volume RAID-5, falhar. Por exemplo, uma falha física que compromete todo o disco. Neste caso existem alguns passos que devem ser efetuados para que o RAID-5 possa ser restabelecido, conforme descrito a seguir.

Passos para restabelecer um volume do tipo RAID-5:

1. Desligue o servidor e substitua o disco com defeito.
2. Reinicialize o servidor, acesse o console de Gerenciamento de disco. Clique com o botão direito do mouse no volume RAID-5 e no menu de opções que é exibido clique em Reativar Volume. Surge uma mensagem de aviso informando que é recomendado o uso do comando chkdsk no volume que está sendo reativado. O comando chkdsk é utilizado para detectar erros em um volume e será explicado mais adiante.
3. Clique em OK para fechar esta mensagem.

4. O volume será reativado e o status mudará de failed redundancy (Falha na redundância) para Resyncing (resincronizando) e depois para Healthy (algo parecido com saudável, com saúde, disponível).
5. Pronto, o RAID-5 foi restabelecido e com tolerância a falhas. É importante salientar que mesmo durante a falha de um dos discos, o volume RAID-5 continua disponível para ser utilizado, porém sem fornecer tolerância a falha, uma vez que se mais um disco falhar (enquanto o primeiro ainda não foi substituído), os dados serão perdidos, aí só restaurando a partir do Backup. Quando um volume RAID-5 apresenta falha em um dos discos e continua sendo utilizado, o desempenho cai muito, a velocidade de acesso fica muito prejudicada.

## O comando Convert:

Este comando é utilizado para converter volumes FAT (file allocation table) e FAT32 para o sistema de arquivos NTFS, deixando intactos os arquivos e pastas existentes. Os volumes convertidos ao sistema de arquivos NTFS não poderão ser convertidos de volta em FAT ou FAT32.

Sintaxe:

```
convert [Volume] /fs:ntfs [/v] [/cvtarea:NomeDoArquivo] [/nosecurity] [/x]
```

O comando convert tem os seguintes parâmetros:

- ◆ **Volume:** Especifica a letra da unidade (seguida de dois-pontos), o ponto de montagem ou o nome do volume a ser convertido em NTFS.
- ◆ **/fs:ntfs:** Necessário. Converte o volume em NTFS.
- ◆ **/v:** Especifica o modo de detalhe, isto é, todas as mensagens serão exibidas durante a conversão.
- ◆ **/cvtarea:nome\_de\_arquivo:** Apenas para usuários avançados. Especifica que a tabela de arquivos mestre (MFT) e outros arquivos de metadados NTFS serão gravados em um arquivo existente de espaço reservado contíguo. O arquivo deve estar localizado na pasta raiz do sistema de arquivos a ser convertido. O uso do parâmetro /CVTAREA poderá resultar em um sistema de arquivos menos fragmentado após a conversão. Para obter melhores resultados, o tamanho do arquivo deve ser 1 KB multiplicado pelo número de arquivos e pastas contidos no sistema de arquivos, no entanto, o utilitário de conversão aceita arquivos de qualquer tamanho.
- ◆ **/nosecurity:** Especifica que as configurações de segurança das pastas e arquivos convertidos poderão ser acessadas por qualquer pessoa.
- ◆ **/x:** Desmonta o volume, se necessário, antes de ser convertido. Os identificadores abertos para o volume não serão mais válidos.

---

**IMPORTANTE:** Não esqueça que é possível usar o comando convert, para converter um volume de FAT ou FAT32 para NTFS, sem perda de dados. Por outro lado, não é possível converter um volume NTFS de volta para FAT ou FAT32. Neste caso, é preciso fazer um backup completo dos dados, excluir o volume, recriá-lo novamente como FAT ou FAT32 e depois baixar os arquivos do backup.

---

Se o comando convert não puder bloquear a unidade (por exemplo, o volume do sistema ou a unidade atual), ele sugerirá que o volume seja convertido na próxima vez que o computador for reiniciado. Se você não puder reiniciar o computador imediatamente para concluir a conversão, planeje o momento de reiniciar o computador e reserve um tempo adicional para o processo de conversão.

No caso de volumes convertidos de FAT ou FAT32 em NTFS, devido à utilização de disco já existente, a MFT é criada em um local diferente, em comparação a um volume originalmente formatado com NTFS. Devido a isso, o desempenho

do volume pode não ser tão bom quanto em volumes originalmente formatados com NTFS. Para obter o desempenho ideal, considere a possibilidade de recriar esses volumes e formatá-los com o sistema de arquivos NTFS.

Os volumes convertidos de FAT em NTFS deixam os arquivos intactos, porém, poderão não dispor de alguns benefícios de desempenho se comparados a volumes inicialmente formatados com NTFS. Em volumes convertidos, por exemplo, a MFT pode ficar fragmentada. Além disso, em volumes de inicialização convertidos, o convert aplica a mesma segurança padrão que é aplicada durante a instalação do Windows.

Exemplo: Para converter o volume na unidade E em NTFS e exibir todas as mensagens, digite:

```
convert e: /fs:ntfs /v
```

## Criptografia – definições e conceitos

O Windows Server 2003 fornece suporte a criptografia de pastas e arquivos através do EFS – Encrypted File System (Sistema de arquivos com Criptografia). O suporte ao EFS foi introduzido no Windows 2000 Server e também está disponível no Windows 2000 Professional e Windows XP Professional. Com o uso de criptografia o usuário tem um nível de segurança maior do que somente com o uso de permissões NTFS (assunto do Capítulo 6). Somente é possível criptografar arquivos e pastas em volumes formatados com o sistema de arquivos NTFS. Com a criptografia o Windows Server 2003 garante que somente o usuário que criptografou um determinado arquivo tenha acesso ao arquivo.

Criptografia é o processo de converter dados em um formato que não possa ser lido por um outro usuário, a não ser o usuário que criptografou o arquivo. Depois que um usuário criptografar um arquivo, esse arquivo permanecerá automaticamente criptografado quando for armazenado em disco.

Descriptografia é o processo de converter dados do formato criptografado no seu formato original. Depois que um usuário descriptografar um arquivo, esse arquivo permanecerá descriptografado quando for armazenado em disco.

Com as permissões NTFS (veja Capítulo 6) temos alguns problemas quanto a segurança dos dados:

- ◆ O Administrador da máquina pode usar o recurso de Take Ownership (Tornar-se dono), tornando-se desta forma dono dos arquivos/pastas desejados, mesmo sem ter permissão de acesso a estes arquivos/pastas. Após ter “dado um Take Ownership”, o Administrador pode atribuir permissões de acesso para si mesmo e, com isso, acessar qualquer arquivo ou pasta.
- ◆ Um usuário pode utilizar um disquete de boot ou instalar um outro sistema operacional no computador e utilizar alguns programas comerciais existentes, para ter acesso a pastas e arquivos protegidas por permissões NTFS.

A grande questão é a seguinte: “Com o uso da criptografia, mesmo que o seu computador seja roubado ou que outro usuário tenha acesso ao computador, não será possível acessar os arquivos e pastas que você criptografou. A única maneira de ter acesso é fazendo o logon com a sua conta e senha”. Em resumo: Com a criptografia, os dados estão protegidos, mesmo que outras pessoas tenham acesso ao seu computador, a única maneira de acessar os arquivos criptografados é fazendo o logon com a conta do usuário que criptografou os arquivos ou com a conta configurada como Agente de Recuperação, conforme descreverei mais adiante. Já com as permissões NTFS, conforme descrito anteriormente, este nível de proteção não existe, no caso do computador ser roubado ou de um usuário mal intencionado ter acesso ao computador.

Claro que existem situações adversas que podem surgir com o uso da criptografia. Por exemplo, vamos supor que um funcionário criptografou arquivos importantes para a empresa. Neste meio tempo o funcionário foi demitido. Como é que a empresa poderá ter acesso aos arquivos criptografados se o funcionário demitido se negar a fazer o logon com a

sua conta e descriptografar os arquivos ou se a sua conta tiver sido excluída?? Por isso que o EFS permite que uma ou mais contas sejam configuradas como Agente de Recuperação, a qual pode ser utilizada em situações como a descrita neste parágrafo. Mais adiante tratarei, em detalhes, sobre o agente de recuperação.

O uso de criptografia é especialmente recomendado para usuários de notebooks e outros dispositivos semelhantes. Não é raro a ocorrência de roubos de notebooks, sendo que estes podem conter dados importantes da empresa, tais como planos estratégicos e relatórios de pesquisa e desenvolvimento de novos produtos. O uso da criptografia é a forma mais indicada para proteger estes dados, mesmo em situações de roubo de um notebook.

A criptografia é transparente para o usuário que criptografou o arquivo. Isso significa que o usuário não precisa descriptografar manualmente o arquivo criptografado para poder usá-lo. Ele pode abrir e alterar o arquivo da maneira habitual. Por exemplo, vamos supor que você criptografou um documento do Word. Ao dar um clique duplo no documento, o Windows Server 2003 descriptografa, automaticamente, o arquivo, abre o Word e carrega o arquivo para você. Observe que para o usuário toda a operação é transparente, ou seja, é como se o arquivo não estivesse criptografado. Se outro usuário, que não o que criptografou o arquivo, tentar utilizá-lo, receberá uma mensagem de acesso negado.

O uso do EFS é semelhante ao uso de permissões para arquivos e pastas. Ambos os métodos podem ser usados para restringir o acesso aos dados. No entanto, um intruso que obtenha acesso físico não-autorizado aos seus arquivos ou pastas criptografados não conseguirá acessá-los. Se o intruso tentar abrir ou copiar sua pasta ou arquivo criptografado, verá uma mensagem de acesso negado. As permissões definidas para arquivos e pastas não os protege contra ataques físicos não-autorizados, conforme já descrito anteriormente.

Você criptografa ou descriptografa uma pasta ou arquivo definindo a propriedade de criptografia para pastas e arquivos da mesma forma como define qualquer outro atributo, como somente leitura, compactado ou oculto. Se você criptografa uma pasta, todos os arquivos e subpastas criados na pasta criptografada serão automaticamente criptografados. É recomendável que você use a criptografia para pastas e não para arquivos individualmente, pois isso facilita a administração dos arquivos criptografados.

Observações importantes sobre a criptografia no Windows Server 2003:

- ◆ Somente arquivos e pastas em volumes NTFS podem ser criptografados.
- ◆ As pastas e os arquivos compactados não podem ser criptografados. Se o usuário marcar um arquivo ou pasta para criptografia, ele será descompactado. Falei sobre a compactação de pastas e arquivos em volumes NTFS, no Capítulo 6.
- ◆ Se você mover arquivos descriptografados para uma pasta criptografada, esses arquivos serão automaticamente criptografados na nova pasta. No entanto, a operação inversa não descriptografa automaticamente os arquivos. Nesse caso, é necessário descriptografar manualmente os arquivos.

---

**NOTA: Você também pode criptografar ou descriptografar um arquivo ou pasta usando o comando cipher.**

---

Os arquivos marcados com o atributo Sistema não podem ser criptografados, bem como os arquivos da pasta raiz do sistema, isto é C:\ ou D:\ e assim por diante.

- ◆ Criptografar um arquivo ou uma pasta não protege contra exclusão ou listagem de arquivos ou pastas. Qualquer pessoa com permissões NTFS adequadas pode excluir ou listar pastas ou arquivos criptografados. A proteção da criptografia é contra o acesso aos arquivos, ou seja, somente o usuário que criptografou o arquivo terá acesso. Para proteção contra listagem e exclusão recomenda-se o uso do EFS em combinação com permissões NTFS (descritas no Capítulo 6), utilizando as permissões NTFS para impedir que outros usuários possam excluir e até mesmo listar os arquivos que estão em um pasta criptografada.

- ◆ Você pode criptografar ou descriptografar pastas e arquivos localizados em um computador remoto ativado para criptografia remota. No entanto, se você abrir o arquivo criptografado na rede, os dados transmitidos na rede através desse processo não serão criptografados. Outros protocolos, como SSL/TLS ou IP Seguro (IPSec), devem ser usados para criptografar dados durante a transmissão.

## Garantindo a recuperação dos dados.

A criptografia utilizada pelo Windows Server 2003 é baseada na utilização de um par de chaves de criptografia. Uma chave é utilizada para criptografar os dados e a outra chave do par é utilizada para descriptografar os dados. A única maneira de descriptografar os dados e ter acesso às informações é tendo acesso as chaves de criptografia. Estas chaves são armazenadas em um Certificado digital, certificado este que é gerado, automaticamente, pelo Windows Server 2003, a primeira vez que o usuário criptografa um arquivo ou pasta. Neste Certificado digital estão todas as informações necessárias para criptografar e descriptografar arquivos.

Cada usuário que criptografa/descriptografa arquivos, possui o seu próprio Certificado digital, gerado automaticamente pelo Windows Server 2003. Um certificado adicional também é gerado para a conta configurada como Agente de recuperação. Desta maneira se o usuário que criptografou arquivos ou pastas deixar a empresa, será possível descriptografar os seus dados, utilizando a conta configurada como Agente de recuperação, uma vez que esta conta possui cópia do Certificado digital necessário a tal operação.

O Certificado digital nada mais é do que um arquivo que contém as informações necessárias para trabalhar com criptografia no Windows Server 2003. Como todo arquivo, fica gravado no disco rígido do computador. Acontece que se houver um problema com o disco rígido, a cópia do certificado do usuário e do certificado do agente de recuperação serão perdidas (caso não haja uma cópia de segurança) e, sem um destes certificados, ficará impossível descriptografar os arquivos/pastas criptografados pelo usuário. Na prática, significa que o acesso aos dados criptografados será perdido. Para evitar que isto aconteça, deve ser feita uma cópia de segurança, preferencialmente em disquete ou em um drive de rede, do Certificado digital gerado para o usuário. É importante lembrar que este certificado, somente será gerado na primeira vez que o usuário criptografa alguma pasta ou arquivo.

Algumas observações muito importantes e que não devem ser esquecidas para o exame:

- ◆ As pastas e os arquivos compactados não podem ser, ao mesmo tempo, criptografados. Se você criptografar uma pasta ou um arquivo compactado, essa pasta ou esse arquivo será descompactado.
- ◆ Os arquivos marcados com o atributo Sistema não podem ser criptografados, bem como os arquivos que se encontram na estrutura de diretórios raiz dos volumes (C:\, D:\ e assim por diante).
- ◆ Ao criptografar um único arquivo, você poderá optar se deseja criptografar a pasta que contém o arquivo. Se você escolher essa opção, todos os arquivos e subpastas que forem adicionados posteriormente à pasta serão criptografados quando forem adicionados.
- ◆ Ao criptografar uma pasta, você poderá optar se deseja que todos os arquivos e subpastas dentro da pasta também sejam criptografados. Se você escolher essa opção, todos os arquivos e subpastas atualmente na pasta serão criptografados, bem como quaisquer arquivos e subpastas que forem adicionados à pasta mais tarde. Se você optar por criptografar somente a pasta, todos os arquivos e subpastas que se encontram atualmente na pasta não serão criptografados. No entanto, quaisquer arquivos e subpastas que forem adicionados à pasta mais tarde serão criptografados quando forem adicionados. É aconselhável que você sempre opte por criptografar todo o conteúdo da pasta. Com isso você não terá que manter um controle sobre quais pastas e/ou arquivos estão criptografados e quais não estão.

---

**NOTA: Para todos os detalhes e exemplos práticos de como fazer o Bakcup e o Restore dos certificados digitais do usuários e do Agente de Recuperação, consulte o Capítulo 5.**

---

## Operações com arquivos criptografados (para o exame, não esqueça destes detalhes).

Ao copiar ou mover arquivos criptografados, diferentes situações podem ocorrer dependendo de a pasta de destino ser ou não criptografada e de estar ou não em um volume formatado com NTFS. A seguir descrevo algumas situações envolvendo ações de copiar e mover com arquivos criptografados.

- ◆ Ao copiar um arquivo não criptografado, para uma pasta criptografada, a cópia do arquivo será criptografada na pasta de destino. Por exemplo, você copia o arquivo não criptografado memo.doc, da pasta Meus documentos para a pasta Documentos pessoais, a qual está criptografada. O arquivo memo.doc copiado para a pasta Documentos pessoais será criptografado.
- ◆ Ao copiar um arquivo criptografado, para um volume NTFS em outro computador com o Windows 2000, Windows XP Professional ou Windows Server 2003, o arquivo manterá a criptografia. Se o computador de destino estiver rodando o Windows NT ou o volume for formatado com FAT, a cópia do arquivo não será criptografada.
- ◆ Se você mover um arquivo criptografado para outra pasta, no mesmo volume, o arquivo mantém a criptografia. Se você mover um arquivo criptografado para outro volume, o Windows Server 2003 considerará esta operação como sendo uma cópia, onde o arquivo é excluído na pasta de origem e copiado para a pasta de destino. Neste caso, o arquivo segue as regras explicadas no primeiro item.
- ◆ Se você renomear um arquivo criptografado, o arquivo continuará criptografado.
- ◆ Ao excluir um arquivo, a cópia do arquivo que fica na Lixeira, continuará criptografada.
- ◆ Se você fizer uma cópia de segurança de arquivos criptografados para uma fita de Backup ou para um outro volume NTFS, a cópia de segurança permanecerá criptografada.
- ◆ Se você quiser utilizar arquivos criptografados em outro computador, terá que importar o seu Certificado digital no computador de destino, conforme descrito anteriormente.

**IMPORTANTE:** Você também pode criptografar arquivos e pastas que estão em pastas compartilhadas, em outros computadores da rede. Basta mapear uma unidade para a pasta compartilhada (pastas compartilhadas e mapeamento de unidades será assunto do Capítulo 6), onde estão os arquivos e pastas a ser criptografados e utilizar os procedimentos descritos neste tópico, para criptografá-los.

**IMPORTANTE:** Se você tentar mover um arquivo criptografado por outro usuário, para um volume formatado com FAT, na tentativa de obter uma cópia não criptografada do arquivo, você receberá uma mensagem de Acesso negado, pois para descriptografar o arquivo (o que é necessário para movê-lo para um volume FAT), você teria que ter acesso ao Certificado digital do usuário que criptografou o arquivo, conforme descrito anteriormente.

## Recomendações sobre a criptografia de pastas e arquivos.

Neste item coloco algumas recomendações sobre a criptografia de pastas e arquivos. Estas recomendações são baseadas na documentação oficial da Microsoft:

- ◆ Para obter o máximo de segurança, criptografe as pastas antes de criar arquivos importantes nelas. Isso faz com que os arquivos criados sejam automaticamente criptografados e seus dados nunca sejam gravados em disco como texto sem formatação.

- ◆ Se você salvar a maior parte dos seus documentos na pasta Meus documentos, criptografe-a. Isso assegura que seus documentos pessoais sejam criptografados por padrão. No caso de perfis de usuários móveis, deve-se fazer isso apenas se a pasta Meus documentos for redirecionada para um local de rede.
- ◆ Criptografe pastas em vez de arquivos individuais para que, caso um programa crie arquivos temporários durante a edição, eles também sejam criptografados.
- ◆ O agente de recuperação designado deverá exportar o certificado de recuperação de dados e a chave particular para um disco, guardá-los em um local seguro e excluir do sistema a chave particular de recuperação de dados. Dessa forma, a única pessoa que poderá recuperar dados do sistema será aquela que possui acesso físico à chave particular de recuperação de dados. Estes procedimentos foram descritos no início deste tópico.
- ◆ Deve-se manter o menor número possível de agentes de recuperação designados. Desse modo, menos chaves ficarão expostas ao ataque criptográfico e haverá mais garantias de que os dados criptografados não sejam descriptografados inadequadamente.

## Alguns links com mais material de estudo:

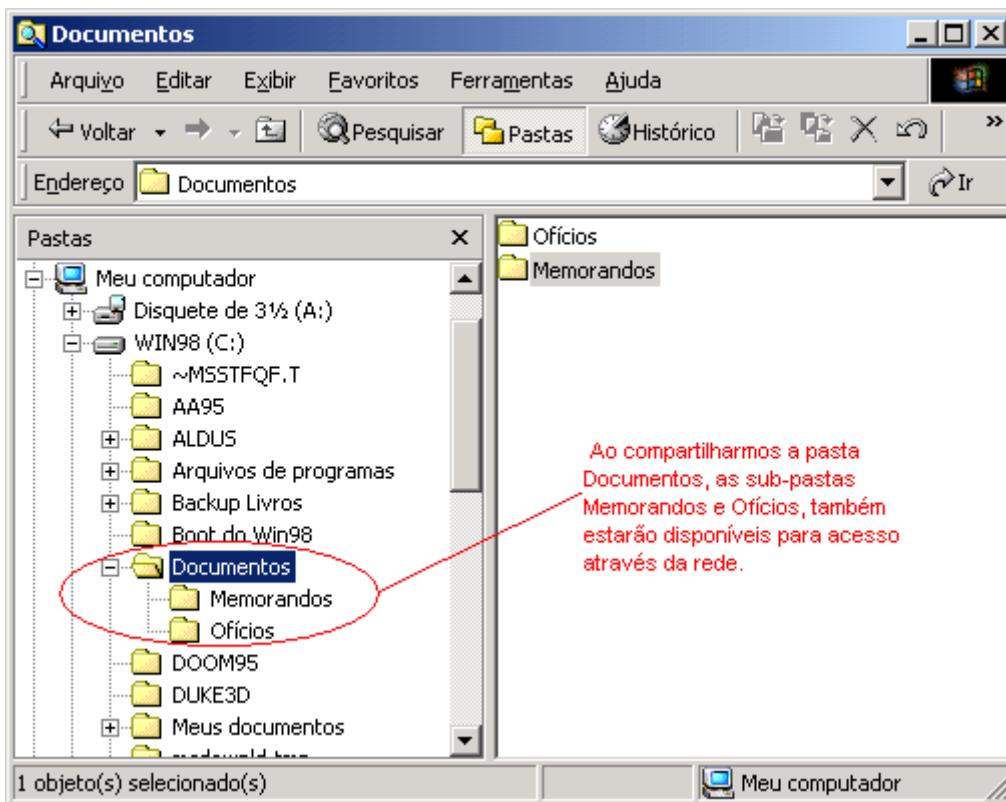
- ◆ <http://www.microsoft.com/windowsserver2003/techinfo/overview/file.mspx>
- ◆ <http://www.microsoft.com/windowsserver2003/techinfo/overview/storage.mspx>
- ◆ <http://www.microsoft.com/windowsserver2003/techinfo/overview/dfs.mspx>
- ◆ <http://support.microsoft.com/default.aspx?scid=kb;en-us;814594>
- ◆ <http://support.microsoft.com/default.aspx?scid=kb;en-us;816307>
- ◆ <http://support.microsoft.com/default.aspx?scid=kb;en-us;324897>
- ◆ <http://www.microsoft.com/windowsserver2003/techinfo/overview/scr.mspx>
- ◆ <http://support.microsoft.com/default.aspx?scid=kb;en-us;304606>
- ◆ <http://support.microsoft.com/default.aspx?scid=kb;en-us;312067>
- ◆ <http://support.microsoft.com/default.aspx?scid=kb;en-us;812547>

## Pastas compartilhadas, Permissões de Compartilhamento e Permissões NTFS.

Quando o administrador compartilha uma pasta, ele está permitindo que o conteúdo da pasta seja acessado por outros computadores da rede. Quando uma pasta é compartilhada, os usuários podem acessá-la através da rede, bem como o conteúdo (subpastas e arquivos) da pasta que foi compartilhada. Por exemplo, você pode criar uma pasta compartilhada onde são colocados documentos, orientações e manuais, de tal forma que os estes possam ser acessados a partir de qualquer estação de trabalho conectada à rede.

Ao compartilhar uma pasta todo o conteúdo da pasta passa a estar disponível para acesso através da rede. Isso significa que se houverem outras subpastas, dentro da pasta compartilhada, estas também estarão disponíveis para acesso pela rede.

Considere o exemplo da Figura 14.35. Se a pasta C:\Documentos for compartilhada, todo o seu conteúdo e também o conteúdo das subpastas C:\Documentos\Ofícios e C:\Documentos\Memorandos estarão disponíveis para acesso através da rede.



**Figura 14.35 Ao compartilhar uma pasta, todo o seu conteúdo estará disponível.**

Quando uma pasta é compartilhada em um computador, é criado um caminho para acessar esta pasta a partir dos demais computadores da rede. Este caminho segue o padrão UNC – Universal Naming Convention (Convenção Universal de Nomes). Todo caminho que segue o padrão UNC inicia com duas barras invertidas, seguida pelo nome do computador onde está o recurso compartilhado (que pode ser uma pasta compartilhada, um impressora compartilhada, etc), mais uma barra invertida e o nome do compartilhamento. Imagine que você está compartilhando recursos em um servidor da rede cujo nome é: SRVRS001. Neste servidor são criadas três pastas compartilhadas com os seguintes nomes de compartilhamento: documentos, manuais e memorandos. No servidor SRVRS001 você também compartilha uma impressora com o nome de compartilhamento lasera1. Qual seria o caminho para acessar estes recursos, segundo o padrão UNC?

\SRVRS001\documentos  
 \SRVRS001\manuais  
 \SRVRS001\memorandos  
 \SRVRS001\lasera1

## Restringindo o acesso às pastas compartilhadas.

Porém quando uma pasta é compartilhada, não significa que o seu conteúdo deva ser acessado por todos os usuários da rede. É possível restringir quais usuários terão acesso à pasta compartilhada, e qual o número máximo de usuários que podem acessar a pasta simultaneamente. Esta restrição é feita através de Permissões de compartilhamento.

Com o uso de permissões de compartilhamento é possível definir quais os usuários que poderão acessar o conteúdo da pasta compartilhada e qual o nível de acesso de cada usuário. Para isso, é criada uma lista com o nome dos usuários e grupos que possuem permissão de acesso. Esta lista é tecnicamente conhecida como ACL – Access Control List (Lista de Controle de Acesso).

Também é possível limitar o que os usuários com permissão de acesso podem fazer. Pode haver situações em que alguns usuários devem ter permissão apenas para ler o conteúdo da pasta compartilhada, podem haver outras situações em que alguns usuários devem ter permissão de leitura e escrita, enquanto outros devem ter permissões totais, tais como leitura, escrita e até exclusão de arquivos e assim por diante.

Na Figura 14.36, mostro um exemplo, em que o grupo Gerentes possui permissões de Controle total, enquanto o grupo Usuários possui permissões apenas para leitura.

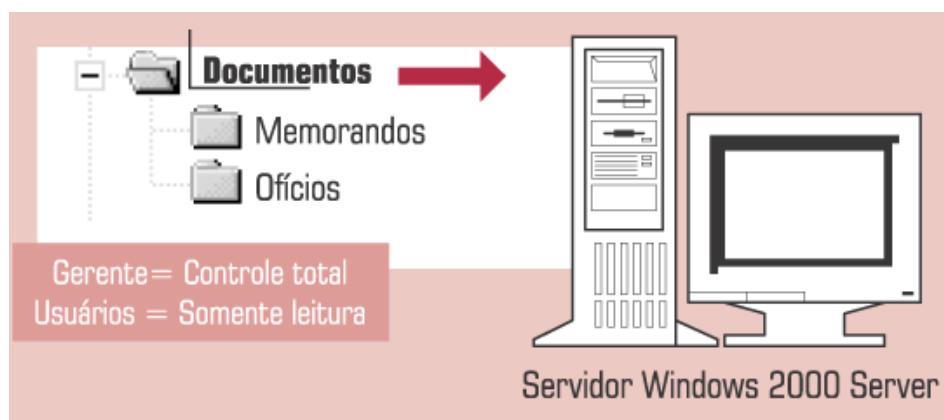


Figura 14.36 Grupos diferentes com permissões diferentes.

Ao criar um compartilhamento em uma pasta, por padrão o Windows Server 2003 atribui como permissão de compartilhamento Read (Somente Leitura) para o grupo Everyone (Todos), que conforme o nome sugere, significa qualquer usuário com acesso ao computador, seja localmente, seja pela rede. Ou seja, ao criar um compartilhamento, automaticamente será permitida a leitura em todo o conteúdo do compartilhamento para todos os usuários da rede. Esta situação já é um pouco melhor do que ocorria com o Windows 2000 Server, onde era definida, por padrão, permissão Full Control (Controle Total) para o grupo Everyone (Todos). Por isso ao criar um compartilhamento, o administrador já deve configurar as permissões necessárias, a menos que esteja sendo compartilhada uma pasta de domínio público, onde todos os usuários devem ter acesso de leitura em todos os arquivos e subpastas da pasta que está sendo compartilhada.

## Entendendo as permissões de compartilhamento.

Existem três níveis de permissões de compartilhamento, conforme descrito a seguir:

Leitura: A permissão de Leitura permite ao usuário:

- ◆ Listar os nomes de arquivos e de subpastas, dentro da pasta compartilhada.
- ◆ Acessar as subpastas dentro da pasta compartilhada.
- ◆ Abrir os arquivos para leitura.
- ◆ Execução de arquivos de programa (.exe, .com, etc).

**IMPORTANTE:** O nome do compartilhamento não precisa ser igual ao da pasta que está sendo compartilhada. É recomendado que o nome do compartilhamento sirva como indicação para o conteúdo da pasta compartilhada, para facilitar a localização dos recursos disponíveis na rede e a pesquisa no Active Directory.

**IMPORTANTE:** As permissões definem o que o usuário pode fazer com o conteúdo de uma pasta compartilhada, desde somente leitura, até um controle total sobre o conteúdo da pasta compartilhada. Porém as permissões de compartilhamento somente tem efeito se o acesso for feito pela rede. Se o usuário fizer o logon no computador onde está a pasta compartilhada e acessa-la localmente, através do drive C: (ou outro drive qualquer onde está a pasta compartilhada), as permissões de compartilhamento não serão verificadas e, portanto, não terão nenhum efeito. Para limitar o acesso, mesmo localmente, usa-se as permissões NTFS, as quais serão descritas mais adiante.

**IMPORTANTE:** Vou insistir para que você não esqueça, de jeito nenhum: “Permissões de compartilhamento, não impedem o acesso ao conteúdo da pasta localmente, isto é, se um usuário

Alteração: Permite ao usuário os mesmos direitos da permissão leitura, mais os seguintes direitos:

- ◆ Criação de arquivos e subpastas.
- ◆ Alteração de dados nos arquivos
- ◆ Exclusão de subpastas e arquivos
- ◆ Controle total: Esta é a permissão padrão que se aplica a todos os novos compartilhamentos. Essa permissão era atribuída ao grupo Everyone (Todos) ao compartilhar um recurso no Windows 2000 Server. Já no Windows Server 2003 é atribuída a permissão Read (Somente Leitura) ao grupo Everyone (Todos) por padrão, quando um novo compartilhamento é criado. Controle total possibilita as mesmas operações que Leitura e Alteração, mais as seguintes:
  - ◆ Alteração de permissões (apenas para arquivos e pastas do NTFS)
  - ◆ Apropriação (Take Ownership), apenas para arquivos e pastas em um volume formatado com NTFS.

As permissões de compartilhamento: Leitura, Alteração e Controle total, podem ser Permitidas ou Negadas. Ou seja podemos permitir o acesso com um determinado nível (leitura, alteração ou Controle total) ou negar explicitamente o acesso para um usuário ou grupo para quaisquer uma destas permissões. Considere um exemplo prático. Suponha que todos os usuários do grupo Gerentes devem ter acesso de Leitura a uma pasta compartilhada, com exceção de um gerente cuja conta de usuário é jsilva, o qual deve ter negado o direito de leitura na referida pasta. Para simplificar a atribuição de permissões o administrador faz o seguinte:

- ◆ Permissão de Leitura para o grupo Gerentes – Permitir.
- ◆ Permissão de Leitura para o usuário jsilva – Negar.

Com isso todos os usuários do grupo Gerentes terão permissão de leitura, com exceção do usuário “jsilva”, o qual teve a permissão de leitura negada. Outra recomendação é que sempre devemos atribuir permissões para grupos de usuários, ao invés de atribuir para usuários individuais, pois isso facilita a administração, conforme descrito no Capítulo 4.

**IMPORTANTE:** Negar sempre tem precedência sobre permitir. Por exemplo, se o usuário pertencer a cinco grupos, sendo que quatro dos quais tem permissão de acesso e o outro grupo tem negada a permissão de acesso, o usuário terá negada a permissão de acesso. A permissão negar acesso, herdada de um dos grupos, terá precedência sobre todas as demais permissões herdadas dos demais grupos. Não esqueça deste detalhe, para o exame.

fizer o logon no computador onde está a pasta compartilhada, o usuário terá acesso a todo o conteúdo da pasta, a menos que as Permissões NTFS estejam configurados de acordo. Permissões NTFS é assunto para daqui a pouco”.

**IMPORTANTE:** Pastas e arquivos possuem atributos, que o Windows Server 2003 utiliza para gerenciar os arquivos. Por exemplo, existe um atributo Somente leitura, que uma vez marcado torna o arquivo somente leitura, isto é, não podem ser feitas alterações no arquivo. Para ver os atributos de um arquivo ou pasta, basta dar um clique com o botão direito do mouse no arquivo ou pasta, e no menu que surge dê um clique na opção Propriedades. O Windows Server 2003 exibe uma janela onde é possível verificar e modificar os atributos do arquivo ou pasta, desde que o usuário tenha as devidas permissões.

**IMPORTANTE:** No Windows Server 2003, objetos como pastas e arquivos possuem um “dono”, o qual por padrão é o usuário que estava logado e que criou a pasta ou arquivo. Conforme mostrarei no final deste capítulo é possível, ao Administrador, tornar-se dono de uma pasta ou arquivo, utilizando uma ação de Take Ownership (Tornar-se dono).

## Quando um usuário pertence a mais de um grupo, como é que fica a permissão efetiva do usuário?

Quando um usuário pertence, por exemplo, a dois grupos e os dois grupos recebem permissão para acessar um compartilhamento, sendo que os dois grupos possuem permissões diferentes, por exemplo, um tem permissão de Leitura e o outro de Alteração. Como é que ficam as permissões do usuário que pertence aos dois grupos?

Para responder a esta questão, considere as seguintes observações:

- ◆ Quando um usuário pertence a mais de um grupo, cada qual com diferentes níveis de permissões para uma pasta compartilhada, o nível de permissão para o usuário que pertence a mais de um grupo, é a combinação das permissões atribuídas aos diferentes grupos.

No exemplo a seguir, o usuário pertence a dois grupos, um com permissão de somente leitura e outro com permissão de alterações. A nível de permissão do usuário é de alterações, pois é a soma das permissões dos dois grupos, conforme indicado na Figura 14.37:

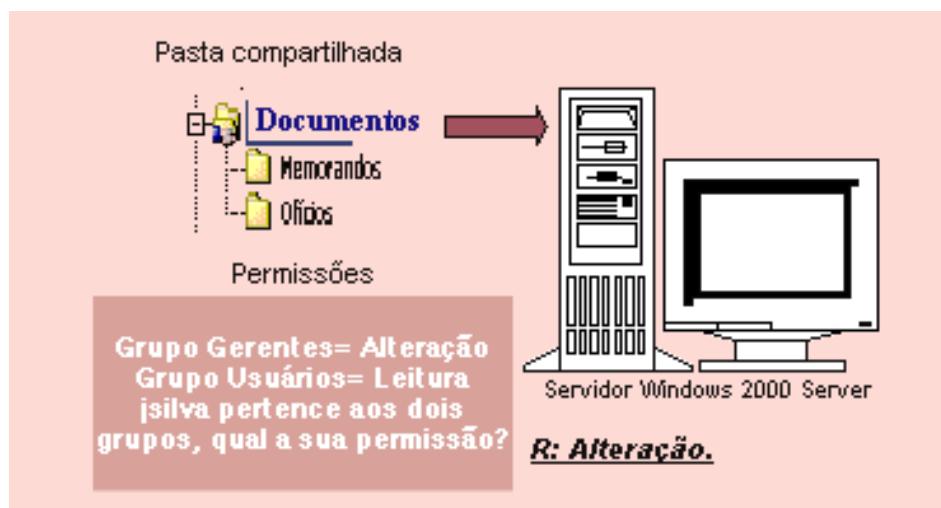


Figura 14.37 Usuário que pertence a mais de um grupo.

- ◆ Negar têm precedência sobre quaisquer outras permissões.

Vamos considerar o exemplo do usuário que pertence a três grupos. Se em um dos grupos ele tiver permissão de leitura e em outro grupo permissão de alteração. Mas se para o terceiro grupo, for negada a permissão de leitura, o usuário terá o acesso negado, uma vez que Negar tem precedência sobre quaisquer outras permissões, conforme indicado pela Figura 14.38.

---

**IMPORTANTE:** Quando uma pasta compartilhada é copiada, a pasta original permanece compartilhada, porém a cópia não é compartilhada. Quando o administrador move uma pasta compartilhada, a pasta deixa de ser compartilhada.

---

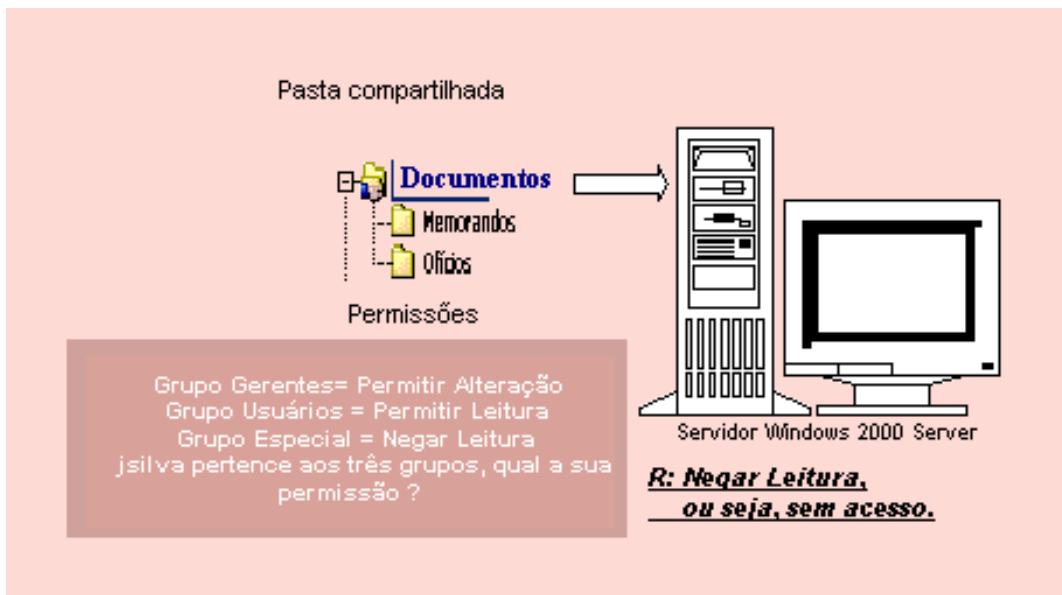


Figura 14.38 Negar tem precedência sobre permitir.

### Orientações para a criação de pastas compartilhadas:

- ◆ Todo compartilhamento deve ter um nome, para que o compartilhamento possa ser acessado pela rede, conforme descrito anteriormente e será demonstrado na parte prática mais adiante. O nome do compartilhamento pode ser diferente do nome da pasta. Uma recomendação importante é para que seja escolhido um nome descriptivo do conteúdo da pasta, de tal maneira que o compartilhamento seja mais facilmente localizada na rede. Você não colocaria um nome de compartilhamento “Projetos” em uma pasta compartilhada com documentos contábeis?
- ◆ Organize os recursos, de tal maneira que todos os pastas que devam ser acessadas pelo mesmo grupo de usuários, com o mesmo nível de permissão, estejam dentro da mesma pasta compartilhada. Por exemplo, se você possui sete pastas com documentos e programas, os quais devem ser acessados pelos grupos Contabilidade e Marketing. Coloque estas pastas dentro de uma pasta principal e compartilhe a pasta principal, ao invés de criar sete compartilhamentos individuais. Em seguida atribua permissões de acesso somente para os grupos Contabilidade e Marketing.
- ◆ Configure o nível de permissão mínimo necessário para que os usuários realizem o seu trabalho. Por exemplo se os usuários precisam apenas ler os documentos em uma pasta compartilhada, atribua permissão de Leitura e não de Alteração ou Controle total.
- ◆ Sempre que possível, atribua permissões para grupos de usuários e não para usuários individuais, pois isso facilita a administração, conforme já salientado diversas vezes neste capítulo e no Capítulo 4.
- ◆ Determine quais grupos necessitam acesso a quais pastas compartilhadas e com quais níveis de permissão. Documente bem todo esse processo, para que você possa ter um bom controle sobre os recursos compartilhados e as permissões atribuídas.

**NOTA:** Se você ainda tem clientes baseados no Windows 3.x ou no MS-DOS, você deve utilizar nomes de compartilhamento com o máximo de 8 caracteres para o nome. Nomes de compartilhamento maiores do que 8 caracteres não estarão visíveis para clientes baseados no Windows 3.x e no MS-DOS. Estes clientes verão os nomes de pastas e artigos no formato truncado, adaptado para o formato 8.3 (oito caracteres para o nome e três caracteres para a extensão), que é o formato suportado pelo Windows 3.x e pelo MS-DOS.

## Sistemas de arquivos e permissões NTFS – conceito.

Agora mostrarei alguns detalhes sobre os sistemas de arquivos que o Windows Server 2003 reconhece e também sobre permissões NTFS.

Um sistema de arquivos determina a maneira como o Windows Server 2003 organiza e recupera as informações no Disco rígido ou em outros tipos de mídia. O Windows Server 2003 reconhece os seguintes sistemas de arquivos:

FAT  
FAT32  
NTFS  
NTFS 5

O sistema FAT vem desde a época do MS-DOS e tem sido mantido por questões de compatibilidade. Além disso se você tiver instalado mais de um Sistema Operacional no seu computador, alguns sistemas mais antigos (DOS, Windows 3.x e as primeiras versões do Windows 95) somente reconhecem o sistema FAT. Com o sistema de arquivos FAT, a única maneira de restringir o acesso ao conteúdo de uma pasta compartilhada, é através das permissões de compartilhamento, as quais, conforme descrito anteriormente, não terão nenhum efeito se o usuário estiver logado localmente, na máquina onde a pasta foi compartilhada. Com a utilização do sistema FAT, alguns recursos avançados, tais como compressão, criptografia e auditoria, não estão disponíveis.

O sistema FAT32 apresenta algumas melhorias em relação ao sistema FAT. Existe um melhor aproveitamento do espaço no disco, o que consequentemente gera menor desperdício do espaço em disco (este melhor uso do espaço em disco tem a ver com a questão da Fragmentação de Volumes, discutida no Capítulo 5). Um grande inconveniente do sistema FAT32 é que ele não é reconhecido pelo Windows NT Server 4.0. Com o sistema de arquivos FAT32, a única maneira de restringir o acesso ao conteúdo de uma pasta compartilhada, é através das permissões de compartilhamento, as quais, conforme descrito anteriormente, não terão nenhum efeito se o usuário estiver logado localmente, na máquina onde a pasta foi compartilhada. Com a utilização do sistema FAT32, alguns recursos avançados, tais como compressão e criptografia e auditoria, não estão disponíveis.

O sistema de arquivos NTFS é utilizado no Windows NT Server 4.0 e foi mantido no Windows 2000 Server por questões de compatibilidade. É um sistema bem mais eficiente do que FAT e FAT32, além de permitir uma série de recursos avançados, tais como:

- ◆ Permissões de controle de acesso a arquivos e pastas – permissões NTFS.
- ◆ Compressão de arquivos e pastas.
- ◆ Auditoria de acesso.
- ◆ Partições bem maiores do que as permitidas com FAT e FAT32.
- ◆ Desempenho bem superior do que com FAT e FAT32.
- ◆ Menor índice de fragmentação de partições e volumes.

**IMPORTANTE:** Se você quiser ocultar um compartilhamento, de tal maneira que ele não seja exibido na lista de recursos compartilhados quando for usado o comando \\nome\_do\_computador, basta finalizar o nome do compartilhamento com o caractere \$. Por exemplo, se você criar um compartilhamento chamado Docs\$, este será um compartilhamento oculto, o qual somente poderá ser acessado se for utilizado o caminho comando : \\nome\_do\_computador\Docs\$. Por padrão, o Windows Server 2003 cria alguns compartilhamentos ocultos para funções específicas do próprio Sistema Operacional. Estes compartilhamentos também têm permissões específicas. Por exemplo, é criado um compartilhamento C\$, o qual dá acesso a pasta raiz do disco rígido, porém somente usuários com conta de Administrador tem acesso a este compartilhamento. Não esqueça: Para ocultar um compartilhamento, basta acrescentar o sinal de \$ como último caractere do nome do compartilhamento. Lembre-se deste detalhe para o exame.

Uma das principais vantagens do NTFS é que ele permite que sejam definidas permissões de acesso para arquivos e pastas, isto é, posso ter arquivos em uma mesma pasta, com permissões diferentes para usuários e grupos diferentes. Além disso, as permissões NTFS têm efeito localmente, isto é, mesmo que o usuário faça o logon no computador onde um determinado arquivo existe, se o usuário não tiver as permissões NTFS necessárias, ele não poderá acessar o arquivo. Isso confere um alto grau de segurança, desde que as permissões NTFS sejam configuradas corretamente.

No Windows 2000 Server foi introduzido NTFS 5, a nova versão do NTFS, que é a versão utilizada pelo Windows Server 2003. O NTFS 5 apresenta diversas melhorias em relação a versão mais antiga do NTFS, tais como:

Criptografia de arquivos e pastas (a criptografia é uma maneira de “embaralhar” a informação de tal forma que mesmo que um arquivo seja copiado, o arquivo se torna ilegível, a não ser para a pessoa que possui a chave para descriptografar o arquivo). Para detalhes sobre Criptografia de arquivos e pastas consulte o Capítulo 5.

- ◆ Quotas de usuário, fazendo com que seja possível limitar o espaço em disco que cada usuário pode utilizar.
- ◆ Gerenciamento e otimização melhorados.

| Permissões especiais           | Controle total | Modificar | Ler e executar | Listar conteúdo de pastas (somente para pastas) | Ler | Gravar |
|--------------------------------|----------------|-----------|----------------|---|-----|--------|
| Desviar pasta/executar arquivo | x              | x         | x              | x   |     |        |
| Listar pasta/Ler dados         | x              | x         | x              | x   | x   |        |
| Ler atributos                  | x              | x         | x              | x   | x   |        |
| Ler atributos estendidos       | x              | x         | x              | x   | x   |        |
| Criar arquivos/Gravar dados    | x              | x         |                |   |     | x      |
| Criar pastas/Acrecentar dados  | x              | x         |                |   |     | x      |
| Gravar atributos               | x              | x         |                |   |     | x      |
| Gravar atributos estendidos    | x              | x         |                |   |     | x      |
| Excluir subpastas e arquivos   | x              |           |                |   |     |        |
| Excluir                        | x              | x         |                |   |     |        |
| Ler permissões                 | x              | x         | x              | x   | x   | x      |
| Alterar permissões             | x              |           |                |   |     |        |
| Apropriar-se                   | x              |           |                |   |     |        |
| Sincronizar                    | x              | x         | x              | x   | x   | x      |

Figura 14.39 Ações associadas com as permissões de pasta e arquivos.

Conforme descrito anteriormente, o administrador pode definir permissões de acesso para pastas ou arquivos, mas somente em unidades formatadas com o sistema de arquivos NTFS (seja na versão do NT Server 4.0 ou o NTFS 5 do

Windows 2000 Server/Windows Server 2003 ). Por isso que é aconselhável instalar o Windows Server 2003 sempre em unidades formatadas com NTFS, pois isso permite uma maior segurança e proteção dos dados. As partições NTFS apresentam um desempenho um pouco inferior do que as partições FAT32, em termos de velocidade. Porém em termos de segurança não existe comparação, por isso recomendo a utilização do sistema NTFS. Se você estiver em dúvida, no momento da instalação do Windows Server 2003, pode optar por formatar o disco rígido utilizando FAT 32. Depois é possível converter para NTFS, sem perda de dados. Porém cuidado, uma vez convertido o disco rígido para NTFS não é possível reverter para FAT32. A única maneira é fazer um backup do disco rígido, formatando-o novamente com FAT32 e restaurar o backup.

Com relação as permissões NTFS, existe um conjunto diferente de permissões quando tratamos de pastas ou arquivos. Na Figura 14.39 apresento um resumo das permissões de pasta e de arquivos, com as ações associadas com cada permissão.

A seguir apresento a descrição, com maiores detalhes, para cada uma das permissões listadas na Figura 14.39:

- ◆ **Traverse Folder/Execute File (Permissão Desviar pasta/Executar arquivo):** Estas permissões são aplicadas a pastas e arquivos. Para as pastas, Desviar pasta permite ou nega o movimento através de pastas para acessar outros arquivos ou pastas, mesmo que o usuário não tenha permissões referentes às pastas desviadas (aplica-se somente a pastas). Por exemplo vamos supor que o usuário tem permissão na pasta C:\Documentos, não tem permissão na pasta C:\Documentos\Ofícios e tem na pasta C:\Documentos\Ofícios\2001. Neste caso, o usuário para chegar até a pasta 2001, terá que passar pela pasta Ofícios, para a qual ele não tem permissão. Para que o usuário possa passar pela pasta Ofício, o administrador deve atribuir-lhe a permissão Desviar pasta. Desviar pasta tem efeito apenas quando o grupo ou usuário não tem o direito de usuário Ignorar verificação com desvio no snap-in de diretivas de grupo. (Por padrão, o grupo Todos tem o direito de usuário Ignorar verificação com desvio.)
- ◆ **Para os arquivos: Execute File (Executar arquivo) permite ou nega a execução de arquivos de programa (aplica-se somente a arquivos).** Ao definir a permissão Traverse Folder (Desviar Pasta) em uma pasta, você não está automaticamente definindo a permissão Executar arquivo em todos os arquivos dessa pasta.
- ◆ **Permissão List Folder/Read Data (Listar Pasta/Ler Dados):** List Folder (Listar Pasta) permite ou nega a exibição de nomes de arquivos e subpastas dentro da pasta. Essa permissão afeta apenas o conteúdo da pasta em questão, não afetando o fato de a pasta na qual a permissão está sendo definida ser listada ou não. Aplica-se somente a pastas. Read Data (Ler Dados) permite ou nega a exibição de dados em arquivos (aplica-se somente a arquivos). Por exemplo, se o usuário tem permissão de Ler dados em um arquivo do Word, este usuário poderá abrir o arquivo, porém não poderá alterá-lo ou excluí-lo.
- ◆ **Permissão Read Attributes (Ler Atributos):** Permite ou nega a exibição de atributos de um arquivo ou pasta, como os atributos somente leitura ou oculto. Os atributos são definidos pelo NTFS. Para acessar os atributos de uma pasta ou arquivo, clique com o botão direito do mouse na pasta/arquivo e, no menu que surge, dê um clique na opção Properties (Propriedades).
- ◆ **Permissão Read Extended Attributes (Ler Atributos Estendidos):** Permite ou nega a exibição de atributos estendidos de um arquivo ou pasta. Os atributos estendidos são definidos por programas e podem variar de acordo com o programa.
- ◆ **Permissão Create Files/Write Data (Criar Arquivos/Gravar Dados):** Criar arquivos permite ou nega a criação de arquivos dentro da pasta (aplica-se somente a pastas). Gravar dados permite ou nega as alterações no arquivo e a substituição de um conteúdo existente (aplica-se somente a arquivos). Esta permissão é mais conhecida por permissão de Escrita (ou Alteração).

- ◆ **Create Folders/Append Data (Permissão Criar Pastas/Acrecentar Dados):** Criar pastas permite ou nega a criação de pastas dentro da pasta na qual a permissão foi definida (aplica-se somente a pastas). Acrecentar dados permite ou nega as alterações no final do arquivo, mas não a alteração, exclusão ou substituição de dados existentes (aplica-se somente a arquivos).
- ◆ **Permissão Write Attributes (Gravar Atributos):** Permite ou nega a alteração de atributos de um arquivo ou pasta, como somente leitura ou oculto. Os atributos são definidos pelo NTFS. A permissão Gravar atributos não implica na criação ou exclusão de arquivos ou pastas, apenas inclui a permissão para efetuar alterações nos atributos de um arquivo ou de uma pasta.
- ◆ **Permissão Write Extended Attributes (Gravar Atributos Estendidos):** Permite ou nega a alteração de atributos estendidos de um arquivo ou pasta. Os atributos estendidos são definidos por programas e podem variar de acordo com o programa. A permissão Gravar atributos estendidos não implica na criação ou exclusão de arquivos ou pastas, apenas inclui a permissão para efetuar alterações nos atributos de um arquivo ou de uma pasta
- ◆ **Permissão Delete Subfolders and Files (Excluir Subpastas e Arquivos):** Permite ou nega a exclusão de subpastas e arquivos, mesmo que a permissão Excluir não tenha sido concedida na subpasta ou arquivo. (aplica-se a pastas). Por exemplo, se você não tem permissão de Excluir na pasta Documentos, mas tem permissão de Excluir em um arquivo memo.doc, que está na pasta Documentos, você conseguirá Excluir o documento memo.doc, pois as permissões de arquivo tem precedência sobre as permissões de pastas, quando conflitantes.
- ◆ **Permissão Delete (Excluir):** Permite ou nega a exclusão da pasta e/ou arquivo. Se o usuário não tiver permissão de excluir em um arquivo ou pasta, ele ainda poderá excluir o arquivo ou pasta, se ele tiver permissão Delete Subfolders and Files (Excluir Subpastas e Arquivos) na pasta pai. Por exemplo, suponha uma pasta Documentos, na qual o usuário tem permissão Delete Subfolders and Files. Dentro da pasta Documentos tem a pasta Ofícios, na qual o usuário não tem permissão Delete. Mesmo assim ele poderá excluir a pasta Ofícios, pois ele tem permissão Delete Subfolders and Files na pasta Pai de Ofícios que é a pasta Documentos.
- ◆ **Permissão Read Permissions (Ler Permissões):** Permite ou nega a leitura de permissões do arquivo ou pasta, como Controle total, Ler e Gravar. Se o usuário não tiver esta permissão, ele não poderá exibir a lista com as permissões definidas para um arquivo e/ou pasta.
- ◆ **Permissão Change Permissions (Alterar Permissões):** Permite ou nega a alteração de permissões do arquivo ou pasta, como Controle total, Ler e Gravar. Esta é uma permissão “poderosa” e que deve ser utilizada com cuidado. Uma vez que o usuário tem permissão para Alterar permissões, ele pode perfeitamente atribuir Controle total para ele mesmo, ou seja, para a sua conta de usuário.
- ◆ **Permissão Take Ownership (Apropriar-se) :** Permite ou nega a apropriação (tornar-se dono) do arquivo ou pasta. O proprietário de um arquivo ou pasta sempre pode alterar permissões, independentemente de qualquer permissão existente que proteja o arquivo ou pasta. O dono de um arquivo ou pasta, por padrão, é o usuário que cria o arquivo /pasta.

Todo arquivo ou pasta em uma unidade formatada com NTFS, possui uma “Lista de controle de acesso (Access Control List) – ACL. Nesta ACL fica uma lista de todas as contas de usuários e grupos para os quais foi garantido acesso para o recurso, bem como o nível de acesso de cada um deles.

**IMPORTANTE:** Existem alguns detalhes que devem ser reforçados/revisados sobre as permissões NTFS. Para o exame, não esqueça os seguintes detalhes:

- ◆ Permissões NTFS são cumulativas, isto é, se um usuário pertence a mais de um grupo, os quais tem diferentes níveis de permissão para um recurso, a permissão efetiva do usuário é a soma das permissões atribuídas aos grupos aos quais o usuário pertence.
- ◆ Permissões NTFS para um arquivo têm prioridade sobre permissões NTFS para pastas. Por exemplo se um usuário têm permissão NTFS de escrita em uma pasta, mas somente permissão NTFS de leitura para um arquivo dentro desta pasta, a sua permissão efetiva será somente a de leitura, pois a permissão para o arquivo tem prioridade sobre a permissão para a pasta.
- ◆ Negar uma permissão NTFS tem prioridade sobre permitir. Por exemplo, se um usuário pertence a dois grupos diferentes. Para um dos grupos foi dado permissão de leitura para um arquivo e para o outro grupo foi Negada a permissão de leitura, o usuário não terá o direito de leitura, pois Negar tem prioridade sobre Permitir.

## Combinando permissões de compartilhamento e permissões NTFS – estudo de casos.

Você pode estar se perguntando como é que o Windows Server 2003 trata quando existem diferenças entre as permissões de compartilhamento e as permissões NTFS. Por exemplo se nas permissões de compartilhamento o usuário maria tem direito de Controle total e nas permissões NTFS o usuário maria tem direito apenas de Leitura. Qual a permissão efetiva do usuário maria?

Eu já fiz alguns comentários sobre a combinação entre as permissões de compartilhamento e as permissões NTFS. Neste tópico vou detalhar este assunto através do uso de mais alguns exemplos.

É hora de analisar algumas situações práticas para fixar bem a combinação entre permissões de compartilhamento e NTFS.

Exemplo 01: Considere a situação indicada na Figura 14.40. Qual a permissão efetiva do usuário jsilva2, na pasta compartilhada Documentos ?

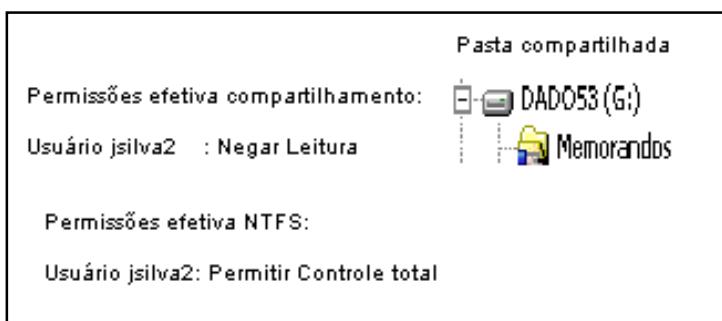


Figura 14.40 A permissão efetiva é a mais restritiva.

Para entender a situação da Figura 14.40, você deve ter em mente que no caso de diferenças entre as permissões de compartilhamento e as permissões NTFS, a permissão efetiva é a mais restritiva.

No exemplo da figura a permissão efetiva do usuário jsilva2 é Leitura a qual é a mais restritiva entre Controle total (a permissão NTFS do usuário jsilva2) e Leitura (permissão de compartilhamento do usuário jsilva2). A mesma análise é válida em relação ao usuário maria.

Agora considere uma situação um pouco mais complexa, onde tem que ser considerada a combinação das permissões dos diferentes grupos aos quais pertence um usuário, além da combinação entre permissões de compartilhamento e permissões NTFS.

**IMPORTANTE:** Quando existem diferenças entre as permissões efetivas resultantes de compartilhamento e as permissões efetivas resultantes NTFS, a permissão efetiva é a MAIS RESTITIVA, isto é, aquele que restringe mais as ações que podem ser tomadas. No exemplo do primeiro parágrafo, a permissão efetiva para o usuário maria seria Leitura, a qual é mais restritiva do que Controle total.

Admita que o usuário jsilva2 pertença aos grupos Contabilidade e Marketing. Com base na Figura 14.41, qual seria a permissão efetiva para o usuário jsilva2 na pasta compartilhada Documentos?

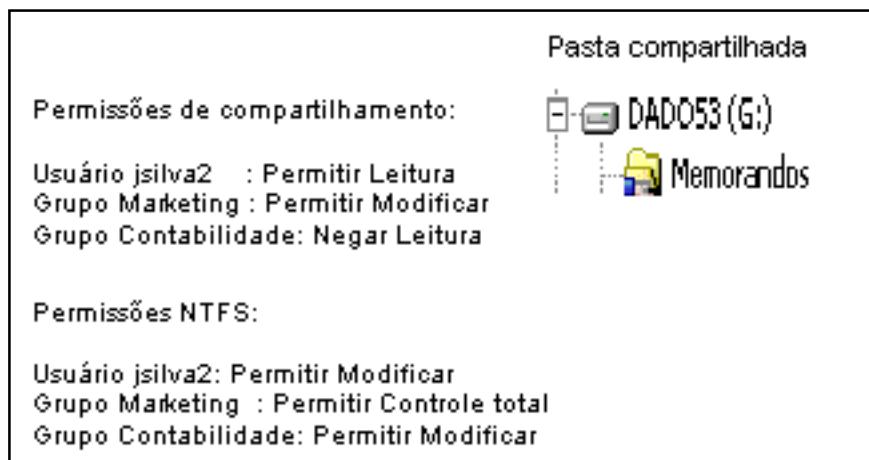


Figura 14.41 Usuário jsilva2 pertence aos grupos Marketing e Contabilidade.

Para definir a permissão efetiva para o usuário jsilva2, devem ser levadas em considerações diversos regras, já apresentadas ao longo deste capítulo:

- ◆ Quando um usuário pertence a vários grupos, os quais recebem diferentes permissões (quer sejam permissões de compartilhamento ou NTFS), a permissão efetiva é a soma das permissões. Além disso você deve lembrar que Negar tem prioridade sobre permitir. No caso das permissões de compartilhamento, um dos grupos ao qual o usuário jsilva2 pertence – grupo Contabilidade – tem a permissão de leitura negada. Logo a permissão efetiva de compartilhamento para jsilva2 é Negar leitura, independente das demais permissões atribuídas aos grupos aos quais pertence o usuário jsilva2.

A permissão efetiva NTFS para o usuário jsilva2 é a soma das permissões do usuário com as permissões dos grupos Marketing e Contabilidade. Com isso a permissão NTFS efetiva é Permitir Controle total.

Com isso é possível reduzir a situação proposta inicialmente, na Figura 14.41, a uma situação mais simplificada, conforme indicado na Figura 14.42:

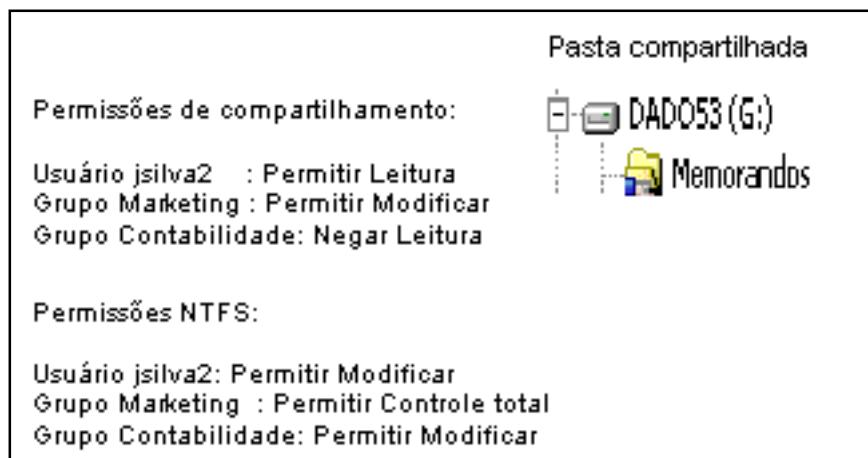


Figura 14.42 Simplificando a situação.

Agora é hora de lembrar que quando existe diferença entre as permissões de compartilhamento e NTFS vale a mais restritiva.

Com isso é possível determinar que a permissão efetiva do usuário jsilva2 no compartilhamento Documentos é “Negar Leitura”, isto é, o usuário não conseguirá nem listar o conteúdo da pasta.

## Pastas Off-line: conceito e utilizações.

Com o Windows Server 2003 (já era possível com o Windows 2000 e também no Windows XP Professional), você pode configurar uma pasta compartilhada, para que o usuário possa ter acesso aos arquivos do compartilhamento, mesmo quando não estiver conectado à rede. Em um primeiro momento pode parecer estranho: “Como ter acesso aos arquivos de uma pasta compartilhada, sem estar conectado à rede??” Na prática o que acontece é que, ao configurar um compartilhamento para acesso Off-line, o administrador está orientando os clientes que acessam o compartilhamento, a fazer uma cópia local dos arquivos do compartilhamento, com isso o usuário fica trabalhando na cópia local, em caso de perda da conexão com a rede. De tempos em tempos as alterações feitas na cópia local (também conhecido como Cache local de arquivos), são sincronizadas com a cópia original, na pasta compartilhada. Se por algum motivo, o computador perder o acesso à rede, o usuário continua trabalhando na cópia local, podendo inclusive desligar o computador. Na próxima vez que o computador for conectado à rede, os arquivos serão sincronizados. Você deve ter notado que o uso de pastas Off-line é ideal para usuários de Notebooks, que precisam trabalhar e alterar arquivos quando não estão conectados à rede da empresa, como por exemplo em casa, em aeroportos ou em uma sala de reunião na empresa de um cliente.

Quando estiver trabalhando com arquivos off-line, você poderá exibi-los na sua pasta Arquivos off-line e excluí-los dela. Também poderá especificar quando e como os arquivos serão sincronizados ou então criptografar os arquivos off-line.

O primeiro passo é configurar os computadores dos clientes para que estes possam trabalhar com arquivos off-line. Por exemplo, você deverá fazer as configurações indicadas a seguir no notebook de um usuário que precise utilizar os arquivos off-line. Para detalhes práticos sobre estas configurações, consulte o Capítulo 6.

Em seguida você deve configurar os compartilhamentos que darão suporte ao uso de arquivos off-line. Estas configurações são feitas nas pastas compartilhadas nos servidores da rede. Para detalhes práticos sobre estas configurações, consulte o Capítulo 6. Ao habilitar o uso de pastas Off-line em um compartilhamento, você tem as seguintes opções:

Você pode utilizar uma das opções descritas a seguir:

- ◆ Apenas os arquivos e programas que os usuários especificarem estarão disponíveis off-line: Ao marcar esta opção (que é a padrão), somente serão armazenados on cache off-line, na estação de trabalho do cliente, aqueles arquivos e programas que o usuário especificamente definiu para estarem disponíveis off-line. Esta opção é a mais indicada para compartilhamentos acessados por muitos usuários, pois aí cada usuário marca para acesso off-line somente os arquivos que forem do seu interesse.
- ◆ Todos os arquivos e programas que os usuários abrirem do compartilhamento estarão automaticamente disponíveis off-line: Com esta opção, sempre que o usuário abrir um arquivo da pasta compartilhada, este arquivo será marcado para estar disponível para acesso off-line. Esta opção é ideal para compartilhamentos que contém arquivos que não são alterados com freqüência e podem estar disponíveis para acesso off-line.
- ◆ Os arquivos ou programas do compartilhamento não estarão disponíveis off-line: Ao marcar esta opção você desabilita o acesso off-line aos arquivos do compartilhamento.

- ◆ Por padrão os arquivos off-line são sincronizados durante o logon e também durante o logoff, para garantir que você sempre tenha uma cópia atualizada dos arquivos.
- ◆ Se você trabalhou desconectado da rede e alterou algum arquivo off-line e o arquivo não foi alterado na pasta compartilhada, o Windows atualiza a versão que está na pasta compartilhada a partir do arquivo atualizado no seu computador.
- ◆ Se você trabalhou desconectado da rede e não alterou nenhum arquivo off-line porém arquivos foram alterados na pasta compartilhada no servidor, o Windows atualiza a sua cópia off-line, para ficar sincronizada com as alterações que houve na pasta compartilhada.
- ◆ Se as duas versões de um arquivo, no servidor e na sua cópia local, foram alteradas, o Windows Server 2003 exibe uma caixa de diálogo perguntando se você deseja manter ambas as versões ou salvar uma em detrimento da outra.
- ◆ Se uma das duas versões for excluída e a outra não foi alterada, durante a sincronização, a outra cópia também será excluída. Por exemplo, se enquanto você esteve off-line, um arquivo foi excluído na pasta compartilhada e você não alterou este arquivo, durante a sincronização, a sua cópia off-line do arquivo também será excluída. Se você alterou o arquivo enquanto esteve off-line, uma caixa de diálogo será exibida, perguntando se você deseja salvar a versão alterada off-line, para a pasta compartilhada no servidor.
- ◆ Se você excluir a versão local e a versão no servidor tiver sido alterada, uma caixa de diálogo será exibida, perguntando se você deseja excluir a versão no servidor ou copiar a versão alterada para o cache local.
- ◆ Se novos arquivos forem adicionados no servidor, estes arquivos serão copiados para o seu cache local, caso você tenha configurado a pasta onde os arquivos foram adicionados, para acesso off-line.

**IMPORTANTE:** Quando você marca uma pasta para estar disponível off-line, o Windows disponibilizará todo o conteúdo da pasta (subpastas e arquivos) para estar disponível off-line. Se a pasta tiver subpastas, será exibida uma janela perguntando se você deseja tornar as subpastas também disponíveis off-line. Ao fazer esta configuração, o Windows faz uma cópia dos arquivos selecionados para o cache local do computador e passa a fazer a sincronização entre a cópia local e os arquivos na pasta compartilhada, de acordo com as seguintes regras:

## Instalação, Configuração e Administração de Impressoras.

Neste item do resumo, apresento alguns tópicos sobre impressão, os quais você não pode esquecer, de maneira alguma, para o exame.

### Termos utilizados pelo sistema de impressão do Windows Server 2003:

Talvez por excesso de criatividade, a equipe da Microsoft tem feito um belo trabalho para “confundir” o administrador do sistema de impressão, ao usar diferentes termos para fazer referência a impressora propriamente dita e ao driver da impressora (o software de controle da impressora instalado no servidor).

Para piorar um pouco mais, esta terminologia mudou novamente no Windows Server 2003, em relação a terminologia que era utilizada no Windows NT Server 4.0 e no Windows 2000 Server. Para ajudar o amigo leitor a se situar um pouco melhor neste “emaranhado” de termos, descrevo a terminologia oficial, utilizada nas diferentes versões do Windows, em relação à Impressoras.

No Windows NT Server 4.0 e no Windows 2000 Server são utilizados os seguintes termos:

- ◆ **print device (dispositivo de impressão):** Este termo refere-se a impressora propriamente dita, ao hardware. Ou seja, uma HP Deskjet 660 C, uma Rima Okidata 1100, uma Epson LX 300 e assim por diante.
- ◆ **printer (impressora):** faz referência ao driver da impressora, ao software instalado e que controla a impressora. É o elemento que aparece na pasta Printers (Impressoras).

No Windows Server 2003 são utilizados os seguintes termos:

- ◆ **printer (Impressora):** Este termo refere-se a impressora propriamente dita, ao hardware. Ou seja, uma HP Deskjet 660 C, uma Rima Okidata 1100, uma Epson LX 300 e assim por diante (que no Windows NT Server 4.0 e Windows 2000 Server era chamado de print device)
- ◆ **logical printer:** faz referência ao driver da impressora, ao software instalado e que controla a impressora. É o elemento que aparece na pasta Printers (Impressoras). Também aparece, em alguns pontos da documentação oficial, o termo printer driver (driver da impressora).

## Impressão através da Internet.

Uma novidade que foi introduzida no Windows 2000 Server e que foi melhorada no Windows Server 2003 é a impressão através da Internet (ou da Intranet da empresa). Você pode configurar uma impressora para que ele seja visível através da Internet ou da Intranet da empresa. Você pode definir quais usuários terão permissão para utilizar esta impressora, a exemplo do que acontece com qualquer tipo de impressora instalada no Windows Server 2003. A impressão via Internet é feita através do protocolo Internet Printing Protocol – IPP. O suporte ao protocolo IPP depende da impressora. Se a impressora não vier de fábrica com suporte a este protocolo, você deverá instalar o protocolo no Windows Server 2003 e também o IIS para que você possa administrar a impressora usando o Browser. No Capítulo 13 você aprenderá a instalar, utilizar e administrar o IIS 6.0.

As impressoras com suporte ao protocolo IPP, normalmente, vem com uma interface de administração via Browser. Ou seja, você conecta o Browser diretamente com o IP configurado para a impressora e é aberta uma página com uma série de comandos de administração da impressora. Normalmente é exigida uma senha para que possa ser feita a administração da impressora, para evitar que qualquer usuário que conheça o IP da impressora faça a conexão e altere as configurações da impressora.

Depois de instalada uma impressora e habilitada para o protocolo IPP, você pode conectar com a impressora, facilmente, usando o Internet Explorer 4.0 ou superior. Por exemplo, para exibir a lista de impressoras do domínio abc.com, basta utilizar o endereço a seguir:

<http://abc.com/printers>

Para fazer a conexão diretamente com uma impressora, cujo nome de compartilhamento seja las-col-01, no domínio abc.com, basta utilizar o endereço a seguir:

<http://abc.com/ las-col-01>

Será exibida uma lista de comandos da impressora. Basta clicar em Install e pronto, o driver da impressora será instalado e você poderá imprimir diretamente neste impressora. Para o usuário aparece com mais uma impressora (logical driver) na lista de impressoras instaladas. Quando o usuário envia uma impressão, o protocolo IPP é responsável por enviar os dados para a impressora de destino para que a impressão seja realizada.

## **Padronização de nomes e outros detalhes importantes para o uso de impressoras em rede.**

O administrador pode selecionar o nome de compartilhamento de cada impressora da rede, bem como definir os comentários, descrição e outras informações sobre cada impressora. Porém é aconselhável que sejam seguidas determinadas recomendações, as quais irão facilitar para o usuário a localização das impressoras através da rede e também as pesquisas no Active Directory. Com a definição de normas para as informações a serem cadastradas para cada impressora, o administrador facilita a vida do usuário, o qual pode fazer pesquisas pelo tipo de impressora (laser, jato de tinta, jato de cera, etc), pela localização, pelas características, pela velocidade e por outros detalhes que possam ser relevantes.

É também importante manter um padrão para a nomeação das impressoras, sempre tendo em mente que o objetivo desta padronização é fazer com que seja fácil para o usuário, localizar uma impressora com as características que ele precisa.

Cada impressora instalada e compartilhada em um servidor tem dois nomes. O primeiro nome é o nome da própria impressora, nome este que é exibido na janela Impressoras ou no Browser, quando o administrador está gerenciando impressoras através do Browser (conforme mostrarei no final deste capítulo). O nome da impressora pode ter até 220 caracteres de comprimento. O outro nome é o nome de compartilhamento. É o nome que é exibido na lista de recursos compartilhados quando o usuário acessa os recursos de um servidor usando o ícone Meus locais de rede ou usando o comando net view \\nome-do-servidor, para exibir a lista de recursos compartilhados em um servidor.

O nome de compartilhamento pode ter até 80 caracteres de comprimento. Porém é importante lembrar que clientes mais antigos, como o Windows 3.x ou MS-DOS, não reconhecem mais do que 8 caracteres como nome de compartilhamento. Somente clientes com o Windows 2000 Server, Windows XP ou Windows Server 2003 são capazes de reconhecer nomes de compartilhamento que contenham espaços. Por isso se você tem clientes baseados no Windows 95/98/Me ou no NT Workstations 4.0, evite utilizar nomes de compartilhamento com espaços.

A idéia básica é que o nome da impressora deve conter informações básicas, tais como o tipo da impressora, localização e indicação de uma característica principal, como nos exemplos a seguir:

- ◆ HP Laser Colorida – Fiscalização
- ◆ Cânon Laser Monocromática – Contabilidade
- ◆ HP Laser – Suporte A3 – Pesquisa

Estes nomes indicam a marca (poderíamos também ter incluído o modelo), uma característica principal (no último exemplo é o suporte a papel tamanho A3) e a localização da impressora.

Os nomes de compartilhamento também deve ser indicativos das características e da localização da impressora. Considere os exemplos a seguir:

- ◆ LasMonoContab
- ◆ LasColPesquisa
- ◆ CeraColRecepção
- ◆ LasColSalaPresidente

## **Atribuindo permissões de acesso para a impressora.**

Neste item mostrarei um exemplo prático de como definir permissões de acesso para uma impressora compartilhada. Também farei uma descrição detalhada dos diferentes níveis de permissão que podem ser definidos para o acesso a

uma impressora. As permissões podem ser atribuídas a usuários ou a grupos. A exemplo da recomendação que foi feita para o caso de pastas compartilhadas, para impressoras compartilhadas também é recomendado sempre definir as permissões para grupos, o que simplifica e facilita a administração destas permissões.

Assim como é possível atribuir permissões para uma pasta compartilhada, é possível definir permissões de acesso para uma impressora compartilhada. As permissões definem quais os usuários que podem utilizar a impressora e qual o nível de permissão de cada usuário. Ao definir permissões para um grupo, os membros do grupo herdam as permissões. Se o usuário pertencer a mais de um grupo, a sua permissão efetiva será a soma das permissões atribuídas a todos os grupos aos quais ele pertence. Negar uma permissão de impressão tem precedência sobre todas as demais permissões. Por exemplo, se o usuário pertence a cinco grupos, grupos estes que tem diferentes permissões de acesso a uma impressora compartilhada. Se ele for incluído em um sexto grupo, o qual tem negada a permissão de acesso à impressora, a permissão efetiva do usuário será acesso negado, ou seja, o negar que ele herdou do sexto grupo, tem precedência sobre todas as demais permissões que ele herdou dos demais grupos aos quais ele pertence.

Quando uma impressora é instalada em uma rede, são atribuídas permissões de impressão padrão, as quais permitem que todos os usuários imprimam e que grupos selecionados gerenciem a impressora, documentos enviados a elas ou ambos. Por padrão é definida a permissão Print (Imprimir) para o grupo Everyone (Todos); a permissão Print (Imprimir), Manage Documents (Gerenciar Documentos) e Manage Printers (Gerenciar Impressoras) para os grupo locais do domínio Administrators (Administradores), Server Operators (Operadores de Servidores) e Print Operators (Operadores de Impressão). Também é adicionada permissões totais para o usuário dono da impressora, que é o usuário que estava logado quando a impressora foi instalada. Como a impressora está disponível, por padrão, para todos os usuários na rede (permissão Imprimir para o grupo Todos), convém limitar o acesso de algumas pessoas atribuindo permissões de impressoras específicas. Por exemplo, você pode conceder a permissão Print (Imprimir) a todos os usuários não administrativos de um departamento e as permissões Print (Imprimir) e Manage Documents (Gerenciar documentos) somente para os gerentes. Desse modo, todos os usuários e gerentes poderão imprimir documentos, mas somente os gerentes poderão alterar o status de impressão de qualquer documento enviado à impressora. (gerenciar documentos).

O Windows fornece três níveis de permissões de segurança de impressão: Print (Imprimir), Manage Printers (Gerenciar impressoras) e Manage Documents (Gerenciar documentos). Quando várias permissões são atribuídas a um grupo de usuários, as permissões menos restritivas se aplicam, ou seja, a permissão efetiva do usuário é a soma das permissões atribuídas aos grupos aos quais ele pertence, mas as permissões atribuídas diretamente a sua conta. No entanto, se a opção Negar tiver sido atribuída, ela terá precedência sobre qualquer permissão, a exemplo do que acontece com as permissões de compartilhamento e com as permissões NTFS. Existem três níveis de permissão, conforme detalhado a seguir:

- ◆ **Print (Imprimir):** Permite ao usuário conectar-se à Impressora e imprimir documentos, pausar, reiniciar e continuar a impressão dos documentos por ele enviados para a impressora. Quando um usuário envia um documento para a impressora, o usuário torna-se o dono daquele documento, por isso que ele pode administrar os documentos por ele enviados. Esta permissão normalmente atribuída para aqueles usuários que simplesmente precisam enviar documentos para a impressora. Por padrão, quando uma nova impressora é instalada, a permissão Print (Imprimir) é atribuída ao grupo Everyone (Todos), conforme descrito anteriormente.
- ◆ **Manage Documents (Gerenciar documentos):** Tem todas as permissões atribuídas a permissão Print (Imprimir), mais Controlar a impressão de todos os documentos (enviados por qualquer usuário) e também pausar, reiniciar e continuar a impressão de qualquer documento enviado por qualquer usuário. Normalmente atribuída para aquele usuário que administra a impressora, resolvendo problemas de impressão, mas sem permissões para alterar propriedades e permissões da impressora. Quando a permissão Manage Documents (Gerenciar documentos) for atribuída a um usuário, ele não poderá acessar documentos existentes que estejam aguardando para serem impressos, na fila de impressão. A permissão se aplicará somente aos documentos enviados para a impressora depois que a permissão tiver sido atribuída ao usuário.

- ◆ **Manage Printers (Gerenciar impressoras):** Todas as permissões de Print (Imprimir) e Manage documents (Gerenciar documentos), mais permissões para cancelar a impressão de todos os documentos pendentes, compartilhar a impressora, alterar as propriedades da impressora, eliminar a impressora e alterar as permissões de impressão. Normalmente atribuída a um usuário que deve ter poderes completos na administração da impressora, inclusive podendo removê-la do sistema. Por padrão, os membros dos grupos Administrators (Administradores), Print Operators (Operadores de Cópia) e Server Operators (Operadores de Servidores) têm esta permissão.

É importante salientar, que as permissões para o uso da impressora tem efeito tanto localmente, quanto para o acesso através da rede. Além disso caso um usuário pertença a mais de um grupo que possui permissões para a impressora, a sua permissão efetiva é a soma das permissões. Também um permissão Negar tem prioridade sobre Permitir (sei que estou repetindo isso pela terceira vez, mas o objetivo é exatamente fazer com que o amigo leitor não esqueça destes detalhes). Por exemplo se o usuário jsilva pertence aos grupos Contabilidade e Marketing. O grupo Contabilidade possui permissão Print (Imprimir), já o grupo Marketing tem permissão Deny Print (Negar Imprimir), então a permissão efetiva do usuário jsilva será Deny Print (Negar Imprimir).

## O serviço Spooler de Impressão:

Podem ocorrer problemas mais sérios, onde o administrador não consegue eliminar os documentos da fila de impressão e a impressora continua imprimindo uma série de páginas com uns caracteres meio estranhos, ou seja, lixo. Ou pode ocorrer de os usuários estarem enviando os trabalhos de impressão, os trabalhos são colocados na fila de impressão mas não são impressos. Muitas vezes o Administrador acaba reinicializando o servidor para poder suspender as impressões com problema.

Quem controla toda a impressão no Windows Server 2003 é um Serviço chamado “Spooler”. Um serviço nada mais é do que um programa que inicializa, automaticamente, quando o Windows Server 2003 é inicializado. O serviço é inicializado e continua operando, sem a necessidade de que ao administrador faça o logon no servidor.

Para eliminar todos os documentos de uma fila de impressão quando a impressão está apresentando problemas maiores, os quais você não consegue solucionar simplesmente administrando a fila de impressão, a maneira mais simples é parar o serviço Spooler e inicializá-lo novamente. Ao fazer isso, todos os documentos que estão na fila de impressão, serão removidos, inclusive o documento que está atualmente sendo impresso.

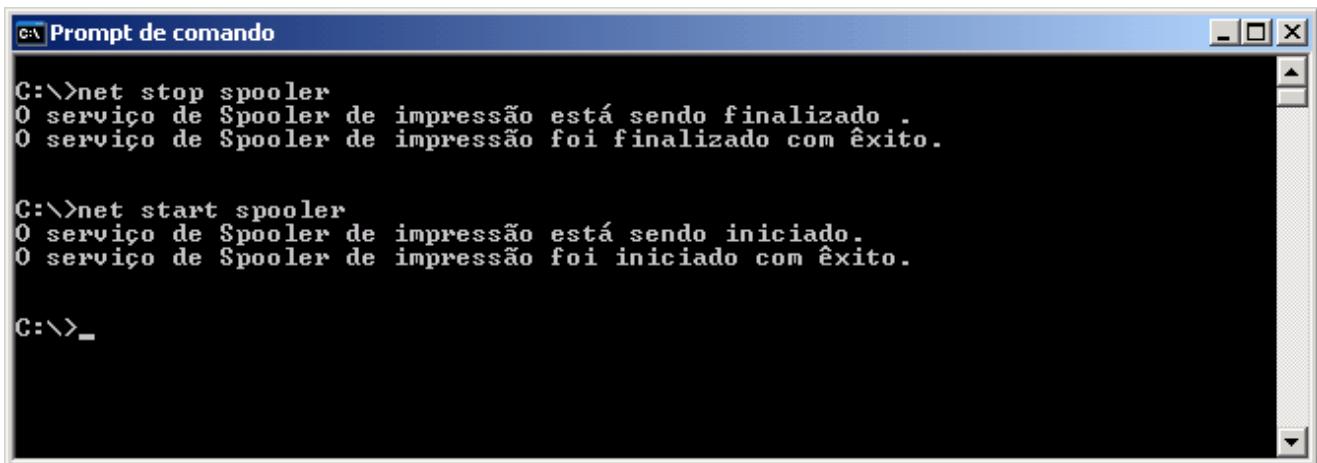
Para parar o serviço Spooler e inicializa-lo novamente.

1. Abra um Prompt de comando.
2. Para parar o serviço Spooler digite o seguinte comando:  
`net stop spooler`
3. Pressione Enter. O serviço Spooler será finalizado e todos os documentos serão removidos da fila de impressão.

**IMPORTANTE:** Um caso especial é o caso do usuário Administrador ou de qualquer usuário que pertença ao grupo Administradores. Mesmo que um usuário do grupo Administradores não possua nenhuma permissão de acesso à impressora, ele poderá ter acesso a guia segurança e atribuir permissões para si mesmo. Isso é feito para que os Administradores possam ter controle sobre todos os recursos da rede.

**IMPORTANTE:** Pode parecer que não existe diferença entre uma “Impressora de rede” e uma “Impressora conectada a outro computador”. Mas existe sim diferenças. Uma Impressora de rede é uma impressora que tem instalada uma placa de rede e é ligada diretamente na rede, através desta placa de rede, tendo inclusive sido configurada com um endereço IP. Uma impressora de rede não é ligada diretamente a nenhum servidor. Já uma impressora conectada a outro computador, é uma impressora ligada na porta paralela (ou em outra porta, como por exemplo Serial ou USB) de um servidor da rede. Esta impressora passa a estar acessível pela rede, quando ela é compartilhada.

4. Para reiniciar o serviço Spooler digite o seguinte comando:  
net start spooler
5. Pressione Enter. O serviço Spooler será reinicializado.
6. Na janela da Figura 14.43, mostro a execução dos dois comandos, onde o serviço Spooler foi “parado” e inicializado novamente:



```
C:\>net stop spooler
O serviço de Spooler de impressão está sendo finalizado .
O serviço de Spooler de impressão foi finalizado com êxito.

C:\>net start spooler
O serviço de Spooler de impressão está sendo iniciado.
O serviço de Spooler de impressão foi iniciado com êxito.

C:\>_
```

Figura 14.43 Parando e reinicializando o serviço Spooler.

7. Para sair do Prompt de comando, digite exit e tecle Enter.

## Configurando propriedades importantes e outras ações.

Existem algumas opções e propriedades das impressoras, que são bastante úteis. O administrador deve conhecer e saber configurar estas propriedades, bem como entender em que situações práticas devem ser utilizadas.

Uma das opções importantes é a disponibilidade. Por padrão, quando uma impressora é instalada, ela fica disponível 24 horas por dia, 7 dias por semana. O administrador pode limitar o tempo em que uma impressora fica disponível. Quando um documento é enviado durante um período em que a impressora está configurada para não estar disponível, o documento fica na fila de impressão e quando chegar o horário em que a impressora está configurada para voltar a estar disponível, o documento será impresso, sempre respeitando a ordem de chegada na fila de impressão e a prioridade de cada documento. Configurar o horário de disponibilidade, pode ser usado para evitar que documentos extensos sejam impressos fora do horário do expediente, sem que o administrador tome conhecimento.

Esta opção pode ser utilizada para fazer com que uma impressora, esteja disponível, em determinados horários do dia, somente para um determinado grupo. Por exemplo, imagine que você tem uma impressora Laser Colorida, a qual na parte da manhã, deve estar disponível apenas para o Grupo Gerentes. No restante do dia, a impressora deve estar disponível para todos. O que você faz? Muito simples, você instala esta impressora, duas vezes, no mesmo servidor. Na primeira instalação, você define que a impressora estará disponível durante todo o dia e

**DICA:** Quando uma impressora tem trabalhos em sua fila de impressão, um ícone com uma figura de uma impressora, é exibido ao lado da hora do sistema, bem no canto inferior direito do vídeo. Para abrir a janela que exibe a fila de impressão, basta dar um clique duplo neste ícone. Depois é só utilizar os comandos que você aprendeu no exemplo anterior, para Gerenciar os documentos da fila de impressão.

define permissão de acesso para o grupo Gerentes e Nega o acesso para os demais grupos. Você oriente os gerentes a utilizar esta impressora. A segunda instalação você compartilha com o grupo Todos, porém configura para estar disponível somente no horário da tarde. Com isso, a impressora, na prática, na parte da manhã, somente poderá ser acessada pelo grupo Gerentes. É isso.

## Diferentes prioridades para diferentes grupos.

Neste item descreverei quais os passos necessários para que o administrador possa definir diferentes prioridades, para diferentes grupos, no uso da mesma impressora. Esta é uma situação bastante comum. Imagine a situação descrita a seguir:

Uma nova impressora Laser, Colorida, de alta resolução e de alta velocidade (15 páginas por minuto) foi instalada no andar da direção. Neste andar, além dos executivos da empresa também trabalham as secretárias e uma equipe de estagiários que fazem uma série de trabalhos de apoio. Todos devem ter permissão para usar a nova impressora, a qual será instalada e compartilhada em um servidor Windows Server 2003 localizado no mesmo andar. Todos os executivos fazem parte do grupo Administração, todas as secretárias fazem parte do grupo Secretárias e todos os estagiários fazem parte do grupo Estagiários. Você, como administrador, foi solicitado para permitir que os grupos Administração, Secretárias e Estagiários tenham acesso a esta nova impressora, porém com diferentes prioridades. O grupo Administração deve ter prioridade Máxima e o grupo Secretárias deve ter uma prioridade menor do que o grupo Administração, porém maior do que o grupo Estagiários. Quais os passos que você deve executar, para implementar a configuração proposta?

Esta é uma questão bastante comum no dia-a-dia da administração de impressoras em uma rede, ou seja, permitir o uso de uma impressora, por diferentes grupos, com diferentes prioridades. Você não tem como definir, nas propriedades da impressora, diferentes prioridades para diferentes grupos. Quando você define uma determinada prioridade para uma impressora (logical printer) você está definindo esta mesma prioridade para todos os usuários que tem permissão de acesso à impressora. Para solucionar esta questão é preciso “apelar” para a criatividade do ser humano. Felizmente somos seres criativos, curiosos por natureza. A resolução deste problema é bastante simples (embora dê um pouco de trabalho manual) e passa pela execução dos seguintes passos:

1. Instale a impressora (instalar o driver da impressora) três vezes, porém com nomes diferentes. No exemplo da Figura 14.44, instalei a impressora HP Deskjet 660C três vezes, porém com nomes diferentes.

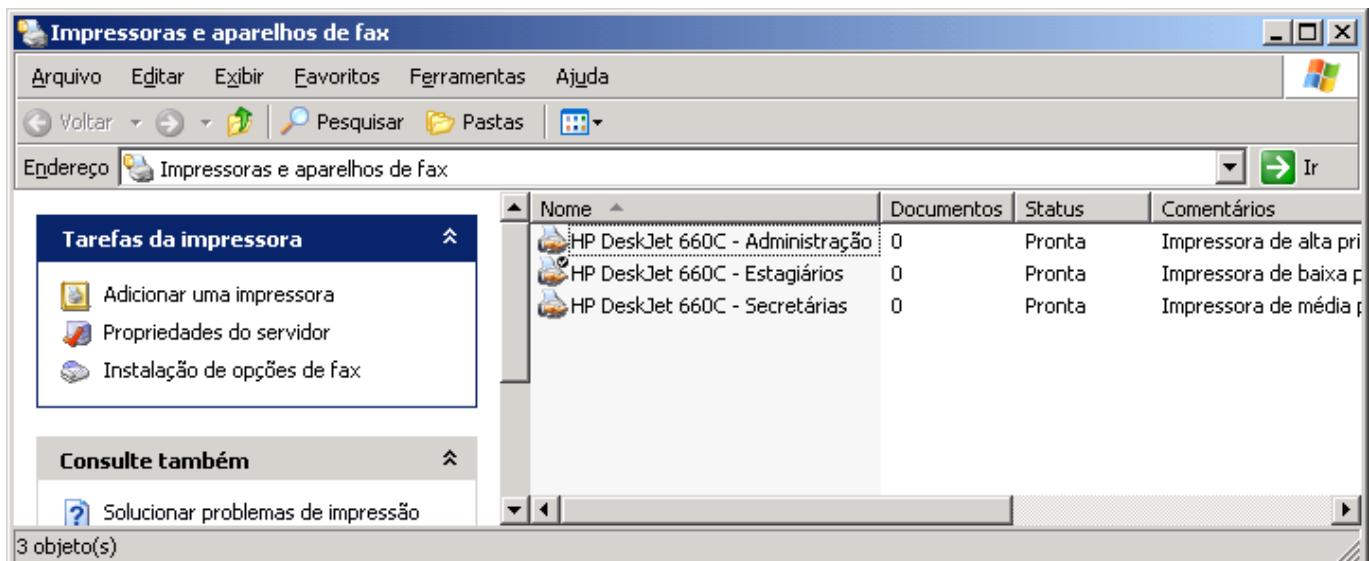


Figura 14.44 - Impressora instalada três vezes com nomes diferentes.

2. As três impressoras também foram compartilhadas com nomes de compartilhamento diferentes, conforme indicado a seguir:

| Grupo         | Nome da impressora              | Nome de compartilhamento |
|---------------|---------------------------------|--------------------------|
| Estagiários   | HP DeskJet 660C – Estagiários   | HP660Est                 |
| Secretárias   | HP Deskjet 660C – Secretárias   | HP660Sec                 |
| Administração | HP DeskJet 660C – Administração | HP660Adm                 |

3. A próxima etapa é definir diferentes propriedades para cada uma das instalações da impressora. Para definir a prioridade de uma instalação basta clicar com o botão direito do mouse na impressora a ser configurada. No menu de opções que é exibido clique em Propriedades. Clique na guia Avançado. No campo Prioridade, informe um valor entre 1 e 99. Quanto maior o valor, maior a prioridade da instalação no uso da fila de impressão. Na Figura 14.45 é exibido o campo para configuração da prioridade da impressora.

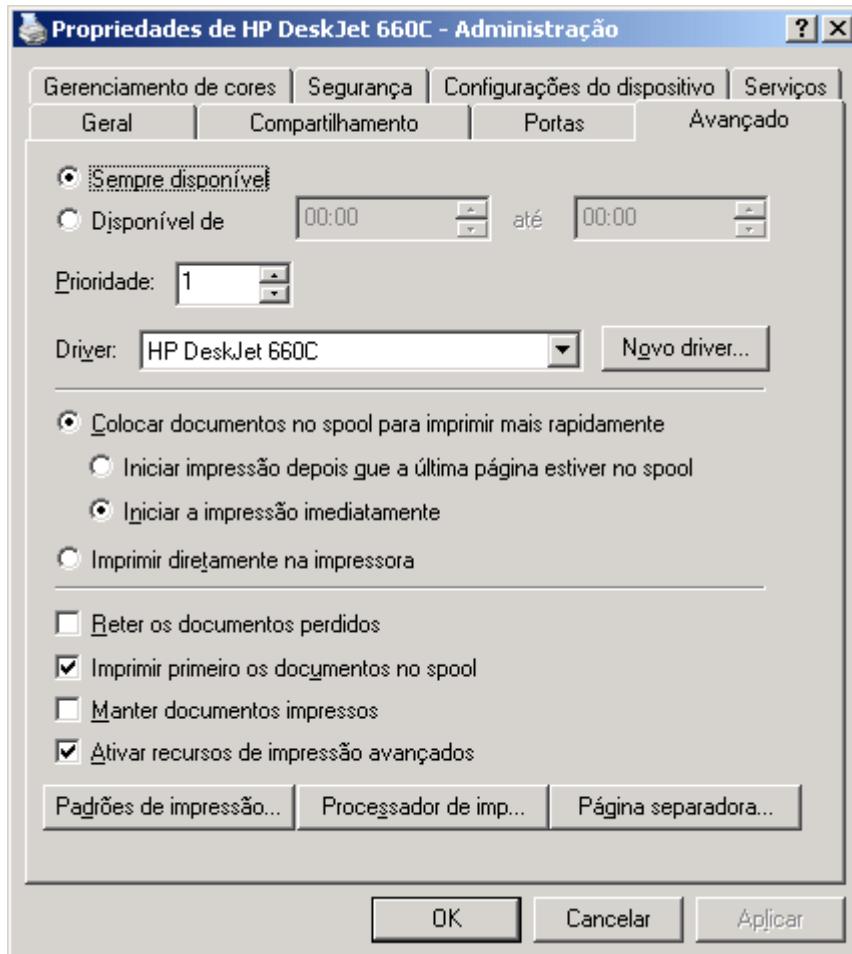


Figura 14.45 – Definindo a prioridade da impressora.

Basta definir a prioridade e clicar em OK. Defina as seguintes prioridades para cada uma das instalações:

| <b>Grupo</b>  | <b>Nome da impressora</b>       | <b>Nome de compartilhamento</b> | <b>Prioridade</b> |
|---------------|---------------------------------|---------------------------------|-------------------|
| Estagiários   | HP DeskJet 660C – Estagiário    | HP660Est                        | 10                |
| Secretárias   | HP Deskjet 660C – Secretárias   | HP660Sec                        | 50                |
| Administração | HP DeskJet 660C – Administração | HP660Adm                        | 99                |

4. Define permissões de acesso específicas em cada instalação, conforme indicado a seguir:

| <b>Grupo</b>  | <b>Nome da impressora</b>       | <b>Permissão para o grupo</b> |
|---------------|---------------------------------|-------------------------------|
| Estagiários   | HP DeskJet 660C – Estagiários   | Estagiários                   |
| Secretárias   | HP Deskjet 660C – Secretárias   | Secretárias                   |
| Administração | HP DeskJet 660C – Administração | Administração.                |

Com isso cada grupo somente poderá acessar a sua respectiva instalação, com o nível de prioridade adequado a cada grupo.

5. Agora configure para que cada usuário accesse o respectivo compartilhamento, conforme indicado a seguir:

| <b>Grupo</b>  | <b>Nome de compartilhamento</b> | <b>Prioridade</b> |
|---------------|---------------------------------|-------------------|
| Estagiários   | HP660Est                        | 10                |
| Secretárias   | HP660Sec                        | 50                |
| Administração | HP660Adm                        | 99                |

Pronto, agora cada usuário somente consegue acessar uma das instalações da impressora e de acordo com o nível de prioridade definido para o respectivo grupo.

Este é um exemplo simples, de uma solução que não existe pronta no Windows Server 2003, mas combinando o conhecimento sobre impressoras, com uma pitada de criatividade, o administrador consegue implementar uma solução para uma demanda real. É um erro esperar por soluções prontas para todas as demandas do mundo real, por que as demandas são muitas e variadas. O trabalho do administrador é utilizar os recursos disponíveis e a sua criatividade para implementar soluções para os problemas reais do dia-a-dia. Até porque, se o sistema operacional já apresentasse soluções prontas para todos os problemas reais, não seria necessária a figura do administrador, ou seja, o próprio sistema operacional tomaria conta de tudo. Bem, deixando a filosofia de lado, vamos a mais uma situação prática que pode ocorrer no caso de grandes volumes de impressão.

---

**NOTA:** Todos os passos para executar as ações práticas deste exemplo, tais como instalar uma impressora, compartilhar a impressora e definir permissões, foram descritos no Capítulo 7.

# Tudo o que você não pode esquecer sobre Backup e Restore

Este é um tópico que você deve conhecer, super bem. Principalmente a parte de tipos de backup e estratégias de Backup/Restore, com base nos tipos de backup que estão sendo utilizados. É fundamental que você conheça as características de cada tipo de backup e como cada tipo é utilizado, quando da necessidade do Restore dos dados. Vamos aos principais tópicos sobre backup e restore.

## Criar múltiplos agendamentos.

É possível criar múltiplos agendamentos para uma mesma tarefa de backup ou qualquer tarefa agendada. Podem existir situações em que uma determinada tarefa tenha que ser executada em diversos horários, os quais é impossível configurar em um único agendamento. Por exemplo, você pode ter que agendar uma tarefa de backup para rodar todos os dias, às 2:00 hs. da madrugada e nas segundas, quartas e sextas, além das duas da madrugada, também no horário do almoço, por exemplo, às 12:00 hs. Neste exemplo, você terá que criar dois agendamentos: Um com programação semanal, para todos os dias da semana, com execução para as 2:00 hs. da manhã. Outro com programação semanal, para execução às segundas, quartas e sextas-feiras às 12:00 hs.

---

**IMPORTANTE:** Volte e revise completamente o Capítulo 8. Este é um capítulo realmente importante e você deve dominar todos os conceitos apresentados neste capítulo.

---

## Estratégias de backup e restore.

Fazer o “Backup”, significa fazer uma ou mais cópias de segurança dos dados dos servidores e também da instalação do Windows Server 2003 das configurações do servidor (Backup do Estado do Sistema). Muitos usuários e até mesmo pequenas empresas simplesmente ignoram a necessidade de implementar uma política de Backup. Muitas vezes os usuários só se dão conta do problema quando é tarde demais, ou seja, quando houve uma perda de dados importantes. É o usuário que perdeu os documentos do Word e figuras da sua tese de mestrado, é a vídeo locadora que perdeu os dados de anos de locações, é o Dentista que perdeu as informações sobre as fichas dos pacientes, sobre quais pacientes deviam e assim por diante. Claro que na rede da sua empresa, a necessidade de backup é indiscutível. Perder dados significa sistemas fora do ar, perda de clientes, e assim por diante. Em resumo: grandes dores de cabeça e prejuízos. Fazer cópia de segurança é uma necessidade real, não temos como fugir deste fato. Além disso o custo é insignificante, isto mesmo: insignificante se compararmos com os prejuízos que podem ser causados pela perda de dados.

---

**IMPORTANTE:** Lembre-se deste detalhe, que em determinadas situações você terá que usar a opção de agendamento múltiplo. Esta opção é preferível ao invés da criação de tarefas separadas, uma para cada agendamento. Lembre-se disso.

---

**IMPORTANTE:** Conheça bem os tipos de backup, as diferenças entre os tipos e em que situações práticas cada tipo deve ser utilizado. Este é um dos tópicos fundamentais para o Exame 70-290.

---

Neste tópico apresentarei alguns detalhes sobre os tipos de backup existentes e sobre estratégias de backup que podem ser implementadas. Também darei algumas sugestões sobre os dispositivos de Backup que você pode utilizar caso nos servidores da rede da sua empresa.

---

**NOTA:** Neste tópico utilizarei a palavra Backup como sinônimo de Cópia de segurança, por ser este termo já conhecido e consagrado.

---

## Definindo o tipo de Backup a ser utilizado.

Dependendo da quantidade de dados e do tempo disponível para o backup, podem ser utilizadas diferentes estratégias de backup. As estratégias de backup são baseadas em um ou mais tipo de backup. Você pode ter estratégias bastante simples,

baseadas na cópia completa de todos os arquivos, até estratégias mais sofisticadas, baseadas na combinação entre diferentes tipos de backup. Vou, inicialmente apresentar os diferentes tipos de backup.

No Windows Server 2003 podemos utilizar os seguintes tipos de backup:

- ◆ **Normal (Normal):** Com este tipo de backup todos os arquivos são copiados, toda vez que o backup for executado, independentemente de os arquivos terem sido alterados ou não. O arquivo é marcado como tendo sido feito o backup, ou seja, o atributo de arquivamento é desmarcado. Cada arquivo tem um atributo que pode ser marcado ou desmarcado. Este atributo serve para informar ao Windows Server 2003 se o arquivo foi ou não modificado desde o último backup normal. A principal vantagem do backup normal é a facilidade para fazer a restauração dos arquivos, quando necessário. Com o backup do tipo normal, para restaurar os dados, você precisa apenas do último backup normal que foi criado. A desvantagem é o tamanho do backup e o tempo para execução. Em cada execução do backup, todos os arquivos e pastas serão copiados, independentemente de terem sido alterados ou não, desde que o último backup normal foi efetuado. Geralmente, o backup normal é executado quando você cria um conjunto de backup pela primeira vez. Nos backup subsequentes é comum a utilização de outros tipos de backup, conforme descreverei logo a seguir.
- ◆ **Copy (Cópia):** Backup que copia todos os arquivos selecionados, mas não marca cada arquivo como tendo sofrido backup (em outras palavras, o atributo de arquivamento não é desmarcado). É idêntico ao backup Normal, com a diferença de que os arquivos não são marcados como tendo sido copiados. A cópia é útil caso você queira fazer backup de arquivos entre os backups normal e incremental (veja descrição do backup incremental logo a seguir), pois ela não afeta essas outras operações de backup ou quando você precisa fazer uma cópia extra dos dados para enviar para um filial da empresa ou para manter a cópia armazenada em um local seguro.
- ◆ **Incremental (Incremental):** Este tipo de backup copia somente os arquivos criados ou alterados desde o último backup normal ou desde o último backup incremental. Os arquivos copiados para o backup são marcados (ou seja, o atributo de arquivamento é desmarcado). Se você utilizar uma combinação de backups normais e incrementais para restaurar os seus dados, será preciso ter o último backup normal e todos os conjuntos de backups incrementais feitos após este backup normal e restaurá-los na seqüência correta. A grande vantagem do backup incremental é que ele reduz o tempo necessário para a execução do backup, pois somente é feita a cópia dos arquivos que foram criados ou modificados desde o último backup normal ou incremental. A grande desvantagem é que para fazer a restauração é necessário o último backup normal e todos os backups incrementais subsequentes. Os backups incrementais devem ser restaurados na seqüência cronológica em que foram criados. Além disso, se um dos backups incrementais apresentar problemas, não será possível restaurar os dados até o ponto do último backup incremental.
- ◆ **Differential (Diferencial):** Este tipo de backup faz a cópia de todos os arquivos criados ou alterados desde o último backup normal ou incremental. Os arquivos que sofreram backup não são marcados como tal (ou seja, o atributo de arquivamento não é desmarcado). Com isso cada backup diferencial, copia todos os arquivos que foram modificados desde o último backup normal (ou incremental, caso algum tenha sido feito). Se você estiver executando uma combinação de backups normal e diferencial, a restauração de arquivos e pastas exigirá que você tenha o último backup normal e o último backup diferencial. A restauração é mais rápida do que quando você usa backups incrementais, pois somente é necessário o último backup diferencial, porém cada backup diferencial passa a ser maior, pois contém a cópia de todos os arquivos criados ou modificados desde o último backup normal ou incremental.
- ◆ **Daily (Diário):** Este tipo de backup copia todos os arquivos selecionados que forem alterados no dia de execução do backup diário. Os arquivos que sofreram backup não são marcados como tal (ou seja, o atributo de arquivamento não é desmarcado). Não é um tipo muito utilizado. Pode ser utilizado em conjunto com backups do tipo normal e incremental.

O tipo ou tipos de backup que estão sendo utilizados, definem as estratégias de restauração (restore) que serão utilizadas, em caso de perda dos dados originais. A estratégia a ser utilizada depende do volume de dados e do valor dos dados a serem protegidos. Por exemplo, para um usuário doméstico que não tem um grande volume de dados, pode ser suficiente uma estratégia de backup normal todos os dias. Já para os servidores com dados de missão crítica da sua empresa, toda proteção adicional é bem vinda.

Porém você tem que estar atentos a alguns detalhes importantes. Por exemplo, não adianta você fazer o backup dos arquivos, no mesmo disco rígido onde estão gravados os arquivos originais (pois você pode fazer o backup em fita, em disco rígido e em vários outros tipos de mídia suportados pelo Windows Server 2003). Neste caso se o disco rígido “pifar”, ou seja, for danificado e não puder ser recuperado, você perderá os arquivos e também o backup. Para usuários domésticos e pequenas empresas, os quais não tem grandes volumes de dados, a utilização de um segundo disco rígido, no qual serão feitas as cópias de backup, pode ser uma estratégia eficiente. A possibilidade de os dois discos rígidos apresentarem problemas ao mesmo tempo é muito pequena. Já para empresas de grande porte o ideal é ter um conjunto de mídias separado dos servidores e dedicado ao backup. Pode ser uma biblioteca de fitas de backup ou um espaço de armazenamento em disco rígido.

Uma opção muito utilizada é o uso de drives de fita como por exemplo do tipo DLT4 de 40 ou 80 GB (já existem padrões de maior capacidade e maior velocidade do que a DLT4). Além disso após feito o backup, as fitas devem ser armazenadas em local separado da sala dos servidores. Se armazenarmos as fitas, na mesma sala onde estão os dados, corremos o risco de perder os dados e também o backup, em caso de incêndio, inundação ou outro desastre. Claro que uma estratégia deste tipo requer investimentos consideráveis, mas com certeza são investimentos plenamente justificados pela importância dos dados para a empresa.

Outro detalhe importante é que as cópias de segurança devem ser sempre testadas. Após fazer o backup, você deve fazer um teste de restauração para verificar se a cópia realmente foi feita com sucesso. Nada pior do que descobrir, na hora do restore, que o backup não foi feito adequadamente. Existe até um piada bastante conhecida entre os administradores de rede e de bancos de dados: “O backup sempre funciona, o que não funciona, às vezes, é o restore”. Ou seja, o objetivo não é o sucesso do backup e sim que, quando necessário, seja possível fazer o restore dos dados a partir do backup. Para garantir que isto seja possível, é preciso que exista uma definição de uma política para testes periódicos do backup.

## Exemplos de estratégias de backup/restore.

Agora irei analisar algumas estratégias de backup/restore, baseadas nos diferentes tipos de backup, descritos anteriormente.

Exemplo 1: É feito diariamente um backup Normal, as 23:00 da pasta Meus documentos. Na sexta-feira, as 14:30 ocorre um problema e a pasta Meus documentos é excluída.

Nesta situação você tem que restaurar o backup Normal feito na quinta-feira. Todos as alterações feitas na sexta-feira serão perdidas, ou seja, os arquivos voltarão a situação que estavam na quinta-feira, quando foi feito o último backup normal.

Exemplo 2: No domingo é feito um backup normal. De segunda a sábado é feito um backup Incremental à noite. Na quinta-feira, as 16:00 ocorre um problema e os dados são excluídos.

Você deve restaurar o backup normal do domingo, o backup incremental da segunda-feira, o backup incremental da terça-feira e o backup incremental da quarta-feira, nesta sequência. Todas as alterações feitas na quinta-feira serão perdidas.

---

**IMPORTANTE:** Entenda bem as diferentes políticas de Backup/Restore, com base nos diferentes tipos de Backup, disponíveis no Windows Server 2003.

---

Exemplo 3: É feito um backup normal aos domingos. De segunda a sábado são feitos os seguintes backups incrementais: 2:00, 9:00, 12:00, 15:00, 17:00 e 21:00 hs. Na quarta-feira, às 14:30 ocorre um problema e os dados tem que ser restaurados do backup.

Você deve restaurar o backup normal do domingo e todos os backups incrementais, em ordem cronológica, até o backup incremental da quarta-feira às 12:00, que é o último backup incremental feito antes da ocorrência do problema às 14:30. Todas as alterações feitas entre às 12:00 hs. e às 14:30 serão perdidas. Observe que com a utilização de backups incrementais durante o dia, você reduz a possibilidade de perda de dados, porém a restauração torna-se mais trabalhosa, pois existe um grande número de backups incrementais a serem restaurados. Uma estratégia deste tipo é normalmente utilizada por grandes empresas, que trabalham com grande volumes de dados e não podem nem sequer pensar em perda de dados.

Exemplo 4: É feito um backup normal aos domingos. De segunda a sábado são feitos backups incrementais às 2:00 da madrugada. Toda quarta-feira é feito um backup diferencial às 3:00 da madrugada. Na sexta-feira, às 14:30 ocorre um problema e os dados tem que ser restaurados do backup.

Você deve restaurar o backup normal do domingo, o backup diferencial da quarta-feira e o backup incremental da quinta-feira, nesta seqüência. Todas as alterações feitas na sexta-feira serão perdidas.

Observe que a utilização de um backup diferencial, em conjunto com os backups incrementais, reduziu o número de backups a serem restaurados. Neste caso somente foi necessário restaurar o último backup normal, o último diferencial e os backups incrementais posteriores. Esta é a estratégia mais complexa, mas que ao mesmo tempo otimiza o tempo de backup e o tempo de restauração. É especialmente indicada para grandes volumes de dados, onde o tempo de parada é um fator crítico.

---

**IMPORTANTE:** Quando você usa uma estratégia de um Backup normal semanal e backups diferenciais diários, é possível restaurar os dados utilizando somente duas fitas de backup. A do Backup normal e o último backup Diferencial. Esta estratégia tem a vantagem de utilizar apenas duas fitas para a restauração, mas tem a desvantagem de fazer o backup de um volume maior de dados, todos os dias, uma vez que o backup Diferencial faz o backup de todos os arquivos que foram alterados, desde o último backup Normal, independentemente de quantos backups Diferenciais tenham sido feitos neste meio tempo.

---

## Dados do estado do sistema:

Com o utilitário de backup, você pode fazer backup dos seguintes componentes de sistema e restaurá-los para fazer backup do estado do sistema. estado do sistema. O estado do sistema é

uma coleção de dados específicos do sistema mantidos pelo sistema operacional dos quais deve ser feito backup como um todo. Não é um backup de todo o sistema. Os dados do estado do sistema incluem o Registro, o banco de dados de registro de classe COM+, os arquivos do sistema, os arquivos de inicialização e os arquivos sob a Proteção de arquivos do Windows. Para servidores, os dados do estado do sistema também incluem o banco de dados dos serviços de certificados (se o servidor for um servidor de certificados). Se o servidor for um controlador de domínio, os dados do estado do sistema incluirão o banco de dados do Active Directory e o diretório SYSVOL. Se o servidor for um nó em um cluster, ele incluirá as informações do banco de dados do cluster. A metabase IIS estará incluída se o IIS estiver instalado.

Na Tabela a seguir, descrevo os componentes do Estado do sistema e quando eles são incluídos no Backup do Estado do sistema.

| Componente  | Quando este componente é incluído no estado do sistema? |
|---|---|
| Registro  | Sempre  |
| Banco de dados de registro de classe COM+                       | Sempre  |
| Arquivos de inicialização, incluindo os arquivos de sistema     | Sempre  |
| Banco de dados de serviços de certificados                      | Se for um servidor de serviços de certificados          |
| Serviço de diretório Active Directory                           | Se for um controlador de domínio                        |
| Pasta SYSVOL  | Somente se for um controlador de domínio                |
| Informações do serviço de cluster                               | Se estiver dentro de um cluster                         |
| Metadiretório IIS (Metabase)                                    | Se estiver instalado o IIS                              |
| Arquivos de sistema que estão na Proteção de arquivo do Windows | Sempre  |

O utilitário de backup se refere a esses componentes de sistema como os dados do estado do sistema. O total de componentes do sistema que constituem os dados do estado do sistema depende do sistema operacional e da configuração do computador.

## O log do backup

O Windows Server 2003 mantém um registro das operações de backup e restauração. Este registro pode ser utilizado pelo Administrador para verificar se as tarefas de backup estão sendo executadas com sucesso.

## Fazendo o Backup e o Restore do Active Directory..

A base de dados do Active Directory contém informações das quais depende todo o funcionamento da rede. Apenas para citar as mais conhecidas, é no Active Directory que ficam armazenadas informações sobre todas as contas de usuários do domínio, sobre todos os grupos, sobre relações de confiança, sobre contas de computadores, sobre OUs, enfim, informações das quais depende o funcionamento da rede.

É claro que o fato de existir vários DCs em um domínio, cada DC com uma cópia completa do Active Directory, reduz os riscos de perdas destas informações. Em caso de catástrofe, tal como a perda do HD onde está instalado o Windows Server 2003, sempre será possível reinstalar o Windows Server 2003 e, através da replicação, obter uma cópia integral do Active Directory a partir de outros DCs

**IMPORTANTE:** Preste atenção quando houver referência a fazer backup da Registry, do Active Directory ou de outras informações que fazem parte do estado do sistema. Se houver este tipo de referência em alguma questão, você deve considerar a hipótese de que a questão refere-se a necessidade de fazer o Backup do estado do sistema.

**IMPORTANTE:** Vou repetir para você não esquecer. Pode haver situações práticas onde você terá que executar um Backup com periodicidades diferentes, como por exemplo: todos os dias às 2:00 da madrugada e somente no Sábado às 8:00 da manhã. Nestas situações você tem que criar múltiplos agendamentos. Um agendamento para fazer o backup de segunda a sexta, às 2:00 da madrugada e um

do domínio. O Backup é útil para agilizar este processo, uma vez que, dependendo do volume de dados do Active Directory, pode demorar algum tempo (até mesmo alguns dias), até que o DC consiga receber uma cópia completa do Active Directory, através da replicação de outros DCs do domínio.

Neste tópico você aprenderá sobre como realizar o Backup do Active Directory, sobre conceitos tais como Backup com e sem autoridade e como fazer o restore do Active Directory. O backup do Active Directory é feito com o utilitário de backup, discutido nos tópicos anteriores. O restore é feito com este mesmo utilitário em conjunto com o comando Ntdsutil, o qual pode ser utilizado para fazer um restore seletivo, apenas de partes específicas do Active Directory.

## Backup do Active Directory:

Com o utilitário de Backup do Windows Server 2003 você pode fazer o backup do Active Directory com o DC estando ligado e na rede e pode ser feito o backup somente do Active Directory ou do Active Directory juntamente com os dados do servidor. O backup pode ser feito em disco ou em qualquer mídia suportada pelo utilitário de backup do Windows Server 2003.

Um detalhe importante a ser observado é que quando é feito o backup do Active Directory, o único tipo de backup suportado é o backup normal. Ou seja, não podem ser utilizados os backups do tipo incremental, diferencial, cópia ou diário, quando é feito o backup do Active Directory. O backup normal faz uma cópia de todo o conteúdo do servidor. Na hora de fazer o restore basta ter disponível o último backup normal que foi efetuado.

Ao fazer o backup do Active Directory, o utilitário de backup do Windows Server 2003 também realiza o backup de todas as informações das quais depende o funcionamento do Active Directory, tais como registros de componentes e DLLs, registry do sistema e assim por diante. Este conjunto de informações é conhecido como estado do sistema. As informações que compõem o estado do sistema são as seguintes:

- ◆ Arquivos de inicialização
- ◆ Registros de componentes COM+
- ◆ Pasta SYSVOL
- ◆ Base de dados do Certificados Digitais (se instalado o Certificate Services)
- ◆ Base do DNS (se instalado)
- ◆ Informações de cluster (se o servidor participa de um cluster)
- ◆ Active Directory

## Restore do Active Directory

Existem duas abordagens diferentes que podem ser utilizadas para restaurar os dados do Active Directory, em caso de falhas que provoquem perda ou corrupção dos dados do Active Directory:

**segundo agendamento para fazer o backup, aos Sábados, às 8:00 da manhã. Para criar múltiplos agendamentos você usa a opção "Mostrar vários agendamentos", a qual já foi descrita no tópico sobre Tarefas agendadas, no início do capítulo 8.**

**IMPORTANTE:** O log de Backup é gravado como parte da Profile da conta com a qual está sendo executado o Backup. Por exemplo, se o usuário jsilva estiver em sua estação de trabalho – micro01, fazendo o backup de pastas de um Servidor server02, o log de backup será gravado na Profile do usuário jsilva, no computador micro01. O log de Backup é um arquivo de texto, o qual pode ser visualizado com o Bloco de Notas. O Log de Backup não faz parte do Log do Sistema e, portanto, não é visualizado usando o console Visualizador de Eventos.

**IMPORTANTE:** Lembre-se de que para fazer um Backup do Certificate Services você precisa fazer o Backup do Estado do Sistema.

1. Reinstalar o Windows Server 2003, promovê-lo a DC e deixar que o mecanismo padrão de replicação entre DCs se encarregue de restaurar a base completa do Active Directory. Esta opção pode ser inviável para escritórios ligados à rede da empresa através de links de WAN de baixa velocidade, principalmente se a base de dados do Active Directory for grande (1 GB ou mais).

Ou

2. Fazer o restore a partir de um backup efetuado previamente. No caso do restore a partir do backup, existem dois métodos diferentes de restore que podem ser executados, conforme descrito a seguir:
  - 2.1. Nonauthoritative (Sem autoridade): Este é um restore normal. Os dados serão restaurados a partir do backup. Uma vez concluída a restauração, o DC passará a receber as atualizações dos outros DCs. Sempre que um outro DC contiver informações mais atualizadas do que as que foram restauradas do backup, estas informações serão replicadas para o DC onde foi feito o restore. É o processo padrão de restore.
  - 2.2. Authoritative (Com autoridade): Esta é uma situação especial. Para ilustrar este tipo de restore, vou utilizar uma situação prática onde ele seria necessário. Imagine que, por engano, um administrador excluiu uma OU e todo o seu conteúdo. Esta informação (ou seja a informação de que a OU foi excluída) será replicada para os demais DCs do domínio. O efeito prático é que esta OU será excluída em todos os DCs do domínio. Você pode imaginar o seguinte: Basta restaurar a OU a partir do Backup e pronto, as informações da OU serão replicadas para os demais DCs e os dados serão recuperados. Nada disso. Ao restaurar a OU usando o método normal (Nonauthoritative), os dados da OU serão considerados mais antigos do que a informação de que não existe a OU. Quando houver a replicação entre o DC onde foi feito o restore da OU e qualquer outro DC do domínio, o que irá acontecer é que a OU será novamente excluída e não enviada para os outros DCs, pois a informação de que ela foi excluída, é mais recente do que os dados da OU. Com o uso de um restore Authoritative é possível recuperar esta informação. Nesta situação, o administrador utiliza o comando Ntdsutil para fazer um restore Authoritative (Com autoridade) da OU que foi excluída. Fazer um restore authoritative significa alterar o número de série dos dados que estão sendo restaurados, de tal maneira que eles sejam considerados as atualizações mais recentes. Com isso, quando houver a replicação entre o DC onde foi feito o restore e os demais DCs, os dados da OU serão considerados mais recentes e a OU e todo o seu conteúdo será replicada para os demais DCs. O efeito prático é que os dados da OU serão recuperados.

Quem tem permissão para fazer o backup do estado do sistema?

Para fazer o backup ou um restore do tipo nonauthoritative, o usuário deve ter as seguintes permissões e direitos de usuário:

- ◆ Para fazer o backup do estado do sistema, o usuário deve pertencer ao grupo Backup Operators (Oper. de cópia) ou ao grupo Local do domínio Administrators (Administradores).
- ◆ Para fazer o restore do estado do sistema, o usuário deve pertencer ao grupo Local do domínio Administrators (Administradores).

A base de dados do Active Directory é composta dos seguintes arquivos, localizados na pasta %windir%\ntds (a não ser que você tenha especificado um caminho diferente quando o servidor foi promovido a DC), onde %windir% refere-se a pasta onde o Windows Server 2003 está instalado:

- ◆ **Ntds.dit:** Este é o banco de dados do Active Directory.
- ◆ **Ebb.chk:** O arquivo de checkpoint, utilizado pelo mecanismo de banco de dados do Active Directory.
- ◆ **Ebb\*.log:** Arquivos onde são registrados os logs de transações do banco de dados do Active Directory. A cada 10 MB é iniciado um novo arquivo de log.

- ◆ Res1.log e Res2.log: Log de transações, reservado.

Fazer o backup do Active Directory, significa fazer o backup do Estado do Sistema, conforme descrito no exemplo prático logo a seguir.

## Fazendo o restore do Active Directory.

Conforme descrito anteriormente existem dois métodos para fazer o restore do Active Directory. O primeiro é reinstalar o Windows Server 2003, usar o comando depromo para instalar o Active Directory e deixar que o processo de replicação entre os DCs do domínio se encarregue de sincronizar o novo DC com os demais DCs do domínio. Com este método o Active Directory é restaurado e sincronizado com as últimas alterações do domínio. Outro método é restaurar o Active Directory a partir de um backup. Este método restaura o Active Directory até a situação do momento em que foi feito o backup. Alterações que foram efetuadas após o backup, serão recebidas a partir dos outros DCs, através do processo de replicação. Observe que com este segundo método, somente serão replicadas as alterações que foram efetuadas após o backup.

Ao fazer o restore a partir do backup você também tem a disposição diferentes métodos. Um dos métodos é conhecido como nonauthoritative (sem autoridade). Este é o método que será utilizado normalmente. O restore é feito a partir de um backup feito previamente. O restore é feito utilizando o utilitário de backup do Windows Server 2003. Por exemplo, imagine que houve um problema com o disco rígido onde estava instalado o Windows Server 2003, em um DC do domínio. Neste caso você pode substituir o HD, reinstalar o Windows Server 2003 e depois restaurar o backup do estado do sistema. Com isso o Active Directory também será restaurado. As alterações que foram efetuadas após o backup, serão repassadas para o DC através do mecanismo de replicação. Observe que este método tem a vantagem de reduzir a quantidade de tráfego gerado na WAN, em relação ao método que restaura toda a base de dados usando replicação. Neste método, grande parte da base de dados do Active Directory é restaurada a partir do backup. Somente as alterações efetuadas após o backup ter sido feito é que serão replicadas.

Conforme descrito anteriormente, outro método de fazer o restore é o restore authoritative (com autoridade), na qual você marca uma parte do Active Directory para ser restaurada com autoridade, o que significa que esta informação será considerada como sendo a mais atualizada e será replicada para os demais DCs. Para fazer um backup authoritative, o administrador tem que utilizar o comando Ntdsutil.

## Efetuando um restore nonauthoritative, usando o utilitário de backup.

Para fazer o restore do Active Directory, você precisa reinicializar o DC em um modo especial, conhecido como Directory Services Restore Mode. Ou seja, o restore não é feito no modo normal, com o DC inicializado normalmente. É preciso reinicializar o servidor e entrar no modo especial Directory Services Restore Mode.

Para colocar o servidor no modo especial Directory Services Restore Mode, siga os passos indicados a seguir:

1. Reinicialize o DC.

**IMPORTANTE:** Você não pode fazer o backup do Estado do Sistema remotamente através da rede. Ou seja, para fazer o backup do Estado do Sistema de um servidor, por exemplo o servidor SRV01, você tem que estar logado localmente neste servidor ou o script que faz o backup tem que estar agendado para execução no servidor SRV01. Os dados do backup podem ser gravados em um volume do próprio servidor SRV01 ou em um drive de rede ou fita de backup, mas a tarefa que executa o backup tem que ser executada no próprio servidor.

2. Ao ser reinicializado, ainda no modo caractere, logo após terminar a contagem da memória RAM do servidor, pressione repetidamente a tecla de Função F8, até que seja exibido o menu de inicialização avançado (sobre o qual falei no Capítulo 12).
3. Neste menu selecione a opção Directory Services Restore Mode (Domain controllers only) e pressione Enter.
4. O DC será reinicializado no modo de restauração do Active Directory. Neste modo o Active Directory não é inicializado e, portanto, você não poderá usar as contas do Active Directory para fazer o logon. Mas se não posso usar as contas do Active Directory para fazer o logon, que contas vou utilizar? A conta local de administrador que foi definida quando o servidor ainda era um Member server. Use esta conta e a respectiva senha para fazer o logon.
5. Pronto, o DC está no modo de restauração do Active Directory. Agora é só utilizar o utilitário de Backup, para restaurar os dados do Active Directory, conforme exemplo prático apresentado no Capítulo 8.

## Terminal Services (Serviços de Terminal):

Outro tópico que é bastante cobrado no exame é sobre o Terminal Services. Você deve conhecer detalhes sobre a utilização, configuração e permissões de acesso, os quais descrevo a seguir.

### Introdução

O Terminal Services foi criado para ser uma ferramenta que facilite a administração dos servidores com o Windows 2000 Server e também com o Windows Server 2003, mas também para ser uma ferramenta de compartilhamento de aplicações, conforme descreverei neste capítulo.

A primeira versão do que hoje é a tecnologia do Terminal Services foi introduzida com o Windows NT Server 4.0, em uma versão separada do NT 4.0, conhecida como: Terminal Server Edition. A partir do Windows 2000 Server e também no Windows Server 2003, o Terminal Services (a partir do Windows 2000 os serviços deixaram de ter a nomenclatura Server para ter a nomenclatura Services) faz parte do próprio sistema operacional.

O Terminal Services trabalha em um modelo Cliente/Servidor, onde o serviço fica instalado em servidores com o Windows Server 2003 ou Windows 2000 Services e diferentes clientes podem se conectar ao servidor. Existe também uma versão reduzida do Terminal Services que é disponibilizada com o Windows XP. Esta versão permite apenas um único usuário conectado ao Windows XP, no recurso conhecido como Desktop Remoto.

### Como funciona o Terminal Services.

A idéia básica do Terminal Services é bastante simples. Usando um software cliente, como por exemplo o Terminal Services Client no Windows 2000 Server ou o Remote Desktop no Windows Server 2003, você pode se conectar a um servidor no qual está rodando o Terminal Services. A se conectar ao servidor, você recebe uma tela de logon, conforme exemplo da Figura 14.46, onde estou fazendo a conexão usando o cliente Remote Desktop em um computador com o Windows Server 2003, para me conectar a um servidor com o Windows 2000 Server, onde está instalado o Terminal Services.

---

**NOTA:** Para detalhes sobre a configuração e utilização do Desktop Remoto no Windows XP, consulte o Capítulo 17 do livro: "Windows XP Home & Professional Para Usuários e Administradores", 820 páginas, Axel Books.

---

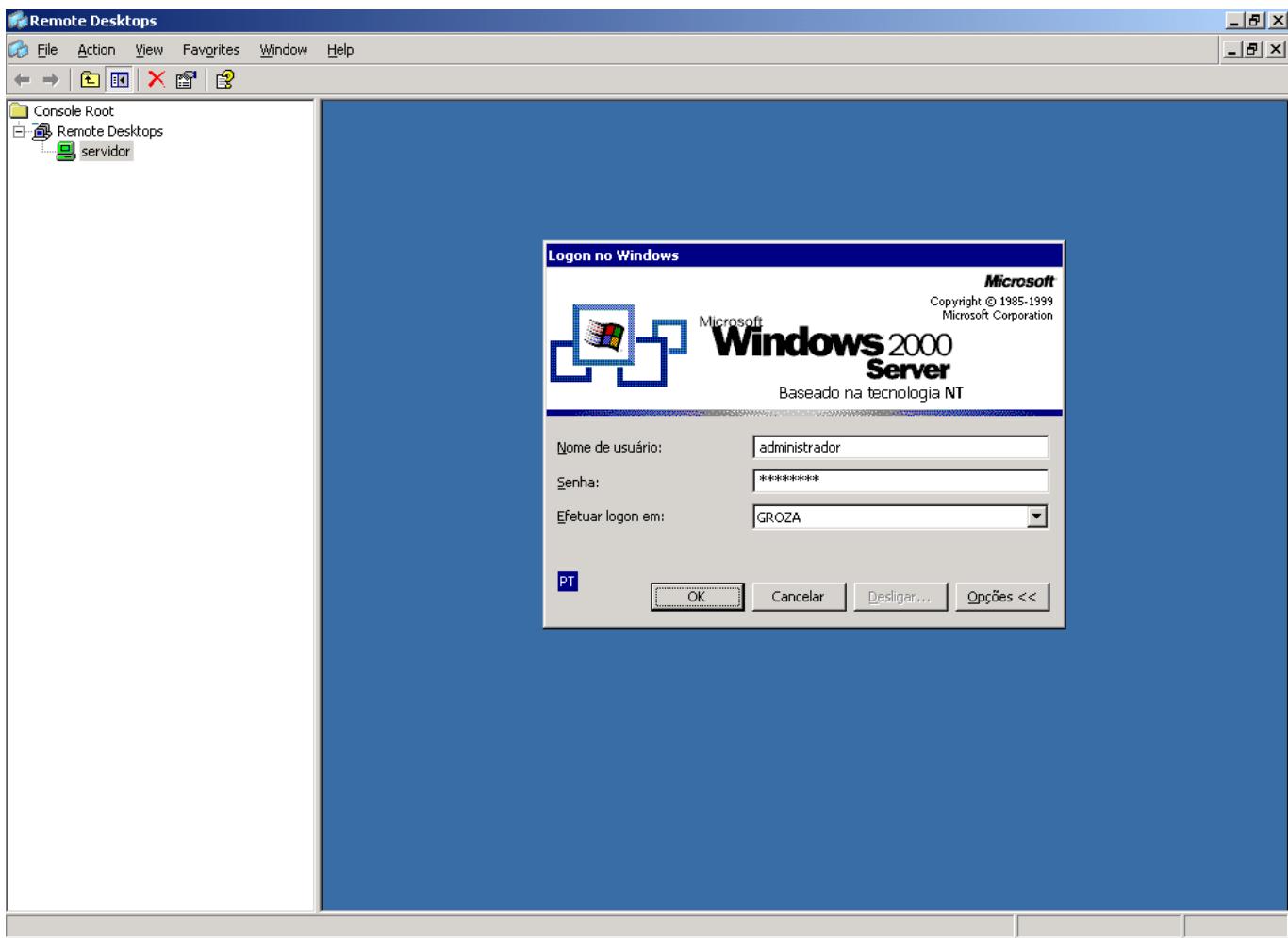


Figura 14.46 A tela de logon ao se conectar com o Terminal Services.

O usuário fornece as informações de logon e clica em OK e pronto. A conexão com o Terminal Services é efetuada e o console (a área de trabalho) do servidor é carregada no computador do cliente, conforme indicado na Figura 14.47. Ou seja, é como se você estivesse localmente conectado e tivesse feito o logon diretamente no servidor de destino, onde Terminal Services está instalado. Na prática é muito parecido com o que acontece quando você usa o comando telnet para fazer uma conexão com um servidor UNIX ou Linux, só que com o Terminal Services o console é gráfico.

Uma vez feita a conexão, é como se você tivesse localmente logado no servidor remoto. Exatamente a mesma área de trabalho é carregada, com botão Iniciar, barra de tarefas e tudo mais. Observe que com o Terminal Services o administrador pode se conectar a qualquer servidor da rede (desde que o servidor tenha o Terminal Services instalado) e administrá-lo como se estivesse localmente logado. Por exemplo, o administrador, da matriz da empresa em São Paulo, pode se conectar, via Terminal Services, com um servidor da filial no Rio de Janeiro e trabalhar como se estivesse “sentado” na frente do servidor no Rio de Janeiro.

A tecnologia do Terminal Services oferece eficientes mecanismos de compactação e cache de telas, transmitindo somente o que muda de uma tela para outra, o que permite que o acesso via Terminal Services tenha desempenho bastante satisfatório, mesmo para conexões remotas, feitas via links de WAN de baixa velocidade.

O cliente envia para o servidor, através da rede, apenas os toques de teclado e as ações de mouse e recebe apenas as atualizações de tela. Este mecanismo de funcionamento, juntamente com a possibilidade de compactação dos dados que são transmitidos e do cache de telas no cliente, faz com que o Terminal Services gere uma quantidade reduzida de

tráfego na rede e por isso possa trabalhar com desempenho aceitável, mesmo através de links de WAN de baixa velocidade.

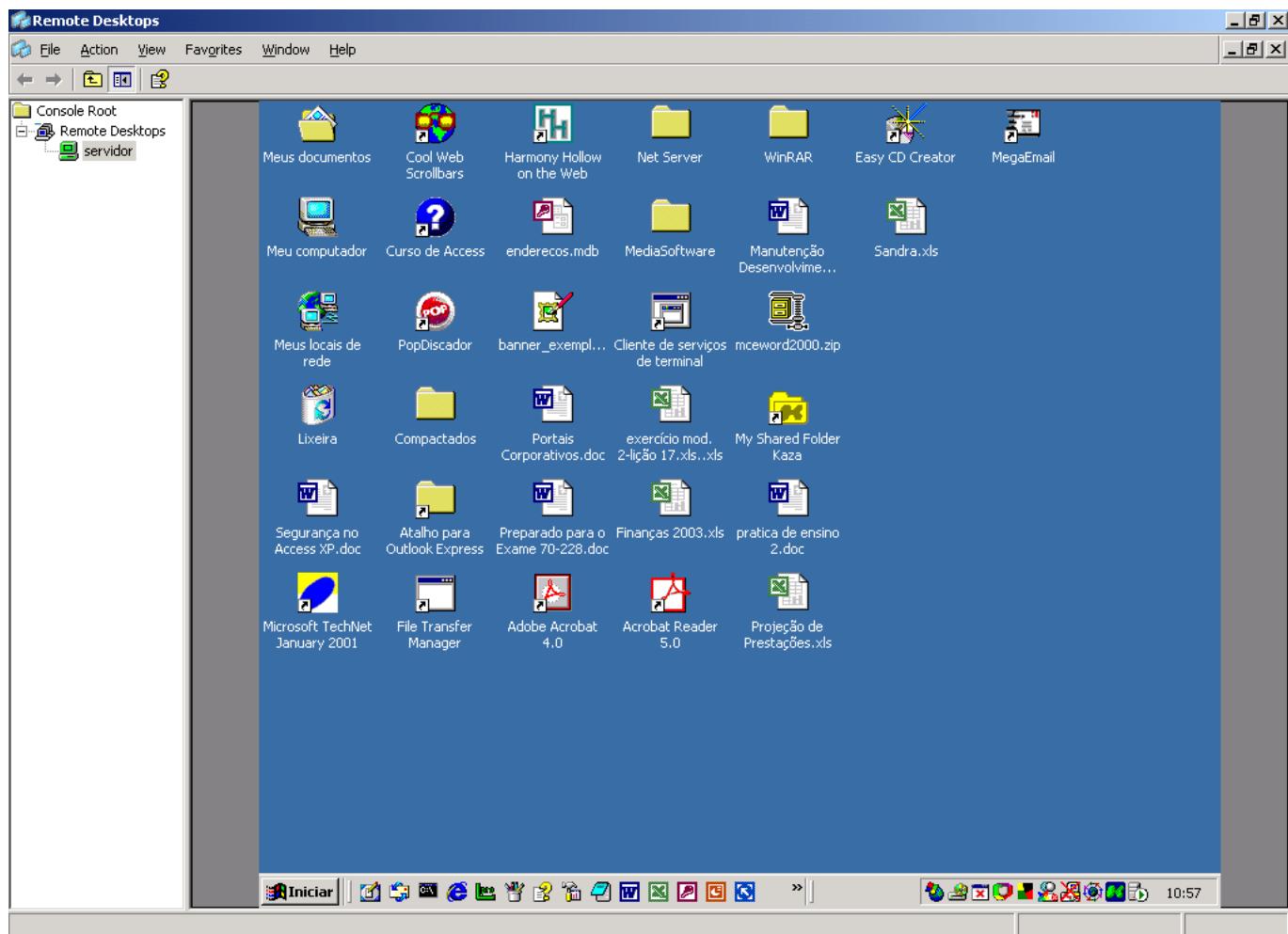


Figura 14.47 A área de trabalho do servidor, carregada via Terminal Services.

O Terminal Services pode ser utilizado em dois modos diferentes:

- ◆ **Modo de Administração Remota:** Neste modo o Terminal Services é utilizado pelos administradores da rede, para se conectar remotamente aos servidores da rede e executar tarefas administrativas remotamente, como se estivessem localmente logados nos respectivos servidores. Para utilizar o Terminal Services neste modo, basta instalar o serviço nos servidores que deverão ser administrados remotamente e instalar o cliente em sua estação de trabalho (Remote Desktop no Windows XP e no Windows Server 2003 ou o Terminal Services Cliente no Windows 2000). Ao instalar o Terminal Services no modo de Administração Remota, este é instalado com licença para até duas conexões simultâneas. Você não precisa adquirir nenhuma licença adicional e não tem prazo de validade para estas licenças.
- ◆ **Modo de Compartilhamento de Aplicações:** Neste modo, o Terminal Services é utilizado para o compartilhamento de aplicações. Por exemplo, você pode querer instalar o Terminal Services no modo de Compartilhamento de Aplicações, para instalar o Microsoft Office no servidor. Desta maneira, os clientes poderão se conectar, até mesmo usando estações de trabalho mais antigas, como por exemplo um 486, apenas com um cliente de acesso ao Terminal Services instalado. O cliente faz a conexão e tem acesso à área de

trabalho do servidor, na qual ele pode usar os aplicativos instalados no servidor, tais como o Word, Excel, Access e PowerPoint, ou quaisquer outros aplicativos instalados para o modo de Compartilhamento de Aplicações. O cliente pode usar os programas no servidor e gravar os dados em sua pasta home (home folder) na rede ou em disquete. A grande vantagem deste procedimento, é que o cliente poderá se conectar ao Terminal Services, usando qualquer computador da rede, no qual exista um cliente de conexão com o Terminal Services. Ao se conectar, usando qualquer um dos computadores da rede, ele receberá sempre a mesma área de trabalho (com os mesmos ícones e configurações) e terá acesso aos seus arquivos de dados. Quando um cliente faz uma conexão com o Terminal Services e faz alguma alteração no ambiente de trabalho, como por exemplo, adicionar um atalho à Área de trabalho, esta alteração é mantida e estará disponível na próxima conexão que o usuário fizer. Com isso é possível manter o ambiente do usuário e este ambiente “acompanha-o” em qualquer computador no qual ele fizer a conexão com o Terminal Services, porque na verdade todas as configurações estão no servidor. Para utilizar o Terminal Services neste modo, você deve adquirir uma licença de conexão para cada usuário que irá utilizar o Terminal Services no modo de Compartilhamento de Aplicações. Mais adiante falarei um pouco mais sobre o licenciamento neste modo.

O uso do Terminal Services traz inúmeras vantagens, dentre as quais podemos destacar as seguintes:

1. O administrador pode se conectar a qualquer servidor da rede, com o Terminal Services instalado e administrar este servidor como se estivesse localmente logado.
2. Com o uso do Terminal Services no modo de compartilhamento de aplicações, você pode criar um ambiente mais seguro e padronizado, onde os usuários acessam suas aplicações diretamente do servidor e gravam seus dados na rede.
3. Com o uso do Terminal Services no modo de compartilhamento de aplicações, fica mais fácil para instalar aplicações e mantê-las atualizadas, uma vez que a instalação e futuras atualizações precisam ser feitas apenas no servidor e não em cada estação de trabalho individualmente.
4. Com o uso do Terminal Services no modo de compartilhamento de aplicações, você pode utilizar clientes de menor capacidade de processamento, os quais não seriam mais aproveitados no modelo tradicional, onde o Windows e todos os aplicativos são instalados na estação de trabalho do cliente.
5. O cliente pode rodar, inclusive, em outros sistemas operacionais. Por exemplo, existem programas clientes para o Terminal Services, fornecido por terceiros, para se conectar através de uma estação de trabalho com o UNIX, Linux, Macintosh e assim por diante. Ou seja, pode haver um cliente UNIX na rede, conectado ao Terminal Services e utilizando o Word.
6. É possível também criar um modelo “misto” de estação de trabalho, na qual o cliente tem o Windows instalado e alguns programas de uso específico, instalados localmente. Já programas de uso geral na empresa, tais como o Word, Excel, Email, etc, o cliente acessa via Terminal Services. Com isso é possível manter um ambiente padronizado e de fácil manutenção para as aplicações utilizadas por todos na empresa, ao mesmo tempo que permite que cada usuário tenha acesso a aplicações específicas, relacionadas com o seu trabalho diário.
7. Redução do tráfego de WAN: Por exemplo, vamos imaginar uma empresa com o servidor de email na sede da empresa e os clientes das filiais com suas caixas de correio neste servidor de email. No modelo tradicional, cada cliente teria o software de email instalado em sua estação de trabalho e acessaria o servidor de email da matriz, através do link de WAN. Neste modelo, todas as mensagens e demais informações são transmitidas do servidor de email para o cliente e de volta para o servidor de email, através do link de WAN. Quem já tentou utilizar um cliente de email como o Lotus Notes, para acessar um servidor que está do outro lado de um link de WAN de 64 ou 128 Kbps, sabe o quanto é penosa esta operação. São minutos para abrir uma única mensagem. Já com o Terminal Services, o cliente abriria o programa de email diretamente no servidor, no mesmo servidor onde está o

servidor de email. Com isso, só é transmitido através do link de WAN, os toques de teclado e mouse do cliente e as atualizações de tela do servidor para o cliente. Além de uma considerável redução no tráfego de WAN, o acesso ao email e demais aplicações fica muito mais rápido.

Para cada usuário que se conecta via Terminal Services é criada uma sessão completamente isolada das demais sessões. Ou seja, se um programa apresentar problemas e travar a sessão de um dos usuários conectados, as demais sessões continuarão funcionando normalmente e não serão afetadas. O Windows Server 2003 também grava informações sobre o ambiente de trabalho de cada usuário quando ele se conecta via Terminal Services. Ou seja, o conceito de Profiles, visto no Capítulo 4 é válido também para conexões via Terminal Services.

Outra área onde o Terminal Services pode ser utilizado com grandes vantagens é para oferecer acesso a usuários remotos, tais como vendedores que trabalham usando um Notebook para acessar a rede da empresa ou funcionários que trabalham em casa mas precisam ter acesso aos recursos da rede da empresa. Estes usuários podem fazer a conexão à rede da empresa usando uma linha discada e ter acesso aos aplicativos que precisam via Terminal Services. Este meio de acesso é bem mais eficiente e rápido do que o acesso através de programas clientes instalados no próprio Notebook e através de drives de redes mapeados, uma vez que neste modo é como se o usuário estivesse diretamente conectado ao servidor da empresa, sendo transmitido através da conexão discada, somente os toques de teclado e mouse do usuário e as atualizações de tela do servidor. Muito mais rápido do que fazer a conexão e depois usar um programa cliente, instalado no próprio Notebook, para fazer conexão com os aplicativos e dados da empresa. Neste segundo modelo, toda a informação e os dados são transmitidos através da conexão discada, o que gera um grande tráfego e tempos de respostas bem mais altos do que com o uso do Terminal Services.

## Algumas considerações importantes sobre o Terminal Services:

Por padrão, somente os membros do grupo Administrators (Administradores) têm permissão para conectar-se remotamente ao Terminal Services no modo de compartilhamento de aplicação. Para permitir que outros usuários possam fazer essa conexão remotamente, você deve adicionar as contas dos usuários que farão a conexão, ao grupo Remote Desktop Users (Usuários da área de trabalho remota), grupo este já descrito anteriormente.

**IMPORTANTES:** Após a instalação no modo de Compartilhamento de aplicações, o terminal services funcionará por 120 dias e depois passará a recusar conexões. Durante este período você deve adquirir as licenças necessárias junto à Microsoft e configurá-las utilizando o Terminal Server Licensing. Não esqueça deste detalhe para os exames de Certificação do MCSE 2003. Seria uma boa questão.

**IMPORTANTES:** Quando o usuário conecta com o Terminal Services ele está utilizando recursos tais como memória RAM e processador, do Servidor. Por isso, se você pretende utilizar o Terminal Services no modo de Compartilhamento de Aplicações, é importante fazer um planejamento cuidadoso da quantidade de recursos de hardware, necessária no servidor. Mais adiante apresentarei mais detalhes sobre a quantidade média de recursos de hardware necessária para cada cliente.

**IMPORTANTES:** Ao adicionar usuários, com permissão para fazer o acesso remoto, na verdade, você adiciona estes usuários, como membros do grupo: Usuários da área de trabalho remota. Ou seja, na prática, para dar permissão a uma conta de usuário, para fazer a conexão remota, basta incluir a referida conta, como membro do grupo Usuários da área de trabalho remota. Na Figura 14.48, mostro que a lista de membros do grupo Usuários da área de trabalho remota. Não esqueça deste detalhe. Se algum usuário tentar fazer a conexão remota e receber uma mensagem de que a sua conta não tem permissão de logon remotamente, basta incluir a referida conta no grupo Usuários da área de trabalho remota, para que este usuário passe a ter permissão de se conectar, remotamente.

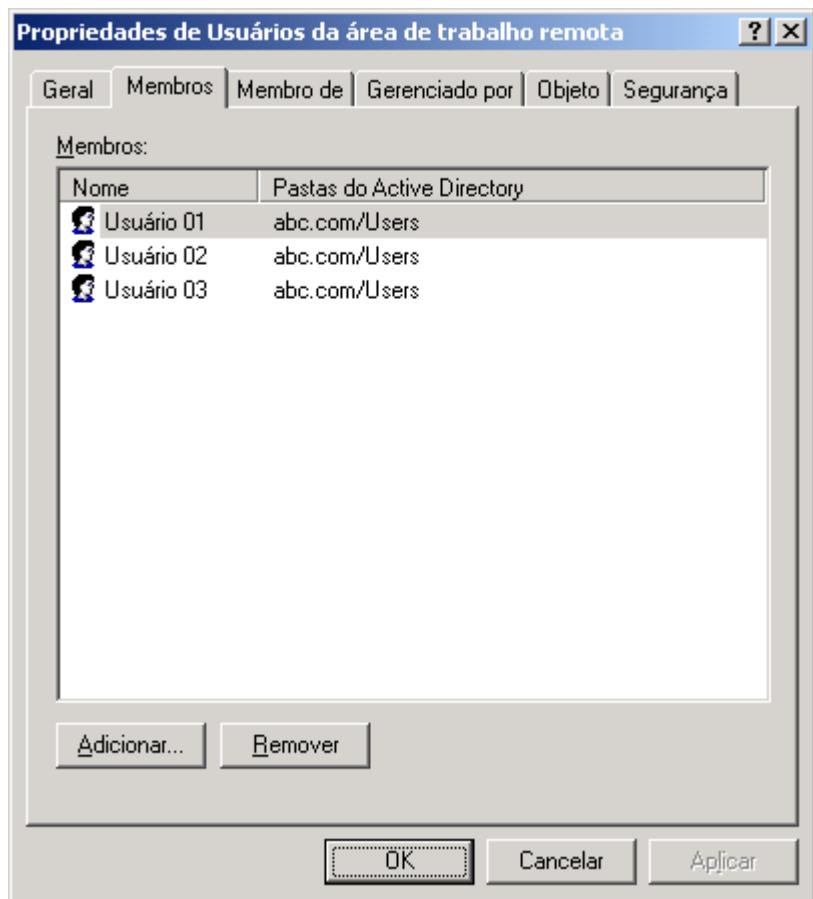


Figura 14.48 Membros do grupo Usuários da área de trabalho remota.

O Terminal Server requer licenças para que os clientes possam fazer o logon no modo de Compartilhamento de aplicações. Qualquer cliente que tente fazer o logon no Terminal Services, deve ser capaz de receber uma licença de acesso válida, a qual é disponibilizada pelo Licenciamento do Terminal Server. Sem receber a licença, não será permitido o logon do cliente.

O licenciamento do terminal services é “separado” do licenciamento do Windows Server 2003. Conforme comentado no Capítulo 1, sobre instalação do Windows Server 2003, devem ser adquiridas as chamadas CAL – Cliente Access License, para que clientes da rede possam se conectar aos servidores com o Windows Server 2003. Já para o Terminal Server é outro tipo de licença, ou seja, o fato de ter licenças para conectar com o Windows Server 2003, não implica que estas licenças também sejam válidas para o Terminal Server no modo de compartilhamento de aplicações. Licenças específicas, para acessar o Terminal Server no modo de compartilhamento de aplicações, devem ser ativadas.

Após ter comprado as licenças de acesso via Terminal Server, junto à Microsoft, você deve utiliar o console Licenciamento do Terminal Server para configurá-las. As informações sobre o número total de licenças disponíveis, o número de licenças em uso e o número de licenças ainda livres para serem utilizadas por novas conexões, são armazenadas no Licenciamento do Terminal Server. Quando um cliente tenta fazer uma conexão com o Terminal Server, este entra em contato com o Licensiamento do Terminal Server, para verificar se existem licenças disponíveis, ou melhor, se existe, pelo menos, uma licença disponível para o novo cliente que está tentando se conectar.

Um único Servidor de licenciamento do Terminal Server, pode ser utilizado por vários servidores com o Terminal Server em modo de compartilhamento de aplicação.

Após ter instalado o Licenciamento do Terminal Server você deve ativá-lo e instalar as licenças de acesso que foram adquiridas junto à Microsoft. Isso é feito através do uso do Assistente para ativação das licenças do Terminal Server

## Administração do Terminal Services.

Uma vez que você instalou e colocou o Terminal Services para funcionar, é hora de conhecer as ferramentas de administração e as opções de configuração disponíveis. Existem, basicamente, três consoles para administração do Terminal Services:

- ◆ **Gerenciador dos serviços de terminal:** Esta ferramenta é utilizada para monitorar e controlar as conexões com o Terminal Services. Com esta ferramenta você pode exibir todas as conexões estabelecidas com o Terminal Services.
- ◆ **Configuração dos serviços de terminal:** Esta ferramenta é executada no servidor onde o Terminal Server está instalado. É utilizada para configurar uma série de propriedades do Terminal Server, conforme você aprenderá logo em seguida.
- ◆ **Licenciamento do Terminal Server:** Esta ferramenta, já utilizada anteriormente, é utilizada para ativar o Terminal Server e para configurar o número de licenças de acesso disponíveis.

## Configurações do Terminal Services:

A maioria das configurações disponíveis são feitas através da opção Conexões, do console Configuração dos serviços de terminal.. Clique na opção Conexões. No painel da direita será exibida a opção RDP-Tcp. Clique com o botão direito do mouse nesta opção. No menu de opções que é exibido, clique em Propriedades. Será aberta a janela de propriedades, na qual você pode definir uma série de propriedades que serão aplicadas às conexões do Terminal Server. Por padrão, a guia Geral vem selecionada.

A guia Sessão da janela de Propriedades RDP-Tcp: Nesta guia são exibidas as opções indicadas na Figura 14.49.

Nesta guia estão disponíveis as seguintes opções de configuração (as quais você deve conhecer, detalhadamente, para o exame):

- ◆ **Primeira opção - Ignorar configurações do usuário:** Especifica se serão substituídas as configurações definidas por padrão na conta do usuário (Guia Terminal Services). Ao marcar esta opção, serão habilitadas as listas: Finalizar uma seção desconectada, Limite de sessão ativa e Limite de sessão ociosa.

Na lista Finalizar uma seção desconectada, você pode digitar ou selecionar o tempo máximo que uma sessão desconectada permanecerá no servidor. Quando o tempo limite é alcançado, a sessão desconectada será encerrada. Quando uma sessão é encerrada, ela é excluída permanentemente do servidor. Selecione Nunca

**NOTA:** Após a instalação do Terminal Server no modo de compartilhamento de aplicações, será possível utilizá-lo, sem a compra das licenças de acesso, durante um período de 120 dias. Terminado este período, os clientes não conseguirão mais se conectar, enquanto não forem ativadas e configuradas as licenças de acesso. Estou repetindo este tópico, várias vezes, propositadamente.

**NOTA:** Para uma descrição completa, de todas as opções de todas as Guias da janela de Propriedades da conexão RDP-Tcp, consulte o Capítulo 16. A seguir descrevo apenas as opções mais importantes, diretamente relacionadas com tópicos do Exame 70-290.

**IMPORTANTE:** Para o exame, você deve conhecer bem as opções de configuração da opção RDP-Tcp.

**IMPORTANTE:** Saiba que é possível sobreescriver as configurações definidas nas propriedades da conta do usuário, em relação ao Terminal Server. Também é importante que você conheça bem, as opções da guia Sessões. Estes são tópicos importantes para o Exame 70-290. Na janela de propriedades da conta do usuário, está disponível a guia Perfil de serviços de terminal. Estas configurações podem ser sobreescritas, pelas configurações definidas na guia Sessões, das propriedades do RDP-Tcp.

para permitir que as sessões desconectadas permaneçam no servidor indefinidamente. Você pode selecionar o espaço de tempo ou digitar o número de minutos, horas ou dias na caixa. Especifique as unidades de tempo usando m para minutos, h para horas e d para dias. O tempo máximo que pode ser especificado é de 49 dias e 17 horas. Não é uma boa prática permitir que sessões desconectadas permaneçam por muito tempo no servidor, antes de serem finalizadas, pois isso faz com que sejam ocupados recursos (memória e processador), do servidor. Pode haver situações onde o tempo de resposta do servidor fica extremamente elevado, devido a um grande número de sessões desconectadas, que continuam ocupando recursos do servidor. Nestas situações, a solução indicada é diminuir o tempo para que uma seção desconectada seja finalizada.

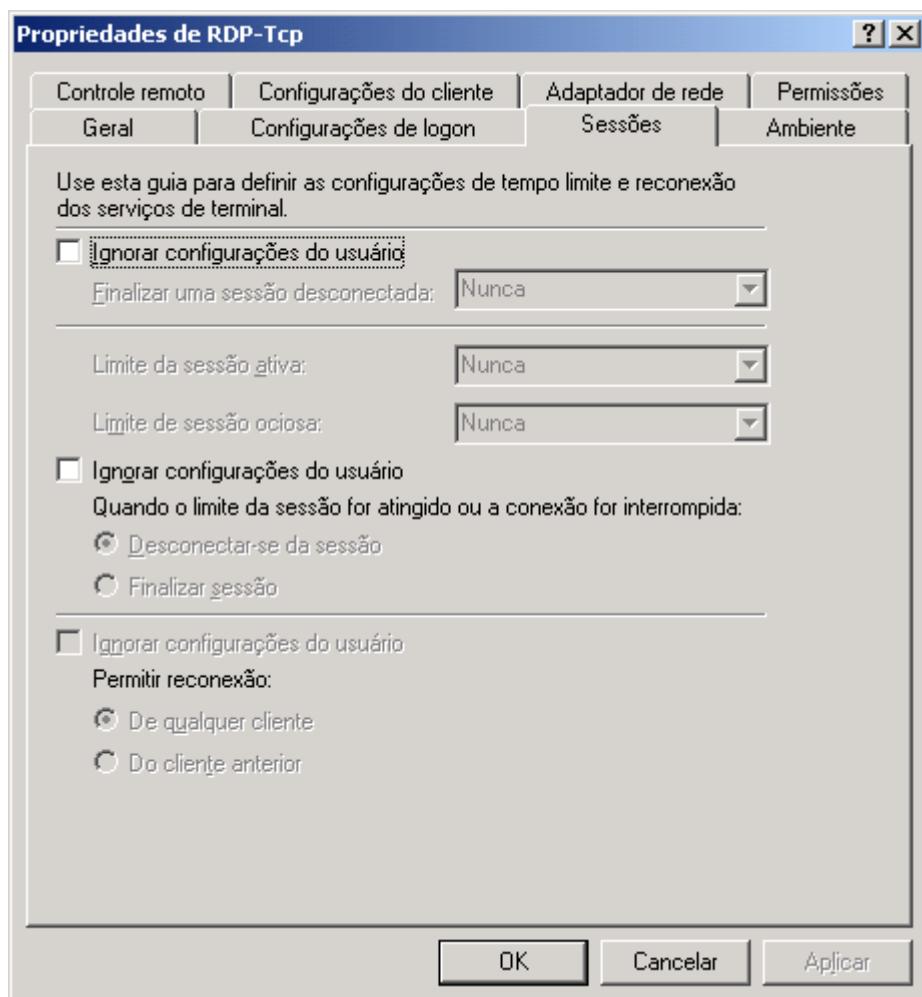


Figura 14.49 A guia Sessões.

Na lista Limite de sessão ativa, você pode digitar ou selecionar o tempo máximo que uma sessão de usuário pode permanecer ativa no servidor. Quando o tempo limite for alcançado, o usuário será desconectado da sessão ou a sessão será encerrada. Quando uma sessão é encerrada, ela é excluída permanentemente do servidor. Selecione Nunca para permitir que a sessão continue indefinidamente. Você pode selecionar o espaço de tempo ou digitar o número de minutos, horas ou dias na caixa. Especifique as unidades de tempo usando m para minutos, h para horas e d para dias. O tempo máximo que pode ser especificado é de 49 dias e 17 horas.

Na lista Limite de sessão ociosa, você pode digitar ou selecionar o tempo máximo que uma sessão ociosa (sessão sem atividade do cliente) permanece no servidor. Quando o tempo limite é alcançado, o usuário é desconectado da sessão ou a sessão é encerrada. Quando uma sessão é encerrada, ela é excluída permanentemente do servidor. Selecione

Nunca para permitir que as sessões desconectadas permaneçam no servidor indefinidamente. Você pode selecionar o espaço de tempo ou digitar o número de minutos, horas ou dias na caixa. Especifique as unidades de tempo usando m para minutos, h para horas e d para dias. O tempo máximo que pode ser especificado é de 49 dias e 17 horas.

- ◆ **Segunda opção - Ignorar configurações do usuário:** Ao selecionar esta opção, serão habilitadas opções para você definir qual deve ser o comportamento do Terminal Server quando o limite de tempo da sessão for atingido ou a conexão for interrompida, sobrescrevendo as opções definidas nas propriedades da conta do usuário, no domínio. Ao marcar esta opção, serão habilitadas as opções a seguir:
  - ◆ **Desconectar-se da seção:** Esta opção especifica que o usuário será desconectado da sessão quando o limite da sessão for alcançado ou quando a conexão for interrompida.
  - ◆ **Encerrar a sessão:** Esta opção especifica que uma sessão será encerrada quando seu tempo limite for alcançado ou a conexão for interrompida. Quando uma sessão é encerrada, ela é excluída permanentemente do servidor.
  - ◆ **Terceira opção – Ignorar configurações do usuário - Permitir reconexão:** Ao selecionar esta opção, serão habilitadas opções para você definir qual deve ser o comportamento do Terminal Server em relação à reconexões, sobrescrevendo as opções definidas nas propriedades da conta do usuário, no domínio. Ao marcar esta opção, serão habilitadas as opções a seguir
- ◆ **De qualquer cliente:** Esta opção especifica que os usuários têm permissão para reconectar-se com uma sessão desconectada a partir de qualquer computador. Por padrão, Serviços de terminal permite a reconexão com uma sessão desconectada em qualquer computador.
- ◆ **Do cliente anterior:** Esta opção especifica que os usuários têm permissão para reconectar-se com uma sessão desconectada apenas a partir do computador no qual a sessão teve origem. Essa opção somente oferece suporte a clientes Citrix ICA que fornecem um número de série ao conectar-se.

A guia Configurações do cliente, da janela de Propriedades RDP-Tcp: Nesta guia são exibidas as opções indicadas na Figura 14.50:

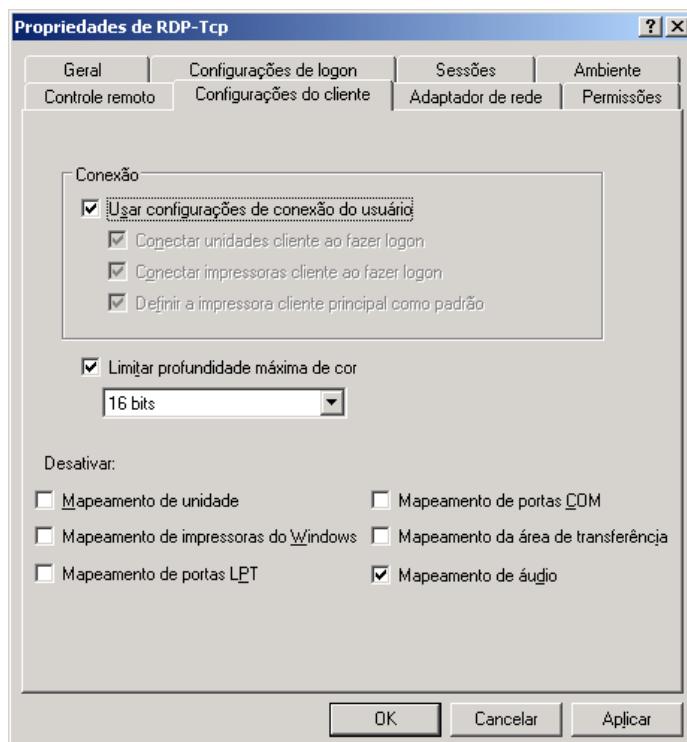


Figura 14.50 A guia Sessões.

Com as opções desta guia você define uma série de configurações relacionadas ao cliente que está criando a sessão. Nesta guia estão disponíveis as seguintes opções de configuração:

- ◆ **Usar configurações de conexão do usuário:** Esta opção define se as configurações de conexão, definidas nas propriedades da conta do usuário serão utilizadas. Ao desmarcar esta opção, serão habilitadas as seguintes configurações adicionais:
- ◆ **Conectar unidades cliente ao efetuar o logon:** Essa opção define se todos os drives de rede, mapeados pelo usuário, devem ser reconectados automaticamente durante o logon.
- ◆ **Conectar impressoras cliente ao efetuar o logon:** Essa opção define que as impressoras de rede, do cliente, devem ser reconectadas automaticamente, durante o logon.
- ◆ **Definir a impressora cliente principal como padrão:** Define a impressora padrão do cliente como sendo também a impressora padrão para a sessão. Ou seja, se dentro da sessão, o usuário enviar alguma impressão, esta será enviada para a impressora definida como padrão, no computador a partir do qual o usuário se conectou ao Terminal Server.
- ◆ **Limitar profundidade máxima de cor:** Define o número máximo de cores, para configuração da tela, que pode ser utilizada através de uma sessão com o Terminal Services.
- ◆ **Desativar o seguinte:** Neste grupo estão disponíveis uma série de opções para desabilitar recursos específicos, tais como:
  - ◆ **Mapeamento de unidade:** Marque esta opção para desabilitar o mapeamento de drivers do cliente.
  - ◆ **Mapeamento de impressoras do Windows:** Especifica se o mapeamento da impressora cliente do Windows será desativado. Por padrão, esse recurso está desmarcado (ativado). Quando ativado (desmarcado), os clientes podem mapear as impressoras do Windows e todas as filas da impressora cliente serão reconectadas automaticamente quando for efetuado logon. No entanto, quando os mapeamentos de porta LPT e COM forem desativados (marcados), não será possível criar as impressoras manualmente. Quando desativado (marcado), os clientes não poderão mapear as impressoras do Windows e as filas da impressora cliente não serão reconectadas quando for efetuado logon. Entretanto, será possível reconectar impressoras manualmente se o mapeamento de porta LPT ou COM estiver ativado (desmarcado).
  - ◆ **Mapeamento de portas LPT:** Especifica se o mapeamento de porta LPT de cliente será desativado. Por padrão, esse recurso está desmarcado (ativado). Quando ativado (desmarcado), as portas LPT do cliente serão mapeadas automaticamente para impressão e estarão disponíveis na lista de portas do Assistente para adicionar impressora. Será preciso criar manualmente a impressora para a porta LPT usando o Assistente para adicionar impressora. Quando desativado (marcado), as portas LPT do cliente não serão mapeadas automaticamente. Você não poderá criar manualmente impressoras usando portas LPT.
  - ◆ **Mapeamento de portas COM:** Especifica se o mapeamento de porta COM de cliente será desativado. Por padrão, este recurso está desmarcado (ativado). Quando ativado (desmarcado), as portas COM de cliente serão mapeadas automaticamente para impressão e estarão disponíveis na lista de portas do Assistente para adicionar impressora. Será preciso criar manualmente a impressora para a porta COM usando o Assistente para adicionar impressora. Quando desativado (marcado), as portas COM de cliente não serão mapeadas automaticamente. Você não poderá criar manualmente impressoras para portas COM.
  - ◆ **Mapeamento da área de transferência:** Especifica se o mapeamento da área de transferência do cliente será desativado. Por padrão, este recurso está desmarcado (ativado).
  - ◆ **Mapeamento de áudio:** Define se o mapeamento de áudio do cliente deve ou não ser desabilitado.

# O novo recurso de Shadow Copies.

O recurso de shadow copies é uma das novidades do Windows Server 2003. Este recurso pode ser habilitado individualmente, em cada volume de um servidor com o Windows Server 2003. Uma vez habilitado este recurso, todas as pastas compartilhadas no volume passarão a utilizar o recurso de shadow copies.

O recurso de shadow copies permite que o Windows Server 2003 mantenha cópias de várias versões de um mesmo arquivo e permite que o usuário, tenha acesso as diferentes versões disponíveis (na prática, havendo espaço disponível, um histórico de até 64 versões do mesmo arquivo, pode ser mantido).

Por exemplo, vamos supor que você crie um arquivo do Word e salve ele em um volume com o recurso de shadow copies habilitado. Daqui a uma semana você abre este mesmo arquivos, faz algumas alterações e salva o arquivo novamente. Com o recurso de shadow copies, será mantida uma cópia da versão anterior, cópia esta que poderá inclusive ser acessada, se for necessário. Podem ser mantidas várias versões do mesmo arquivo. O número de versões que é mantida pelo recurso de shadow copies depende do tamanho do próprio arquivo e do espaço em disco reservado para este recurso.

Este recurso funciona como se fosse uma “lixeira” da rede, porém uma lixeira modificada, onde são mantidas várias versões do mesmo arquivo, podendo estas versões serem acessadas pelo cliente. Este recurso funciona também como um backup alternativo. Rapidamente o usuário pode recuperar uma versão mais recente do arquivo (provavelmente mais recente do que a versão que está na fita de backup), sem ter que esperar uma hora ou mais até que o arquivo seja restaurado a partir de uma fita de backup.

O recurso de shadow copies traz muitos benefícios, dentre os quais gostaria de destacar os seguintes:

- ◆ Recuperação rápida e fácil de arquivos que foram excluídos acidentalmente. Se você excluir, por engano, um arquivo, poderá abrir uma versão anterior e copiá-la para um local seguro.
- ◆ Recuperação rápida e fácil de arquivos que foram sobreescritos por engano.
- ◆ Comparação de versões dos arquivos. Você pode utilizar uma versão anterior para identificar as mudanças que foram efetuadas em um determinado arquivo.

É fundamental lembrar que o recurso de shadow copies não é um recurso que irá substituir o backup. Principalmente porque as diferentes versões do mesmo arquivo são gravadas no mesmo disco. Ou seja, se o disco for danificado você perderá a última versão e também todas as versões mantidas no recurso de shadow copies. Nesta situação a única maneira de recuperar as informações é restaurando a partir do backup. Existe a possibilidade de configurar o recurso de Shadow Copies, para que as copias sejam armazenadas em um volume diferente do volume original. Esta pode ser uma boa estratégia em termos de desempenho, porém nem nesta situação, o recurso de Shadow Copies deve ser considerado um substituto para o Backup.

Quando o espaço reservado para a manutenção de versões anteriores dos arquivos for preenchido, os arquivos mais antigos serão descartados, para que novos possam ser gravados. Você aprenderá a configurar o espaço reservado para o recurso de shadow copies mais adiante, nos exemplos práticos.

**NOTA:** Permitam que eu me queixe, mais uma vez, das traduções que são feitas. Já vi algumas traduções de shadow copies como sendo “sombras de cópia”, mas, sinceramente, me recuso a utilizar esta tradução. Por isso, neste tópico, vou utilizar o termo original: **shadow copies**.

**NOTA:** O recurso de shadow copies é configurado através da janela de propriedades do volume (C;D; e assim por diante), na guia **Shadow Copies**, conforme mostrarei na parte prática mais adiante. É importante salientar que o recurso de **Shadow Copies** é habilitado a nível de volume e não a nível de pasta ou compartilhamento. Ou seja, uma vez habilitado o recurso de **Shadow Copies** em um volume, todas as pastas e compartilhamentos do volume, passarão a ter o recurso de **Shadow Copies** habilitado.

## Mais algumas observações sobre o recurso de shadow copies.

A quantidade mínima de espaço que pode ser reservada para este recurso é de 100 MB. O valor padrão é 10% do tamanho do volume onde o recurso de shadow copies será habilitado. As versões antigas, mantidas pelo recurso de shadow copies poderão ser gravadas em um volume diferente do volume original.

O volume a ser reservado para este recurso depende da forma como os arquivos são utilizados. Se você tem arquivos que são alterados diariamente, será necessário uma boa quantidade de espaço para este recurso. Se você tem arquivos que raramente são alterados, a quantidade de 10% do volume pode ser mais do que suficiente.

## O agendamento do recursos de shadow copies.

Quando você habilita o recurso de shadow copies, o Windows Server 2003 cria um agendamento padrão e define um intervalo. A cópia dos arquivos é feita de acordo com este agendamento.

Este agendamento pode ser alterado e deve ser adaptado de acordo com as características de uso do volume. Na parte prática você aprenderá a alterar este agendamento.

## Instalando o cliente de shadow copies.

Para que um usuário acessando uma pasta compartilhada no servidor (pasta esta que está em um volume para o qual o recurso de shadow copies foi habilitado) possa utilizar o recurso de shadow copies, é necessário que o cliente de shadow copies seja instalado na estação de trabalho do usuário. Os arquivos de instalação do cliente shadow copies estão disponíveis na seguinte pasta, de qualquer servidor com o Windows Server 2003 instalado:

```
%systemroot%\system32\clients\twclient\x86\twcli32.msi
```

Onde %systemroot% é a pasta onde o Windows Server 2003 foi instalado.

O arquivo twcli32.msi é um arquivo de instalação, no padrão do Microsoft Installer. Este arquivo pode ser instalado em todas as estações de trabalho da rede, usando o recurso de distribuição de software via GPO ou pode ser disponibilizado em um drive de rede para que os usuários instalem em suas estações de trabalho. Este arquivo tem apenas 287 KB.

## Log de Eventos e de Auditoria – Conceito.

Quando você trabalha com o Windows Server 2003, o qual é utilizado como sistema operacional para servidores da rede, a segurança é uma preocupação constante. Não poderia ser diferente. O sistema operacional deve ser capaz de disponibilizar alguns serviços básicos em relação a segurança: identificação (através do mecanismo de contas de usuários, logon e do protocolo Kerberos),

**IMPORTANTE:** Para que os clientes possam utilizar o recurso de shadow copies, deve ser instalado o software cliente de shadow copies em cada estação de trabalho que irá utilizar este recurso. Na parte prática mostrarei como fazer esta instalação. Em resumo, para o exame, não se esqueça que para habilitar o recurso de Shadow Copies, são necessários dois passos. O primeiro é habilitar este recurso no volume onde está a pasta compartilhada, que será acessada através da rede. O segundo passo é instalar o cliente de Shadow Copies, em todas as estações de trabalho que deverão ter acesso a este recurso. Lembre-se bem destes dois passos, para o exame.

**IMPORTANTE:** As versões anteriores dos arquivos, mantidas pelo recurso shadow copies são somente leitura, ou seja, você não poderá fazer alterações diretamente nestas cópias. Você poderá abrir estas cópias e salvar em uma nova pasta e fazer alterações, mas não diretamente nas cópias mantidas pelo recurso de shadow copies. Por exemplo, se você abrir uma planilha do Excel ou um documento do Word, a partir de uma cópia mantida pelo recurso de Shadow Copies, esta cópia será somente leitura. Se você fizer alterações e tentar salvar, será emitida uma mensagem

restrição de acesso aos recursos (com base no mecanismo de permissões de acesso, através do uso de uma ACL – Access Control List, Lista de Controle de Acesso a cada recurso da rede) e também deve ser capaz de registrar as ações que estão sendo executadas nos recursos da rede, juntamente com informações sobre o horário da ação, quem foi o usuário que executou a ação e outras informações relevantes. O registro do que é feito na rede é gravado no Log do Sistema. O sistema de log do Windows Server 2003 permite o registro de um grande número de eventos, conforme mostrarei neste capítulo. A ação de pesquisar/consultar o log de eventos, em busca de informações é conhecido como auditoria.

Auditoria é um processo de acompanhamento das ações que são executadas nos servidores do domínio, através da rede, tanto ações do próprio Sistema operacional, como por exemplo a inicialização de um serviço, mas principalmente ações do usuário, como um logon ou um acesso aos arquivos de uma pasta compartilhada. Por exemplo, toda vez que o Windows Server 2003 é inicializado uma série de serviços são iniciados automaticamente, como o serviço spooler que controla a impressão, o serviço Workstation que controla a interface gráfica do Windows Server 2003 e assim por diante. Cada um destes serviços é capaz de escrever eventos nos logs de auditoria do Windows Server 2003. Um evento é uma mensagem que pode ser informativa, pode ser um aviso e pode ser uma mensagem de erro. Um outro exemplo, quando um usuário tenta fazer o logon e informa uma senha errada, um evento é gravado no log de segurança, neste caso é gravado uma mensagem (evento) de falha de logon.

A auditoria de segurança monitora vários eventos relativos à segurança. O monitoramento de eventos do sistema é necessário para detectar invasores e tentativas de comprometer os dados do sistema. Uma tentativa de logon sem êxito é um exemplo de um evento que pode ser submetido à auditoria.

Os tipos mais comuns de eventos a serem submetidos à auditoria são:

- ◆ Acesso a objetos, como arquivos e pastas. Por exemplo, repetidas tentativas de acessar determinados arquivos, por um usuário que não tem permissão de acesso, podem caracterizar uma tentativa de quebra de segurança.
- ◆ Gerenciamento de contas de usuários e grupos: ficam registradas informações sobre quem fez alterações nas contas de usuários e grupos.
- ◆ Quando os usuários fazem logon e logoff no sistema. Por exemplo, logons efetuados fora do horário normal de trabalho, merecem uma atenção especial do administrador.

Além da auditoria de eventos relacionados à segurança, um log de segurança é gerado, oferecendo um meio para que você visualize os eventos de segurança registrados no log. O log de segurança pode ser exibido com o console Visualizar eventos, o qual você aprenderá a utilizar neste capítulo.

Uma mensagem no log do sistema, possui informações tais como o usuário que executou a ação, a ação executada e se esta foi executada com sucesso ou não.

informando que a cópia é somente leitura. Você pode usar o comando Arquivo -> Salvar como, para salvar a cópia em um local alternativo. A cópia salva no local alternativo, usando o comando Arquivo -> Salvar como, poderá ser alterada.

**NOTA:** Se você tiver que alterar o volume onde são gravadas as cópias, todas as cópias existentes serão excluídas e um novo histórico começará a ser criado no novo volume. Por isso é importante planejar com cuidado o espaço necessário, antes de habilitar o recurso de shadow copies em um volume. Este é mais um dos motivos pelos quais o recurso de Shadow Copies não pode ser utilizado em substituição ao Backup.

**NOTA:** Para as ações práticas relativas ao recurso de Shadow Copies, consulte o Capítulo 9.

**IMPORTANTE:** Não utilize o recurso de shadow copies em servidores que estão configurados para dual-boot com outras versões do Windows. Nestes casos pode acontecer de os arquivos de shadow copies serem corrompidos.

O log de eventos do Windows Server 2003 pode ser configurado, de tal maneira que o administrador escolha quais eventos devem ser gravados no log, como por exemplo: tentativas de logon com sucesso, tentativas de logon sem sucesso ou ambas . Por exemplo, o administrador pode definir que seja registrado um evento no log de segurança, toda vez que um usuário tentar acessar um determinado arquivo, sem ter a devida permissão (tentativa de acesso sem sucesso).

Também é possível definir se o acesso a arquivos, pastas e impressoras devem ser monitorados ou não (por padrão este monitoramento está desabilitado). Além disso, você pode definir se devem ser monitorados somente acessos bem sucedidos ou acessos negados (sem sucesso), tais como um usuário com permissão somente de leitura que tenta alterar um determinado arquivo, em uma pasta compartilhada.

Os logs do sistema são acessados utilizando a opção Event Viewer (Visualizar eventos) do console Gerenciamento do computador. Também é possível utilizar o console Visualizar eventos que é acessado através da opção Iniciar -> Ferramentas Administrativas -> Visualizar eventos. O console Visualizar eventos é configurado para carregar apenas o Snap-in para trabalhar com eventos, diferente do console Gerenciamento do Computador, o qual é configurado para carregar uma série de Snap-ins, dentre eles, o Snap-in Visualizar eventos.

Por padrão, são criados três logs no sistema de log do Windows:

- ◆ **Application (Log do aplicativo):** Contém erros, avisos e mensagens informativas de diversos programas que rodam no Windows Server 2003. Por exemplo, o Microsoft SQL Server 2000 (banco de dados da Microsoft), grava uma série de eventos no log Aplicativo. O log do aplicativo contém eventos registrados por aplicativos ou programas. Por exemplo, um programa de banco de dados pode registrar um erro de arquivo no log do aplicativo. Os desenvolvedores de software decidem quais eventos monitorar, isto é, ao desenvolver um programa, é possível definir quais eventos o programa irá gravar no log de eventos do Windows Server 2003. Linguagens como o Delphi, VB.NET, Visual Basic 6 e C#, fornecem comandos para que um programa possa gravar eventos no log do Windows Server 2003.
- ◆ **Security (Log de segurança):** Contém informações sobre o sucesso ou não de eventos de auditoria, de acordo com definições da política de auditoria. Conforme mostrarei mais adiante, a política de auditoria define quais eventos de segurança serão monitorados. O log de segurança registra eventos como tentativas de logon válidas e inválidas, assim como eventos relacionados ao uso de recursos, como criar, abrir ou excluir arquivos ou outros objetos. Um administrador pode especificar os eventos que serão registrados no log de segurança. Por exemplo, se você ativou a auditoria de logon, as tentativas de logon no sistema serão registradas no log de segurança. Por padrão somente usuários com permissão de administrador podem acessar o log de segurança.
- ◆ **System (Log do sistema):** Contém erros, avisos e informações geradas pelo próprio Windows Server 2003. O Windows Server 2003 define quais os eventos serão gerados. O log do sistema contém eventos registrados pelos componentes de sistema do Windows Server 2003. Por exemplo, a falha de um driver ou de outro componente do sistema ao ser carregado durante a inicialização é registrada no log do sistema. Os tipos de evento registrados no log pelos componentes do sistema são determinados previamente pelo Windows Server 2003.

---

**NOTA:** A medida que novos serviços vão sendo instalados, novas opções vão sendo adicionadas ao console Visualizar eventos. Por exemplo, ao instalar o DNS em um servidor Windows Server 2003, uma opção DNS é adicionada ao Visualizador de eventos, entrada essa que trata de eventos relacionados com o serviço de DNS. Outro exemplo, em um servidor configurado como DC, uma nova categoria de eventos é criada: Directory Service (Serviço de Diretório), conforme exemplo da Figura 14.51, onde são exibidas as opções de log disponíveis em um DC com o Windows Server 2003 instalado:

---

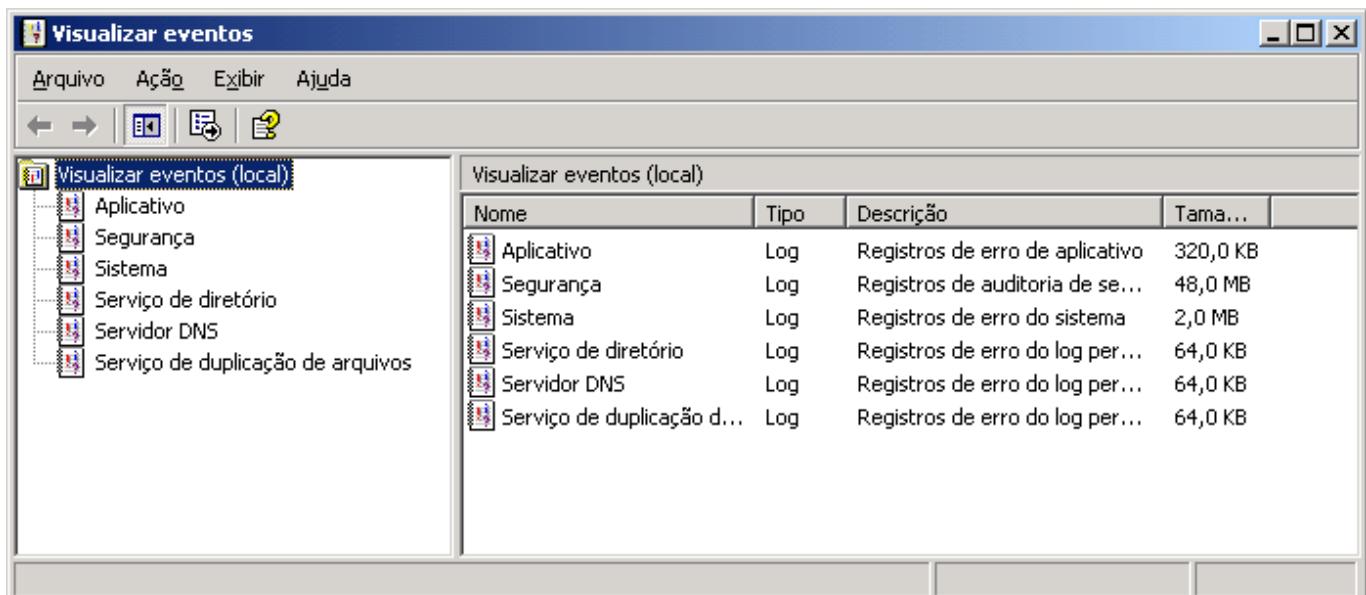


Figura 14.51 Opções de log em um DC com o Windows Server 2003.

Cabe aqui salientar que o principal objetivo da existência de um sistema de Auditoria/Log, é manter um acompanhamento de tudo o que está acontecendo no sistema. Quando algum problema acontece, como por exemplo, um serviço que deixa de funcionar, o primeiro lugar que o administrador vai em busca de informação é no log do sistema. Informações importantes sobre segurança podem ser encontrados no log de Segurança.

## Habilitando eventos de auditoria.

O Windows Server 2003 permite que o administrador configure quais eventos de segurança devem e quais não devem ser auditados. Para que sejam auditadas determinadas ações ligadas com a segurança - tais como tentativas de logon e acesso a arquivos e pastas – algumas diretivas tem que ser habilitadas. As opções de segurança, são habilitadas através de diretivas de segurança, configuradas via GPO.

Em um computador com o Windows Server 2003, configurado como member Server ou como standalone Server, deve ser utilizado o console Local Security Policy (Diretiva de segurança local), acessada através da opção Ferramentas administrativas.

No exemplo a seguir, utilizarei o console Domain Security Policy (Diretivas de Segurança do Domínio). Com isso estou configurando opções que serão válidas para todos os computadores (clientes e servidores do domínio). Depois farei uma tentativa de logon com uma senha errada e você observará se foi gerado um evento no log de segurança. Então mãos a obra.

Neste exemplo mostrarei como habilitar algumas opções de auditoria, as quais não estão habilitadas por padrão. Por exemplo, a auditoria do acesso à arquivos e pastas não é habilitado por padrão. Para que o administrador possa auditar o acesso a pastas e arquivos (isto é, fazer com que sejam gravados eventos no log de eventos, quando os usuários acessam uma determinada pasta e seus arquivos), primeiro o administrador tem que habilitar uma diretiva de auditoria, para que o Windows

**IMPORTANTE:** Os logs são gravados individualmente, em cada servidor. Este é um problema que já existia no Windows 2000 Server e não foi solucionado no Windows Server 2003, ou seja, não existe uma base única, centralizada, com todos os eventos de Log da rede. Imagine que você está investigando um funcionário suspeito de participar de uma fraude. Como você fará para ter acesso a todos os eventos de logon no domínio, da conta do usuário? Você terá que conectar o console Visualizador de eventos com cada DC do domínio, aplicar um Filtro para exibir apenas os eventos para o usuário que está sendo investigado, exportar estas informações para o formato de arquivo .txt e depois importar todos

Server 2003 passe a auditar o acesso a pastas e arquivos. Outro exemplo seria a auditoria do uso de impressoras, a qual por padrão também é desabilitada. Neste exemplo, mostrarei quais os passos para que o administrador possa habilitar as diretivas de auditoria e apresentarei uma descrição das diretivas disponíveis.

estes arquivos em um banco de dados como o Microsoft Access ou SQL Server 2000. Ufa, um trabalho e tanto. Seria bem mais simples se houvesse uma base única de logs, para todo o domínio.

**IMPORTANTE:** Porém não basta habilitar as diretivas. Por exemplo, não basta habilitar a diretiva que orienta o Windows Server 2003 a monitorar o acesso a pastas e arquivos. Depois de habilitada a auditoria, o administrador tem que definir quais pastas e arquivos devem ser monitoradas (por padrão nenhuma pasta é monitorada, mesmo após a respectiva diretiva de segurança ter sido habilitada) e para quais usuários e grupos deve ser feito o monitoramento. Esta segunda etapa na configuração de auditoria de acesso a pastas, arquivos e impressoras será descrita em exemplos mais adiante, neste capítulo.

Exemplo: Para habilitar a auditoria de eventos de segurança, siga os seguintes passos:

1. Faça o logon com uma conta com permissão de administrador.
2. Abra o console Diretivas de segurança de domínio: Iniciar -> Ferramentas Administrativas -> Políticas de Segurança do Domínio.
3. Será aberta a janela Configurações de segurança padrão de Domínio, conforme indicado na Figura 14.52:

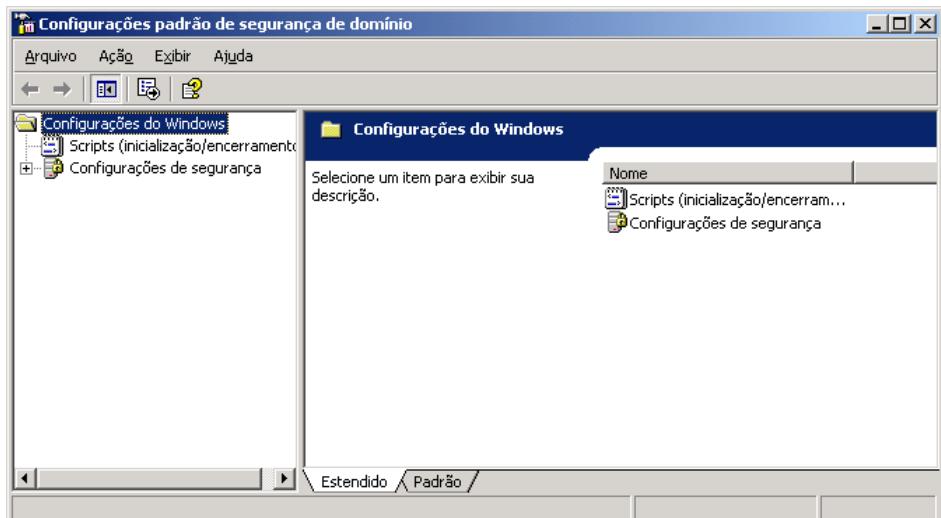


Figura 14.52 O console para configurações das diretivas de segurança do domínio.

4. Clique no sinal de + ao lado da opção Configurações de segurança, para exibir as opções disponíveis. Clique no sinal de + ao lado da opção Diretivas locais, para exibir as opções disponíveis.
5. Nas opções que surgem, dê um clique na opção Diretivas de auditoria. No painel da direita são exibidas as várias diretivas de auditoria disponíveis, as quais são indicadas na Figura 14.53 e explicadas logo a seguir. Observe ao lado do nome de cada diretiva, o status Não-definido, indicando que não existe definição para esta diretiva, isto é, esta diretiva estivesse desabilitada.

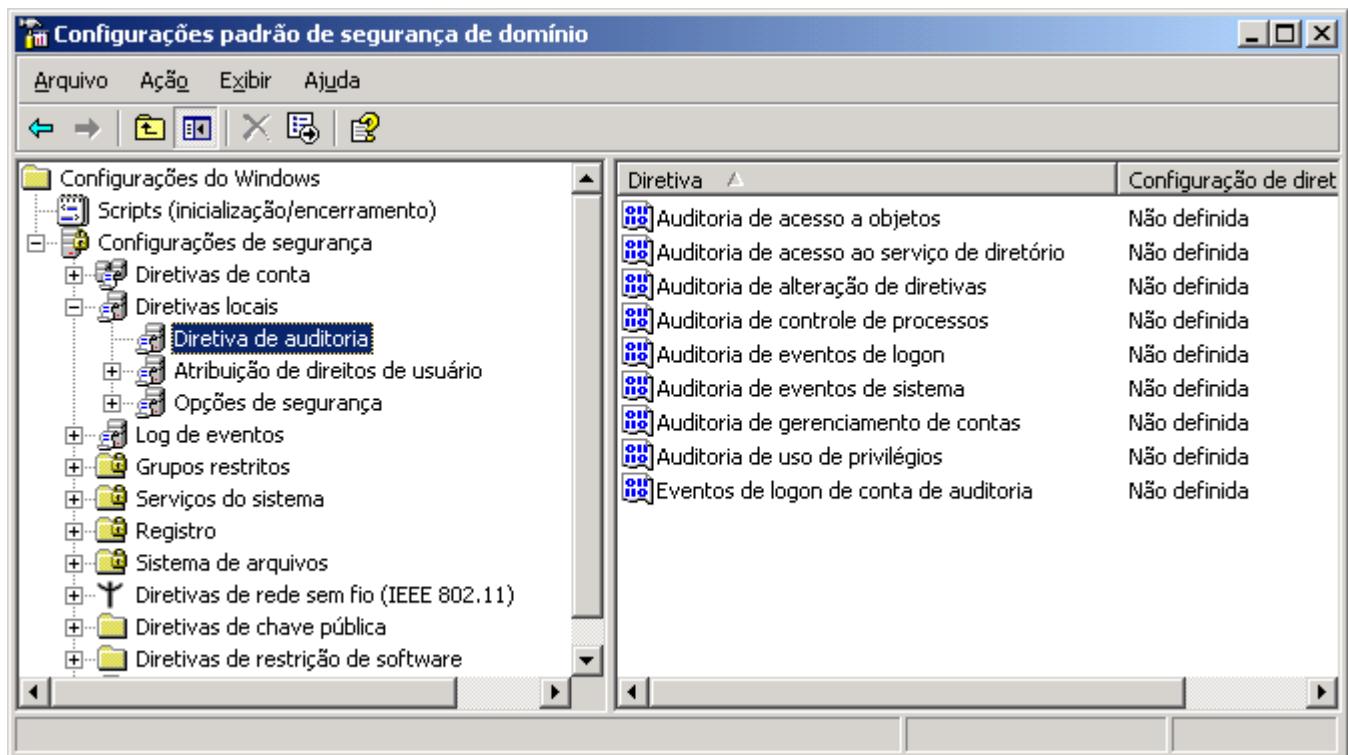


Figura 14.53 Opções para configuração das Diretivas de auditoria.

A seguir apresento uma descrição das diretivas de auditoria disponíveis:

- ◆ Audit account logon events (Auditoria de eventos de logon de conta):

Com esta opção você pode configurar se os eventos de logon devem ou não ser auditados. São considerados eventos de logon, qualquer logon feito em uma estação de trabalho da rede, que pertença ao domínio e com uma conta do domínio.

**IMPORTANTE:** É muito importante que você conheça este ponto, ou seja, para fazer a auditoria de eventos de logon de contas do domínio, a diretiva a ser habilitada é a diretiva Auditoria de eventos de logon de conta. Existe uma outra auditoria, com um nome semelhante – Auditoria de eventos de logon, porém esta segunda é usada para fazer a auditoria de eventos de logon usando contas locais dos computadores e não as contas do domínio. Certifique-se de que você entendeu bem a diferença entre estas duas diretivas, pois este é um ponto importante para o exame.

Conforme descrito anteriormente, a validação do logon é feita nos DCs, onde está instalado o Active Directory. Neste caso se o usuário jsivila fizer o logon com a sua conta de domínio, na sua estação de trabalho, um evento de logon será gerado para este usuário. Além disso você define se devem ser auditados os eventos com sucesso (quando o usuário faz o logon normalmente) ou com falha (quando o usuário não consegue fazer o logon, por exemplo, por ter digitado uma senha incorreta). Para configurar esta auditoria, basta dar um clique duplo nela. Será aberta a janela Propriedades de Eventos de logon de conta de auditoria (a confusão

**NOTA:** Estas opções de auditoria também poderiam ser configuradas através da GPO (Group Policy Object) padrão do domínio. No Capítulo 9 você teve uma introdução ao assunto GPO, focando nos pontos cobrados no Exame 70-290. Para um estudo completo sobre GPOs, consulte o Capítulo 18 do meu livro: Windows Server 2003 – Curso Completo, 1568 páginas.

**IMPORTANTE:** O nome correto desta auditoria é Auditoria de eventos de logon de conta, porém no console Configurações padrão de segurança do domínio, esta diretiva aparece, incorretamente, com o seguinte nome: Eventos de logon de conta de auditoria. Esta é mais uma pérola da tradução, que contribui para tornar confuso um recurso que é fácil de utilizar.

no nome é por conta da equipe de tradução). Para habilitar esta diretiva você deve marcar a opção Definir as configurações dessas diretivas (o plural também é por conta da equipe de tradução). Ao marcar esta opção, serão habilitadas as opções Êxito e Falha. Para passar a registrar os eventos de logon com sucesso, marque a opção Êxito. Com isso sempre que um usuário fizer um logon no domínio, com sucesso, será registrado um evento no log de eventos do DC que autenticou o usuário. Para passar a registrar os eventos de falha de logon, marque a opção Falha. Com isso, sempre que um usuário fizer uma tentativa de logon sem sucesso, será registrado um evento no log de eventos do DC onde a tentativa de logon foi feita. Na Figura 14.54 é exibida a janela de propriedades desta diretiva e as opções que podem ser configuradas para esta auditoria. Após ter definido as configurações desejadas, basta clicar em OK. O mais comum para este diretiva é habilitar tanto os eventos de sucesso, quanto os eventos de falha, para que fique registrado no log do servidor, todos os eventos de logon, que seja com sucesso, quer seja com falha.

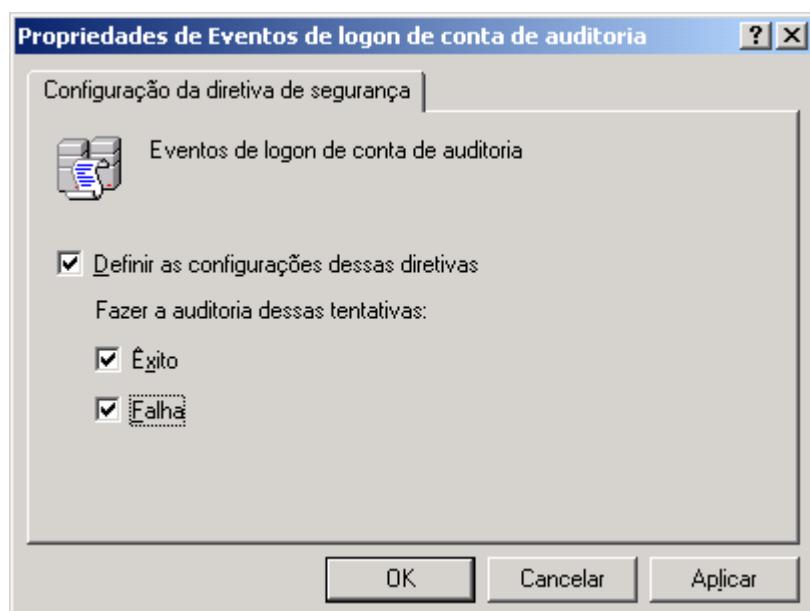


Figura 14.54 Opções para a diretiva de auditoria de eventos de logon.

- ◆ **Audit account management (Auditoria de gerenciamento de contas):** Esta diretiva determina se deve ser feita a auditoria de cada evento de gerenciamento de conta de um usuário, grupo ou computador do domínio. Os exemplos de eventos de gerenciamento de conta incluem: criação ou alteração de uma conta, renomeação de uma conta, ativação/desativação da conta, incluir um usuário em um grupo ou retirar o usuário de um grupo, o administrador definir a senha de uma conta e assim por diante.

As configurações padrão para esta diretiva são as seguintes:

- ◆ Sucesso em controladores de domínio.
- ◆ Sem auditoria nos Member Servers

Para configurar esta auditoria, basta dar um clique duplo nela. Será aberta a janela de propriedades da auditoria. Para habilitar esta diretiva você deve marcar a opção Definir as configurações dessas diretivas. Ao marcar esta opção, serão habilitadas as opções Êxito e Falha. Para passar a registrar os eventos de gerenciamento de contas com sucesso, marque a opção Sucesso. Com isso sempre que o administrador ou outro usuário com as devidas permissões, fizer alterações em uma conta, um evento será gravado no log de eventos. Para passar a registrar os eventos de falha de gerenciamento de contas, marque a opção Failure. Com isso, sempre que o administrador ou um usuário sem as

devidas permissões, fizer uma tentativa alterar uma conta, será registrado um evento no log de eventos. Na Figura 14.55 é exibida a janela de propriedades desta auditoria e as opções que podem ser configuradas para esta auditoria. Após ter definido as configurações desejadas, basta clicar em OK. O mais comum para esta diretiva é habilitar apenas o log dos eventos sem sucesso, ou seja, de tentativas que um usuário faz de alterar contas do domínio, sem ter as devidas permissões para isso. Esta situação pode acontecer quando, por exemplo, um usuário está tentando alterar a senha de outro usuário para fazer um logon com a conta deste segundo usuário.

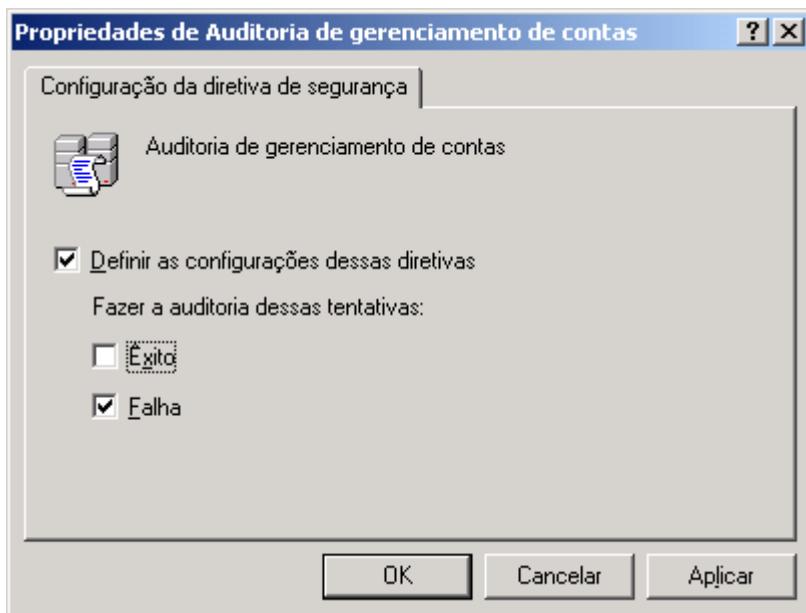


Figura 14.55 Opções para a diretiva de auditoria de eventos de gerenciamento de contas.

- ◆ **Auditoria de acesso ao serviço de diretório:** Define se serão auditadas tentativas de acesso com sucesso, com falha ou ambas, a objetos do Active Directory, para os quais tenha sido habilitada a auditoria dos acessos. O Active Directory, conforme explicado no Capítulo 02, é a base de dados na qual ficam armazenados uma série de objetos, como por exemplo: contas de usuários, grupos de usuários, Unidades organizacionais, domínios, sites, etc. Por exemplo, podemos implementar uma política para detectar tentativas de alteração sem sucesso, nas contas que fazem parte do grupo Administradores. Por padrão esta política está desabilitada para controladores de domínio e indefinida para os demais computadores. Um cuidado que deve ser tomado é o de habilitar somente as auditorias realmente necessárias, de acordo com a política de segurança da empresa, pois se forem habilitadas auditoria em um grande número de objetos, pode haver uma queda de desempenho, além de um crescimento exagerado no tamanho do log de segurança. Por padrão esta auditoria está desabilitada.
- ◆ **Audit logon events (Auditoria de eventos de logon):** Esta diretiva determina se deve ser feita a auditoria de cada instância de logon ou logoff de usuário, bem como de qualquer conexão de rede com o computador local, ou no caso com o DC que eu estou utilizando. Se você estiver registrando no log os eventos da Auditoria de eventos de logon de conta com êxito em um controlador de domínio, as tentativas de logon de um usuário, a partir da sua estação de trabalho não gerarão auditorias de logon (as quais serão geradas se a diretiva Auditoria de eventos de logon de conta, descrita anteriormente, estiver habilitada). Somente tentativas de logon de rede e interativas no próprio controlador de domínio gerarão eventos de logon. Resumindo, Auditoria de eventos de logon de conta são gerados no local onde reside a conta; ou seja, no DC. Eventos de logon são gerados no local onde ocorre a tentativa de logon. Se for um logon interativo no DC, no próprio DC, se for um logon interativo em um member server, no log de auditoria local do member server. Você pode configurar para que sejam

auditadas tentativas de logon com sucesso, com falha ou ambas. No caso de um computador com o Windows Server 2003, as tentativas de logon são consideradas as tentativas locais ou tentativas feitas via Terminal Service Client.

- ◆ **Audit object access (Auditoria de acesso a objetos):** Determina se deve ser feita a auditoria do acesso de um usuário a um objeto — por exemplo, um arquivo, uma pasta, uma chave da Registry, uma impressora etc. São considerados objetos, todos aqueles elementos que possuem uma ACL – Access Control List (Lista de Controle de Acesso). Por exemplo, uma pasta em uma partição NTFS, onde são definidas permissões de acesso (além de habilitar esta diretiva, posteriormente a pasta deve ser configurada para registrar eventos de acesso no log de auditoria, conforme exemplo mais adiante). Se você definir esta configuração de diretiva, poderá especificar se haverá auditoria de acessos com êxito, acessos sem êxito ou se não ocorrerá auditoria desse tipo de evento. As auditorias com êxito geram uma entrada de auditoria quando um usuário acessa com êxito um objeto. Por exemplo, o usuário tem permissão de leitura em um arquivo e ele acessa o arquivo para leitura. Este é um evento com sucesso. As auditorias sem êxito geram uma entrada de auditoria quando um usuário tenta acessar sem êxito um objeto, como por exemplo, tentar imprimir em uma impressora na qual ele não tem permissão ou tentar alterar um arquivo para o qual ele tenha apenas permissão de leitura. É interessante observar que a definição de Auditoria de acesso a objetos ocorre em duas etapas. Primeiro o administrador deve habilitar esta diretiva, para acessos com sucesso, com falha ou ambos. Em seguida, em cada objeto (pasta, impressora, arquivo, etc) a ser auditado, o administrador deve configurar a auditoria e especificar quais usuários ou grupos devem ser monitorados. Apenas habilitar a diretiva não fará com que o acesso aos objetos sejam auditados. Por padrão esta diretiva está desabilitada.
- ◆ **Audit policy change (Auditoria de alteração de diretivas):** Determina se deve ser feita a auditoria das alterações efetuadas nas diretivas de segurança. O normal é habilitar a auditoria de eventos sem sucesso, para tentar identificar tentativas de alteração das diretivas, por usuários não autorizados. Alterar as diretivas é uma das maneiras de criar brechas na segurança do sistema, por isso somente usuários autorizados devem ter este nível de permissão.
- ◆ **Audit process tracking (Auditoria de controle de processos):** Determina se deve ser feita a auditoria de informações de controle de eventos detalhadas, como ativação de programas, término de processo, duplicação de identificador e acesso indireto a objeto. Esta diretiva é utilizada para fazer uma auditoria dos programas que estão rodando no computador, na tentativa de detectar usuários que estão tentando utilizar programas para os quais eles não tem permissão ou tentando instalar processos que possam abrir o servidor para ataques de segurança.
- ◆ **Audit system events (Auditoria de eventos de sistema):** Determina se deve ser feita a auditoria quando um usuário reiniciar ou desligar o computador, ou quando ocorrer um evento que afete a segurança do sistema ou o log de segurança.

**IMPORTANTE:** Vou insistir neste ponto. Lembre-se que a diretiva Auditoria de eventos de logon de conta é utilizada para fazer auditoria de logon de contas do domínio, já a diretiva Auditoria de eventos de logon, é utilizada para a auditoria de eventos de logon de contas locais.

- ◆ **Audit privilege use (Auditoria de uso de privilégios):** Determina se deve ser feita a auditoria de cada instância do uso de um direito do usuário. Direitos (rights) são permissões especiais, como por exemplo incluir um computador como membro de um domínio, fazer o logon interativamente nos controladores de domínio, alterar a hora dos servidores e assim por diante. Estes direitos podem ser configuradas pelo Administrador, o qual pode “dar” estes direitos para determinados usuários ou grupos.

## Configurando a auditoria de acesso a arquivos, pastas e impressoras.

Conforme já descrevi brevemente, no início do Capítulo, a auditoria de acesso a objetos (pastas compartilhadas, impressoras compartilhadas e qualquer outro objeto para o qual seja permitido definir uma lista de permissões de acesso, tais como objetos do Active Directory, chaves da Registry e assim por diante), é um processo em duas etapas, conforme descrito a seguir:

1. Habilitar a Diretiva de auditoria: Auditoria de Acesso a objetos. Esta diretiva é habilitada, para sucesso, falha ou ambas as situações, utilizando o console Configurações locais de segurança, já descrito anteriormente. Em um dos exemplos anteriores você aprendeu a habilitar esta e outras diretivas de segurança. É também importante salientar que, para o Windows Server 2003, é considerado objeto, todo elemento que tiver uma Lista de Controle de Acesso – ACL (Access Control List). Com isso, entradas da Registry, todo e qualquer elemento do Active Directory, são considerados objetos.
2. Após ter habilitada a Diretiva de auditoria descrita no item 1, o administrador tem que configurar a auditoria em cada um dos objetos a serem auditados. Por exemplo, para monitorar o acesso a uma pasta e ao conteúdo desta pasta (subpastas e arquivos), o administrador deve acessar as propriedades desta pasta e configurar quais usuários/grupos terão o acesso monitorado. Por exemplo, o administrador pode definir que o grupo Gerentes terá o acesso a uma determinada pasta monitorada, tanto para evento de sucesso quanto de falha. Com isso, toda vez que um membro deste grupo acessar o conteúdo da pasta que está sendo monitorada, será gravado um evento no log de eventos.

## Monitoração de desempenho

Sobre este tópico, o mais importante é você conhecer os valores limite, que indicam problemas de desempenho com os principais objetos, tais como Memória, Processador e Sistema de discos. Existem alguns indicadores que mostram, claramente, que existe um problema de desempenho em um destes componentes. A solução é fazer um upgrade no referido componente.

### Monitoração de desempenho – conceitos básicos.

Monitorar a utilização dos principais recursos de um servidor é uma tarefa importante para o administrador do sistema, principalmente em computadores que estão sendo utilizados por um grande número de usuários da rede, para acesso a recursos tais como pastas compartilhadas, impressoras, servidores Web de Intranet, servidores de banco de dados, DCs do domínio e assim por diante. Os principais elementos de hardware a serem monitorados são os seguintes:

- ◆ Memória RAM.
- ◆ Processador.

---

**IMPORTANTE:** Conheça bem estas diretivas. Este é um tópico muito importante para o Exame 70-290.

---

- ◆ Placa de rede.
- ◆ Sistema de discos.

Existem outros elementos que podem prejudicar o desempenho como um todo, porém estes quatro são os mais importantes. Podem existir situações, por exemplo, em que a utilização da memória RAM e do Processador esteja baixa, porém o Sistema de discos esteja sobrecarregado, e neste caso, o desempenho do sistema como um todo fica bastante prejudicado. Dependendo do tipo de função que o servidor está exercendo, um recurso de hardware pode ter mais ou menos influência no desempenho como um todo. Por exemplo, servidores de banco de dados são muito dependentes de bons processadores, já servidores de arquivos dependem de um bom sistema de disco e de uma conexão rápida com a rede.

Quando um determinado componente está sobrecarregado, dizemos que este componente representa um “gargalo” para o sistema (do termo inglês “bottleneck”), isto é, é o componente que está limitando (“engargalando”, se é que existe esta palavra.), o desempenho do sistema como um todo. Ou seja, o desempenho de um sistema é tão bom quanto for o desempenho do seu componente mais lento. Por exemplo, de que adianta vários processadores, com muita memória RAM e com um sistema de discos antigo, extremamente lento.

Dependendo do papel que o servidor esteja desempenhando na rede, a utilização de cada um destes componentes será maior ou menor. Por exemplo, computadores que atuam como Servidores de Banco de dados (com o Microsoft SQL Server, por exemplo), ou Servidores de aplicação (com o Microsoft Transaction Server, por exemplo), fazem um uso muito intensivo dos Processadores. Neste caso pode ser recomendável, dependendo do número de usuários, a utilização de servidores multi-processados. Já no caso de Servidores de arquivos, a utilização da interface de rede e do sistema de discos pode ser bastante elevada, neste caso a utilização de placas mais velozes ou até mesmo de mais de uma placa de rede e de sistemas de discos mais rápidos, pode ser uma solução para melhorar o desempenho.

A monitoração do desempenho ajuda a determinar qual o componente que está sendo o principal limitador do desempenho do sistema (o ‘gargalo’ do sistema), além de permitir a análise da carga de trabalho a qual o respectivo componente está submetido (por exemplo, o processador está com 80% de utilização, o sistema de discos está constantemente com dados na fila de espera para leitura e gravação e assim por diante). O administrador também pode utilizar a monitoração do desempenho para fazer uma estimativa do crescimento na utilização dos componentes do sistema. Com isso fica mais fácil fazer uma previsão sobre as necessidades futuras de atualizações de Hardware. Além disso, de posse de dados de monitoração consistentes, fica mais fácil justificar o gasto envolvido na aquisição e atualização de componentes de hardware.

A monitoração é feita através do console Desempenho, também conhecido como System Monitor. Este console é acessado através da opção Desempenho, no menu Ferramentas administrativas. No console de desempenho você adiciona “Objetos” a serem monitorados. Um exemplo de objeto pode ser um Processador, Memória, Disco físico, Fila de impressão, etc. Um objeto representa um elemento que pode ser monitorado pelo Windows Server 2003. Para cada objeto, estão disponíveis vários contadores que são indicativos da utilização dos recursos do respectivo objeto. Por exemplo para o objeto Processador, dentre outros, existem os seguintes contadores: “Porcentagem de tempo do processador”, “Interrupções por segundo” e assim por diante. Para o objeto Fila de impressão, existem os contadores “Total de páginas impressas”, “Trabalhos no spool”, e assim por diante.

Vários objetos e seus respectivos contadores são instalados durante a instalação do Windows Server 2003. A medida que novos serviços ou aplicativos são instalados, novos Objetos e contadores são adicionados. Por exemplo, ao instalar o Microsoft SQL Server 2000, novos objetos são adicionados. Outro exemplo, quando é instalado o servidor Web IIS, novos objetos são adicionados e assim por diante.

Saber exatamente quais objetos e quais contadores utilizar é um processo que envolve testes e muita paciência. Somente com a experiência é que o administrador saberá quais os contadores observar para verificar a existência de problemas de desempenho.

A otimização do desempenho é um processo contínuo. Muitas vezes em uma primeira análise, o administrador descobre que um dos componentes está sendo o gargalo do sistema, por exemplo, a memória RAM. Aí mais memória RAM é acrescentada ao servidor. Pode ser que outro componente passe a ser o gargalo, por exemplo a Placa de rede ou o processador. Monitorar e otimizar o desempenho é um desafio bastante grande, porém é uma necessidade. Não é possível simplesmente trocar de equipamento, toda vez que houver problemas de desempenho, pois isso seria um desperdício de dinheiro.

Também é possível configurar o console Desempenho para que seja feita a captura de dados automaticamente. O administrador pode configurar a captura de dados para que seja feita a captura apenas de determinados contadores de determinados objetos, ou seja, somente aqueles contadores que interessam ao administrador. Com base nesta captura é possível verificar os limites normais de operação para componentes como o Processador, memória RAM e assim por diante. Entenda-se por limites normais de operação, as taxas de utilização dos diversos componentes de hardware e software, durante o horário normal de expediente. Depois faz-se o agendamento de um monitoramento contínuo e compara-se os resultados obtidos com os limites de operação obtidos durante a primeira captura. Quando um determinado componente começar a apresentar aumento na sua taxa de utilização deve ser verificado o motivo para este aumento e, se for o caso, providenciar a substituição do dispositivo antes que a sua taxa de utilização atinja limites que possam comprometer o desempenho do servidor.

## Contadores a serem monitorados em servidores.

Na tabela a seguir, da ajuda do Windows Server 2003, apresento uma lista de contadores que a Microsoft recomenda que sejam monitorados permanentemente nos servidores da rede.

| Componente | Aspecto do desempenho sendo monitorado  | Contadores a monitorar |
|------------|---|------------------------|
| Disco      | Uso PhysicalDisk\Leituras de disco/s<br>PhysicalDisk\Gravações de disco/s<br>LogicalDisk%\ de espaço livre<br>Interprete cuidadosamente o contador % tempo de disco. Como a instância _Total desse contador pode não refletir com precisão o uso em sistemas de vários discos, é importante usar também o contador % Tempo ocioso. Observe que esses contadores não podem exibir um valor acima de 100%.  |                        |
| Disco      | Gargalos Disco físico\ Comprimento médio da fila de disco (todas as instâncias)   |                        |
| Memória    | Uso Memória\Bytes disponíveis<br>Memória\Bytes de cache   |                        |
| Memória    | Gargalos ou vazamentos Memória\Páginas/s<br>Memória\Leituras de página/s<br>Memória\Falhas de transição/s<br>Memória\Bytes de pool paginável<br>Memória\Bytes de memória não-paginável<br>Embora não sejam especificamente contadores do objeto Memória, as opções a seguir também são úteis para análise de memória:<br>Arquivo de paginação%\ uso (todas as instâncias)<br>Cache\Acertos de mapa de dados %<br>Servidor\Bytes de pool paginável e Servidor\Bytes de memória não-paginável |                        |

| Componente  | Aspecto do desempenho sendo monitorado  | Contadores a monitorar   |
|-------------|---|--|
| Rede        | Taxa de transferência<br>Interface de rede\Total de bytes/s<br>Interface de rede\Pacotes/s<br>Servidor\Total de bytes/s ou Servidor\Bytes transmitidos/s e Servidor\Bytes recebidos/s | Contadores de transmissão de protocolo (varia de acordo com o protocolo de rede); para TCP/IP:<br>Interface de rede\Total de bytes/s<br>Interface de rede\Pacotes/s<br>Servidor\Total de bytes/s ou Servidor\Bytes transmitidos/s e Servidor\Bytes recebidos/s |
| Processador | Uso Processador%\ tempo de processador ( todas as instâncias)   |  |
| Processador | Gargalos Sistema\Comprimento da fila de processador (todas as instâncias)<br>Processador\Interrupções/s<br>Sistema\Alternâncias de contexto/s   |  |

## Valores indicativos de limites de desempenho para contadores.

Definir exatamente qual é o limite aceitável para o valor de um ou mais contadores não é uma ciência exata. Por exemplo, afirmar que sempre que a taxa de utilização do processador se mantiver em torno de 80%, por longos períodos, é um indicativo de queda no desempenho ou um indicativo de que o processador deve ser substituído, não é algo preciso. Claro que existem valores para determinados contadores que servem para disparar o alarme, isto é, servem para alertar o administrador que uma parte do sistema pode estar sendo responsável pela queda de desempenho, ou seja, pode estar sendo o que chamamos de ‘gargalo do sistema’.

Na tabela a seguir, da Ajuda do Windows Server 2003, apresento alguns valores para determinados contadores, valores estes que, pelas recomendações da Microsoft, devem servir de alerta ao administrador.

| Recurso | Objeto\Contador  | Limite sugerido                             | Comentários  |
|---------|--|---|--|
| Disco   | Disco físico%\ espaço livre<br>Disco lógico%\ espaço livre             | 15%   |  |
| Disco   | Disco físico%\ tempo de disco<br>Disco lógico%\ tempo de disco         | 90%   |  |
| Disco   | Disco físico\Leituras de disco/s,<br>Disco físico\Gravações de disco/s | Depende das especificações<br>do fabricante | Verifique a taxa de transferência<br>especificada para seus discos, para<br>ter certeza de que ela não<br>ultrapassa as especificações. Em<br>geral, os discos Ultra Wide SCSI<br>podem gerenciar de 50 a 70<br>operações de E/S por segundo.<br>Observe que o fato de a E/S ser<br>seqüencial ou aleatória pode ter<br>um forte efeito sobre os valores de<br>leituras de disco/s e gravações de disco/s. |

**IMPORTANTE:** Para o exame é de fundamental importância que você saiba quais os valores limites para os contadores indicados na tabela a seguir. Valor limite significa que uma vez atingido este valor, o respectivo objeto está causando um problema de desempenho e deve ser substituído ou deve ser feito um Upgrade.

| Recurso              | Objeto\Contador                                 | Limite sugerido  | Comentários   |
|----------------------|---|--|---|
| Disco                | Disco físico\Comprimento da fila de disco atual | Número de eixos mais 2   | Esse contador é instantâneo. Observe seu valor durante vários intervalos. Para obter uma média ao longo do tempo, use Disco físico\ Comprimento médio da fila de disco.   |
| Memória              | Memória\Bytes disponíveis                       | Para computadores com mais memória, mais de 4 MB                                 | Pesquise o uso da memória e adicione memória se necessário.   |
| Memória              | Memória\Páginas/s                               | $n$ páginas/s por arquivo de paginação   | Pesquise a atividade de paginação. Observe o volume de E/S transferido para os discos com arquivos de paginação.  |
| Arquivo de paginação | Arquivo de paginação%\ uso                      | Acima de 70%   | Revise este valor juntamente com Bytes disponíveis e Páginas/s para entender a atividade de paginação do computador.  |
| Processador          | Processador%\ tempo de processador              | 85%  | Descubra o processo que está usando uma alta porcentagem do tempo do processador. Atualize para um processador mais rápido ou instale um processador adicional.   |
| Processador          | Processador\Interrupções/s                      | Depende do processador; um bom ponto de partida é 1.000 interrupções por segundo | Um aumento brusco no valor desse contador, sem um aumento correspondente na atividade do sistema, indica um problema de hardware. Identifique o adaptador de rede, o disco ou outro tipo de hardware que está causando as interrupções. |
| Servidor             | Servidor\Total de bytes/s                       |  | Se a soma de Total de bytes/s para todos os servidores for aproximadamente igual às taxas de transferência máximas de sua rede, convém segmentar a rede.  |

| Recurso              | Objeto\Contador                                   | Limite sugerido          | Comentários   |
|----------------------|---|--------------------------|---|
| Servidor             | Servidor\Falta de itens de trabalho               | 3                        | Se o valor atingir este limite, considere adicionar as entradas DWORD InitWorkItems (o número de itens de trabalho alocados para um processador durante a inicialização) ou MaxWorkItems (o número máximo de buffers de recebimento que um servidor pode alocar) no Registro (em HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters). A entrada InitWorkItems pode variar de 1 a 512, enquanto MaxWorkItems pode variar de 1 a 65.535. Comece por qualquer valor para InitWorkItems e um valor igual a 4.096 para MaxWorkItems e dobre esses valores até que o limite de Servidor\Falta de itens de trabalho fique abaixo de 3. |
| Servidor             | Servidor\Pico de pool paginável                   | Quantidade de RAM física | Esse valor é um indicador do tamanho máximo do arquivo de paginação e da quantidade de memória física.  |
| Servidor             | Filas de trabalho do servidor\Comprimento da fila | 4                        | Se o valor atingir esse limite, poderá haver um gargalo no processador. Esse contador é instantâneo. Observe seu valor durante vários intervalos.   |
| Vários processadores | Sistema\Comprimento da fila de processador        | 2                        | Esse contador é instantâneo. Observe seu valor durante vários intervalos.   |

Claro que estes são apenas valores sugeridos, os quais servem como alertas para o administrador. Conforme descrito anteriormente, o processo de monitoração é um processo contínuo, de acompanhamento na evolução dos principais contadores, sugeridos anteriormente.

A seguir apresento de uma forma resumida, os principais contadores e respectivos limites, ou seja, valores que podem indicar que o problema é com o respectivo componente:

- ◆ **Processador\% tempo de processador:** Não deve estar por longos períodos acima dos 80%
- ◆ **Sistema\Comprimento da fila de processador:** Não deve ser maior do que 2.
- ◆ **LogicalDisk\Comprimento da fila de disco atual:** Se este valor estiver constantemente acima de 2, o sistema de discos deve ser substituído por um sistema mais rápido. Por exemplo, se os discos forem IDE, você pode substituir por um sistema SCSI. Outra alternativa é implementar um Volume Set sem Paridade.
- ◆ **LogicalDisk\Comprimento da fila de disco atual:** Valem os mesmos comentários do item anterior.
- ◆ **Memória\Páginas/s:** Um valor maior do que 20, pode indicar a necessidade de um Upgrade de memória, normalmente com a adição de mais memória RAM.
- ◆ **Memória\Bytes confirmados:** Deve ser sempre menor do que a quantidade total de memória instalada.

## Configurando o console Desempenho para capturar dados automaticamente.

Na introdução sobre a monitoração de desempenho, falei sobre a possibilidade de configurar o console Desempenho para efetuar a captura automática de dados, conforme destacado no trecho a seguir:

“Também é possível configurar o console Desempenho para que seja feita a captura de dados automaticamente. O administrador pode configurar o console desempenho para que sejam capturados dados sobre os Objetos/contadores a serem monitorados. Com base nesta captura, o administrador pode verificar os limites normais de operação para componentes como o Processador, memória RAM e assim por diante. Depois faz-se um monitoramento contínuo e compara-se os resultados obtidos com os limites de operação obtidos em outras medições. Quando um determinado componente começar a apresentar aumento na sua taxa de utilização o administrador deve verificar o motivo para este aumento e, se for o caso, providenciar a substituição do elemento que está apresentando elevação em suas taxas de utilização, antes que a sua taxa de utilização atinja limites que possam comprometer o desempenho do servidor.”

Conforme pode ser concluído pelo parágrafo anterior, o principal objetivo em configurar a coleta automática de dados é para determinar quais as taxas normais de utilização dos componentes a serem monitorados, em situação normal de uso. Depois são feitas novas observações para acompanhar a evolução destas taxas de ocupação, para poder agir preventivamente quando um determinado componente estiver atingindo níveis elevados de utilização.

A captura automática de dados é feita utilizando a opção Logs e alertas de desempenho, do console Desempenho. Com esta opção, você pode coletar automaticamente dados de desempenho de computadores locais ou remotos. Você pode visualizar os dados que foram gravados no log usando a opção Monitor do sistema ou exportar os dados para programas de planilha ou banco de dados, para fins de análise e geração de relatórios. Por exemplo, você pode importar os dados gravados em um log de desempenho, para um banco de dados do Microsoft Access e utilizar estes dados para a criação de relatórios personalizados.

Com a opção Logs e alertas de desempenho, estão disponíveis os seguintes recursos:

- ◆ Coleta de dados em formato separado por vírgulas ou por tabulações para facilitar a importação por programas de planilha ou programas de banco de dados. É fornecido também um formato de arquivo de log binário para

**IMPORTANTE:** Certifique-se de que você conhece os limites para os contadores da lista anterior e que entendeu o funcionamento de cada um destes contadores. Este é um ponto importante para o exame

registro em log circular ou para registro em log de instâncias, como segmentos ou processos, que podem começar depois do início da coleta de dados. (O registro em log circular é o processo de registro contínuo de dados em um único arquivo, sobrepondo os dados anteriores com novos dados.)

- ◆ Você também pode coletar dados em formato de banco de dados SQL. Essa opção define o nome de um banco de dados SQL e conjunto de logs existentes dentro do banco de dados em que os dados de desempenho serão lidos ou gravados. Esse formato de arquivo é útil ao coletar e analisar dados de desempenho de toda a empresa, em vez de servidor por servidor. Por exemplo, a partir de um único console Desempenho, você pode obter dados sobre diversos servidores da rede e armazenar estes dados centralizadamente em um único banco de dados do SQL Server.
- ◆ Os dados do contador coletados podem ser visualizados durante a coleta ou após seu término.
- ◆ Como o log funciona da mesma maneira que um serviço do Windows Server 2003, a coleta de dados ocorre independentemente de haver um usuário logado ou não, no servidor que está sendo monitorado.
- ◆ Você pode definir os momentos de início e parada, nomes de arquivos, tamanho máximo de arquivo e outros parâmetros para a geração automática do log.
- ◆ Você pode gerenciar várias sessões de log em uma única janela de console.
- ◆ Você pode definir um alerta em um contador, especificando que uma mensagem seja enviada, um programa seja executado e uma entrada seja feita no log de eventos do Windows Server 2003 ou um log seja iniciado quando o valor do contador selecionado for superior ou inferior a uma configuração especificada. Por exemplo, você pode monitorar a taxa de utilização do processador e solicitar que o Administrador seja avisado quando esta taxa ultrapassar um determinado patamar, digamos 85 %, ou você pode monitorar o espaço livre em todas as unidades de disco ou em todos os volumes, de todos os servidores da rede e pedir que seja disparado um alerta para o administrador, sempre que uma unidade apresentar espaço livre inferior a 20%.

**IMPORTANTE:** Lembre-se que quando houver a necessidade de capturar dados de desempenho de diversos servidores e consolidar estas dados em um único banco de dados, a opção mais indicada é fazer com que os dados obtidos, sejam gravados em um banco de dados do SQL Server 2000.

**IMPORTANTE:** Para que a coleta de dados possa funcionar corretamente, o serviço "Logs e alertas de desempenho" deve ter sido inicializado corretamente. Antes de prosseguir você irá verificar (no exemplo logo a seguir) se este serviço está configurado para inicialização automática. Caso não esteja, irá configurá-lo para que seja inicializado automaticamente.

## Mais um resumo de contadores, para você não esquecer:

A seguir coloco uma lista resumida (em relação a lista apresentada anteriormente) dos contadores mais comumente utilizados para verificação do desempenho do computador como um todo e que são candidatos a serem configurados para coleta automática, utilizando logs de desempenho. Esta lista é obtido na documentação oficial do Windows Server 2003.

Contadores para identificar gargalos em recursos de memória:

- ◆ Memória\Bytes disponíveis
- ◆ Memória\Páginas/s

Contadores para identificar gargalos em recursos de disco:

- ◆ PhysicalDisk -> % tempo de disco e % Tempo ocioso
- ◆ PhysicalDisk -> Leituras de disco/seg e Gravações de disco/seg

- ◆ PhysicalDisk -> Comprimento médio da fila de disco
- ◆ LogicalDisk -> % de espaço livre

Contadores para identificar gargalos em recursos do processador:

- ◆ Processador -> Interrupções por segundo
- ◆ Processador -> % tempo de processador
- ◆ Processo(processo) -> % tempo de processador
- ◆ Sistema -> Comprimento da fila de processador

Contadores para identificar gargalos em recursos de rede:

- ◆ Interface de rede -> Total de bytes/segundo, Bytes enviados/s e Bytes recebidos/s
- ◆ Objeto\_de\_camada\_de\_protocolo -> Segmentos recebidos/s, Segmentos enviados/s, Quadros enviados/s e Quadros recebidos/s
- ◆ Servidor -> Total de bytes/segundo, Bytes recebidos/s e Bytes enviados/s

Contadores para identificar gargalos em recursos de impressora:

- ◆ Fila de impressão -> Bytes impressos/s
- ◆ Fila de impressão -> Erros de trabalhos

**NOTA:** O administrador pode configurar alertas com base em contadores de desempenho. Por exemplo, posso configurar um alerta que é disparado sempre que um determinado contador atinge um valor limite. Podem ser configuradas diferentes ações como resposta a um alerta: Enviar uma mensagem para um usuário, normalmente o Administrador, Gravar um evento no log de eventos do Windows Server 2003, executar um programa ou iniciar a captura de dados de desempenho, com base nas configurações de um log pré-definido.

**IMPORTANTE:** Monitore contadores de memória para determinar se a paginação excessiva está sobrecregando o disco. Quando o computador tem pouca memória, o Windows Server 2003 é obrigado a utilizar intensivamente os arquivos de paginação (Swap). O arquivo de trocas fica na raiz do disco C:, com o nome de pagefile.sys ou pode também ficar em outros discos e até mesmo distribuídos em dois ou mais discos, conforme configurações efetuadas pelo administrador. Com o uso intenso do arquivo de trocas, as taxas de utilização do disco rígido aumentam significativamente, porém o problema não é com o sistema de discos e sim devido à falta de memória (que é a causa da paginação excessiva). Ao acrescentar mais memória RAM, você irá reduzir a utilização do arquivo pagefile.sys e, consequentemente, reduzir as taxas de utilização do disco rígido.

## Ferramentas de recuperação a desastres.

Sem dúvidas, a principal ferramenta de recuperação a desastres é o Backup/Restore, já descrito anteriormente neste resumo. Nunca é demais salientar que é de fundamental importância que você conheça os tipos de backup e como utilizá-los em diferentes estratégias de Backup/Restore. Também é importante que você revise os tópicos sobre o processo de Boot do Windows Server 2003, o arquivo Boot.ini e os caminhos ARC e o tópico sobre a Registry d Windows Server 2003, tópicos estes apresentados no Capítulo 12.

## O Modo Seguro, Last Know Good Configuration e Control Sets..

Neste tópico veremos conceitos importantes, principalmente quando acontecem problemas na reinicialização do sistema. Vamos tratar dos seguintes tópicos:

**NOTA:** Um número muito elevado de Interrupções por segundo pode ser causado por problemas em um dispositivo de Hardware, ou em um driver de hardware, conforme descrito anteriormente.

- ◆ Opções de inicialização do Windows Server 2003 e o Modo seguro.
- ◆ Last Known Good Configuration e Control Sets.

## Opções de inicialização do Windows Server 2003 e o Modo seguro.

Ao inicializar o Windows Server 2003, será exibido um menu de opções (caso esteja instalada mais de uma versão do Windows Server 2003), menu este que é montado a partir de informações do arquivo boot.ini, conforme descrito anteriormente. Este menu somente é montado e exibido se existirem, pelo menos duas opções de inicialização diferentes, no arquivo boot.ini. Consideramos como sendo “diferentes opções de inicialização”, diferentes versões do Windows (9x, Me, NT, 2000 ou XP) ou uma mesma versão com diferentes chaves de inicialização como por exemplo /fastdetect e /basevideo. Se houver uma única opção o menu não será exibido.

Quando o menu é exibido você pode selecionar uma das opções do menu e pressionar Enter. Logo após pressionar Enter é exibida a mensagem Iniciando ... Se neste momento você pressionar a tecla F8, será exibido um menu de opções avançadas de inicialização. Se não for exibido o menu, ou seja, se houver uma única opção de inicialização, você deve ficar atento à tela do computador. Quando as primeiras mensagens começarem a aparecer na tela, você deve pressionar a tecla F8 para exibir o menu com as opções avançadas de inicialização, opções estas que serão descritas neste item.

No Windows Server 2003 você pode pressionar a tecla F8 enquanto o menu de inicialização, com as diferentes versões do Windows estiver sendo exibido. Ao pressionar F8 será exibido o menu de opções avançadas do Windows, no qual são exibidas as seguintes opções de inicialização:

- ◆ Safe Mode (Modo seguro)
- ◆ Safe Mode with Networking (Modo seguro com rede)
- ◆ Safe Mode with Command Prompt (Modo seguro com prompt de comando)
- ◆ Enable Boot Logging (Ativar log de inicialização)
- ◆ Enable VGA Mode (Ativar modo VGA)
- ◆ Last Known Good Configuration (Última configuração válida)
- ◆ Directory Service Restore Mode (Modo de restauração de serviços de diretório (só control. de domínio))
- ◆ Debugging Mode (Modo de depuração)

É comum utilizarmos o menu de opções avançadas quando estamos com problemas na inicialização do Windows Server 2003. Nestas situações, as opções do menu avançado podem nos ajudar na solução de problemas, conforme veremos na seqüência. Vamos analisar cada uma destas opções, iniciando pelas opções de Modo seguro.

## Entendendo o Modo seguro de inicialização – Safe mode.

Quando o Windows Server 2003 não está conseguindo inicializar no modo Normal, temos a opção de inicializá-lo no Modo seguro. No Modo seguro apenas os drivers e serviços estritamente necessários à inicialização do sistema são carregados. O sistema é inicializado utilizando um driver de vídeo padrão VGA, com resolução de 640x480 e com suporte a milhões de cores (24 bits), com suporte ao mouse, teclado, monitor, sistema de armazenamento local (discos rígidos, disquete, etc). Os programas configurados para serem inicializados automaticamente são ignorados no Modo seguro. Todo este cuidado é tomado para que o Windows Server 2003 possa inicializar, mesmo que com um conjunto mínimo de drivers e serviços. Uma vez inicializado, você poderá alterar as configurações que estão impedindo que o Windows Server 2003 initialize no modo Normal.

A maioria das ferramentas de configuração estão disponíveis no modo Seguro, para que você possa fazer as configurações necessárias, para corrigir os problemas que estão impedindo o Windows Server 2003 de inicializar no modo Normal. Por exemplo, no modo Seguro temos acesso ao Painel de controle, às Ferramentas Administrativas, ao utilitário de Backup, ao Editor de registro, às configurações de rede e assim por diante.

Se você desconfia que o problema é com algum hardware recém instalado ou com o driver de hardware instalado, utilize o Gerenciador de dispositivos para verificar se existe algum problema de hardware. Se o Windows Server 2003 consegue inicializar no modo Seguro é porque os serviços básicos do Sistema Operacional estão funcionando corretamente. Se o Windows Server 2003 deixou de inicializar normalmente após a instalação de um driver é provável que o respectivo driver seja a causa do problema. Estando no Modo Seguro você pode utilizar o Gerenciador de Dispositivos para desinstalar ou desabilitar o driver que está causando problemas. Uma vez desabilitado o referido driver, o Windows Server 2003 deverá voltar a inicializar normalmente.

Ao fazer a inicialização no Modo Seguro, o Windows Server 2003 vai exibindo cada driver e serviço que vai sendo carregado. A inicialização no Modo Seguro utiliza a chave /sos, já descrita anteriormente. Ao iniciar o computador no modo Seguro você deve fazer o logon como Administrador ou com uma conta do tipo Administrador do computador, para que você possa ter acesso a todas as configurações do Windows Server 2003 e fazer as alterações necessárias. Após fazer o logon uma mensagem é emitida, avisando sobre as limitações do Modo seguro e perguntando se você realmente deseja entrar neste modo, conforme indicado na Figura 14.56. Clique em Sim e o Windows Server 2003 será carregado no Modo seguro.

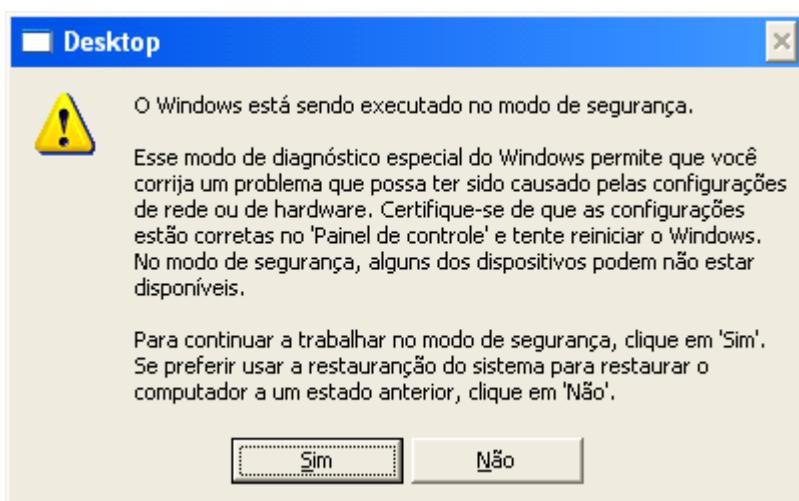


Figura 14.56 Confirmação para entrar no Modo Seguro.

Uma vez tendo feita as alterações necessárias você deve reiniciar o computador para testar se as alterações que foram feitas surtiram o efeito desejado, qual seja, permitir que o Windows Server 2003 possa voltar a inicializar no modo Normal.

Se você precisa acessar recursos da rede, ao invés da opção Modo seguro, deve selecionar a opção Modo seguro com rede. Com esta opção o sistema de rede do Windows será carregado (desde que não existam problemas que impeçam a carga dos componentes de rede) e, mesmo no Modo Seguro, você terá acesso aos recursos da rede.

---

**NOTA: O Modo Seguro também é conhecido como Modo de Segurança. As duas expressões são sinônimos.**

---

A opção Modo seguro com prompt de comando carrega o Windows Server 2003 porém não carrega a interface gráfica, mas sim a interface de linha de comando (Cmd.exe) com suporte a todos os comandos reconhecidos pelo Windows Server 2003. Devido às facilidades da interface gráfica, dificilmente alguém vai optar por esta opção, a não ser que você seja um fã de carteirinha da interface baseada na linha de comando.

Em resumo podemos afirmar que o Modo Seguro (ou Modo de Segurança) é uma ferramenta especialmente útil quando o Windows Server 2003 está com problemas para inicializar no Modo Normal. Nestas situações podemos inicializar no Modo Seguro e fazer as alterações necessárias para que o Windows Server 2003 possa voltar a inicializar no modo Normal.

Agora vamos entender um pouco melhor a opção Ultima configuração válida (Last Know Good Configuration) e a sua relação com os chamados Control Sets. Na parte final deste item trataremos das demais opções do Menu de opções avançadas do Windows.

## Last know good configuration e Control Sets.

A opção Última configuração válida é indicada em situações onde a instalação de um novo driver está causando problemas sérios, impedindo que o Windows Server 2003 possa inicializar normalmente. Vamos supor que você baixou da Internet uma nova versão para o driver da placa de rede do servidor. Você instala a nova versão do driver e ao reiniciar o computador, o Windows Server 2003 não consegue inicializar normalmente. Nesta situação você pode inicializar utilizando as opções avançadas do menu de inicialização e selecionar a opção Last know good configuration. Com isso serão carregadas as configurações da última configuração com a qual o Windows Server 2003 conseguiu inicializar normalmente, ou seja, as configurações anteriores a atualização do driver que está causando o problema.

Ao selecionar a opção Last know good configuration o Windows Server 2003 será inicializado usando as informações da Registry que o Windows Server 2003 salvou na última vez que você fez o logon no Windows Server 2003 com sucesso, ou seja, as informações da Última configuração válida. As informações sobre a Última configuração válida são armazenadas na Registry do Windows Server 2003.

Ao inicializar um computador com o Windows Server 2003 estão disponíveis duas configurações para inicialização: Default and LastKnownGood. Estas configurações são conhecidas como Control Sets. Um Control Set é um conjunto de configurações da Registry, configurações estas utilizadas para inicializar o computador. Quando você faz o logon no Windows Server 2003 normalmente e faz alterações nas configurações, como por exemplo instalar uma nova versão de um driver, estas alterações são salvas no Current control set. Ao encerrar o Windows Server 2003 (Shutdown) as alterações são copiadas para o control set Default. Na próxima vez que você fizer o logon com sucesso, as configurações do control set Default serão copiadas para o control set Last Known Good Configuration. Se você não conseguir fazer o logon com sucesso devido às últimas alterações, você tem a opção de reinicializar o sistema e utilizar a opção Last know good configuration. Observe que as configurações da Última configuração válida somente são sobrescritas depois que você faz as alterações, reinicia o computador e consegue fazer o logon com sucesso. Se devido às alterações você não conseguir fazer o logon ou sequer reiniciar o Windows Server 2003, as configurações da Última configuração válida não serão sobrescritas e você terá a opção de carregá-las na próxima inicialização, revertendo as alterações que foram feitas e estão impedindo o Windows Server 2003 de inicializar corretamente.

**IMPORTANTE: O Modo seguro com rede não funcionará em computadores portáteis que estão utilizando cartões PCMCIA de rede. O suporte a cartões PCMCIA é desabilitado no Modo seguro, mesmo quando você seleciona a opção Modo seguro com rede.**

Você pode utilizar a Última configuração válida em situações tais como:

- ◆ Você instalou uma novo driver ou uma nova versão de um driver existente e o Windows Server 2003 não consegue mais inicializar corretamente. Nesta situação você pode reiniciar utilizando a opção Last know good configuration. Com isso as configurações anteriores a alteração que não está funcionando serão carregadas e o Windows Server 2003 volta a inicializar normalmente.
- ◆ Por engano ou por sabotagem um dispositivo fundamental, como por exemplo o controlador IDE foi desabilitado. Se um dispositivo como o controlador IDE for desabilitado, o Windows Server 2003 não conseguirá inicializar normalmente. Nestas situações você pode utilizar a Última configuração válida para restaurar as configurações que estavam funcionando normalmente.

## Outras opções de configuração do Menu de opções avançadas do Windows.

Vamos analisar as demais opções do Menu de opções avançadas.

- ◆ Ativar log de inicialização: Ao selecionar esta opção o Windows Server 2003 cria um log com a descrição da carga e inicialização de drivers e serviços. Este log é gravado em um arquivo chamado NTBTLOG.TXT, o qual é gravado na pasta onde o Windows Server 2003 está instalado. Ao inicializar o Windows Server 2003 no Modo Seguro este log também é automaticamente criado.
- ◆ Ativar modo VGA: Esta opção inicializa o Windows Server 2003 utilizando um driver VGA com configurações mínimas. Esta opção é útil quando você está tendo problemas com o driver da placa de vídeo ou do monitor.
- ◆ Última configuração válida: Já descrita anteriormente.
- ◆ Modo de depuração: Inicializa o Windows Server 2003 no modo de depuração do Kernel.

**IMPORTANTE:** Lembre que se após ter feito alguma alteração, o Windows Server 2003 reiniciar e você conseguir fazer um logon, as configurações do control set Last Know Good Configuration serão sobreescritas pelas configurações atuais. Nesta situação você não poderá mais utilizar a opção Última configuração válida, para voltar à situação anterior. Para estas situações é que existe a opção Restauração do sistema, a qual veremos mais adiante.

## O recurso ASR – Automated System Recovery Disks

No Windows NT Server 4.0 e no Windows 2000 Server o administrador pode criar um disco chamado ERD – Emergency Repair Disk. Este disco contém informações que podem ser utilizadas para reparar o servidor em situações de emergência, como por exemplo quando um arquivo de inicialização (ntldr, ntoskrnl.exe, etc.) é corrompido. O administrador pode dar um boot usando o CD do Windows 2000 Server, iniciar a instalação e bem no início informar que será feita uma reparação de uma instalação já existente. Neste momento é que será necessário o disquete ERD. Já no Windows Server 2003 este procedimento mudou bastante. Não existe mais o conceito de ERD. Ao invés disso foi criado o chamado ASR - Automated System Recovery (recuperação automatizada do sistema).

O administrador pode criar um conjunto de discos ASR, regularmente, como parte de um plano de recuperação do sistema em caso de falhas. Os discos do ASR contêm informações fundamentais para o funcionamento do Windows Server 2003, informações estas que podem ser utilizadas para substituir arquivos corrompidos, corrigir defeitos no setor de boot e no ambiente de inicialização do Windows Server 2003. O recurso ASR deve ser utilizado como uma

última tentativa de recuperar o sistema, depois que várias outras tentativas foram esgotadas, tais como usar o modo seguro, a opção Last Known Good Configuration e o console de recuperação (que será descrito mais adiante).

O recurso ASR é composto de duas partes: O backup ASR e o restore ASR. Para fazer o Backup ASR, utilizamos o Automated System Recovery Preparation (Assistente de preparação para a recuperação do sistema) do ASR, o qual está disponível como uma das opções do utilitário de backup. Este assistente faz o backup do estado do sistema, dos serviços configurados e de todos os discos associados com a instalação do Windows Server 2003. Também é criado um disquete, qual contém informações sobre o backup, configurações dos discos do sistema (incluindo informações dos discos básicos e discos dinâmicos) e informações sobre como deve ser efetuada a restauração do sistema. Este disquete é denominado ASR disk ou disco ASR.

Para fazer a restauração do sistema, usando os discos criados pelo assistente de backup do ASR, você deve iniciar uma instalação normal do Windows Server 2003 (por exemplo, a partir de um boot pelo CD-ROM, usando o CD de instalação do Windows Server 2003). Em uma das etapas da instalação, bem no início, ainda na parte de texto, tem uma mensagem informando que você pode pressionar a tecla F2 para fazer uma restauração do sistema. Nesta etapa você pressiona F2 e será solicitado que você insira o disquete ASR no drive. O ASR lê as informações sobre os discos do sistema a partir do disquete ASR e restaura todas as assinaturas de discos, volumes e partições, pelo menos nos discos necessários para que o Windows Server 2003 seja inicializado. O ASR tentará restaurar as configurações de todos os discos e volumes/partições, mas pode acontecer de ele não conseguir restaurar as informações sobre todos os volumes. O ASR irá instalar uma versão simplificada do Windows Server 2003, apenas com o suficiente para iniciar um restore a partir do backup feito pelo ASR, utilizando o Automated System Recovery Preparation Wizard, backup este que normalmente é feito em fita.

Observações sobre o ASR:

- ◆ O ASR não faz o backup dos arquivos de dados, apenas dos arquivos do sistema, necessários ao funcionamento do ASR. O backup dos dados deve ser feito separadamente, usando uma política de backup e agendamento de tarefas de backup, conforme descrito no Capítulo 8.
- ◆ O ASR tem suporte a volumes FAT16 com tamanho máximo de 2.1 GB. O ASR não tem suporte para volumes FAT16 com tamanho de 4 GB, volumes estes que utilizam um tamanho de cluster de 64 Kb. Se o servidor tiver uma partição FAT 16 de 4 GB (o que é muito pouco provável), primeiro você deve converter este volume para NTFS, para depois usar o ASR. Para converter um volume de FAT16 ou FAT32 para NTFS basta usar o comando convert. Por exemplo, para converter o drive C: de FAT para NTFS, utilize o seguinte comando:  
**convert C: /fs:NTFS**

Após a criação do Backup via ASR, ele poderá ser utilizado para restaurar o servidor em caso de falhas graves. Para usar o backup do ASR você deve iniciar uma instalação do Windows Server 2003 normalmente e, em uma das etapas iniciais, fique atento a mensagem que indica que você deve pressionar a tecla F2 para restaurar o estado do sistema usando um backup do ASR.

O que é contém o disquete do ASR: O disquete do ASR é como se fosse um “mapa” para encontrar as demais informações necessárias ao processo de restauração. No disquete do ASR são gravados os seguintes arquivos:

- ◆ **Setup.log**: Contém a localização dos arquivos do sistema.
- ◆ **Asr.sif**: Contém informações sobre os discos, partições, volumes e sobre a mídia utilizada para fazer o backup do ASR.
- ◆ **Asrpnp.sif**: Contém informações sobre os dispositivos de hardware, instalados no servidor, e que são compatíveis com o padrão Plug and Play.

---

**IMPORTANTE: O backup do ASR não poderá ser feito diretamente em CD ou DVD, mesmo que você tenha um drive gravador de CD ou gravador de DVD.**

---

## Criando um disquete de boot.

O conceito de disquete de boot no Windows NT, Windows 2000, Windows XP ou Windows Server 2003 é bem diferente do conceito de disquete de boot no Windows 95/98/Me. No Windows 95/98/Me ao usar um disquete de boot, o sistema é inicializado no modo caractere, é aberto um prompt de comando e você tem acesso ao disco rígido e demais unidades de disco. Já no Windows NT/2000/XP/2003, o disquete de boot não inicializa o sistema no modo caractere, com um prompt de comando e acesso aos volumes (C:, D:, etc). Além disso, o uso do disquete de boot terá pouca utilidade, principalmente com a disponibilidade do Console de recuperação, o qual descreverei mais adiante.

Mas existem algumas circunstâncias em que o disquete de boot pode ser útil, mais especificamente para auxiliar na inicialização do sistema, quando ocorrer um dos seguintes problemas:

- ◆ Quando o setor de boot do disco rígido estiver corrompido.
- ◆ Quando o MBR – master boot Record do disco rígido estiver corrompido.
- ◆ Quando um vírus tiver infectado o MBR.
- ◆ Quando os arquivos ntldr ou ntdetect.com estiverem corrompidos ou tiverem sido excluídos por engano.

**IMPORTANTE:** Outra situação prática em que o disco de boot pode ser útil é quando você tem um volume espelhado, no qual está instalado o Windows Server 2003. Pode acontecer do disco principal do espelhamento (aquele a partir do qual o Windows Server 2003 é carregado) apresentar problemas. Neste caso você pode usar um disquete de boot, alterando o arquivo boot.ini para que carregue o Windows Server 2003 a partir do disco que ainda está funcionando. O Windows Server 2003 é carregado normalmente. Aí você desfaz o espelhamento, desliga o servidor e substitui o disco com problemas. Em seguida você usa o disquete de boot novamente para inicializar o servidor, reconhece o disco recém instalado e refaz o espelhamento. Pronto, o próximo boot já pode ser feito a partir do novo HD instalado e devidamente espelhado. Este método dá bem menos trabalho (e tem bem menos probabilidade de dar problemas) do que usando um backup tradicional, principalmente se o servidor for um DC, onde são necessários cuidados especiais para o restore do Active Directory, conforme descrito no Capítulo 8.

**IMPORTANTE:** Sempre que você estiver para fazer alterações importantes no servidor, tais como instalação de novos dispositivos de hardware ou instalação de novos serviços e sistemas, é recomendado que, antes de fazer as modificações, você faça um backup do ASR. Com isso, você poderá usar este backup para restaurar o servidor a uma situação de normalidade, caso aconteça algum erro grave, devido as modificações que estão sendo feitas. É importante salientar novamente, que o restore a partir de um backup do ASR deve ser considerado como uma última alternativa, quando outros recursos como o Modo de segurança e a última configuração válida já falharam. Alterações tais como inserção de um novo disco ou exclusão de volumes e criação de novos volumes também podem ser consideradas grande alterações e, consequentemente, antes de fazer estas alterações, crie um novo backup do ASR. Após ter feito as alterações e o servidor estar funcionando normalmente, é hora de criar o backup do ASR novamente, para que agora ele já contenha as últimas alterações, as quais estão funcionando sem problemas.

**IMPORTANTE:** O disco de boot que você cria em um servidor, servirá para inicializar este servidor e não qualquer servidor com o Windows Server 2003. Na prática outros servidores poderão ser inicializados, mas somente se tiverem exatamente as mesmas configurações de discos e de volumes, do servidor onde foi feito o disquete de boot.

Exemplo: Para criar um disquete de boot para um determinado servidor, siga os passos indicados a seguir:

1. Faça o logon como administrador ou com uma conta com permissão de administrador.
2. Insira um disquete em branco no drive de disquete
3. Abra um Prompt de comando: Iniciar -> Todos os programas -> Acessórios -> Prompt de comando.
4. Execute o comando format a: /u
5. Aguarde a conclusão do comando e copie os arquivos Ntdetect.com e Ntldr, da pasta i386 do CD de instalação do Windows Server 2003, para o disquete. Copie também o arquivo Boot.ini, que se encontra na raiz do C:\.
6. Pronto, está criado o CD de boot, o qual é específico para o servidor onde foi criado e que poderá ser utilizado nas situações descritas no início deste tópico.

## O Console de Recuperação.

O Console de Recuperação foi uma das novidades introduzidas com o Windows 2000 Server e que também está presente no Windows XP Professional e no Windows Server 2003. O Console de Recuperação não é instalado, automaticamente, quando o Windows Server 2003 é instalado. Neste item mostrarei como instalar o Console de Recuperação.

Após instalar o console de recuperação, este será adicionado como uma opção do menu de inicialização do computador, conforme descrito anteriormente. Ao selecionar a opção para inicializar no modo de recuperação, o servidor será inicializado em um modo muito parecido com o Prompt de comando. Neste modo estarão disponíveis uma série de comandos (descritos mais adiante). Estão disponíveis comandos para acessar os arquivos do disco rígido, para habilitar/desabilitar drivers e assim por diante.

Se o modo de segurança e outras opções de inicialização não funcionarem, você poderá considerar o uso do Console de recuperação (claro que este deve ter sido instalado previamente). No entanto, esse método é recomendado somente se você for um usuário avançado ou administrador que possa usar comandos básicos para identificar e localizar drivers e arquivos com problemas.

Para usar o Console de recuperação, você precisa efetuar o logon na conta Administrador. Esse console fornece comandos que podem ser usados para executar operações simples, como mudar de diretório ou exibir um diretório, e operações mais complexas, como corrigir o setor de inicialização. Você pode acessar a Ajuda para os comandos no Console de recuperação digitando help no prompt de comando do Console de recuperação.

Ao usar o Console de recuperação, você pode iniciar e interromper serviços, ler e gravar dados em uma unidade local (inclusive unidades formatadas com o sistema de arquivos NTFS), copiar dados de um disquete ou CD, formatar unidades, corrigir o setor de inicialização ou o registro de inicialização mestre (MBR) e executar outras tarefas administrativas. O Console de recuperação será especialmente útil se você precisar reparar o sistema copiando um arquivo de um disquete ou CD-ROM para a unidade de disco rígido ou se precisar reconfigurar um serviço que está impedindo o computador de ser iniciado corretamente. Por exemplo, o Console de recuperação poderia ser usado para substituir um arquivo de driver sobreescrito ou danificado por uma cópia perfeita a partir do disquete.

Exemplo: Para instalar o console de recuperação, siga os passos indicados a seguir:

1. Faça o logon como administrador ou com uma senha com permissão de administrador.
2. Abra um Prompt de comando e acesse a pasta i386, do cd de instalação do Windows Server 2003.
3. Para instalar o console de recuperação, execute o seguinte comando:  
winnt32 /cmdcons

4. Será exibida uma mensagem informando que você pode instalar o console de recuperação como uma das opções de inicialização do computador, conforme indicado na Figura 14.57:

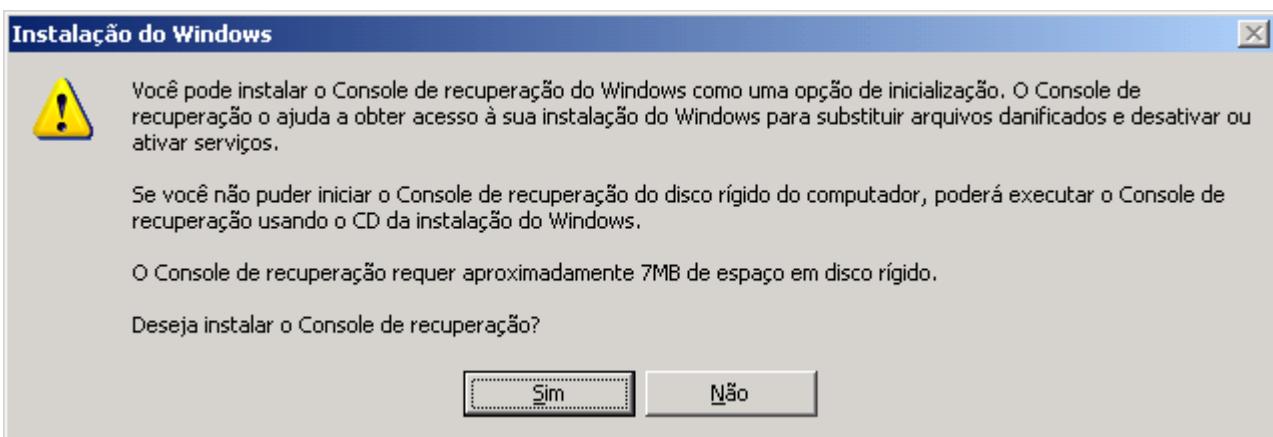


Figura 14.57 Instalando o console de recuperação.

5. Clique em Sim, para prosseguir com a instalação do console de recuperação.  
6. A instalação é concluída e uma mensagem é exibida informando que o console de recuperação foi adicionado como uma das opções de inicialização e que você pode utilizar o comando HELP, para ver uma lista dos comandos disponíveis. Clique em OK para fechar esta mensagem e pronto, o console de recuperação está instalado. No próximo exemplo mostrarei como utilizar o console de recuperação.

Exemplo: Para utilizar o console de recuperação, após tê-lo instalado, siga os passos indicados a seguir:

1. Reinicialize o servidor.
2. Será apresentado um menu, onde a primeira opção é a instalação normal do Windows Server 2003. Se houver outras versões do Windows, estas serão exibidas na seqüência. A última opção é Microsoft Windows Recovery Console (Console de Recuperação do Microsoft Windows). Selecione esta opção e pressione Enter.
3. Após alguns instantes, será exibido um novo menu de opções para que você selecione qual instalação do Windows você deseja acessar. Este menu será exibido mesmo que haja uma única instalação do Windows. Digite o número da instalação a ser carregada e pressione Enter. Nesta etapa você também pode digitar Exit e pressionar Enter para reiniciar o computador.
4. Será solicitada a senha de acesso. Se o servidor for um DC, é importante salientar que está não é a senha da conta Administrator (Administrador) do domínio, mas sim a senha que foi definida durante a instalação do Active Directory, senha esta que também é utilizada para inicializar o servidor no modo de Restauração do Active Directory, conforme descrito no Capítulo 8. Digite a senha e pressione Enter.
5. A inicialização usando o console de recuperação será completada e será exibido um prompt de comando. Para obter uma lista completa dos comandos disponíveis digite help e pressione Enter. Será exibida uma lista com todos os comandos disponíveis no console de recuperação.
6. Para obter ajuda sobre um comando específico, digite help nome\_do\_comando e tecle Enter. Por exemplo para obter ajuda sobre o comando enable, digite help enable e pressione enter.
7. Para sair do console de recuperação e reiniciar o servidor, digite EXIT e pressione Enter. O servidor será reiniciado, agora selecione o modo normal de inicialização. A seguir apresento uma descrição resumida dos principais comandos disponíveis no console de recuperação.

# Internet Information Services 6.0 – IIS 6.0 e Software Update Services – SUS

Neste tópico você deve conhecer, principalmente o funcionamento do SUS. Pelo fato de o SUS ser uma novidade do Windows Server 2003, certamente será um tópico bastante explorado no Exame 70-290.

---

**NOTA:** Para uma referência sobre os principais comandos que podem ser utilizados no Console de Recuperação, consulte o Capítulo 12.

---

## Pontos importantes sobre o IIS, a serem lembrados para o exame:

Para que você possa tornar um servidor com o Windows Server 2003 em um servidor Web, você precisa instalar o IIS – Internet Information Services. O IIS é o serviço responsável pela disponibilização dos serviços http (para disponibilização de páginas) e ftp (para cópia de arquivos). Outros serviços também são disponibilizados pelo IIS, tais como serviços de SNMT e NNTP. Para maiores detalhes sobre os serviços de SNMT e NNTP, consulte o Capítulo 24, do livro: Windows Server 2003 – Curso Completo, 1568 páginas. A versão do IIS disponível com o Windows Server 2003 é a versão 6.0. Neste capítulo farei referência simplesmente utilizando IIS.

Caso você não tenha instalado o IIS quando da instalação do Windows Server 2003, é possível fazer a instalação quando for necessário. No próximo exemplo, você aprenderá passo-a-passo a instalar o IIS 6.0.

Antes de instalar o IIS, é importante fazer algumas observações, relacionadas com a segurança do IIS. No Windows 2000 Server, ao instalar o IIS, por padrão, são habilitadas uma série de funcionalidades. O problema é que muitas destas funcionalidades não são necessárias em muitas situações práticas. O mais grave é que muitas das falhas de segurança do IIS 5.0, estavam justamente nestas funcionalidades que eram habilitadas automaticamente durante a instalação do produto. Já com o IIS 6.0, no Windows Server 2003, é adotada uma política de habilitar apenas um conjunto mínimo de serviços, durante a instalação. A medida que o administrador precisa de novas funcionalidades ele as habilita. Obviamente que os problemas de segurança detectados no IIS 5.0 já foram corrigidos através do uso de Service Packs no Windows 2000 Server e não estão presentes no IIS 6.0. Mas habilitar somente os serviços realmente necessários, é uma política bem mais sensata, tanto em termos de segurança, quanto em termos de uso de recursos do servidor.(tais como memória e processador). Quando houver necessidade de utilizar uma funcionalidade que não está habilitada, basta que o Administrador configure o IIS para habilitar a respectiva funcionalidade.

---

**IMPORTANTE:** Quando você instala o IIS, o serviço é instalado em um modo de alta segurança. Por padrão, ele está configurado para servir apenas conteúdo estático (páginas HTML padrão). Para que possam ser executados conteúdos dinâmicos - páginas ASP e ASP.NET, scripts CGI, Internet Server Application Programming Interface (ISAPI) e Web Distributed Authoring and Versioning (WebDAV) – estes recursos devem ser habilitados pelo administrador, conforme mostrarei neste capítulo.

---

Você pode usar a opção Extensões de serviços da Web para configurar quais extensões do servidor IIS estarão habilitadas e quais estarão desabilitadas. Para habilitar/desabilitar uma determinada extensão, basta clicar na extensão a ser habilitada/desabilitada para marcá-la, no console de Gerenciamento do IIS. Em seguida clique no botão Permitir, para habilitar a extensão ou no botão Proibir, para desabilitar a extensão. Ao clicar em Permitir, para habilitar uma extensão, será exibida uma janela pedindo confirmação para a habilitação. Clique em Sim, para prosseguir com a habilitação.

Nunca é demais lembrar que somente devem ser habilitadas as funcionalidades realmente necessárias, para evitar problemas de segurança e uso desnecessário dos recursos do servidor.

Comparando WebDav com FTP:

| Protocolo | Senha de segurança   | Criptografia de dados   |
|-----------|--|---|
| WebDAV    | Sempre que o servidor Web estiver usando a SSL; às vezes quando ele não estiver usando | Sempre que o servidor Web estiver usando a SSL; nunca quando ele não estiver usando |
| FTP       | Nunca  | Nunca   |

O WebDAV protege a senha e os dados criptografados quando você envia informações para um servidor Web executando SSL (Secure Sockets Layer). Se o servidor não estiver executando a SSL, o WebDAV poderá proteger a sua senha se ele estiver configurado para usar a autenticação do Windows. Entretanto, você não pode criptografar os dados enviados ao servidor, se este não estiver usando SSL. Se o servidor estiver executando a SSL, o endereço do servidor na Internet será iniciado por https:// em vez de http://.

O FTP não usa criptografia ou outro mecanismo de segurança para proteger a sua senha quando você faz logon em um servidor. Além disso, você não pode criptografar os dados quando usar o FTP para enviar arquivos para/de um servidor. Isso coloca suas informações em risco, pois qualquer pessoa que use hardware ou software de rede pode capturá-las à medida que são transferidas.

O uso do WebDAV para a transferência de arquivos, pastas e outros dados para servidores Web que executam a SSL é a maneira mais segura de transferir informações.

## SUS – Software Update Services

### Introdução ao SUS

O SUS – Software Update Services é um serviço utilizado para automatizar o processo de download e instalação das correções do Windows, a partir do site Windows Update. No Windows Server 2003, em Português, este serviço é denominado de Serviço de Atualizações Automáticas. Já há alguns anos, que a Microsoft disponibiliza o site Windows Update, através do qual você pode baixar e instalar atualizações e correções de segurança para as diferentes versões do Windows. Porém o usuário deve tomar a iniciativa de usar o comando Windows Update, para conectar o seu computador com o site do Windows Update, para fazer a instalação das últimas correções disponíveis. O SUS leva este processo um nível a frente. Você estala o SUS em um servidor da rede e pode configurar este servidor para baixar, automaticamente, as atualizações a partir do site Windows Update. Depois de baixadas para o servidor, estas atualizações poderão ser aplicadas, automaticamente, em todos os demais computadores da rede. Este processo tem inúmeras vantagens, as quais serão descritas neste capítulo.

O SUS é instalado como um site/aplicativo Web, baseado no IIS. Conforme você verá neste tópico, todo o processo de administração do SUS é feito via browser, através da página de administração do SUS.

O SUS é uma aplicação Cliente/Servidor. Você instala o SUS em um servidor baseado no IIS. No servidor você configura um agendamento para o download automático das atualizações, aprova as atualizações críticas de segurança e faz uma série de outras configurações. Nos clientes, você instala o software client do SUS, o qual se comunica com o servidor e baixa e instala, automaticamente, as atualizações disponíveis no servidor.

## Componentes do SUS:

Neste item farei uma breve descrição sobre os elementos que compõem o SUS, os quais permitem que seja montado uma infra-estrutura para download e instalação automática das atualizações do Windows. O SUS é formato, basicamente, pelos seguintes componentes:

1. O site do SUS rodando em um servidor com o IIS: Ao instalar o SUS será criado um site no servidor IIS, no qual estão todos os recursos necessários a administração e a configuração do SUS. Este é o componente de servidor do SUS. Este é o componente responsável por entrar em contato com o site Windows Update e por baixar as atualizações disponíveis. Você verá que é possível configurar um agendamento, para que o SUS verifique sobre a disponibilidade de novas atualizações no site Windows Update. Você aprenderá a instalar o SUS e a fazer as principais configurações disponíveis. Mostrarei que a interface de administração do SUS são simplesmente páginas hospedadas no IIS, as quais você acessa através do Internet Explorer.
2. O site de Administração do SUS: Esta é o componente de administração do SUS. A interface de administração do SUS nada mais é do que um conjunto de páginas, hospedadas em um site do IIS. Ao instalar o SUS, o site de administração é criado e configurado. Toda a administração do SUS é feita usando o navegador.
3. Atualizações Automáticas: Este é o componente cliente, na arquitetura Cliente/Servidor do SUS. O cliente é instalado em cada estação de trabalho e pode ser configurado para baixar as atualizações diretamente do site Windows Update ou de um servidor SUS. O cliente também pode ser configurado para buscar por atualizações dentro de um agendamento determinado. Você pode definir se as atualizações devem ser aplicadas automaticamente ou se deve ser apenas exibido um aviso sobre a disponibilidade das novas atualizações, de tal maneira que o usuário opte por iniciar ou não a instalação das novas atualizações.
4. Configurações das políticas de segurança: Este é um aspecto muito importante e que você deve conhecer muito bem para o exame. Por padrão, o cliente de Atualizações Automáticas, é configurado para baixar as atualizações a partir do site Windows Update. Você pode alterar estas configurações, para fazer com que o cliente de Atualizações Automáticas, baixe as atualizações a partir de um servidor com o SUS instalado. Estas configurações podem ser feitas via GPO (que é a maneira preferencial, a qual automatiza o processo de configuração), ou alterando, manualmente, a Registry de cada computador da rede. Mais adiante mostrarei qual a diretiva de GPO a ser alterada e qual a chave da Registry, caso você tenha optado por fazer as configurações do cliente via Registry.

**IMPORTANTE:** Algumas vezes pode acontecer de todos os serviços do SUS pararem de funcionar corretamente. As atualizações não são mais baixadas automaticamente, atualizações que já foram baixadas não são instaladas ou você não consegue se conectar com a página de administração do SUS. Nestas situações, a causa mais provável do problema é que o próprio IIS está com problemas. Quando isso ocorrer é recomendado que você pare e reinicialize todos os serviços relacionados ao IIS. Normalmente esta reinicialização dos serviços do IIS, faz com que o SUS normalize também.

## Instalando o SUS

O SUS não é incluído como parte do Windows Server 2003. O SUS é gratuito e pode ser copiado do site da Microsoft, a partir do seguinte endereço:

<http://www.microsoft.com/windowsserversystem/sus/default.mspx>

Antes de baixar e instalar o SUS é importante que você saiba que a partição onde o SUS será instalado e a partição do sistema, devem estar formatadas com o sistema de arquivos NTFS. Esta não é uma recomendação, mas sim um pré-requisito para que o SUS possa ser instalado.

A instalação do SUS faz com que os seguintes componentes sejam instalados no servidor:

- ◆ O serviço Software Update Synchronization Service, o qual é responsável por fazer o download das correções do site Windows Update para o servidor SUS
- ◆ Um site no IIS, o qual é utilizado para administração do SUS.
- ◆ Uma página para administração do SUS, a qual é utilizada para sincronização do servidor SUS e para aprovação das atualizações que foram baixadas, antes que estas sejam instaladas nos clientes.

As atualizações que precisam, obrigatoriamente, ser aprovadas, antes de serem instaladas nos clientes, são as atualizações críticas de segurança. Pode ocorrer de ser publicada uma atualização da atualização. Ou em outras palavras, uma correção da correção. Nestas situações, você pode configurar o SUS para que ele aprove automaticamente, uma correção a uma correção que já foi aprovada previamente. Por exemplo, imagine que na segunda-feira você baixou uma correção crítica de segurança e usou o SUS para aprovar esta correção. Na sexta-feira, a equipe da Microsoft disponibiliza uma correção a esta correção baixada na segunda-feira. Você pode configurar o SUS para que baixe esta correção à correção e que a aprove, automaticamente, uma vez que ele é uma correção a uma correção já aprovada anteriormente.

O SUS também pode ser instalado em um servidor com o Windows 2000 Server e com o IIS 5.0. Neste caso, durante a instalação, será executado o assistente conhecido como Lockdown Wizzard. Este assistente irá configurar o IIS para deixá-lo mais seguro, desativando serviços e portas que não sejam necessárias.

Ao fazer o download do SUS, você irá copiar para o servidor o seguinte arquivo:

**SUS10SP1.exe**

Esta é a versão do SUS já com o SP1 do SUS, ou seja, já com um pacote de correções do SUS, em relação a primeira versão que foi lançada. Este arquivo tem 32,2 MB. A seguir descrevo os passos para instalação do SUS:

Para instalar o SUS, siga os passos indicados a seguir:

**IMPORTANTE:** No momento em que escrevo este resumo (04-04-2004), o SUS está disponível somente nas versões em Inglês e Japonês. Um ponto importante a salientar é que o que está em Inglês é a interface de administração do SUS, mas isso não impede que você possa utilizá-lo para baixar atualizações para o Windows em outros idiomas, como por exemplo, Português do Brasil. Você verá mais adiante, que ao configurar o SUS, você define para quais idiomas (o termo técnico ao invés de Idioma seria Localidade) você quer que um servidor com o SUS baixe as atualizações. Por exemplo, se a sua empresa tem escritórios no Brasil, EUA e Itália, você pode configurar um único servidor SUS, para baixar atualizações para os três idiomas. O cliente de Atualizações Automáticas saberá identificar, automaticamente, as correções adequadas ao idioma da estação de trabalho. Ainda usando o exemplo da empresa que tem filiais no Brasil, EUA e Itália, cabe salientar que se você estiver usando um servidor SUS em cada localidade, você deve configurar este servidor para baixar apenas as atualizações para a localidade. Por exemplo, o servidor da filial da Itália deve ser configurado para baixar apenas as atualizações para o idioma Italiano; o servidor da filial Brasileira, deve ser configurado para baixar apenas as atualizações para o idioma Português/Brasil e assim por diante. Este procedimento reduz o tráfego nos links de WAN e libera a banda disponível para outros serviços.

1. Faça um logon com uma conta com permissão de Administrador, em um servidor com o IIS já instalado.
2. Faça o download do SUS, usando o endereço descrito anteriormente.
3. Após ter feito o download deste arquivo, basta dar um clique duplo no arquivo SUS10SP1.exe para iniciar a instalação do SUS. Ao dar um clique duplo no arquivo SUS10SP1.exe, será aberto o assistente de instalação do SUS.
4. A primeira tela do assistente é apenas informativa. Clique em Next para seguir para a próxima etapa do assistente.
5. Na segunda etapa você deve aceitar o contrato de licença. Marque a opção “I accept the terms in the License Agreement” e clique em Next para seguir para a próxima etapa do assistente.
6. Nesta etapa você deve optar por fazer uma instalação Típica (Typical) ou Personalizada (Custom), conforme indicado na Figura 14.58:

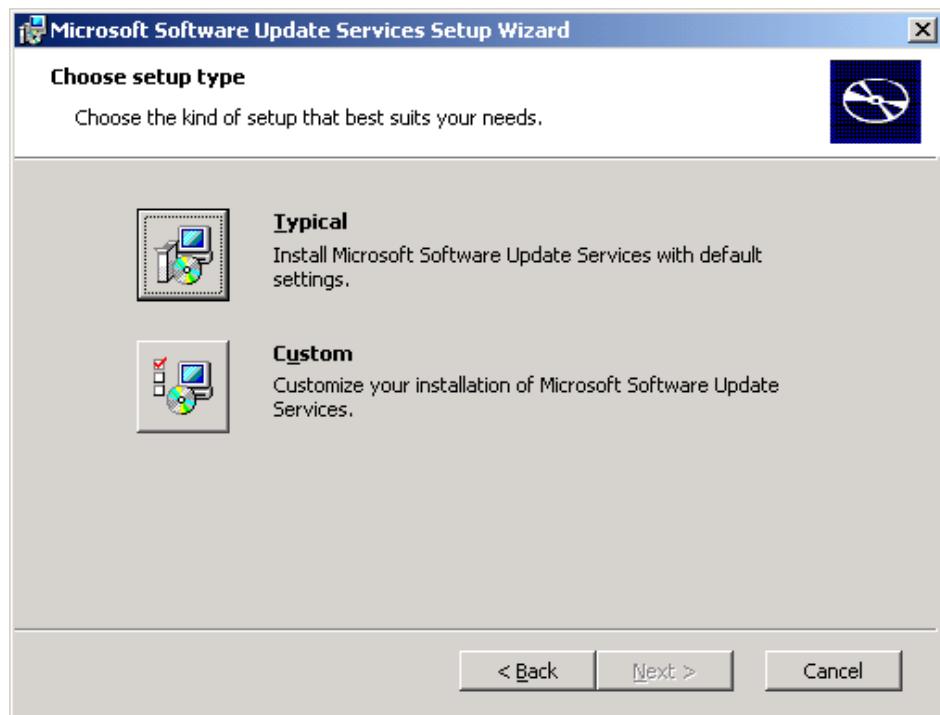


Figura 14.58 Definindo o tipo de instalação do SUS.

7. Clique em Custom.
8. Nesta etapa você define se o SUS deve baixar as atualizações para uma pasta local no servidor (por padrão é sugerida a pasta C:\SUS) ou se deve deixar as atualizações no site Windows Update e baixar apenas as informações sobre quais atualizações estão disponíveis. O mais usual é baixar as atualizações para o disco local do servidor. Os clientes então conectam-se com o servidor SUS da rede local e fazem a instalação a partir deste servidor. Certifique-se de que a opção Save the updates to this local folder esteja selecionada, conforme indicado na Figura 14.59:

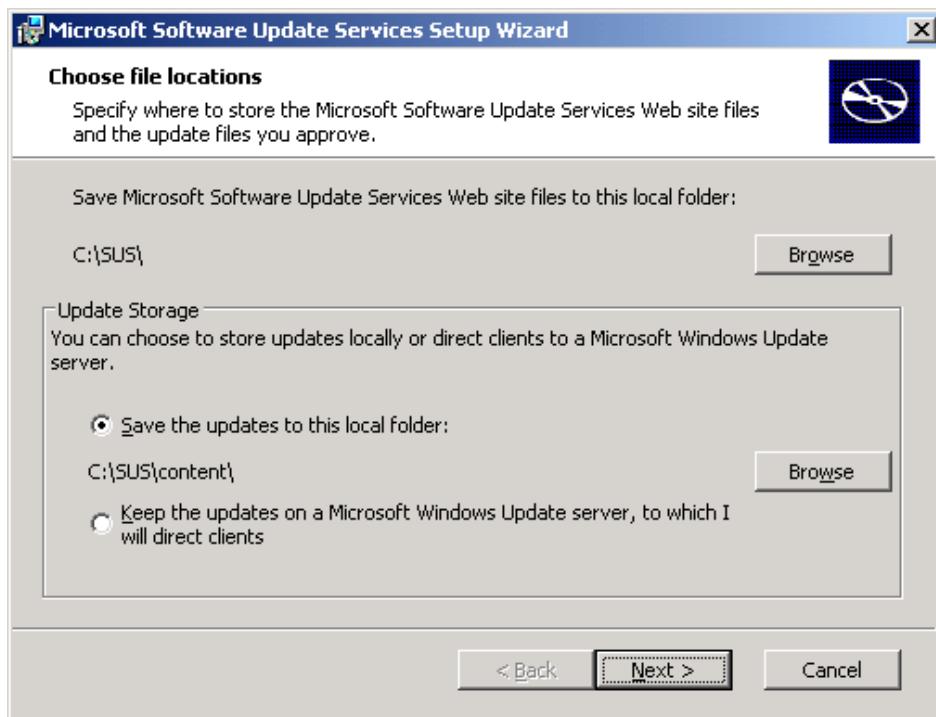


Figura 14.59 Baixando as atualizações para o servidor SUS.

9. Clique em Next para seguir para a próxima etapa do assistente.
10. Nesta etapa é que você define para qual ou quais idiomas é que devem ser baixadas as atualizações. Vou repetir o que foi colocado antes, devido a importância. A interface do SUS, por enquanto, está disponível apenas em Inglês e Japonês. Neste exemplo estou utilizando a interface em Inglês. Uma coisa é o idioma da interface de administração e outra, completamente separada é o idioma para os quais serão baixadas as atualizações. Nesta etapa é que você define para qual ou quais idiomas, o SUS irá baixar as atualizações a partir do site Windows Update. Você pode selecionar a opção English only, para baixar apenas as atualizações para o Windows em Inglês, ou você pode selecionar All available languages, para baixar todas as atualizações disponíveis, em todos os idiomas. Conforme descrito anteriormente, esta não é uma boa opção. Você deve configurar o SUS para baixar as atualizações, somente para os idiomas que serão realmente utilizados. Por exemplo, se na rede onde o servidor SUS está sendo instalado, você tem computadores que utilizam o Windows em Inglês e outros que utilizam o Windows em Português, você deve configurar o SUS para baixar as atualizações apenas para estes dois idiomas. Para configurar quais as versões para as quais serão baixadas as atualizações, clique na opção Specific languages. O botão Choose Languages será habilitado, conforme indicado na Figura 14.60.
11. Clique no botão Choose Languages.
12. Na janela que é exibida, deixe selecionados apenas os idiomas para os quais você deseja baixar as atualizações, conforme exemplo da Figura 14.61, onde dei marcado apenas as opções English e Portuguese (Brazilian).
13. Após ter selecionado os idiomas clique em OK. Você estará de volta ao assistente de instalação do SUS.
14. Clique em Next para seguir para a próxima etapa do assistente.
15. Nesta etapa é que você define como deverão ser tratadas, novas versões de atualizações já previamente aprovadas. Você pode optar por aprovar automaticamente as novas versões de atualizações já previamente aprovadas (Automatically approve new versions of previously approved updates) ou pode definir que as novas versões de atualizações já previamente aprovadas, devam ser novamente aprovadas pelo Administrador (I will manually approve new versions of approved updates). Selecione a opção desejada e clique em Next para seguir para a próxima etapa do assistente.

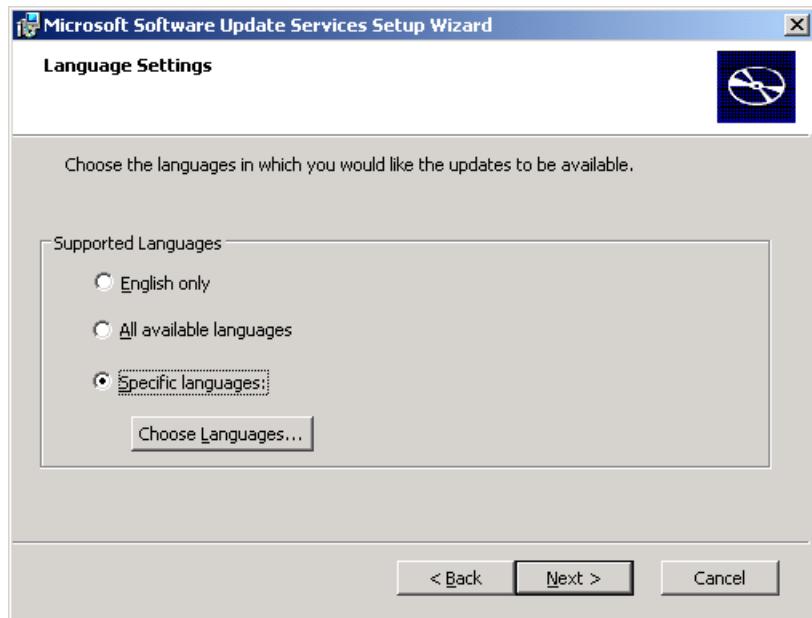


Figura 14.60 A opção Choose Languages.

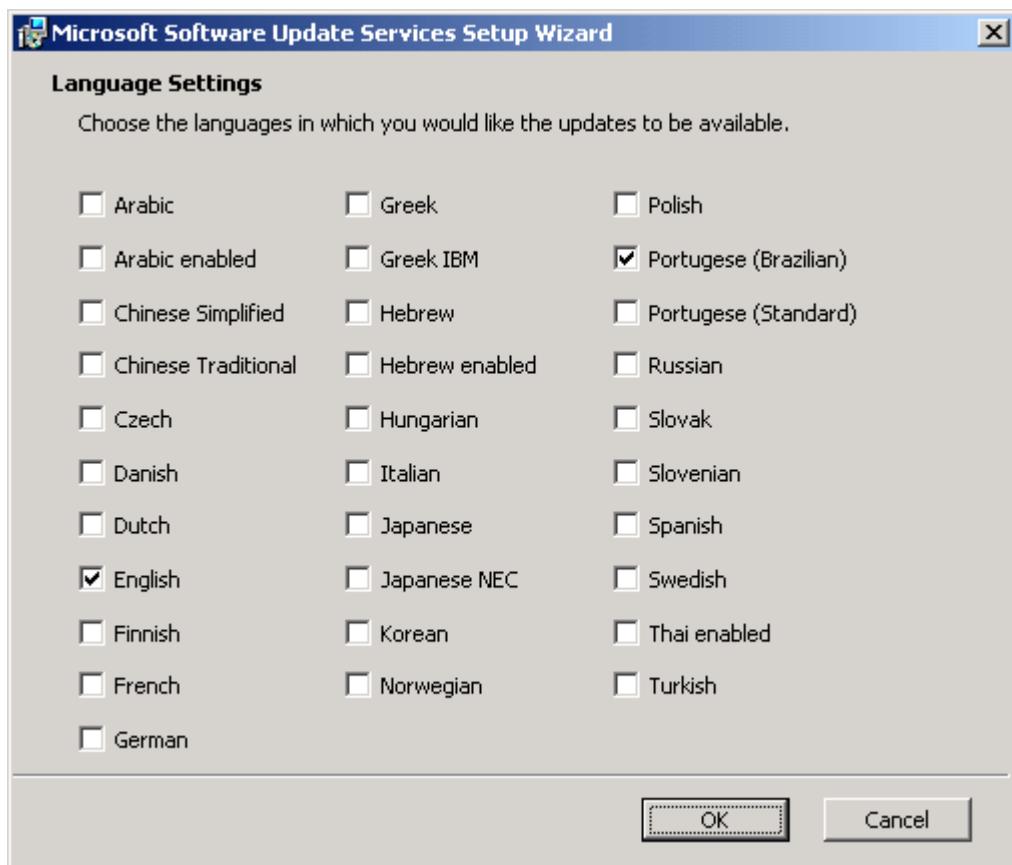


Figura 14.61 Selecionando os idiomas.

16. Será exibida a tela final do assistente. Nesta tela tem uma informação muito importante. Nesta tela é informado o endereço que deve ser informado nos clientes (quer seja via Registry ou via GPO). Ou seja, é informada a URL com a qual os clientes devem se conectar, para baixar as atualizações disponíveis no SUS. Por padrão a URL é formada

pelo nome do servidor. No exemplo da figura 13.30, estou instalando o SUS em um servidor cujo nome é SRV70-290. Com isso, a URL de conexão para os clientes é <http://SRV70-290>, conforme destacado na Figura 14.62:

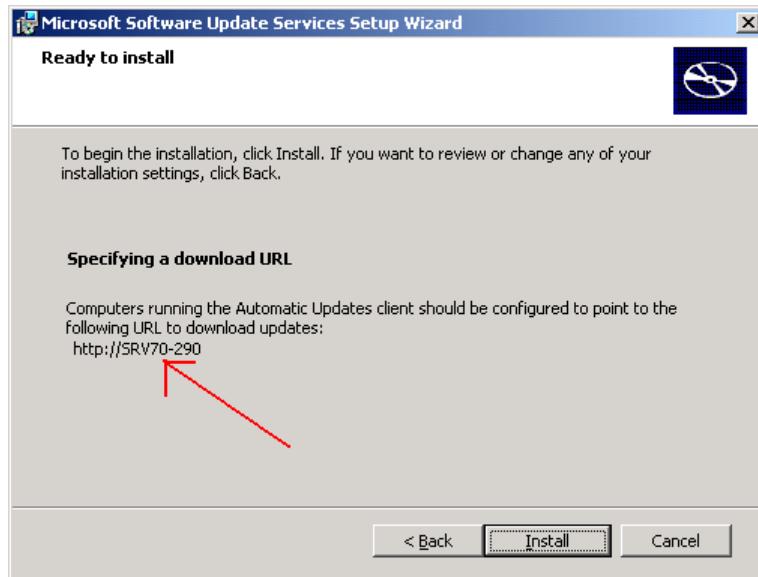


Figura 14.62 A URL de conexão para os clientes.

17. Clique em Install para finalizar a instalação do SUS.
18. O assistente irá finalizar o processo de instalação e exibir uma mensagem informando que a instalação foi concluída com sucesso. Clique em Finish para fechar esta mensagem.

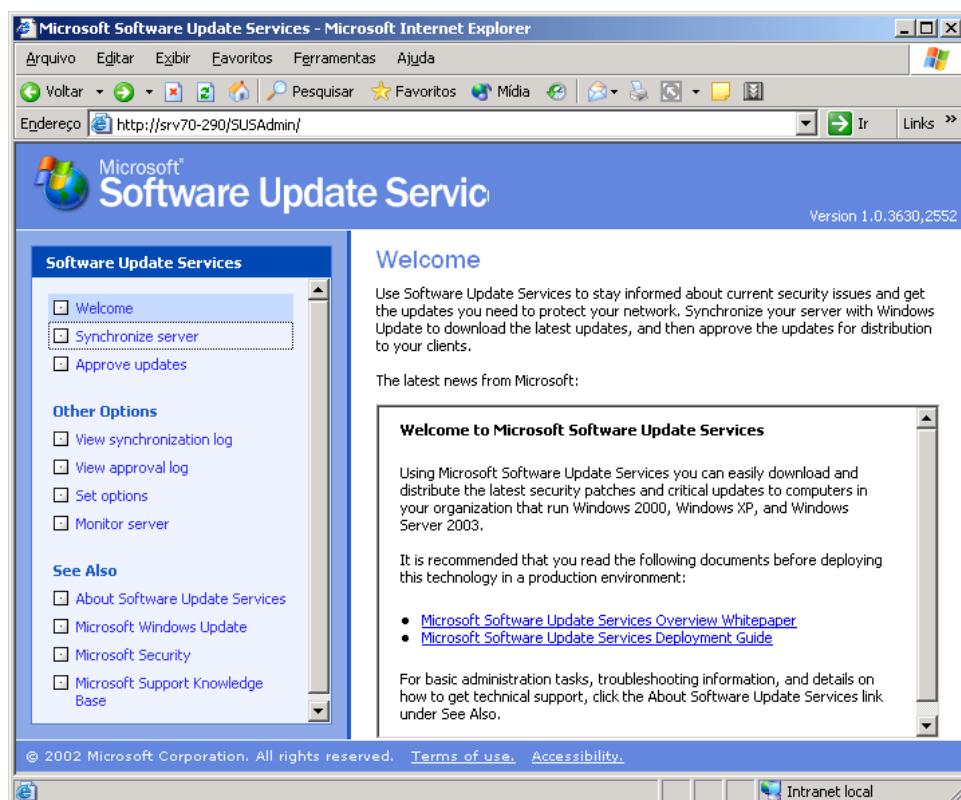


Figura 14.63 O site de administração do SUS.

19. Após concluir a instalação, a página de administração do SUS será automaticamente carregada no Internet Explorer. Observe o endereço da página de administração, o qual é no seguinte formato: <http://nome-do-servidor/SUSAdmin>. No nosso exemplo, onde o SUS foi instalado no servidor SRV70-290, a página de administração do SUS é acessada no seguinte endereço: <http://srv70-290/SUSAdmin>, conforme indicado na Figura 14.63:
20. Mantenha esta página aberta, pois iremos utilizá-la nos próximos tópicos.

Muito bem, o SUS foi instalado e está pronto para ser configurado e utilizado. Agora temos mais duas etapas a vencer:

- ◆ Aprender a administrar o SUS.
- ◆ Configurar os clientes para utilizar o SUS.

## Administrando o SUS

Neste tópico, você acompanhará um exemplo prático, onde mostrarei as principais opções de configuração do SUS.

Exemplo: Para administrar o SUS, siga os passos indicados a seguir:

1. Faça o logon com uma conta com permissão de Administrador.
2. Abra o Internet Explorer e acesse o seguinte endereço, substituindo SRV70-290 pelo nome do servidor onde o SUS está instalado:  
<http://srv70-290/SUSAdmin>
3. Será aberta a página de administração do SUS. No painel da esquerda estão disponíveis links para as diversas categorias de opções de configuração, disponíveis no SUS. Na página inicial estão disponíveis links para um White Paper sobre o SUS e para um guia de implementação do SUS. Dê um conferida nestes documentos, vale realmente a pena.
4. No painel da esquerda, clique em Synchronize Server. Será carregada uma página, onde você tem duas opções, conforme indicado na Figura 14.64:

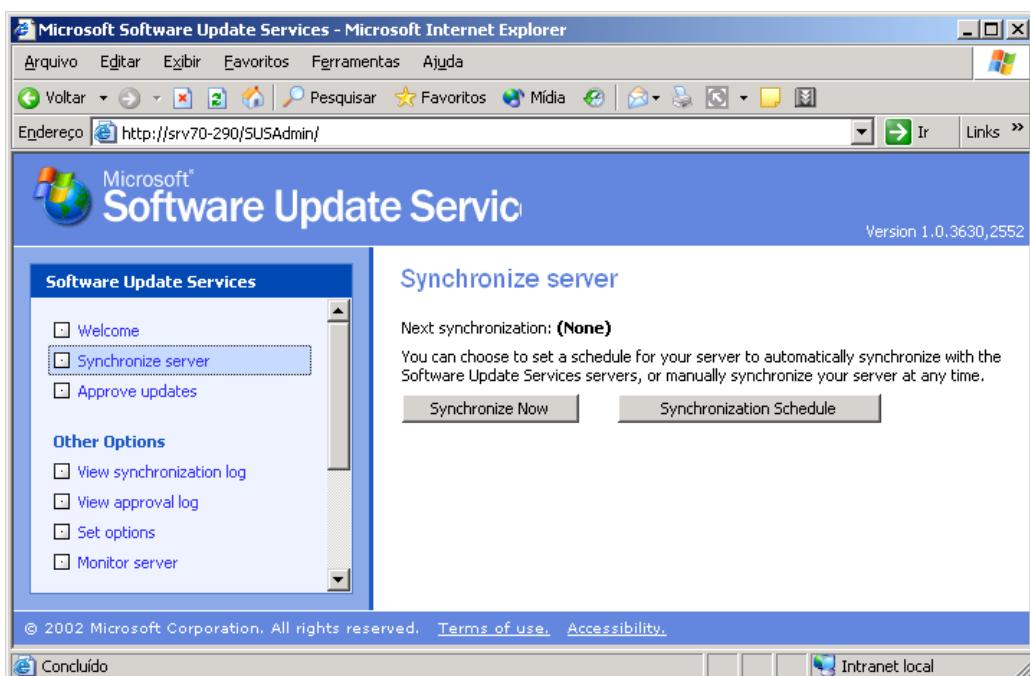


Figura 14.64 Opções de sincronização do SUS.

Você utiliza a opção Synchronize Now, para fazer com que o SUS se conecte imediatamente com o site do Windows Update e baixe as atualizações disponíveis. A opção Synchronization Schedule, é utilizada para criar um agendamento de sincronização. Ou seja, você define dias e horários em que o SUS irá se conectar com o site Windows Update e baixar as atualizações disponíveis. Ao clicar em Synchronization Schedule, será exibida a janela Indicada na Figura 14.65, na qual você pode definir um agendamento para o SUS. No exemplo da Figura 14:65 foi definida uma sincronização diária, as 00:00 hs.



Figura 14.65 Definindo um agendamento.

5. Clique em Synchronize Now,
6. O SUS irá se conectar com o site Windows Update e baixar as atualizações disponíveis. A medida que vai baixando as atualizações, o SUS exibe uma barra indicando o percentual do processo que já foi concluído.
6. Ao finalizar a sincronização (a primeira sincronização pode demorar um bom tempo, uma vez que um grande número de atualizações será copiado a partir do site Windows Update), será exibida uma mensagem informando que o servidor foi sincronizado com sucesso e que agora você pode selecionar a aprovar as atualizações que foram baixadas.
7. Clique em OK para fechar esta mensagem.

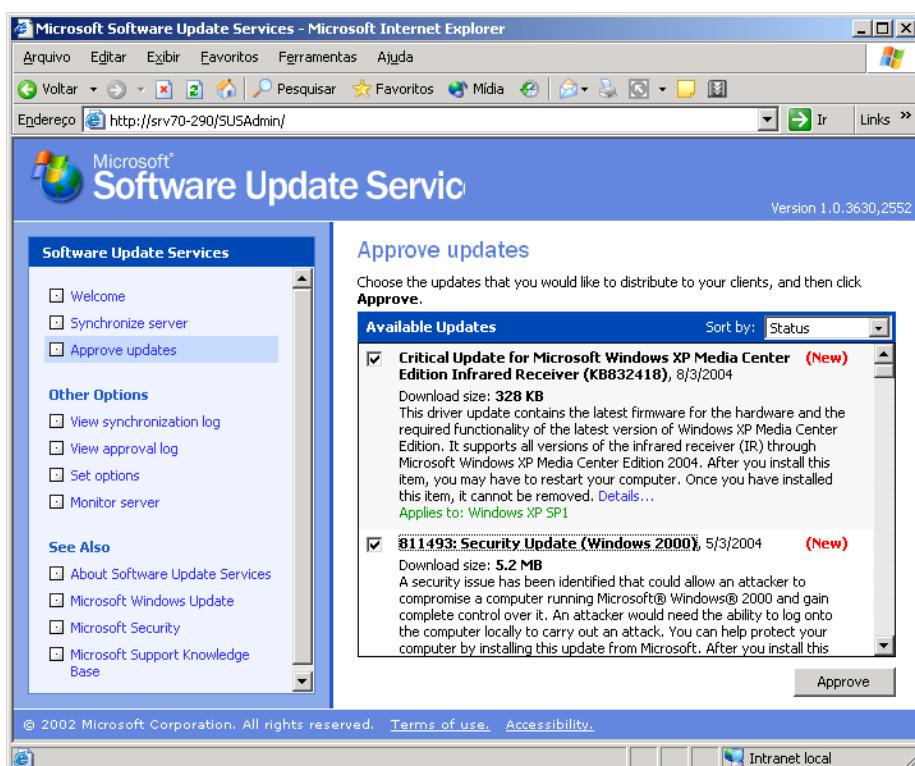
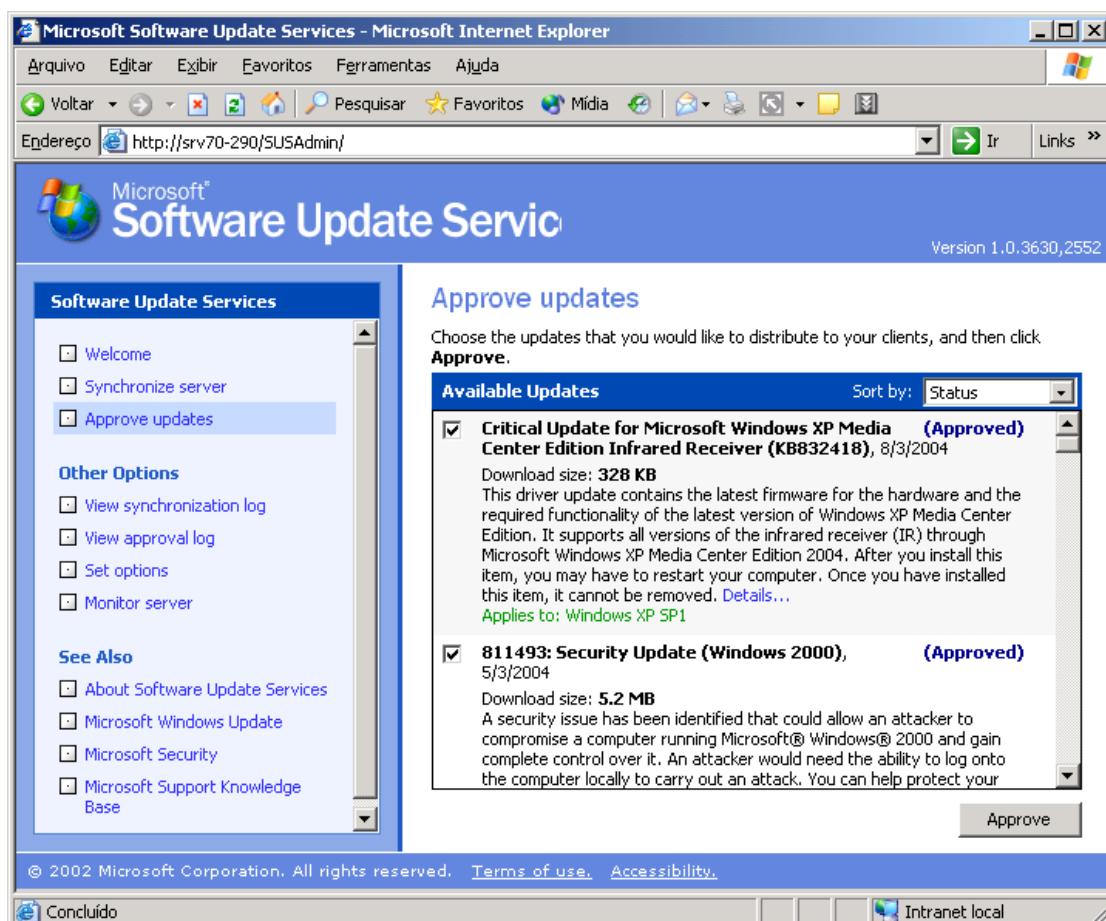


Figura 14.66 Aprovando atualizações críticas de segurança.

8. A opção Aprove updates será automaticamente selecionada, no painel da esquerda. No painel da direita será exibida a lista de atualizações aguardando aprovação. Lembre-se de que as atualizações críticas não serão aplicadas aos clientes, até que não tenham sido aprovadas pelo administrador do SUS.
9. Para aprovar uma atualização, basta marcá-la e clicar em Approve, conforme indicado na Figura 14.66, onde duas atualizações foram marcadas para aprovação.
10. Selecione as atualizações a serem aprovadas e clique no botão Approve. Surge uma mensagem informando que você está aprovando uma nova lista de atualizações as quais estarão disponíveis para os clientes e que esta nova lista substituirá qualquer lista existente previamente. Clique em Sim para criar a nova lista de atualizações aprovadas e prontas para serem instaladas nos clientes.
11. Se alguma das atualizações exigir que você concorde com um Termo de serviços, será exibida uma mensagem solicitando que você aceite o termo de serviços. Clique em Accept para aceitar e aprovar a atualização. Ao final será exibida uma mensagem informando que uma nova lista foi criada. Clique em OK para fechar esta mensagem.
12. As atualizações já aparecem com o status de aprovado (Approved), conforme indicado na figura 14.67:



**Figura 14.67 Atualizações já aprovadas.**

13. No painel da esquerda, clique na opção View synchronization log. No painel da direita será exibido o log de eventos de sincronização do servidor SUS. Na listagem a seguir, apresento a parte inicial deste log:

```
*****
```

**Manual Sync Started- segunda-feira, 22 de março de 2004 22:11:27 Successful**

**Updates Added:**

Security Update, July 19, 2000 - q261255\_OF334C94167F1C095608F7B0599891EA83B56A0A.exe  
Security Update, July 19, 2000 - q261255\_CECBAD4A43916313EC45E5DB5E7A8461E1A01E5F.exe  
Q328676: Security Update (Outlook Express 5.5 SP2) -  
q328389\_3016A5C05107C80B472F83955BDD424027D051C3.exe  
Q328676: Security Update (Outlook Express 5.5 SP2) -  
q328389\_825151815CDA30A1AF0B652FA17A10437C73CF82.exe  
Security Update, February 14, 2002 (Internet Explorer 5.01) -  
VBS51NEN\_6679B4E5AD916D6462A3AB5B4C2B81C2867CA1E6.EXE  
Security Update, February 14, 2002 (Internet Explorer 5.01) -  
VBS51NEN\_EA35DB61E858F2175BCF7DEDF0304C6DB48D8763.EXE  
October 2003, Cumulative Patch for Internet Explorer 5.01 for Windows 2000 Service Pack 4  
(KB828750) - q828750\_2d9563d8fbe81b44f9c1ee21e858952.exe  
\*\*\*\*\*

14. No painel da esquerda, clique na opção View approval log. No painel da direita será exibido o log de eventos relacionados a aprovação de atualizações no servidor SUS. Na listagem a seguir, apresento a parte inicial deste log:

\*\*\*\*\*  
Approved List Modified-terça-feira, 23 de março de 2004 19:40:02 Successful  
Approved By: ABC\Administrador  
List of Approved Updates:  
811493: Security Update (Windows 2000)  
Critical Update for Microsoft Windows XP Media Center Edition Infrared Receiver  
(KB832418)  
List of UnApproved Updates:  
Security Update for Microsoft Windows XP (KB328940)  
329170: Security Update (Windows 2000)  
329170: Security Update  
October 2003, Cumulative Patch for Internet Explorer 5.5 Service Pack 2 (KB828750) -  
q828750\_f45f5a468a9cd3933305594418529bd.exe  
October 2003, Cumulative Patch for Internet Explorer 5.5 Service Pack 2 (KB828750) -  
q828750\_e79d902ddfea3eee5913e2580f4dee.exe  
Cumulative Security Update for Internet Explorer 5.5 SP2 (KB824145) -  
q824145\_81926bcee2daa2c6185379a6722bb05.exe  
Cumulative Security Update for Internet Explorer 5.5 SP2 (KB824145) -  
q824145\_0e72e43b82edd2cdc3eb0dd92fd0273.exe  
\*\*\*\*\*

15. No painel da esquerda, clique em Set options. Esta opção nos dá acesso a uma série de configurações do servidor SUS. Nesta opção você pode definir se o servidor SUS se conecta diretamente à Internet ou através de um servidor Proxy, você define o nome que deve ser utilizado pelos clientes para se conectar com o servidor SUS, define se o servidor SUS irá baixar as atualizações diretamente do site Windows Update ou a partir de outro servidor SUS da empresa. Por exemplo, você pode ter um servidor SUS na matriz, sincronizando diretamente

com o site Windows Update e configurar os servidores SUS das filiais, para sincronizar a partir do servidor SUS da matriz. Com isso as atualizações são baixadas uma única vez pela Internet, a partir do site Windows Update para o servidor SUS da matriz. Do servidor SUS da matriz, as atualizações são transferidas para os servidores SUS das filiais. Com isso você pode montar uma hierarquia de servidores SUS, com dois ou mais níveis. Outra opção importante que você pode definir nesta página é se as novas versões de atualizações já aprovadas serão automaticamente aprovadas ou se deverão ser aprovadas novamente. Por último você também pode definir um ou mais idiomas/localidades, para os quais serão baixadas atualizações.

16. Defina as configurações desejadas e clique no botão Apply para aplicar as alterações.
17. Muito bem, sobre as opções de administração do SUS é isso. Feche a página de administração do SUS.

## Configurar os clientes para utilizar o SUS.

Muito bem, já aprendemos a fazer o download e a instalar o SUS. A próxima etapa é aprender a configurar os clientes da rede, para que estes passem a baixar as atualizações a partir do servidor SUS. Para que os clientes possam utilizar o SUS eles devem ter o Cliente de Atualizações Automáticas (Automatic Updates Client) instalado. O Cliente de Atualizações Automáticas faz parte do Windows 2000, Windows Server 2003 ou Windows XP e é instalado, automaticamente, a primeira vez que você utilizar o Windows Update.

A configuração do cliente de atualizações automáticas é feita através da guia Atualizações automáticas, da janela de propriedades do Sistema (clique com o botão direito do mouse em Meu computador e, no menu que é exibido, clique em Propriedades). A janela Atualizações automáticas está indicada na Figura 14.68:

**NOTA:** Se por algum motivo o cliente SUS não estiver instalado, você pode fazer o download a partir do seguinte endereço: <http://www.microsoft.com/windows2000/downloads/recommended/susclient/default.asp>

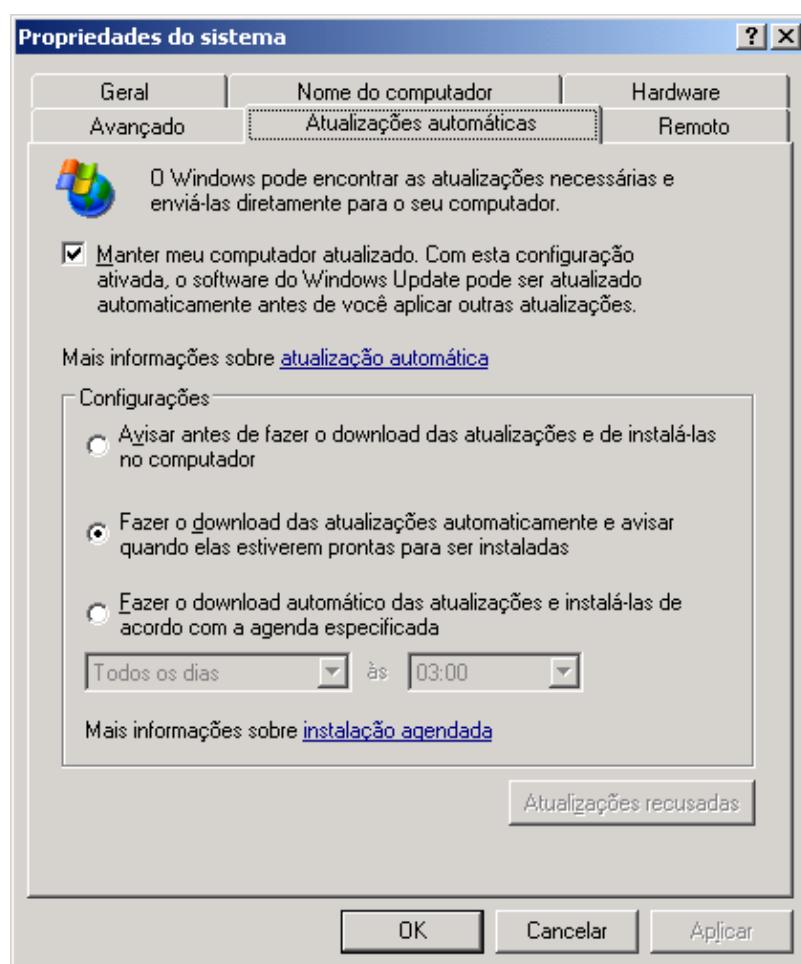


Figura 14.68 A guia Atualizações automáticas.

A seguir descrevo as opções disponíveis nesta guia:

- ◆ **Manter o meu computador atualizado.** Com esta configuração ativa, o software Windows Update pode ser atualizado automaticamente antes de você aplicar outras atualizações. É recomendado que você mantenha esta opção sempre marcada.
- ◆ **Avisar antes de fazer o download das atualizações e de instalá-las no computador:** Ao marcar esta opção, o Windows irá avisá-lo antes de fazer o download de qualquer atualização. O Windows irá avisá-lo novamente quando as atualizações estiverem prontas para serem instaladas.
- ◆ **Fazer o download das atualizações automaticamente e avisar quando elas estiverem prontas para serem instaladas:** Esta opção faz com que o Windows faça o download automaticamente das atualizações disponíveis. Após ter concluído o download, o Windows aviso o usuário para que este possa iniciar a instalação das atualizações que foram baixadas. Esta é a opção recomendada se você quer automatizar o processo de download, mas quer que o Windows notifique você antes de instalar as atualizações, dando a você a opção de instalá-las ou não.
- ◆ **Fazer o download automático das atualizações e instalá-las de acordo com a agenda especificada:** Esta opção permite que você defina um agendamento para a instalação das atualizações. O Winodws fará o download automático das atualizações e irá isntalá-las de acordo com o agendamento configurado.

Após ter definido as configurações desejadas, clique em OK para aplicá-las. Muito bem, a guia Atualizações automáticas, apenas define de que maneira as atualizações serão baixadas e aplicadas. A questão agora é como fazer com que o cliente de atualizações automáticas baixe as atualizações a partir do servidor SUS e não diretamente do site Windows Update. Muito bem, existem duas maneiras de fazer isso: via GPO ou via Registry das estações de trabalho. A seguir mostro estas duas maneiras para configurar os clientes para utilizar o servidor SUS.

## Configurando os clientes via GPO:

Você pode utilizar o recurso de GPOs, descrito no Capítulo 9, para configurar os clientes para que utilizem o servidor SUS, ao invés de se conectar com o site Windows Update. Você deve acessar o seguinte grupo de GPOs: Configurações do computador -> Modelos administrativos -> Componentes do Windows – Windows Update, conforme ilustrado na figura 14.69:

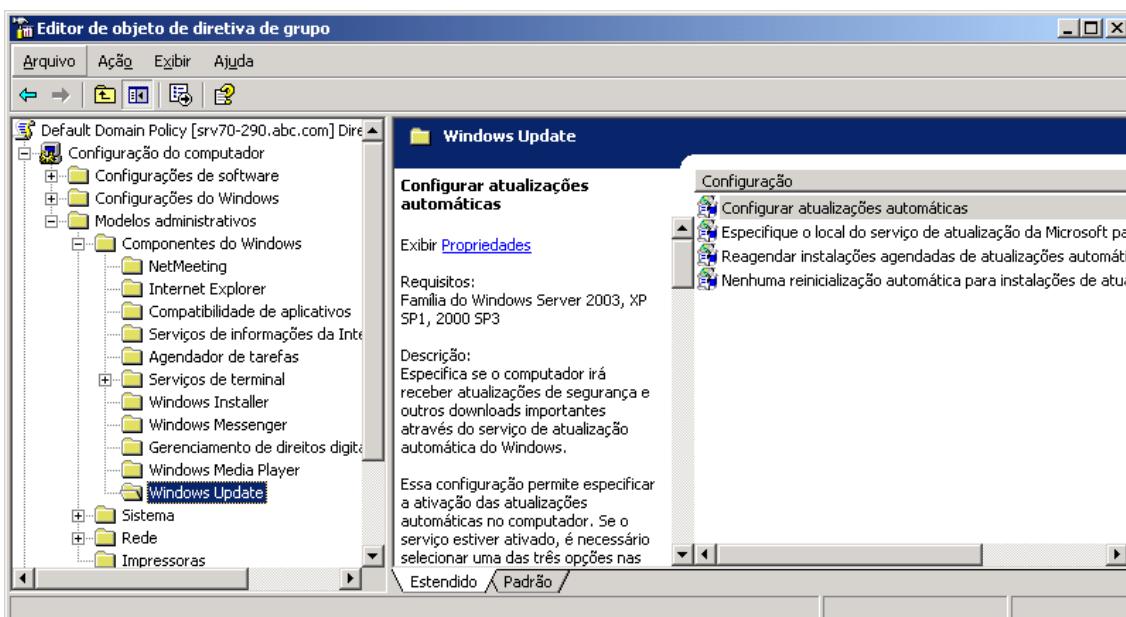


Figura 14.69 Opções de GPO relacionadas ao SUS.

Neste grupo estão disponíveis as seguintes polices:

- ◆ **Configurar atualizações automáticas:** Ao abrir esta police, serão exibidas as opções indicadas na Figura 14.70:

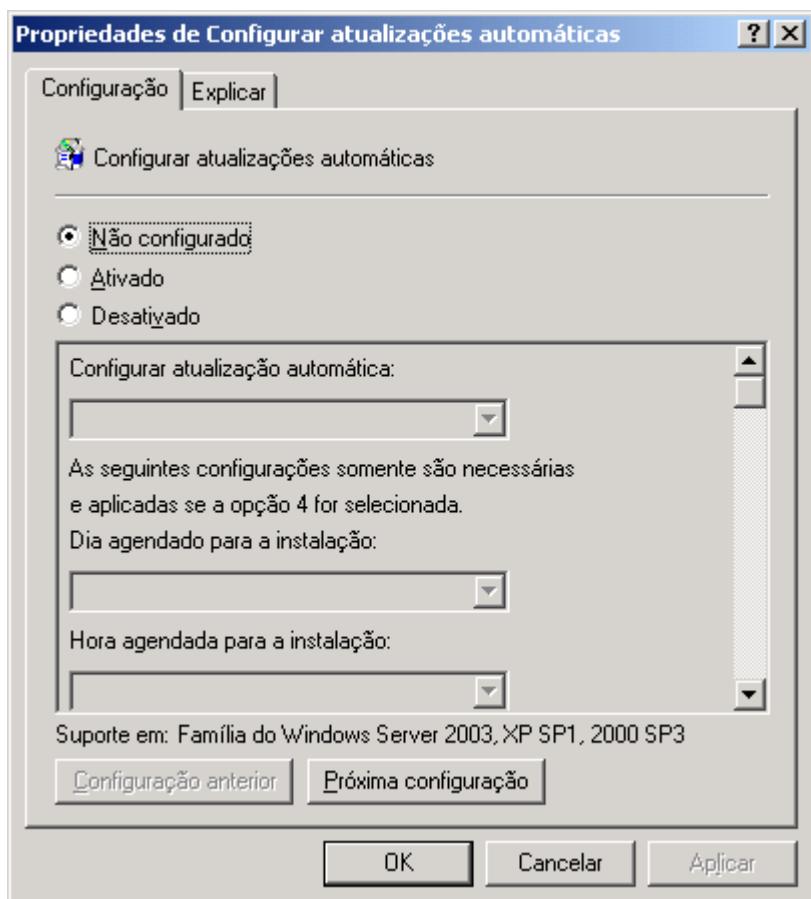


Figura 14.70 A police Configurar atualizações automáticas.

A police Configurar atualizações automáticas especifica se o computador irá receber atualizações de segurança e outros downloads importantes através do serviço de atualização automática do Windows.

Essa configuração permite especificar a ativação das atualizações automáticas no computador. Ao marcar a opção Ativado, você deve selecionar uma das opções a seguir, na lista Configurar atualização automática (observe que estas são exatamente as opções disponíveis na guia Atualizações automáticas):

2 - Avisar antes de fazer o download das atualizações e de instalá-las no computador: Quando o Windows encontra atualizações que se aplicam ao computador, ele exibe um ícone na área de status com uma mensagem para fazer o download das atualizações. Clique no ícone ou na mensagem a fim de selecionar as atualizações cujo download você deseja fazer. Em seguida, o Windows fará o download das atualizações selecionadas em segundo plano. Quando o download estiver concluído, o ícone aparecerá novamente na área de status, avisando que as atualizações já estão disponíveis para serem instaladas. Clique no ícone ou na mensagem para selecionar as atualizações que deseja instalar.

3 - (Configuração padrão) Fazer o download das atualizações automaticamente e avisar quando elas estiverem prontas para serem instaladas: Com esta opção o Windows encontra atualizações que se aplicam ao computador e faz o download delas em segundo plano (o usuário não é avisado ou interrompido durante esse processo). Quando o download estiver concluído, o ícone aparecerá na área de status, avisando que as atualizações estão prontas para serem instaladas. Clique no ícone ou na mensagem para selecionar quais atualizações deseja instalar.

4 - Fazer o download automático das atualizações e instalá-las no agendamento especificado abaixo: Ao selecionar esta opção, você pode especificar o agendamento usando as demais opções disponíveis nesta diretiva. Se nenhum agendamento for especificado, o agendamento padrão para todas as instalações será todo dia às 15 horas. Se for necessário reiniciar o computador para concluir a instalação, o Windows irá reiniciá-lo automaticamente. (Se um usuário fizer logon no computador quando o Windows estiver pronto para reiniciar, o usuário será notificado e será fornecida a opção para reiniciar depois.)

Para usar essa configuração, clique em Ativado e selecione uma das opções (2, 3, ou 4). Caso tenha selecionado a opção 4, é possível configurar um agendamento recorrente (se não houver agendamento especificado, todas as instalações irão ocorrer todo dia às 15 horas).

Se o status estiver configurado como ‘Ativado’, o Windows reconhecerá quando o computador estiver on-line e usará sua conexão com a Internet para procurar por atualizações que se apliquem ao computador no site Windows Update.

Se o status estiver configurado como ‘Desativado’, deverão ser feitos o download e a instalação manual de qualquer atualização que esteja disponível no site Windows Update em <http://windowsupdate.microsoft.com>.

Se o status estiver definido como ‘Não configurado’, o uso das atualizações automáticas não será especificado pelo nível da diretiva de grupo. Porém, um administrador ainda pode configurar as atualizações automáticas através da guia Atualizações Automáticas, descrita anteriormente.

- ◆ Especifique o local do serviço de atualização da Microsoft para a intranet: Ao abrir esta police, serão exibidas as opções indicadas na Figura 14.71:

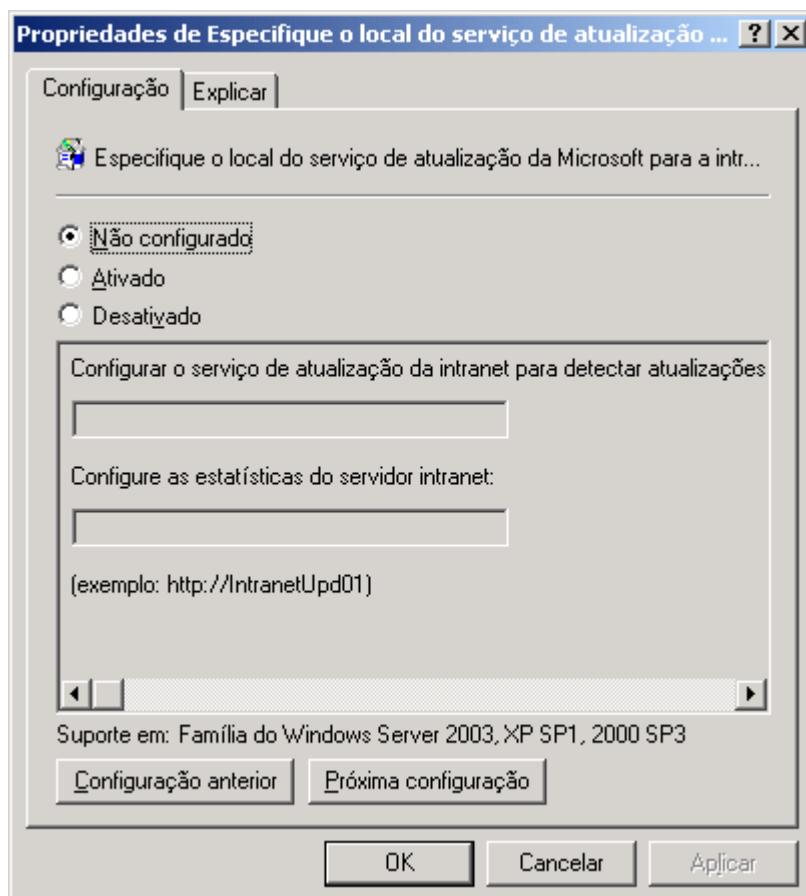


Figura 14.71 A police Especifique o local do serviço de atualização da Microsoft para a intranet.

Esta é a police utilizada para especificar o servidor SUS que será utilizado pelos clientes. Ou seja, é nesta police que você informa o nome do servidor SUS a partir do qual os clientes irão copiar as atualizações disponíveis.

Essa configuração permite especificar um servidor na rede para funcionar como um serviço de atualização interno – servidor SUS. O cliente das atualizações automáticas procurará no serviço atualizações que se apliquem aos computadores da rede.

Para usar essa configuração, é necessário configurar dois valores de nome de servidor: o servidor a partir do qual o cliente das atualizações automáticas detecta e faz o download das atualizações, e o servidor para o qual as estações de trabalho atualizadas carregam as estatísticas. É possível configurar os dois valores para o mesmo servidor.

Se o status desta police estiver configurado como ‘Ativado’, o cliente das atualizações automáticas se conecta ao servidor SUS ao invés de se conectar com o site Windows Update, para procurar e fazer o download de atualizações. Ativar essa configuração significa que os usuários finais na organização não precisam atravessar um firewall para obter atualizações, assim como permite testar atualizações antes de implantá-las.

Se o status estiver configurado como ‘Desativado’ ou ‘Não configurado’, e se as atualizações automáticas não forem desativadas pelas diretrivas ou preferências do usuário, o cliente das atualizações automáticas irá se conectar diretamente ao site Windows Update na Internet.

Reagendar instalações agendadas de atualizações automáticas: Ao abrir esta police, serão exibidas as opções indicadas na Figura 14.72:

**IMPORTANTE: Se a diretiva “Configurar atualizações automáticas” estiver desativada, essa diretiva não terá efeito.**

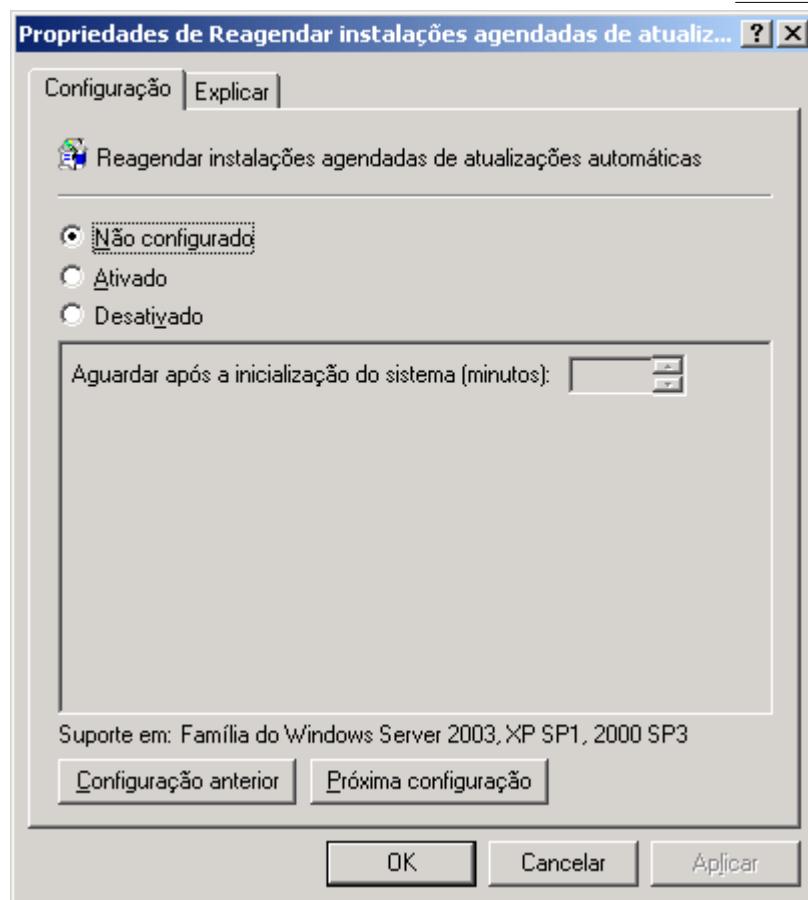


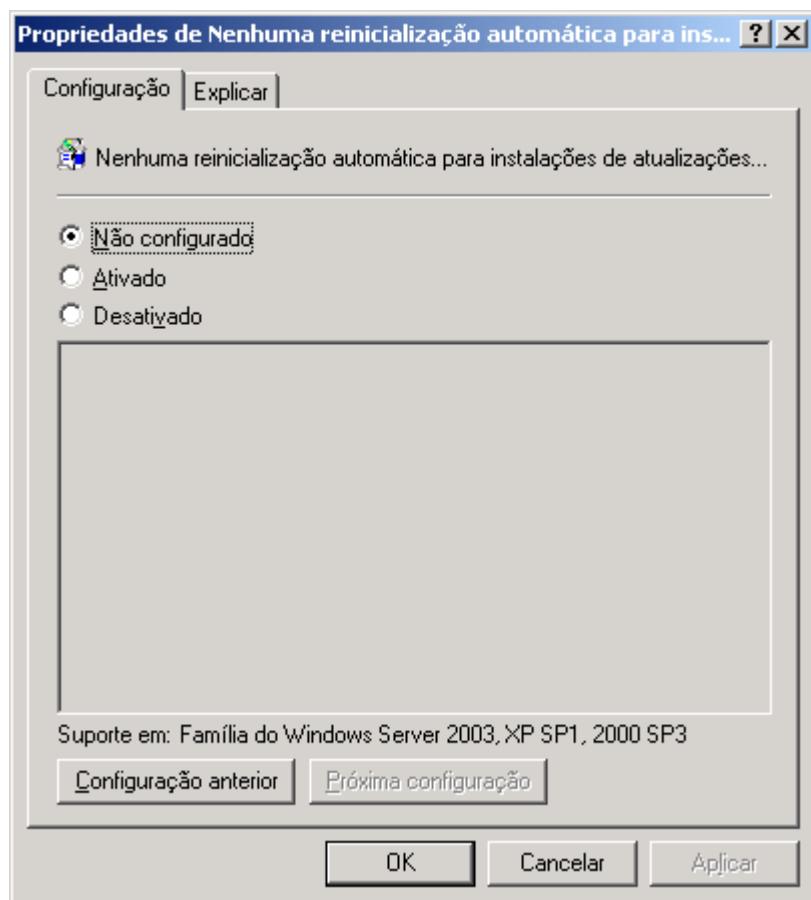
Figura 14.72 A police Reagendar instalações agendadas de atualizações automáticas.

Esta police é utilizada para especificar por quanto tempo as atualizações automáticas devem esperar, após a inicialização do sistema, para proceder com uma instalação agendada que tenha sido perdida anteriormente, isto é, que não tenha sido feita no horário agendado anteriormente.

Se o status estiver definido como Ativado, uma instalação agendada que não ocorreu anteriormente irá ocorrer após o número especificado de minutos nesta police, depois da inicialização do computador.

Se o status estiver definido como Desativado ou Não configurado, uma instalação agendada perdida irá ocorrer na próxima instalação agendada.

- ◆ Nenhuma reinicialização automática para instalações de atualizações automáticas agendadas: Ao abrir esta police, serão exibidas as opções indicadas na Figura 14.73:



**IMPORTANTE:** Esta diretiva se aplica somente quando as atualizações automáticas estão configuradas para executar instalações agendadas de atualizações. Se a diretiva “Configurar atualizações automáticas” estiver desativada, esta diretiva não tem efeito algum.

**Figura 14.73** A police Nenhuma reinicialização automática para instalações de atualizações automáticas agendadas.

Esta police é utilizada para definir que, para a conclusão de uma instalação agendada, as atualizações automáticas aguardarão até que o computador seja reiniciado por qualquer usuário que tenha feito logon, em vez de fazer com que o computador seja reiniciado automaticamente.

Se o status for definido como ‘Ativado’, as atualizações automáticas não reiniciarão um computador automaticamente durante uma instalação agendada se um usuário tiver feito logon no computador. Em vez disso, as atualizações automáticas notificarão o usuário de que é necessário reiniciar o computador para concluir a instalação.

Se esta police for configurada como Desativado ou Não configurado, o cliente de atualizações automáticas irá notificar o usuário que o computador irá reiniciar, automaticamente, em cinco minutos, para que as atualizações recém instaladas possam ser aplicadas.

---

**IMPORTANTE:** Com esta police ativada, o cliente de atualizações automáticas, não conseguirá detectar novas atualizações até que o computador tenha sido reinicializado.

---

### Opções da Registry relacionadas com o SUS:

Existem, basicamente, duas chaves da registry relacionadas com o SUS. Estas chaves são úteis em uma situação onde o cliente de atualizações passa a não receber as atualizações, embora elas estejam disponíveis no SUS. Nestas situações, você deve acessar o seguinte caminho da Registry: HKEY\_LOCAL\_MACHINE\Software\Polices\Microsoft\Windows\WindowsUpdate e verificar o valor das chaves descritas a seguir:

- ◆ WUServer: Esta chave deve conter a URL que aponta para o servidor SUS, como por exemplo: http://SRV70-290
- ◆ WUStatusServer: Esta chave deve conter a URL do mesmo servidor SUS indicado na chave WUServer ou a URL de um servidor IIS, o qual é utilizado para gravação das estatísticas de sincronização.
- ◆ SubChave UseWUServer: Esta subchave deve sempre estar configurada com o valor: 00000001.

---

**IMPORTANTE:** Esta police somente se aplica quando o cliente de atualizações automáticas estiver configurado para fazer atualizações agendadas. Se a police Configurar atualizações automáticas estiver desabilitadas, esta police não terá efeito prático.

---

## Conclusões finais e uma proposta de Plano de Estudos.

Neste livro apresentei todos os tópicos que fazem parte do programa oficial para o Exame 70-290. Além dos conceitos teóricos, associados a cada tópico, apresentei também exemplos práticos, detalhados passo-a-passo, para melhor fixação dos conteúdos.

O candidato pode e deve complementar os seus estudos, pesquisando na Ajuda do Windows e na Internet, mais detalhes sobre algum tópico que não tenha sido perfeitamente compreendido. Eu classificaria o Exame 70-290 com um grau de dificuldade de 3,8, em uma escala que vai entre 1 e 5. Não é dos exames mais difíceis, mas exige um bom conhecimento do candidato.

Sugestão de plano de estudos:

Vamos supor que você disponha de três semanas para se preparar para o Exame 70-290. Você precisa passar neste exame para garantir o seu emprego. Você trabalha durante o dia. Para isso você está disposto a estudar 4 horas todas as noites e oito horas nos finais de semana. A pergunta é: Você tem tempo suficiente para se preparar para o exame?

A resposta é um sonoro SIM , você tem tempo até de sobra.

Assim, você tem um total de 108 horas para estudar: 15 dias a 4 horas por dia, mais 6 dias (três finais de semana) a 8 horas por dia. A questão é a seguinte: “Com o tempo disponível é possível passar neste exame”? A resposta é um sonoro sim . Eu até diria que você tem tempo de sobra. Sugiro o seguinte programa de estudo:

| <b>Material utilizado</b>   | <b>Tempo de estudo</b>                  |
|---|---|
| Livros: Sugiro a utilização de dois livros:<br>O Training Kit Oficial Para o Exame, em Inglês   | Este Livro que você está lendo 60 horas |
| Resumos: Disponíveis nos sites:<br><ul style="list-style-type: none"> <li>• <a href="http://www.cramsession.com">www.cramsession.com</a></li> <li>• <a href="http://www.examnotes.net">www.examnotes.net</a></li> </ul> | 10 horas                                |
| Simulado da Transcender: Fazer e revisar os resultados.<br><ul style="list-style-type: none"> <li>• <a href="http://www.transcender.com">www.transcender.com</a></li> </ul>   | 20 horas                                |
| Revisão do livro e dos resumos.   | 10 horas                                |
| Revisão final : Principalmente do Transcender e dos resumos, para ser feita na véspera do exame.  | 08 horas                                |
| <b>Total:</b>   | <b>108 horas</b>                        |

Seguindo este plano, você candidato terá grandes chances de ser aprovado. Volto a repetir: Eu estou até exagerando no tempo necessário e na quantidade de materiais a serem utilizados. Seguindo este plano de estudos você terá excelentes chances de ser aprovado.

É um exame difícil? Não muito, desde que você esteja bem preparado. É perfeitamente possível de ser aprovado. Com uma boa dose de dedicação e estudo você conseguirá ser aprovado, não tenha dúvidas disso.

Agradeço imensamente por ter adquirido e estudado este livro. É meu mais sincero desejo que você seja aprovado em mais este exame. Não deixe de enviar suas sugestões e críticas para o meu email: [webmaster@juliobattisti.com.br](mailto:webmaster@juliobattisti.com.br). Consulte periodicamente meu site – [www.juliobattisti.com.br](http://www.juliobattisti.com.br), para novos artigos, dicas, tutoriais, simulados e um fórum de discussão exclusivo sobre as Certificações da Microsoft. Vale a pena conferir.

# CAPÍTULO

# 15

## Simulado para o Exame 70-290 – 60 Questões

Neste capítulo eu apresento um simulado com 60 questões. Em cada questão apresento, além da resposta, comentários sobre a questão, sempre salientando os pontos principais relacionados e cobrados na referida questão. Peço que o amigo leitor estude com muita atenção o conteúdo que foi apresentado neste livro, bem como o resumo do Capítulo 14, este simulado e os links indicados ao longo do livro.

Outra excelente fonte de informações e de estudos para o exame 70-290 é o simulado Transcender ([www.transcender.com](http://www.transcender.com)). Este simulado tem dois pontos, digamos assim, que podem representar problemas: é caro (cerca de 150 dólares) e somente está disponível em Inglês. Mas para o amigo leitor que domina a leitura do Inglês técnico, o Transcender é uma excelente opção. São três simulados com 45 questões cada um. Além das questões, você encontra explicações detalhadas sobre cada questão. Você também tem a opção de imprimir os simulados com as respostas e comentários de cada questão. Ao imprimir os três simulados serão mais de 200 páginas de excelente conteúdo.

### Simulado para o Exame 70-290 – 60 questões – respostas – comentários:

**Questão 01:** Você é o Administrador da rede da empresa, a qual é baseada no Windows Server 2003 Server e no Active Directory. A rede foi a pouco tempo migrada para o Windows Server 2003 e é formada por um único domínio: abc.com. Você ainda não implementou uma estrutura de Unidades Organizacionais. Com isso você teve que incluir oito contas de usuários como membros do grupo Admins. do Domínio, para que estes usuários possam administrar os servidores, usuários e grupos de suas localidades. Um dos administradores está excluindo, indevidamente, contas de usuários de outras localidades. Como você pode descobrir qual dos administradores está fazendo estas exclusões indevidas?

- a) Abra o console Usuários e Computadores do Active Directory e pesquise por registros de exclusões de conta em todo o domínio.
- b) Abra o console Usuários e Computadores do Active Directory e pesquise por registros de uso do direito de exclusão de contas.
- c) Faça uma pesquisa no log de Segurança de todos os controladores de domínios do domínio abc.com, pesquisando por eventos de gerenciamento de contas de usuários.
- d) Faça uma pesquisa no log de Segurança de todos os controladores de domínios do domínio abc.com, pesquisando por eventos de acesso às contas de usuários.
- e) Faça uma pesquisa no log do Sistema de todos os controladores de domínios do domínio abc.com, pesquisando por eventos de gerenciamento de contas de usuários.

**Resposta certa: c**

**Comentários:** Esta questão descreve um dos problemas que, sem sombra de dúvida, mais irritava os administradores de redes baseadas no Windows 2000 Server e que,

para minha surpresa, persiste com o Windows Server 2003: Não existe uma consolidação, em uma base de dados centralizada, dos logs de evento de todos os servidores de um domínio. Ou seja, o log é individual, separado em cada servidor (DC ou member server) do domínio. Esta questão ilustra bem este problema. Neste caso, o administrador terá que pesquisar o log de Segurança em cada DC do domínio, para identificar eventos de gerenciamento de contas de usuários. Um dos tipos de eventos de gerenciamento de contas de usuários é a exclusão de usuários. Nestes eventos fica registrada, dentre outras, informações do nome da conta excluída, o nome do usuário que excluiu a conta e a data e hora da exclusão. Mas o problema é, digamos assim, “mais problemático”, porque o usuário que excluiu a conta, tem permissão de Administrador (pertence ao grupo Admins. do Domínio) e, com isso, poderia também “limpar” o log de Segurança em todos os DCs. Ou seja, poderia cometer o crime e destruir as provas.

**Questão 02:** Você é o administrador de uma rede baseada no Windows Server 2003 Server e no Active Directory. A rede é formada por um único domínio e todos os servidores estão baseados no Windows Server 2003. Para descentralizar a administração dos recursos do domínio, tais como contas de usuários, grupos e computadores, você criou uma estrutura de Unidades Organizacionais e usou o Assistente para delegação de Tarefas, para delegar tarefas, em nível de Unidade Organizacional. Você usou o Assistente de Delegação para delegar tarefas tais como gerenciamento de contas de usuários e adição de novas contas de computadores ao domínio. Como administrador do domínio, você gostaria de ter gravado nos Logs do sistema, as ações executadas pelos usuários que tiveram permissões delegadas em uma ou mais OUs do domínio. Foram delegadas permissões somente para atuar sobre objetos do Active Directory, tais como contas de usuários, computadores e grupos. Quais os passos para implementar a gravação de eventos descrita?

- a) Crie um grupo chamado Gerentes de OUs.

Adicione ao grupo Gerentes de OUs, as contas dos usuários que tiveram tarefas delegadas.

Crie uma nova GPO e associe-a ao container Domain Controllers.

Configure as permissões desta GPO, de tal maneira que seja aplicada apenas ao grupo Gerentes de OUs.

Configure esta GPO para auditar o acesso aos serviços do Active Directory e ao gerenciamento de contas.

- b) Crie um grupo chamado Gerentes de OUs.

Adicione ao grupo Gerentes de OUs, as contas dos usuários que tiveram tarefas delegadas.

Crie uma nova GPO e associe-a ao domínio abc.com

Configure as permissões desta GPO, de tal maneira que seja aplicada apenas ao grupo Gerentes de OUs.

Configure esta GPO para auditar o acesso aos serviços do Active Directory e ao gerenciamento de contas.

- c) Crie uma nova GPO e associe-a ao container Domain Controllers.

Configure as permissões desta GPO, de tal maneira que seja aplicada apenas ao grupo Gerentes de OUs.

Configure esta GPO para auditar o acesso aos serviços do Active Directory e ao gerenciamento de contas.

- d) Crie um grupo chamado Gerentes de OUs.

Adicione ao grupo Gerentes de OUs, as contas dos usuários que tiveram tarefas delegadas.

Configure as permissões da GPO padrão do domínio, de tal maneira que seja aplicada apenas ao grupo Gerentes de OUs.

Configure a GPO padrão do domínio para auditar o acesso aos serviços do Active Directory e ao gerenciamento de contas.

- e) Configure as permissões da GPO padrão do domínio, de tal maneira que seja aplicada apenas ao grupo Gerentes de OUs.

Configure a GPO padrão do domínio para auditar o acesso aos serviços do Active Directory e ao gerenciamento de contas.

Resposta certa: a

**Comentários:** Esta questão testa uma série de conhecimentos sobre GPO, auditoria e grupos. Primeiro é recomendado que você crie um grupo e inclua, neste grupo, as contas que receberam permissões nas OUs, via delegação de tarefas. Em seguida você cria uma nova GPO e configura as permissões de segurança da GPO, de tal maneira que a GPO somente seja aplicada ao grupo criado no primeiro passo. A próxima etapa é associar a GPO ao container Domain Controllers. Isso porque foram delegadas tarefas relativas a objetos do Active Directory, ou seja, todas as ações ocorrerão nos DCs dos domínios. Por isso que a GPO será associada ao container Domain Controllers. O passo final é configurar essa GPO para fazer a auditoria das ações que foram delegadas para os usuários. <body text>Questão 03: Quais as condições necessárias para que um usuário possa fazer o logon em um computador com o Windows XP Professional, o qual faz parte de um domínio baseado no Windows Server 2003 e no Active Directory:

- I. O computador deve ter uma conta no Active Directory.
- II. A conta de computador deve estar habilitada..
- III. O usuário deve ter uma conta de usuário no Active Directory.
- IV. A conta do usuário não pode estar bloqueada.
- V. A conta do usuário não pode estar desativada.

Estão corretas as seguintes afirmativas:

- a) I, II
- b) I, II e III
- c) I, II e IV
- d) II, III, IV e V
- e) I, II, III, IV e V

Resposta certa: e

**Comentários:** Todas estas condições têm que ser atendidas, para que o usuário possa fazer o logon em um domínio do Active Directory. Primeiro o computador que está sendo utilizado deve ter uma conta no Active Directory e esta conta não pode estar desabilitada. Contas desabilitadas aparecem marcadas com um x vermelho, no console Usuários e Computadores do Active Directory. Você pode habilitar uma conta que foi desabilitada, clicando com o botão direito do mouse na respectiva conta e, no menu de opções que é exibido, clicar em Ativar conta. Além da conta de computador, o usuário que está fazendo o logon deve ter uma conta de usuário válida no Active Directory e esta conta não pode estar bloqueada e nem desativada. Uma conta é bloqueada, normalmente, quando o usuário faz um determinado número de tentativas de logon sem sucesso, dentro de um determinado intervalo. Como por exemplo, três logons sem sucesso, dentro de uma hora. O administrador pode desbloquear uma conta, acessando as propriedades da conta, clicando na guia Conta e desmarcando a opção “A conta está bloqueada”.

**Questão 04:** Você é o Administrador da rede da sua empresa. A rede é baseada em servidores com o Windows Server 2003 Server instalado e com o Active Directory. A rede possui um único domínio: abc.com.br. O domínio está no modo Windows 2000 Nativo. Você criou um grupo de escopo Global, do tipo Distribuição, chamada Gerentes e adicionou todos os gerentes, como membros deste grupo. Você deseja utilizar este grupo, para atribuir permissões de

acesso ao grupo Gerentes, nos compartilhamentos \\srv01\docs e \\srv01\memos, as quais devem ter acesso restrito aos gerentes. O que você deve fazer para limitar o acesso aos compartilhamentos, somente ao grupo Gerentes.

- a) Altera o modo do domínio para Windows Server 2003
- b) Altera o modo do domínio para Windows Server 2003

Atribua as permissões de compartilhamento e NTFS,somente para o grupo Gerentes.

- c) Exclua o grupo Gerentes.

Crie-o novamente, como sendo do tipo Segurança.

Configure as permissões NTFS e de Compartilhamento, de tal maneira que somente o grupo Gerentes tenha acesso aos compartilhamentos docs e memos.

- d) Exclua o grupo Gerentes.

Crie-o novamente, como sendo do tipo Segurança.

Adicione todos os gerentes como membros do grupo Gerentes.

Configure as permissões NTFS e de Compartilhamento, de tal maneira que somente o grupo Gerentes tenha acesso aos compartilhamentos docs e memos.

- e) Altere o tipo do grupo Gerentes de Distribuição para Segurança.

Configure as permissões NTFS e de Compartilhamento, de tal maneira que somente o grupo Gerentes tenha acesso aos compartilhamentos docs e memos.

**Resposta certa: e**

**Comentários:** Esta questão é bastante interessante, pois ela tenta “distrair” o candidato, em torno de pontos que não são relevantes para a questão. Nesta questão existe um único ponto que deve ser focado: GRUPOS DO TIPO DISTRIBUIÇÃO NÃO PODEM SER UTILIZADOS PARA RECEBER PERMISSÕES DE COMPARTILHAMENTO E NTFS. Portanto a solução é fazer com que o grupo Gerentes seja do tipo Segurança. Aqui pode surgir uma outra dúvida: Para alterar o tipo de um grupo é preciso excluí-lo e criá-lo novamente, ou basta acessar as propriedades do grupo? A resposta é que você pode alterar o tipo de um grupo, sem ter que excluí-lo e criá-lo novamente. Para isso basta acessar a guia Geral, das propriedades do grupo e clicar no tipo desejado, para alterar o tipo do grupo. Com isso ficamos com a alternativa E, ou seja, você deve alterar o tipo do grupo e depois configurar as permissões de tal maneira que somente os membros do grupo Gerentes, tenham acesso aos compartilhamentos docs e memos.

**Questão 05:** Você é o administrador de uma rede baseada no Windows Server 2003 Server e no Active Directory. A rede é formada por um único domínio juliobattisti.com.br. Neste domínio você é o responsável por administrar uma impressora Laser, de alta velocidade, a qual está compartilhada para os usuários do setor de projetos. Um usuário entra em contato, informando que um trabalho que ele enviou as 8:30 para a impressora, ainda não foi impresso e já são 11:30. O trabalho tem apenas duas páginas e não poderia demorar tanto tempo para ser impresso. Você verifica a fila de impressão da impressora e descobre que 23 trabalhos de impressão que foram enviados estão na fila e não foram impressos. Como primeira opção você tenta excluir os trabalhos da fila, mas o Windows não consegue eliminar os trabalhos da fila. O que você deve fazer para que os usuários possam imprimir normalmente?

- a) Reinicialize o servidor onde a impressora está compartilhada.

Após a reinicialização os trabalhos voltarão a ser impressos, normalmente.

- b) Reinicialize o servidor onde a impressora está compartilhada.  
Faça o logon como Administrador e exclua todos os trabalhos da fila de impressão.  
Peça aos usuários que enviem os trabalhos novamente.
- c) Use o comando net stop spooler para parar o serviço de impressão.  
Use o comando net start spooler para reiniciar o serviço de impressão.  
Peça aos usuários que enviem os trabalhos novamente.
- d) Desligue a impressora.  
Exclua os documentos da fila de impressão.  
Peça aos usuários que enviem os trabalhos novamente.
- e) Acesse as propriedades da Impressora e altere o horário de disponibilidade, de tal maneira que os trabalhos da fila de impressão possam ser impressos.

Resposta certa: c

**Comentários:** Existe um ponto que é a chave para esta questão, que é a seguinte afirmação, contida no enunciado da questão: “Como primeira opção você tenta excluir os trabalhos da fila, mas o Windows não consegue eliminar os trabalhos da fila”. Esta afirmação é o indicativo claro, de que o serviço de impressão (Spooler) está com problema. Este serviço em determinadas situações mostra-se instável e deixa de funcionar corretamente. O maior indício de que o serviço Spooler está com problemas é quando você tenta excluir serviços da fila de impressão e o Windows mostra o status Excluindo mas não vai adiante e não consegue excluir os trabalhos da fila de impressão. Nestas situações só resta um remédio. Parar o serviço de impressão usando o comando net stop spooler. Reiniciar o serviço usando o comando net start spooler. Em algumas situações, após reiniciar o serviço Spooler, os trabalhos ainda estarão na fila de impressão, porém agora você conseguirá excluí-los, sem problemas. Outra situação que pode acontecer é você mandar imprimir um documento e o Windows emitir uma mensagem de erro, dizendo que antes de imprimir você deve ter uma impressora configurada. Este erro é causado também pelo serviço Spooler, o qual em algumas situações para por conta própria. Ou seja, estando o serviço Spooler parado é como se não existisse nenhuma impressora disponível. Nestas situações, basta executar o comando net start spooler, para reiniciar o serviço de impressão. Com isso ficamos com a letra C.

**Questão 06:** Você é o Administrador de uma rede com servidores baseados no Windows Server 2003 Server e no Active Directory. Os clientes são baseados no Windows 2000 Professional e alguns clientes no Windows XP Professional. A rede é formada por um único domínio: juliobattisti.com.br. Como parte da política de segurança da empresa, você quer registrar nos logs de auditoria, todas as tentativas de logon no domínio, quer seja logon com sucesso, quer seja logon com falha. Qual a maneira mais fácil de implementar esta exigência?

- a) Altere as diretivas de segurança local em cada Controlador de Domínio.  
Habilite a diretiva: Auditoria de Eventos de Logon, tanto para Sucesso quanto para Falha.
- b) Altere as diretivas de segurança local em cada Controlador de Domínio.  
Habilite a diretiva: Eventos de Logon de Conta de Auditoria, tanto para Sucesso quanto para Falha.  
(a tradução não é minha, a diretiva original em Inglês é: Audit account logon events. A tradução é um verdadeiro desastre)

- c) Altere GPO padrão do domínio.

Habilite a diretiva: Eventos de Logon de Conta de Auditoria, tanto para Sucesso quanto para Falha.

(a tradução não é minha, a diretiva original em Inglês é: Audit account logon events. A tradução é um verdadeiro desastre)

- d) Altere GPO padrão do domínio.

Habilite a diretiva: Auditoria de Eventos de Logon, tanto para Sucesso quanto para Falha.

- e) Crie uma nova GPO e associe com a OU Domain Controllers.

Habilite a diretiva: Auditoria de Eventos de Logon, tanto para Sucesso quanto para Falha.

**Resposta certa: c**

**Comentários:** O primeiro ponto importante, nesta questão é a seguinte parte do enunciado: “Qual a maneira mais fácil de implementar esta exigência? A maneira mais fácil é alterar a GPO padrão do domínio, com isso as configurações serão aplicadas em todo o domínio. Isso já descarta as alternativas a e b. O próximo ponto que o candidato deve conhecer é que a diretiva Auditoria de Eventos de Logon, é utilizada para auditar o logon local, usando contas locais nos computadores do domínio. Para auditar as tentativas de logon no domínio, deve ser utilizada a diretiva, Audit account logon events, maravilhosamente traduzida como: Eventos de Logon de Conta de Auditoria. Com isso ficamos com a letra C.

**Questão 07:** Você é o Administrador de uma rede com servidores baseados no Windows Server 2003 Server e no Active Directory. A rede é formada por um único domínio: abc.com. Os clientes são baseados no Windows 2000 Professional e alguns clientes no Windows XP Professional. Você gostaria de restringir o acesso as configurações de rede, tais como as configurações do protocolo TCP/IP para os usuários da rede. Estas restrições serão impostas via GPO. Você criou uma nova GPO chamada SemAcessoRede, na qual você fez as configurações para desabilitar o acesso as propriedades de configuração da interface de rede local. A GPO foi associada ao domínio abc.com. Pergunta-se: a solução proposta atende os requisitos de bloquear o acesso dos usuários as propriedades de configuração da interface de rede e apresenta algum inconveniente?

- a) A solução proposta atende os requisitos e não apresenta nenhum inconveniente.
- b) A solução proposta não apresenta nenhum inconveniente porém não atende aos requisitos.
- c) A solução proposta não apresenta nenhum inconveniente porém atende apenas parcialmente aos requisitos, uma vez que através da linha de comando, os usuários conseguirão alterar as propriedades da interface de rede.
- d) A solução proposta atende os requisitos mas apresenta o inconveniente de bloquear o acesso inclusive dos administradores, às propriedades de configuração da rede.
- e) A solução proposta atende os requisitos mas apresenta o inconveniente de bloquear o acesso inclusive dos administradores, às propriedades de configuração da rede, fazendo com que estes somente possam alterar estas propriedades através de um Prompt de comando, usando o comando ipconfig /all.

**Resposta certa: d**

**Comentários:** Ao aplicar uma GPO que nega o acesso às propriedades de configuração da interface de rede, esta GPO será aplicada a todos os usuários do domínio, inclusive aos membros do grupo Admins. do Domínio (Domain Admins). O inconveniente é que os membros do grupo Admins. de Domínio (Domain Admins) devem ter acesso a estas propriedades, para poder configurar as estações de trabalho da rede e prestar suporte aos usuários com problemas. Na

prática, inclusive o grupo de técnicos de suporte também deve ter acesso a estas propriedades. Por isso ficamos com a alternativa “d”, ou seja, a GPO como proposta, atende aos requisitos, mas com o inconveniente (ou efeito colateral como prefiram) de bloquear o acesso também para os membros dos grupos que precisam acesso a estas propriedades, tais como Administradores e Técnicos de suporte. A boa notícia é que tem solução para este problema. Veja a questão 08 para a descrição da solução para este inconveniente.

**Questão 08:** Você é o Administrador de uma rede com servidores baseados no Windows Server 2003 Server e no Active Directory. A rede é formada por um único domínio: abc.com. Os clientes são baseados no Windows Server 2003 Professional e alguns clientes no Windows XP Professional. Você gostaria de restringir o acesso as configurações de rede, tais como as configurações do protocolo TCP/IP para os usuários da rede. Estas restrições serão impostas via GPO. Você criou uma nova GPO chamada SemAcessoRede, na qual você fez as configurações para desabilitar o acesso as propriedades de configuração da interface de rede local. A GPO foi associada ao domínio abc.com. Porém você quer que o acesso às propriedades de configuração da interface de rede sejam liberadas para os membros dos grupos Domain Admins. (Admins. do Domínio) e Suporte Técnico. Quais os passos para que as restrições sejam aplicadas a todos os usuários, com exceção dos membros dos grupos Domain Admins e Suporte Técnico?

- a) Crie um grupo chamado Usuários da rede ou outro nome que preferir.

Inclua as contas de todos os usuários neste grupo, menos as contas dos administradores e dos técnicos.

Na GPO SemAcessoRede, garante a permissão Apply Group Policy (Aplicar diretiva de grupo), para o grupo Usuários da rede.

Na GPO SemAcessoRede, marque a opção Deny (Negar), para a permissão Apply Group Policy (Aplicar diretiva de grupo), para os grupos Domain Admins e Suporte Técnico.

- b) Crie um grupo chamado Usuários da rede ou outro nome que preferir.

Inclua as contas de todos os usuários neste grupo, menos as contas dos administradores e dos técnicos.

Na GPO SemAcessoRede, garante a permissão Apply Group Policy (Aplicar diretiva de grupo), para o grupo Usuários da rede.

- c) Crie um grupo chamado Usuários da rede ou outro nome que preferir.

Inclua as contas de todos os usuários neste grupo, menos as contas dos administradores e dos técnicos.

Na GPO SemAcessoRede, garante a permissão Apply Group Policy (Aplicar diretiva de grupo), para o grupo Usuários da rede.

Na GPO SemAcessoRede, marque a opção Deny (Negar), para o grupo Everyone (Todos).

- d) Crie um grupo chamado Usuários da rede ou outro nome que preferir.

Inclua as contas de todos os usuários neste grupo, menos as contas dos administradores e dos técnicos.

Na GPO SemAcessoRede, marque a opção Deny (Negar), para a permissão Apply Group Policy (Aplicar diretiva de grupo), para os grupos Domain Admins e Suporte Técnico.

- e) Não é possível implementar a solução proposta.

**Resposta certa: a**

**Comentários:** Continuando a discussão da questão 07, a solução para o inconveniente descrito na questão 07, que é o que pede o enunciado da questão 08, está descrito na alternativa a. Primeiro cria-se um grupo com todos os usuários

para os quais deve-se aplicar a permissão e atribui-se a permissão Apply Group Policy (Aplicar diretiva de grupo) a este grupo. Com isso, as configurações da GPO serão aplicadas a este grupo, o que na prática irá bloquear o acesso as configurações da rede para este grupo. O próximo passo é fazer com que as configurações da GPO não sejam aplicadas aos grupos Domain Admins e Suporte Técnico. Para tal basta negar a permissão Apply Group Policy (Aplicar diretiva de grupo) para estes grupos. O resultado prático é que os grupos Domain Admins e Suporte Técnico não terão o acesso às propriedades da rede, bloqueado, ou seja, exatamente o que propõem o enunciado da questão.

**Questão 09:** Você é o Administrador de uma rede com servidores baseados no Windows Server 2003 e no Active Directory. O servidor SRVSUS01 será utilizado com servidor SUS, o qual será utilizado para distribuir aplicações críticas para as estações cliente da rede. Inicialmente você instalou e configurou o IIS neste servidor. O próximo passo é instalar o SUS. Você instalou e configurou o SUS para fazer a distribuição de atualizações para os clientes da rede. Agora você precisa fazer o backup das configurações do SUS, para que estas possam ser rapidamente restauradas, em caso de falha. Quais os passos para fazer o backup das informações de configuração do SUS?

- a) Faça um backup do Estado do Sistema.
- b) Faça um backup do Estado do Sistema.  
Faça um backup da pasta C:\InetPub
- c) Faça um backup do Metabase do IIS (IIS Metabase)  
Em seguida use o Backup de Utilitário para fazer um backup do arquivo de backup da Metabase e das demais configurações do IIS.
- d) Faça um backup do Metabase do IIS (IIS Metabase)
- e) Use o utilitário de Backup, para fazer um backup completo do IIS.

**Resposta certa: c**

**Comentários:** Esta questão é interessante e exige que o candidato lembre de alguns pontos importantes: Primeiro você fazer um backup da Metabase, a qual contém uma série de configurações do IIS. O SUS depende do IIS, por isso você deve fazer, além do backup da Metabase, um backup das configurações do IIS, tal como o Site Padrão e outras. Feito o backup da Metabase em um arquivo, você pode utilizar o utilitário de backup, para fazer um backup deste arquivo. Com isso ficamos com a alternativa C, ou seja, primeiro uso o console de Administração do IIS para fazer um backup da Metabase e em seguida, uso o utilitário de backup do Windows, para fazer o backup deste arquivo e das demais configurações do IIS.

**Questão 10:** Considere as afirmações a seguir, em relação aos tipos de Backup do Windows Server 2003:

- I. Backup Normal: Com este tipo de backup todos os arquivos são copiados, toda vez que o backup for executado, independentemente de os arquivos terem sido alterados ou não. O arquivo é marcado como tendo sido feito o backup, ou seja, o atributo de arquivamento é desmarcado
- II. Backup Cópia: Backup que copia todos os arquivos selecionados, mas não marca cada arquivo como tendo sofrido backup (em outras palavras, o atributo de arquivamento não é desmarcado). É idêntico ao backup Normal, com a diferença de que os arquivos não são marcados como tendo sido copiados.
- III. Cada arquivo tem um atributo que pode ser marcado ou desmarcado. Este atributo serve para informar ao Windows Server 2003 se o arquivo foi ou não modificado desde o último backup normal
- IV. A principal vantagem do backup normal é a facilidade para fazer a restauração dos arquivos, quando necessário. Com o backup do tipo normal, para restaurar os dados, você precisa apenas do último backup normal que foi criado.

- V. A desvantagem do backup normal é o tamanho do backup e o tempo para execução. Em cada execução do backup, todos os arquivos e pastas serão copiados, independentemente de terem sido alterados ou não.

São verdadeiras as seguintes afirmações:

- a) I, II, III
- b) I, II, IV
- c) I, II, III, IV
- d) I, III, IV, V
- e) I, II, III, IV e V

Resposta certa: e

**Comentários:** Esta questão testa os conhecimentos do candidato em relação aos tipos de Backup disponíveis no Windows Server 2003. Todas as afirmações estão corretas e descrevem as características dos backups do tipo Normal e Cópia. É muito importante que você conheça bem os diferentes tipos de Backup disponíveis no Windows Server 2003 e as diferentes estratégias de Backup/Restore. Estes são pontos muito importantes para o exame.

**Questão 11:** Considere as afirmações a seguir, em relação aos tipos de Backup do Windows Server 2003:

- I. Geralmente, o backup normal é executado quando você cria um conjunto de backup pela primeira vez. Nos backup subsequentes é comum a utilização de outros tipos de backup, tais como o tipo Incremental ou Diferencial.
- II. O Backup do tipo cópia é útil caso você queira fazer backup de arquivos entre os backups normal e incremental, pois ela não afeta essas outras operações de backup ou quando você precisa fazer uma cópia extra dos dados para enviar para um filial da empresa ou para manter a cópia armazenada em um local seguro.
- III. Backup Incremental: Este tipo de backup copia somente os arquivos criados ou alterados desde o último backup normal ou desde o último backup incremental. Os arquivos copiados para o backup são marcados (ou seja, o atributo de arquivamento é desmarcado).
- IV. Se você utilizar uma combinação de backups normais e incrementais para restaurar os seus dados, será preciso ter o último backup normal e todos os conjuntos de backups incrementais feitos após este backup normal e restaurá-los na seqüência correta.
- V. A grande vantagem do backup incremental é que ele reduz o tempo necessário para a execução do backup, pois somente é feita a cópia dos arquivos que foram criados ou modificados desde o último backup normal ou incremental. A grande desvantagem é que para fazer a restauração é necessário o último backup normal e todos os backups incrementais subsequentes.
- VI. Os backups incrementais devem ser restaurados na seqüência cronológica em que foram criados. Além disso, se um dos backups incrementais apresentar problemas, não será possível restaurar os dados até o ponto do último backup incremental.

São verdadeiras as seguintes afirmações:

- a) I, II, III, IV
- b) I, II, IV
- c) I, II, III, IV, VI
- d) I, III, IV, V
- e) I, II, III, IV, V e VI

Resposta certa: e

**Comentários:** Esta questão testa os conhecimentos do candidato em relação aos tipos de Backup disponíveis no Windows Server 2003. Todas as afirmações estão corretas e descrevem as características dos backups do tipo Normal e todos os detalhes sobre o Backup do tipo Incremental. É muito importante que você conheça bem os diferentes tipos de Backup disponíveis no Windows Server 2003 e as diferentes estratégias de Backup/Restore. Estes são pontos muito importantes para o exame.

**Questão 12:** Você é o Administrador de uma rede formada por um único domínio: abc.com. Todos os servidores são baseados no Windows Server 2003. O servidor SRVDC01 é um controlador de domínio. Você é o Administrador responsável por este servidor. Você está planejando uma política de Backup para o servidor SRVDC01. O Backup deve incluir cópias de segurança da Registry, dos arquivos de inicialização, das informações do servidor de Certificados e informações sobre o registro das classes COM+. Qual opção de backup você deve utilizar?

- a) Backup da pasta %SystemRoot%
- b) Backup Normal do C:
- c) Backup de Cópia do C:
- d) Backup do Estado do Sistema (System State)
- e) Backup da pasta %Windir%

**Resposta certa: d**

**Comentários:** Para fazer o Backup das informações citadas - Registry, arquivos de inicialização, informações do servidor de Certificados e Registro das classes COM+, deve ser feito um backup do Estado do Sistema. O Backup do Estado do Sistema (System State), inclui as seguintes informações (informações e dados que são incluídos neste tipo de Backup):

- ◆ Registro
- ◆ COM+ Banco de dados de registro de classe
- ◆ Arquivos de inicialização, incluindo os arquivos de sistema
- ◆ Banco de dados Serviços de certificados
- ◆ Serviço de diretório do Active Directory
- ◆ Diretório SYSVOL
- ◆ Informações do serviço de cluster

O Backup se refere a esses componentes de sistema como os dados do estado do sistema. Para o Windows 2000 Professional, os dados do estado do sistema incluem somente o registro, o COM+ Banco de dados de registro de classe e os arquivos de inicialização. Para os sistemas operacionais do Windows 2000 Server, os dados do estado do sistema incluem o registro, o COM+, Banco de dados de registro de classe, os arquivos de inicialização e o banco de dados Serviços de certificados (caso o servidor seja um servidor de certificados - Certificate Services). Se o servidor for um controlador de domínio, o diretório SYSVOL e o Active Directory também serão incluídos nos dados do estado do sistema. Além disso, se você estiver executando o domain name service (DNS, sistema de nomes de domínios) em um controlador de domínio, a parte do Active Directory dos dados do estado do sistema também irá conter todas as informações da área do DNS. Se o servidor estiver executando o serviço de cluster, os dados do estado do sistema também irão incluir quaisquer pontos de verificação do registro de recurso e o log de recuperação do recurso de quorum que contém as informações mais recentes do banco de dados de cluster.

Quando você escolhe fazer backup ou restaurar os dados do estado do sistema, todos os dados do estado do sistema relevantes ao computador são restaurados ou colocados em backup. Você não pode escolher fazer backup ou restaurar componentes individuais dos dados do estado do sistema. Isso é devido às dependências entre os componentes do

estado do sistema. Porém, você pode restaurar os dados do estado do sistema em um local alternativo. Se você fizer isso, somente os arquivos da Registry, os arquivos de diretório SYSVOL, os arquivos de informações do banco de dados do agrupamento e os arquivos de inicialização do sistema serão restaurados no local alternativo. O banco de dados de serviços de diretório do Active Directory, os bancos de dados Serviços de certificados e o COM+ Banco de dados de registro de classe não serão restaurados se você designar um local alternativo ao restaurar os dados do estado do sistema.

Além disso, se você possuir mais de um controlador de domínio na sua organização e o serviço de diretório do Active Directory for replicado para qualquer um desses outros servidores, você talvez tenha que restaurar com autorização quaisquer dados do Active Directory que deseje restaurar. Para fazer isso, você precisa executar o utilitário Ntdsutil após ter restaurado os dados do estado do sistema mas antes de reiniciar o servidor na rede. O utilitário Ntdsutil permite a você marcar objetos do Active Directory para restauração de autorização. Isso irá assegurar que quaisquer dados distribuídos ou replicados que você restaurar sejam replicados corretamente ou distribuídos na sua organização.

Por exemplo, se você inadvertidamente excluir ou modificar objetos armazenados no serviço de diretório do Active Directory e esses objetos forem replicados ou distribuídos para outros servidores, você precisará restaurar a autorização desses objetos para que sejam replicados ou distribuídos a outros servidores. Se você não restaurar a autorização desses objetos, eles nunca serão replicados ou distribuídos aos seus outros servidores pois irão parecer serem mais antigos do que os objetos atualmente nos seus outros servidores. Usar o utilitário Ntdsutil para marcar objetos para restauração de autorização assegura que os dados que você deseja restaurar serão replicados ou distribuídos na sua organização. Por outro lado, se o seu disco de sistema falhou ou o banco de dados do Active Directory foi corrompido, você pode simplesmente restaurar os dados sem autorização sem usar o utilitário Ntdsutil.

O utilitário de linha de comando Ntdsutil pode ser executado a partir do prompt de comando. Também é possível obter ajuda para o utilitário Ntdsutil no prompt de comando digitando ntdsutil /?.

Observações:

- ◆ Você deve ter permissões ou direitos de usuário específicos para fazer o backup de arquivos e pastas.
- ◆ Para restaurar os dados do estado do sistema em um controlador de domínio, você deve primeiro iniciar o computador no modo de restauração de serviços de diretório. Isso irá permitir a você restaurar o diretório SYSVOL e o Active Directory.
- ◆ Você só pode fazer o backup e restaurar os dados do estado do sistema em um computador local. Você não pode fazer o backup e restaurar os dados do estado do sistema em um computador remoto.
- ◆ Embora você não possa alterar quais os componentes do estado do sistema dos quais foi feito backup, pode fazer backup de todos os arquivos de sistema protegidos com os dados do estado do sistema definindo as opções de backup avançadas.

**Questão 13:** Você é o Administrador de uma rede com servidores baseados no Windows Server 2003 Server e no Active Directory. Para auxiliar na administração do ambiente, você está utilizando o recurso de Assistência Remota. Você gostaria de utilizar este recurso, mesmo quando estiver acessando a rede da empresa a partir de casa, através de uma conexão via Internet. Toda conexão da rede da Empresa para a Internet e vice-versa é feita através de um Firewall. Para que você possa utilizar o recurso de Administração remota, através do Firewall, o que deve ser feito?

- a) A porta 3389 deve ser habilitada no Firewall
- b) A porta 443 deve ser habilitada no Firewall
- c) A porta 80 deve ser habilitada no Firewall
- d) O recurso de NAT deverá ser desabilitado.
- e) O recurso de VPN deverá ser desabilitado.

Resposta certa: a

**Comentários:** Como usar a assistência remota através de um firewall:

A assistência remota usa o protocolo de área de trabalho remota (RDP - Remot Desktop Protocol) para estabelecer uma conexão entre um usuário que está solicitando ajuda e um assistente que está oferecendo a ajuda. O RDP usa a porta TCP 3389 para essa conexão. Para permitir que os usuários de uma organização solicitem ajuda fora da organização usando a assistência remota, a porta 3389 deverá estar aberta no firewall. Para proibir os usuários de solicitarem ajuda fora da organização, essa porta deverá estar fechada no firewall.

Se fechar a porta 3389, você também bloqueará todos os serviços de terminal e de área de trabalho remota. Se desejar permitir esses serviços, mas limitar as solicitações de assistência remota, use o recurso de GPOs, para configurar as diretivas relacionadas a assistência remota e ao terminal services. Se a porta estiver aberta somente para tráfego de saída, um usuário poderá solicitar assistência remota usando o Windows Messenger.

Com isso ficamos com a alternativa a, ou seja, a porta 3389 deve ser habilitada. A porta 443 é utilizada pelo protocolo SSL - Security Sockets Layer. A porta 80 é a porta padrão para o HTTP. E o uso da assistência remota não tem nada a ver com o fato de os recursos de NAT ou VPN estarem sendo utilizados.

**Questão 14:** Considere as afirmativas a seguir, em relação as diretivas de auditoria que podem ser configuradas via recurso de GPO, para um domínio baseado no Windows Server 2003:

- I. A diretiva Audit account logon events (Auditoria de eventos de logon de conta) deve ser habilitada quando você deseja fazer a auditoria de eventos de logon feitos com contas pertencentes ao domínio.
- II. O nome correto desta auditoria é Auditoria de eventos de logon de conta, porém no console Configurações padrão de segurança do domínio, esta diretiva aparece, incorretamente, com o seguinte nome: Eventos de logon de conta de auditoria. Esta é mais uma pérola da tradução, que contribui para tornar confuso um recurso que é fácil de utilizar.
- III. Com esta diretiva você pode configurar se os eventos de logon devem ou não ser auditados. São considerados eventos de logon, qualquer logon feito em uma estação de trabalho da rede, que pertença ao domínio e com uma conta do domínio.
- IV. Existe uma outra auditoria, com um nome semelhante – Auditoria de eventos de logon, porém esta diretiva é usada para fazer a auditoria de eventos de logon usando contas locais dos computadores e não as contas do domínio.

Estão corretas as seguintes afirmativas:

- a) I
- b) I e II
- c) I, II e III
- d) I, II e IV
- e) I, II, III e IV

Resposta certa: e

**Comentários:** Esta questão testa o conhecimento do candidato sobre duas diretivas muito importantes, as quais tem nome semelhantes. Para piorar um pouco a situação, uma das diretivas foi pessimamente traduzida. Para responder corretamente a esta questão, o candidato deve conhecer bem as seguintes diretivas:

◆ **Audit account logon events (Auditoria de eventos de logon de conta):**

Com esta opção você pode configurar se os eventos de logon devem ou não ser auditados. São considerados eventos de logon, qualquer logon feito em uma estação de trabalho da rede, que pertença ao domínio e com uma conta do domínio.

Conforme descrito anteriormente, a validação do logon é feita nos DCs, onde está instalado o Active Directory. Neste caso se o usuário jsivla fizer o logon com a sua conta de domínio, na sua estação de trabalho, um evento de logon será gerado para este usuário. Além disso você define se devem ser auditados os eventos com sucesso (quando o usuário faz o logon normalmente) ou com falha (quando o usuário não consegue fazer o logon, por exemplo, por ter digitado uma senha incorreta). Para configurar esta auditoria, basta dar um clique duplo nela. Será aberta a janela Propriedades de Eventos de logon de conta de auditoria (a confusão no nome é por conta da equipe de tradução). Para habilitar esta diretiva você deve marcar a opção Definir as configurações dessas diretivas (o plural também é por conta da equipe de tradução). Ao marcar esta opção, serão habilitadas as opções Êxito e Falha. Para passar a registrar os eventos de logon com sucesso, marque a opção Êxito. Com isso sempre que um usuário fizer um logon no domínio, com sucesso, será registrado um evento no log de eventos do DC que autenticou o usuário. Para passar a registrar os eventos de falha de logon, marque a opção Falha. Com isso, sempre que um usuário fizer uma tentativa de logon sem sucesso, será registrado um evento no log de eventos do DC onde a tentativa de logon foi feita. O mais comum para este diretiva é habilitar tanto os eventos de sucesso, quanto os eventos de falha, para que fique registrado no log do servidor, todos os eventos de logon, que seja com sucesso, quer seja com falha.

◆ **Audit logon events (Auditoria de eventos de logon):**

Esta diretiva determina se deve ser feita a auditoria de cada instância de logon ou logoff de usuário, bem como de qualquer conexão de rede com o computador local, ou no caso com o DC que eu estou utilizando. Se você estiver registrando no log os eventos da Auditoria de eventos de logon de conta com êxito em um controlador de domínio, as tentativas de logon de um usuário, a partir da sua estação de trabalho não gerarão auditorias de logon (as quais serão geradas se a diretiva Auditoria de eventos de logon de conta, descrita anteriormente, estiver habilitada). Somente tentativas de logon de rede e interativas no próprio controlador de domínio gerarão eventos de logon.

Resumindo, Auditoria de eventos de logon de conta são gerados no local onde reside a conta; ou seja, no DC. Eventos de logon são gerados no local onde ocorre a tentativa de logon. Se for um logon interativo no DC, no próprio DC, se for um logon interativo em um member Server, no log de auditoria local do member server. Você pode configurar para que sejam auditadas tentativas de logon com sucesso, com falha ou ambas. No caso de um computador com o Windows Server 2003, as tentativas de logon são consideradas as tentativas locais ou tentativas feitas via Terminal Service Client.

**IMPORTANTE:** O nome correto desta auditoria é Auditoria de eventos de logon de conta, porém no console Configurações padrão de segurança do domínio, esta diretiva aparece, incorretamente, com o seguinte nome: Eventos de logon de conta de auditoria. Esta é mais uma pérola da tradução, que contribui para tornar confuso um recurso que é fácil de utilizar.

**IMPORTANTE:** É muito importante que você conheça este ponto, ou seja, para fazer a auditoria de eventos de logon de contas do domínio, a diretiva a ser habilitada é a diretiva Auditoria de eventos de logon de conta. Existe uma outra auditoria, com um nome semelhante – Auditoria de eventos de logon, porém esta segunda é usada para fazer a auditoria de eventos de logon usando contas locais dos computadores e não as contas do domínio. Certifique-se de que você entendeu bem a diferença entre estas duas diretivas, pois este é um ponto importante para o exame.

**IMPORTANTE:** Vou insistir neste ponto. Lembre-se que a diretiva Auditoria de eventos de logon de conta é utilizada para fazer auditoria de logon de contas do domínio, já a diretiva Auditoria de eventos de logon, é utilizada para a auditoria de eventos de logon de contas locais.

**Questão 15:** Você é o administrador de uma rede baseada no Windows Server 2003 Server e no Active Directory. A rede é formada por um único domínio: abc.com. Você é o administrador responsável pela monitoração do desempenho de 15 servidores da rede. O objetivo é coletar os dados de diversos contadores (tais como % tempo de processador, bytes comprometidos, etc) e armazenar estas informações em um banco de dados centralizado, onde você possa fazer análises, pesquisas e comparações. Das opções a seguir, qual a mais indicada para implementar a solução desejada?

- a) Salvar os dados coletados no formato de arquivos .csv, em um drive de rede.  
Criar scripts para importar estes dados em um banco de dados do SQL Server.
- b) Salvar os dados coletados no formato de arquivos .csv, em um drive de rede.  
Criar scripts para importar estes dados em um banco de dados do Microsoft Access.
- c) Salvar os dados coletados no formato de arquivos .csv, em um drive de rede.  
Utilizar o Microsoft Excel para importar os arquivos .csv.
- d) Criar um log onde você adicionar contadores dos diversos servidores.  
Configurar o tipo de arquivo de log, para salvar os dados em um banco de dados do SQL Server.
- e) Criar um log onde você adicionar contadores dos diversos servidores.  
Configurar o tipo de arquivo de log, para salvar os dados em um arquivo binário.  
Importar o arquivo binário em um banco de dados do SQL Server.

Resposta certa: d

**Comentários:** Esta questão testa se o candidato conhece a possibilidade de configurar um log, para que salve os dados diretamente em um banco de dados do SQL Server. Ao criar um novo log, você pode acessar as propriedades do log e clicar na guia Arquivos de log. Na lista Tipo de arquivo de log, você pode selecionar a opção Banco de dados SQL. Selecione esta opção e clique no botão Configurar... Será aberta uma janela, para que você selecione uma fonte ODBC, do tipo DSN de sistema, a qual faz a conexão com o banco de dados do SQL Server. Antes de usar esta opção, você já deve ter criada a fonte ODBC, usando a opção Iniciar -> Ferramentas administrativas -> Fontes de dados (ODBC).

**Questão 16:** Você é o Administrador de uma rede com servidores baseados no Windows Server 2003 Server e no Active Directory. A rede é formada por um único domínio: abc.com. A WAN da empresa é formada pela rede local da matriz em SP e pelas redes locais das filiais em SC, RS e PR. Você está em fase de implementação da rede e gostaria de limitar o número de usuários com permissões de Administrador em todos os recursos do domínio, ou seja, você quer reduzir o número de usuários que serão incluídos no grupo Admins. do Domínio (Domain Admins.). Porém você gostaria de ter usuários com permissão para gerenciar recursos tais como contas de usuários e computadores em cada uma das redes locais. Por exemplo, você gostaria de permitir que um usuário da matriz em SP possa gerenciar recursos apenas para os usuários, servidores e recursos da rede local de SP. Que tipo de objeto do Active Directory você pode utilizar para implementar a solução proposta?

- a) Unidades Organizacionais
- b) Group Policy Objects
- c) Diretivas de IPSec
- d) Diretivas locais de segurança
- e) Grupos de distribuição

**Resposta certa: a**

**Comentários:** O conceito de Unidade organizacional foi introduzido no Windows 2000 Server, juntamente com o Active Directory e veio para solucionar um problema sério de Administração existente no Windows NT Server 4.0.

Com o NT Server 4.0, não havia como atribuir permissões de acesso apenas a uma parte do domínio. Ou você atribuía permissões de Administrador no domínio inteiro ou não tinha como atribuir permissões de administrador para um usuário apenas para parte dos recursos do domínio. Imagine uma empresa que tem uma rede, com filiais em todos os estados brasileiros. No nosso exemplo, o domínio é composto pelas redes das filiais do RS, SC, PR e SP. Com o NT Server 4.0, você não teria como definir que um usuário tivesse permissões de Administrador somente nos servidores da filial do RS. Uma vez que você atribuía permissões de Administrador, o usuário teria estas permissões em todos os recursos do domínio. No nosso exemplo, o usuário seria Administrador nos servidores e em todos os recursos das filiais do RS, SC, PR e SP, ou seja, em todos os servidores do domínio.

Esta situação gerava inconvenientes (e noites de sono perdidas) muito sérios. Era comum a situação onde um domínio tinha 10 ou mais contas de usuários com permissão de Administrador. Ora, eram 10 ou mais contas com permissões total em todos os servidores do domínio. Nada bom.

Com a disponibilidade de Unidades Organizacionais, a partir do Windows Server 2003 Server, este problema foi minimizado. Agora você pode criar, dentro do domínio, várias Unidades organizacionais. Em seguida você desloca para dentro de cada unidade organizacional, as contas de usuários, grupos e computadores, de acordo com critérios geográficos ou funcionais. Em seguida você pode delegar tarefas administrativas a nível de Unidade organizacional (OU – Organizational Unit).

**Questão 17:** O usuário jsilva pertence aos seguintes grupos: Gerentes, Técnicos e Marketing. O usuário jsilva precisa ter acessos somente de leitura nos documentos do Word que estão em uma pasta compartilhada, no servidor \\SRV01\worddocs. O usuário deve ter permissão somente de leitura, quer ele esteja acessando a pasta worddocs através da rede ou localmente logado no servidor SRV01.

As permissões NTFS e de compartilhamento desta pasta e o seu conteúdo, estão configuradas da seguinte maneira:

- ◆ Permissões NTFS:
  - ◆ Gerentes: Leitura e alteração
  - ◆ Técnicos: Leitura
  - ◆ Marketing: Acesso total
- ◆ Permissões de Compartilhamento:
  - ◆ Gerentes: Leitura
  - ◆ Técnicos: Leitura
  - ◆ Marketing: Leitura

O que deve ser alterado para que o usuário jsilva não possa alterar os documentos desta pasta, mas sim somente ler o conteúdo dos documentos, quer seja através da rede, quer seja acessando localmente no servidor SRV01?

- a) Atribua a permissão Negar Leitura a conta jsilva.
- b) Retire o usuário jsilva do grupo Gerentes.
- c) Retire o usuário jsilva do grupo Marketing.
- d) Define permissão de leitura para a conta jsilva.
- e) Retire o usuário jsilva do grupo Gerentes e também do grupo Marketing.

**Resposta certa: e** Você Respondeu:

**Comentários:** Para responder corretamente a esta questão, é importante que você lembre de algumas regras básicas das permissões NTFS, quando o usuário pertence a mais de um grupo:

- ◆ A permissão efetiva é a soma das permissões de todos os grupos aos quais o usuário pertence.
- ◆ Negar tem precedência sobre qualquer outra permissão.
- ◆ Quando combinamos a permissão de compartilhamento resultante, com a permissão NTFS resultante, vale a mais restritiva.

Também é importante lembrar que quando existem diferenças entre as permissões NTFS e as permissões de Compartilhamento, vale a mais restritiva. Neste caso a permissão mais restritiva é a de compartilhamento que é somente Leitura. Neste caso o usuário jsilva, quando acessando através da rede, terá somente leitura. Não esqueça que as permissões de compartilhamento somente tem efeito para o acesso através da rede. Se o usuário jsilva fizer o logon no servidor SRV01 e acessar a pasta worddocs localmente, valerão apenas as permissões NTFS. Neste último caso, acessando localmente, o usuário jsilva teria permissão Controle Total na pasta worddocs. Por isso devemos retirá-lo dos grupos Gerentes e Marketing para que, localmente, ele também tenha permissão somente de leitura, a qual é herdada do grupo Técnicos.

**Questão 18:** Como administrador da rede você está em busca de uma solução que possa reduzir o número de drives de rede utilizados pelos usuários. Atualmente você está utilizando sete drives diferentes, conforme descrito a seguir:

| <b>Drive</b> | <b>Servidor</b> | <b>Compartilhamento</b> | <b>Descrição</b>                       |
|--------------|-----------------|-------------------------|--|
| F            | SRV01           | Docs                    | Documentos de domínio público          |
| G            | SRV01           | Manuais                 | Manuais de treinamentos.               |
| H            | SRV02           | Programas               | Programas de instalação.               |
| I            | SRV02           | Contab                  | Usados pela seção de contabilidade.    |
| J            | SRV02           | Pessoais                | Documentos pessoais dos usuários.      |
| K            | SRV03           | Modelos                 | Modelos de memorandos e ofícios.       |
| L            | SRV03           | Projetos                | Documentos compartilhados por projeto. |

Ao invés de usar sete drives diferentes, você gostaria de usar um único drive e que, cada compartilhamento, aparecesse como uma pasta dentro deste drive. Por exemplo, você gostaria de utilizar um drive R: e dentro do R: deveriam aparecer as pastas Docs, Manuais, Programas, Contab, Pessoais, Modelos e Projetos. Qual tecnologia/serviço você deve utilizar para implementar a solução proposta?

- a) Utilize Mounted Volumes.
- b) Crie um volume do tipo Striped Set com Paridade, usando um disco para cada partição.
- c) Utilize o DFS - Distributed File System.
- d) Utilize links simbólicos.
- e) Utilize o Script de Logon para consolidar os diversos compartilhamentos em um único drive.

**Resposta certa: c**

**Comentários:** Para consolidar diversos compartilhamentos em um único ponto de acesso, utilizamos o serviço DFS - Distributed File System. O DFS já faz parte do Windows 2000 Server e do Windows Server 2003, sendo instalado automaticamente durante a instalação do Windows. Para configurar o DFS usamos o console “Distributed File System”, o qual é acessado através do menu Ferramentas Administrativas.

**Questão 19:** Você é o Administrador de uma rede com servidores baseados no Windows Server 2003 Server e no Active Directory. Os clientes são baseados no Windows 2000 Professional e alguns clientes no Windows XP Professional. A rede é formada por um único domínio: abc.com. Todas as estações de trabalho estão configuradas para fazer parte do domínio. Você quer implementar configurações de tal maneira que os usuários tenham acesso a todas as suas configurações da Área de trabalho (Desktop), à pasta Meus documentos e aos seus aplicativos em qualquer computador da rede, independentemente de onde o usuário estiver logado. Por questões de segurança e facilidade de Backup, você quer que a pasta Meus documentos dos usuários, fiquem gravadas em servidores da rede. Quais recursos você deve utilizar para implementar as funcionalidades propostas?

a) Roaming Profiles.

Usar GPO para redirecionar a pasta Meus documentos dos usuários.

Usar GPO para associar programas com os usuários.

b) Configurar a Registry de cada estação de trabalho, para redirecionar o usuário para uma profile em um servidor da rede.

Usar GPO para redirecionar a pasta Meus documentos dos usuários.

Usar GPO para associar programas com os usuários.

c) Configurar Script de logon de cada usuário, para redirecionar o usuário para uma profile em um servidor da rede, quando este fizer o logon.

Usar GPO para redirecionar a pasta Meus documentos dos usuários.

Usar GPO para associar programas com os usuários.

d) Configurar nas propriedades da conta do usuário, para que ele utilize Roaming Profiles, para que seja redirecionada a pasta Meus documentos para uma pasta em um servidor da rede e para definir quais programas devem ser associados com o usuário.

e) Configurar Script de Inicialização de cada estação de trabalho, para redirecionar o usuário para uma profile em um servidor da rede, quando este fizer o logon.

Usar GPO para redirecionar a pasta Meus documentos dos usuários.

Usar GPO para associar programas com os usuários.

**Resposta certa: a**

**Comentários:** Esta questão testa os conhecimentos do candidato em relação as configurações do ambiente do usuário. Para que o usuário tenha as mesmas configurações da Área de Trabalho e do menu Iniciar, independentemente da estação na qual ele fizer o logon, você deve configurar uma Roaming Profile para o usuário. Esta configuração é feita nas propriedades da conta do usuário, na guia Perfil. Para redirecionar a pasta Meus documentos e para associar Software com o usuário (distribuição de Software), é utilizado o recurso de Group Policy Objects - GPO

**Questão 20:** Você é o Administrador de uma rede com servidores baseados no Windows Server 2003 Server e no Active Directory. Ao todo você tem 100 estações de trabalho com o Windows XP Professional, sendo que todas as estações estão configuradas para fazer parte do domínio abc.com. A rede é formada por um único domínio: abc.com. Em um computador chamado FILES01, você compartilhou uma pasta com o nome de compartilhamento DOCS. Você configurou o script de logon, para mapear uma unidade M:, automaticamente, durante o logon. A unidade M: está

associada com o caminho \\FILES01\DOCS. Em alguns horários do dia, você recebe chamadas dos usuários, informando que não é possível usar o drive M, que a conexão com FILES01 é recusada. Você observou que não são sempre os mesmos usuários que tem o problema de conexão, ou seja, usuários que em determinados momentos conseguem acessar o drive M; em outros momentos não conseguem e vice-versa. Qual a causa mais provável deste problema?.

- a) Problemas nas permissões NTFS da pasta DOCS
- b) O computador FILES01 é um computador com o Windows XP Professional.
- c) Problemas nas permissões de compartilhamento da pasta DOCS
- d) A pasta DOCS está criptografada.
- e) A pasta DOCS está compactada.

Resposta certa: b

**Comentários:** Existe um trecho do enunciado que é fundamental para esta questão: “Você observou que não são sempre os mesmos usuários que tem o problema de conexão, ou seja, usuários que em determinados momentos conseguem acessar o drive M; em outros momentos não conseguem e vice-versa”. Este trecho é uma indicação clara de que não é um problema de permissão (isso descarta as alternativas “a” e “c”) e nem um problema de criptografia (isso descarta a alternativa D). A alternativa “e” não tem nada a ver. A causa mais provável deste problema, é que o computador FILES01 é um computador com o Windows XP Professional instalado. Computadores com o Windows XP Professional, Windows 2000 Professional ou Windows NT Workstation 4.0, tem uma limitação de, no máximo, 10 conexões simultâneas. Esta é uma limitação das versões clientes do Windows. Em um ambiente de rede, com 100 estações de trabalho, certamente este limite será alcançado. Quando o limite de 10 conexões é atingido, novas conexões são recusadas. Por isso a mensagem de erro que alguns usuários recebem ao tentar fazer a conexão.

**Questão 21:** Você é o Administrador da rede da empresa, a qual é baseada no Windows Server 2003 Server e no Active Directory. As estações de trabalho da rede são baseadas no Windows XP Professional e no Windows 2000 Professional. Você quer implementar um ambiente personalizado, onde determinados atalhos devem estar presentes na área de trabalho dos usuários, independentemente do computador no qual o usuário fizer o logon. Além disso, o usuário não deve ser capaz de fazer alterações neste ambiente personalizado. O objetivo desta padronização deve é garantir um ambiente padronizado e reduzir o número de chamadas de suporte técnico. O que você deve fazer para implementar o ambiente personalizado, descrito nesta questão?

- a) Utilize o recurso de GPOs, para criar Roaming Profiles para os usuários.
- b) Utilize o DFS para criar Roaming Profiles para os usuários.
- c) Crie uma profile com as configurações desejadas.

Copie a profile para um servidor da rede.

Renomeie o arquivo Ntuser.dat para Ntuser.man

Configure as propriedades da conta de cada usuário, para que seja utilizada uma profile em um servidor da rede.

- d) Crie uma profile com as configurações desejadas.

Copie a profile para um servidor da rede.

Renomeie o arquivo Ntuser.dat para Ntuser.pol

Configure as propriedades da conta de cada usuário, para que seja utilizada uma profile em um servidor da rede.

- e) Não é possível implementar a solução proposta.

**Resposta certa: c**

**Comentários:** Esta questão testa o conhecimento do usuário em relação ao recurso de Profiles do Windows. O Windows mantém configurações separadas para cada usuário. Por exemplo, o usuário jsilva faz o logon e cria um ícone na área de trabalho. Este ícone não será exibido na área de trabalho de outros usuários, quando estes fizerem o logon no computador. O Windows também mantém diversas outras configurações separadamente para cada usuário, como por exemplo: papel de parede, opções do menu iniciar, configurações do Internet Explorer e do Outlook Express, associação de extensões de arquivos, configurações da barra de tarefas e assim por diante. A pasta Meus documentos também é individualizada para cada usuário. O Windows Server 2003 mantém estas configurações separadamente para cada usuário, através de uma estrutura de pastas e subpastas, dentro da pasta C:\Documents and settings. Dentro desta pasta o Windows Server 2003 cria uma pasta para cada usuário, pasta esta com o nome de logon do usuário. Por exemplo, todas as configurações do usuário jsilvap são gravadas e mantidas em uma estrutura de subpastas, dentro de C:\Documents and settings\jsilvap; todas as configurações do usuário pedro2 são gravadas e mantidas em uma estrutura de subpastas, dentro de C:\Documents and settings\paulo2 e assim por diante.

Este conjunto de configurações, que define o ambiente de trabalho de cada usuário, é conhecido como Profile do usuário (User Profile). Quando você trabalha em um ambiente de rede, baseado em um domínio do Windows 2000 Server ou do Windows Server 2003, é possível salvar as configurações da Profile de cada usuário em pastas em um servidor da rede. Este tipo de Profile é conhecido como Roaming Profile (eu me arriscaria a traduzir como Profile Viajante). O Roaming significa que a Profile acompanha (viaja com) o usuário através da rede. Ou seja, independente da estação de trabalho que o usuário estiver utilizando, ele receberá as configurações de sua Profile, as quais serão carregadas a partir da rede. Com a combinação do recurso de User Profiles com a distribuição de Software via GPO, é possível fazer com que os programas e as configurações “sigam” o usuário através da rede, ou seja, em qualquer estação de trabalho que o usuário faça o logon, ele terá a mesma área de trabalho, com o mesmo conjunto de ícones, atalhos e programas.

O caminho onde fica armazenada a Roaming Profile para o usuário é informada nas propriedades da conta do usuário, na guia Perfil, usando o campo Caminho do Perfil. Nesta guia você informa o caminho onde encontra-se a profile do usuário, como por exemplo: \\serv01\profiles\jsilva. O mais comum é, ao invés de informar o nome do usuário, usar a variável %username%, conforme exemplo a seguir: \\serv01\profiles%\username%. O uso da variável %username% evita problemas devido a erros de digitação. Para que o usuário não possa fazer alterações nas configurações contidas na Profile, você deve renomear o arquivo Ntuser.dat para Ntuser.man. Com isso você torna a profile Mandatory, ou seja, obrigatória, no sentido de que o usuário não pode alterar as configurações da profile. Ele até conseguirá alterar, mas ao fazer o logoff no computador, as alterações serão descartadas. Com isso ficamos com a alternativa C.

**Questão 22:** Você é o administrador de uma rede baseada no Windows Server 2003 Server e no Active Directory. A rede é formada por um único domínio e todos os servidores estão baseados no Windows Server 2003. Como parte da política de segurança da empresa, você instalou o SUS - Software Update Services (Serviço de Atualização Automática) em um dos servidores da Intranet. Ao consultar o site [www.microsoft.com/security](http://www.microsoft.com/security) você ficou sabendo que três novas atualizações críticas de segurança, foram disponibilizadas. Você acessou a página de administração do SUS e verificou que as novas atualizações já foram baixadas. Qual o próximo passo para que estas atualizações críticas de segurança sejam aplicadas nas estações de trabalho dos usuários?

- a) Você deve reiniciar todas as estações de trabalho dos usuários.
- b) Você deve configurar a GPO padrão do domínio, para aplicar as novas atualizações.
- c) Você deve usar a página de administração do SUS para aprovar as novas atualizações críticas de segurança.
- d) Use o comando gpupdate em todas as estações de trabalho.
- e) Basta reiniciar o IIS, no servidor onde o SUS está instalado.

**Resposta certa: c**

**Comentários:** O SUS é utilizado para automatizar o download de correções a partir do Windows Update. Um servidor com o SUS instalado, pode ser configurado consultar periodicamente o site Windows Update e fazer o download de novas atualizações, sempre que estas estiverem disponíveis. As chamadas atualizações críticas de segurança, após terem sido copiadas pelo SUS, devem ser aprovadas pelo Administrador, antes de serem aplicadas nas estações de trabalho da rede. Em situações onde as atualizações críticas já foram baixadas mas ainda não foram aplicadas, a causa mais provável é que estas ainda não foram aprovadas pelo Administrador. Para aprovar-las, basta que o administrador acesse a página de Administração do SUS e aprove as atualizações críticas.

**Questão 23:** Considere as afirmações a seguir em relação aos usos que o Administrador pode fazer do recurso de User Profiles:

- I. O uso de User Profiles é uma ferramenta de grande auxílio para o administrador, principalmente para a padronização do ambiente de trabalho dos usuários.
- II. O Administrador pode criar uma profile padrão e distribuir esta profile para um grupo de usuários da rede. Esta opção é útil para usuários que devam ter acesso restrito as opções de personalização do Windows. Por exemplo, posso usar uma profile para definir, automaticamente, os ícones da área de trabalho.
- III. O Administrador pode utilizar o recurso de profiles para automatizar a distribuição de software para as estações de trabalho da rede.
- IV. O Administrador pode criar as chamadas “Mandatory user profile”. Este tipo de profile não permite que o usuário faça alterações nas configurações definidas na profile. O usuário até consegue alterar o seu ambiente de trabalho, mas no momento em que for feito o log off, as alterações não serão salvas. Ao fazer o próximo logon, o usuário receberá as configurações definidas na profile que está no servidor, sem as alterações que ele fez, mas que não foram salvas. As configurações são copiadas para o computador do usuário cada vez que este faz o logon. Quando o usuário faz alterações, estas são feitas na sua cópia local da profile. Ao fazer o logoff, estas alterações não são repassadas para a profile que está gravada no servidor. No próximo logon é esta profile que está no servidor (sem alterações) que é novamente copiada para a estação de trabalho do usuário, sobrepondo as alterações que por ventura ele tenha feito. O resultado prático é que sempre que o logon é feito, são carregadas as configurações definidas na profile do tipo Mandatory, armazenada no servidor e para a qual somente o Administrador tem permissão para fazer alterações.

Estão corretas as seguintes afirmativas:

- a) I, II
- b) I, II e III
- c) I, III e IV
- d) I, II e IV
- e) I, II, III e IV

**Resposta certa: d**

**Comentários:** Esta questão trata de alguns dos usos que o Administrador pode fazer para o recurso de User Profiles. Cada alternativa descreve um uso específico ou uma vantagem, com exceção da afirmação III, a qual está incorreta. A distribuição de Software é feita usando GPOs e não profiles. O uso de profiles é apenas uma maneira de padronizar o ambiente de trabalho dos usuários e de poder armazenar estas configurações em um servidor da rede, para que a profile seja carregada para o usuário, a partir do servidor, em qualquer computador da rede onde o usuário fizer o

logon. Com isso a alternativa III está incorreta, ou seja, o recurso de profiles não pode ser utilizado para a distribuição de software.

**Questão 24:** Você trabalha com Administrador de uma rede baseada no Windows Server 2003 e com Clientes utilizando o Windows 2000 Professional ou o Windows XP Professional. Como Administrador da rede você está utilizando a seguinte política de Backup para o drive do servidor, onde estão os arquivos de dados dos usuários:

|                     |                       |
|---------------------|-----------------------|
| -> Domingo à noite: | <b>Backup Normal.</b> |
| -> Segunda à noite: | Backup incremental.   |
| -> Terça à noite:   | Backup incremental.   |
| -> Quarta à noite:  | Backup Diferencial.   |
| -> Quinta à noite   | Backup incremental.   |
| -> Sexta à noite    | Backup incremental.   |
| -> Sábado à noite:  | Backup diferencial.   |
| -> Domingo à noite: | <b>Backup Normal.</b> |

No sábado alguns usuários trabalharam, alterando diversos arquivos no drive do Servidor. Na segunda pela manhã, ao chegar ao serviço, você constata que o disco do servidor, onde estavam os arquivos dos usuários, foi danificado. Ao consultar o log do Backup, consta que o Backup do domingo foi feito normalmente, o que leva você a concluir que o problema com o disco ocorreu na madrugada de domingo para segunda. Você substitui o disco e agora deseja restaurar os dados. Qual ou quais o(s) backup(s) você deve restaurar e em que seqüência?

- a) Normal do domingo anterior.
  - ◆ Incremental de segunda-feira.
  - ◆ Incremental de terça-feira.
  - ◆ Incremental de quarta-feira.
  - ◆ Incremental de quinta-feira.
  - ◆ Incremental de sexta-feira.
- b) Normal do domingo anterior.
  - ◆ Incremental de segunda-feira.
  - ◆ Incremental da quarta-feira.
  - ◆ Incremental de sexta-feira.
- c) Normal do domingo anterior.
  - ◆ Incremental de sexta-feira.
- d) Incremental da sexta-feira.
- e) Normal do último domingo.

Resposta certa: e

**Comentários:** O Backup Normal faz a cópia de todos os dados, independentemente de terem sido alterados ou não. O Incremental faz o backup apenas dos dados que foram alterados desde o último backup incremental. O Diferencial faz o backup de todos os dados que foram alterados desde o último backup normal. Para restaurar os dados até a condição de que estavam no Domingo, mantendo com isso as alterações feitas no Sábado, você deve restaurar o último backup normal, ou seja, o backup Normal do último domingo. Com isso você volta a condição do Domingo anterior. Nesta situação não haverá nenhuma perda de dados, pois as últimas alterações feitas no Sábado estarão todas contidas no Backup Normal de domingo. Com isso ficamos com a alternativa “e”.

**Questão 05:** Considere as afirmações a seguir em relação aos recursos do Terminal Server:

- I. Os Serviços de terminal do Windows 2000 Server podem adicionar e reconectar automaticamente impressoras conectadas aos clientes de Serviços de terminal.
- II. Os usuários podem agora recortar e colar entre programas que estão sendo executados no computador local e no Terminal server.
- III. Existe suporte a desconexão móvel. Esse recurso permite que os usuários se desconectem de uma sessão sem efetuar logoff. A sessão pode permanecer ativa enquanto está desconectada, permitindo que o usuário reconecte-se à sessão existente de outro computador ou posteriormente. O logon é necessário para a reconexão, mantendo sempre cada sessão segura.
- IV. Existe suporte a vários logons. Os usuários podem efetuar logon em várias sessões simultaneamente de um ou mais clientes, em vários Windows 2000 Servers ou em um único servidor diversas vezes. Como resultado, o usuário pode executar diversas tarefas ao mesmo tempo ou executar várias sessões de área de trabalho únicas.

Estão corretas as seguintes afirmações:

- a) Todas
- b) Somente I, II e III
- c) Somente I e II
- d) Somente II, III e IV
- e) Somente III e IV

**Resposta certa:** a

**Comentários:** Todas as afirmações estão corretas e representam recursos que foram introduzidos no Terminal Server a partir do Windows 2000 Server e que também estão presentes no WIndows Server 2003.

**Questão 26:** Você é o Administrador de uma rede com servidores baseados no Windows Server 2003 e no Active Directory. Os clientes são baseados no Windows 2000 Professional e alguns clientes no Windows XP Professional. A rede é formada por um único domínio: juliobattisti.com.br. Como parte da política de administração remota dos servidores da rede, você quer disponibilizar as ferramentas administrativas, tais como console de administração do DNS, DHCP, RRAS, Usuários e Computadores do Active Directory e assim por diante, nas estações de trabalho de cinco funcionários (estações baseadas no Windows XP Professional), os quais fazem parte do grupo Admins. do Domínio, para que estes funcionários possam administrar estes serviços, nos diversos servidores do domínio, remotamente. O que você deve fazer?

- a) As Ferramentas Administrativas não podem ser utilizadas em uma estação de trabalho.  
Utilize o Terminal Server no modo de Administração remota.
- b) Faça o logon em cada uma das estações de trabalho onde as ferramentas administrativas devem ser instaladas.

Conecte-se com o drive onde o Windows Server 2003 está instalado, em um dos servidores.

Acesse a pasta %windir%/system32

Dê um clique duplo no arquivo Adminpak.msi

Siga as instruções para concluir o assistente de instalação.

c) Faça o logon em cada uma das estações de trabalho onde as ferramentas administrativas devem ser instaladas.

Conecte-se com o drive onde o Windows Server 2003 está instalado, em um dos servidores.

Acesse a pasta %windir%/system32

Dê um clique duplo no arquivo AdminTools.msi

Siga as instruções para concluir o assistente de instalação.

d) Faça o logon em cada uma das estações de trabalho onde as ferramentas administrativas devem ser instaladas.

Acesse a opção Adicionar ou remover programas, do Painel de controle.

Altere a instalação do Windows, para adicionar o pacote de Ferramentas administrativas.

e) Faça o logon em cada uma das estações de trabalho onde as ferramentas administrativas devem ser instaladas.

Utilize o Windows Update para instalar o pacote de ferramentas administrativas.

**Resposta certa: b**

**Comentários:** As ferramentas administrativas (conjunto de consoles para administração de uma série de serviços e recursos do WIndows Server 2003 e do Active Directory), podem ser instaladas em uma estação de trabalho com o WIndows 2000 Professional ou Windows XP Professional. O pacote de ferramentas administrativas está disponível no arquivo Adminpak.msi. Este arquivo, por padrão, está disponível na pasta %windir%/system32, de todos os servidores com o Windows 2000 Server ou Windows Server 2003. Onde %windir% representa a pasta onde o Windows foi instalado. Com isso ficamos com a alternativa “c”.

**Questão 27:** Você está instalando o Windows Server 2003 em um novo Servidor. Este servidor tem quatro discos SCSI de 30 GB cada um. Você pretende configurar os discos da seguinte maneira. Juntar o disco 0 e o disco 1 formando um Volume Set de 60 GB. Neste Volume Set você pretende instalar o Windows Server 2003 e todos os aplicativos do Servidor. O disco 2 será utilizado para compartilhamento de arquivos, o qual os usuários irão acessar através de um drive mapeado. O disco 3 será utilizado para Backup do Estado do Sistema Operacional.

A instalação proposta poderá ser implementada ou existe algo que impede a implementação da referida proposta?

a) Sim, nada impede a implementação proposta.

b) Sim, apenas crie um Volume do tipo RAID-5 ao invés de um Volume Set. Com isso você garante tolerância a falhas.

c) Não. Não é possível implementar um Volume Set em discos maiores do que 20 GB

d) Não. Não é possível instalar o Windows 2000 Server em um Volume Set.

e) Não. Não é possível criar um Volume Set maior do que 50 GB

**Resposta certa: d**

**Comentários:** O Windows 2000 Server e o Windows Server 2003 somente podem ser instalados em um Volume Simples ou em um volume do tipo Mirror Set, também conhecido como Raid-1. Não pode ser instalado em um Volume Set ou Volume do tipo RAID-5.

**Questão 28:** Você é o Administrador de um servidor com o Windows Server 2003 instalado. O servidor é um DC (Controlador de Domínio). Você configura a pasta C:\documentos para que somente os usuários da sua filial tenham acesso aos documentos da pasta. Você configura as diretivas de auditoria de tal maneira que seja habilitada a auditoria de acessos (com sucesso e com falha) a objetos como Pastas, Arquivos e Impressoras.. Alguns dias após ter habilitado a auditoria você abre o Visualizador de eventos porém nenhum evento relacionado ao acesso dos arquivos da pasta C:\Documentos é encontrado. Qual a causa mais provável do problema?

- a) Você não configurou as propriedades avançadas da pasta Documentos para informar quais grupos ou usuários deveriam ter o acesso auditado.
- b) A diretiva de auditoria “Auditoria de acesso a objetos” não está habilitada.
- c) A pasta C:\Documentos está criptografada.
- d) A pasta C:\Documentos está compactada.
- e) As permissões NTFS da pasta C:\Documentos estão incorretamente configuradas.

**Resposta certa:** a

**Comentários:** Para que a auditoria de acesso a pastas, arquivos, impressoras e objetos que tenham uma lista de controle de acesso (ACL), possa funcionar são necessários dois passos:

- ◆ Habilitar a diretiva “Auditoria de acesso a objetos”. Para habilitar esta auditoria você deve usar o recurso de GPOs.
- ◆ Em seguida configurar quais grupos/usuários serão monitorados em quais pastas/arquivos. Isso é feito nas propriedades do objeto a ser monitorado.

Na questão do exemplo a diretiva está habilitada, porém o segundo passo não foi executado, por isso que os eventos não estão sendo gravados no log de eventos, embora a diretiva de auditoria tenha sido habilitada. A partição já é NTFS, pois se fosse FAT ou FAT 32, a guia segurança, através da qual configuramos a auditoria, nem sequer estaria disponível. Pelo enunciado da questão, vemos que o usuário acessou as configurações de segurança da pasta Documentos (para definir as permissões NTFS de acesso), o que significa que é uma partição NTFS.

**Questão 29:** Você é o Administrador de uma rede com servidores baseados no Windows Server 2003 Server e no Active Directory. O servidor SRVSUS01 será utilizado com servidor SUS, o qual será utilizado para distribuir atualizações críticas para as estações cliente da rede. Inicialmente você instalou e configurou o IIS neste servidor. O próximo passo é instalar o SUS. Você instalou e configurou o SUS para fazer a distribuição de atualizações para os clientes da rede. Agora você precisa fazer o backup das configurações do SUS, para que estas possam ser rapidamente restauradas, em caso de falha. Quais os passos para fazer o backup das informações de configuração do SUS?

- a) Faça um backup do Estado do Sistema.
- b) Faça um backup do Estado do Sistema.  
Faça um backup da pasta C:\InetPub
- c) Faça um backup da Metabase do IIS (IIS Metabase)

Em seguida use o Backup de Utilitário para fazer um backup do arquivo de backup da Metabase e das demais configurações do IIS.

- d) Faça um backup do Metabase do IIS (IIS Metabase)
- e) Use o utilitário de Backup, para fazer um backup completo do IIS.

**Resposta certa: c**

**Comentários:** Esta questão é interessante e exige que o candidato lembre de alguns pontos importantes:

- ◆ Primeiro você deve fazer um backup da Metabase, a qual contém uma série de configurações do IIS.
- ◆ O SUS depende do IIS, por isso você deve fazer, além do backup da Metabase, um backup das configurações do IIS, tal como o Site Padrão e outras.
- ◆ Feito o backup da Metabase em um arquivo, você pode utilizar o utilitário de backup, para fazer um backup deste arquivo.

Com isso ficamos com a alternativa C, ou seja, primeiro uso o console de Administração do IIS para fazer um backup da Metabase e em seguida, uso o utilitário de backup do Windows, para fazer o backup deste arquivo e das demais configurações do IIS.

**Questão 30:** Você é o administrador de uma rede baseada no Windows Server 2003 e no Active Directory. Todos os clientes são baseados no Windows XP Professional. Você é o administrador responsável pelo planejamento e execução do Backup no servidor SRVFILES01, o qual é utilizado para o compartilhamento de arquivos. Você agendou uma tarefa de Backup, a qual faz um Backup Normal de todos os dados dos usuários, no servidor SRVFILES01. O Backup é feito em uma unidade de fita DLT. A tarefa está agendada para iniciar as 3:00 hs da madrugada. Com o aumento da quantidade de dados, gravados pelos usuários no servidor, o Backup não está mais sendo concluído antes do início do horário normal de trabalho, que é as 8:00 hs. da manhã. O Backup tem sido concluído entre 9:00 e 9:30 da manhã. No período entre 8:00 da manhã e o término do Backup, os usuários estão reclamando que o acesso aos arquivos do servidor SRVFILES01 está muito lento. Como Administrador do Backup no servidor SRVFILES01, o que você deve fazer para solucionar o problema descrito?

- a) Definir cotas de disco para os usuários, limitando o espaço em disco que cada usuário pode usar.
- b) Altere a tarefa agendada que executa o Backup, para iniciar a 1:00 da madrugada.
- c) Exclua a tarefa agendada que executa o Backup.

Crie uma nova tarefa para execução do Backup.

Configure esta nova tarefa para iniciar a 1:00 da madrugada.

- d) Faça a criptografia de todos os dados do servidor SRVFILES01
- e) Faça o Backup em Disco ao invés de fazê-lo em fita.

**Resposta certa: b**

**Comentários:** O ponto básico desta questão é que a tarefa de Backup não está sendo concluída em tempo hábil, antes do início do expediente. Como o backup continua sendo executado durante o expediente - entre 8:00 e 9:30, o servidor apresenta problemas de desempenho neste período, já que a tarefa de Backup utiliza intensivamente os recursos do servidor, principalmente o acesso a disco. A solução é iniciar o Backup duas horas antes do que está sendo feito atualmente, para que dê tempo de o Backup ser concluído antes do início do expediente. Você deve alterar as configurações da tarefa agendada para que ela seja iniciada a 1:00 da madrugada, ao invés das 3:00. Com isso, o Backup passará a ser concluído entre 6:00 e 7:30 da manhã, ou seja, antes do início do expediente. Fazer o backup em disco, certamente seria mais rápido do que fazer em fita, porém esta não é uma política recomendada. Ao fazer o Backup em fita, você poderá armazenar as fitas em local seguro, distante da sala dos servidores. Neste caso, se houver um desastre, tal como um incêndio ou inundação, as fitas estarão preservadas e os dados poderão ser recuperados a partir das fitas. Se você fizer o backup em um ou mais discos do próprio servidor, os dados e as cópias de backup

estarão no mesmo local físico. Se der um incêndio na sala dos servidores, você perderá os dados e também as cópias de Backup, ou seja, não haverá como restaurar os dados. Outro ponto importante a ser observado nesta questão é que não é necessário excluir a tarefa agendada e criá-la novamente. Para alterar o agendamento de uma tarefa agendada, basta acessar as propriedades da tarefa e fazer as alterações necessárias.

**Questão 31:** Você possui cinco impressoras de rede da mesma marca e modelo, ou seja, impressoras que utilizam o mesmo driver de impressão. Como administrador da rede, você gostaria de usar estas impressoras como se fossem uma única impressora no servidor de impressão, de tal maneira que a medida que os trabalhos de impressão fossem chegando, fossem sendo direcionados, alternadamente, para uma das cinco impressoras. Com isso você conseguaria um distribuição do trabalho de impressão e para os usuários seria como se existisse uma única impressora. Qual opção das propriedades de impressão permite a configuração desejada?

- a) Ativar porta compartilhada.
- b) Ativar Pool de Impressão.
- c) Ativar alternância de porta.
- d) Ativar balanceamento de carga.
- e) Ativar compartilhamento do spool de impressão.

**Resposta certa: b**

**Comentários:** A única opção que existe e que é a correta para esta questão é o uso de um Pool de Impressão. Para que possa ser ativado um Pool de Impressão devemos ter impressoras que utilizem o mesmo driver de impressão. Com isso podemos fazer com que um determinado número de impressoras apareça como uma única impressora disponível. A medida que os trabalhos de impressão vão chegando, o Windows Server 2003 vai direcionando estes trabalhos, de maneira alternada, para as diferentes impressoras componentes do Pool de Impressão. A opção Ativar Pool de Impressão está disponível na guia Portas das propriedades da impressora. Normalmente uma das impressoras que faz parte do Pool é local e as demais são impressoras de rede. Após marcar a opção Ativar Pool de Impressão, basta marcar as portas das impressoras que farão parte do Pool de Impressão.

**Questão 32:** Você é o Administrador de uma rede formada por um único domínio: abc.com. Todos os servidores são baseados no Windows Server 2003. Qual a maneira mais rápida para obter uma listagem de todas as contas de usuários que não fizeram o logon no domínio nos últimos 90 dias?

- a) Use o comando DSQUERY
- b) Use o comando NSLOOKUP
- c) Use o comando DSADD
- d) Use o comando DSRM
- e) Use o comando CSVDE

**Resposta certa: a**

**Comentários:** O comando DSQUERY é uma das novidades do Windows Server 2003 em relação ao Windows 2000 Server. Este comando é utilizado para fazer uma pesquisa no Active Directory e retornar uma lista de objetos (computadores, grupos, unidades organizacionais ou usuários), os quais atendem a um ou mais critérios de pesquisa. O comando dsquery tem diferentes opções, conforme descrito a seguir:

```
dsquery computer  
dsquery contact
```

```
dsquery group  
dsquery ou  
dsquery site  
dsquery server  
dsquery user  
dsquery quota  
dsquery partition
```

Na ajuda do Windows Server 2003, fazendo uma pesquisa por DSQUERY, você encontra uma referência completa de todas as opções do comando DSQUERY e encontra também diversos exemplos práticos de utilização.

**Questão 33:** Você é o administrador da rede da empresa, a qual tem 20 servidores baseados no Windows Server 2003. Um usuário gravou cerca de 10 GB de conteúdo no disco de um dos servidores. No conteúdo gravado pelo usuário estão arquivos de música no formato .mp3 e vídeos e fotos com material pornográfico. Após a demissão do funcionário por justa causa, você observou que, antes de sair, o referido funcionário colocou apenas a sua própria conta de logon na lista de contas com permissões NTFS de acesso à pasta onde estão gravados os 10 GB de conteúdo impróprio para o trabalho da empresa. Como administrador, qual a maneira mais rápida para ganhar acesso ao conteúdo da pasta e excluir este conteúdo?

- a) Faça o logon com a conta configurada como agente de recuperação e exclua a pasta.
- b) Faça o logon com uma conta do grupo Usuários Avançados e exclua a pasta.
- c) Faça o logon com uma conta com permissão de Administrador e exclua a pasta.
- d) Faça o logon com uma conta com permissão de Administrador.

Dê um “Take Ownership” na pasta e em todo o seu conteúdo.

Exclua a pasta e todo o seu conteúdo.

- e) Faça o logon com uma conta com permissão de Administrador.

Dê um “Take Ownership” na pasta e em todo o seu conteúdo.

**Resposta certa: d**

**Comentários:** Antes de sair, o funcionário demitido configurou as permissões NTFS de tal maneira que somente ele mesmo pudesse ter acesso ao conteúdo da pasta. Os usuários do grupo Administradores tem permissão para dar um “Take Ownership” (Alterar o proprietário), mesmo em pastas e arquivos para os quais eles não tenham permissões NTFS de acesso. Ao dar um Take Ownership é atribuída a permissão Controle Total para o grupo Administradores. Com isso o Administrador poderá excluir a pasta, como no caso desta questão, ou definir permissão de acesso para outros usuários, caso isso seja necessário, mantendo o conteúdo da pasta. Para dar um “Take Ownership” basta fazer o logon com uma conta com permissões de Administrador, acessar as propriedades da pasta, clicar na guia Segurança. Na guia Segurança clique no botão Avançado e na janela de propriedades avançadas dê um clique na guia Proprietário. Nesta guia você tem a opção para tornar-se dono da pasta e de todo o seu conteúdo.

**Questão 34:** Você é o administrador de uma rede baseada no Windows Server 2003 e no Active Directory. Um dos servidores da rede é um DC com o nome SRVDC07. Este servidor será utilizado também como Servidor de Certificados. Para isso você instalou e configurou o Microsoft Certificate Services no servidor SRVDC07. Agora você deve montar uma política de Backup/Restore para este servidor. A política de Backup/Restore deve incluir todas as informações necessárias para restaurar o funcionamento do servidor SRVDC07 no caso de falhas, incluindo também as informações necessárias para restauração dos serviços de certificados. Em relação à política de Backup/Restore que deve ser montada para o servidor SRVDC07, considere as afirmações a seguir:

- I. Para que possa ser feito o Restore do servidor como um todo, em caso de falhas, você deve fazer um backup Normal de todo o drive C:
- II. Para que possa ser feito o Restore do servidor como um todo, em caso de falhas, você deve fazer um backup Normal da pasta %windir% e da pasta raiz do drive C:
- III. Você deve fazer um backup dos dados dos usuários e também do Estado do Sistema (System State).
- IV. Para restaurar o servidor, no caso de falhas, você deve inicializá-lo no modo de Restauração do Active Directory (Directory Services Rstore Mode) e fazer um restore do tipo nonauthoritative do Active Directory.
- V. Para restaurar o servidor, no caso de falhas, você deve inicializá-lo no modo de Restauração do Active Directory (Directory Services Rstore Mode) e fazer um restore do tipo authoritative do Active Directory.

Estão corretas as seguintes afirmativas:

- a) III e IV
- b) I e II
- c) II e III
- d) I, II, IV e V
- e) II, III e V

**Resposta certa: a**

**Comentários:** Esta questão exige que o candidato conheça alguns pontos importantes:

- ◆ Para fazer um backup do sistema, de tal maneira que seja possível restaurar a instalação do Windows Server 2003, de todos os seus serviços e do Active Directory, é preciso fazer um backup do estado do sistema (System State). No Backup do estado do sistema, dentre outras, estão incluídas todas as informações do Active Directory, da Registry e do Certificate Services.
- ◆ Para fazer um restore do estado do sistema, é preciso reinicializar o servidor em um modo especial, conhecido como Modo de Restauração do Active Directory (Directory Services Restore Mode).
- ◆ O terceiro ponto que o candidato deve conhecer, para responder esta questão, é a diferença entre o backup do tipo authoritative e nonauthoritative. Descrevo estas diferenças logo a seguir:

**Restore Nonauthoritative (Sem autoridade):** Este é um restore normal. Os dados serão restaurados a partir do backup. Uma vez concluída a restauração, o DC passará a receber as atualizações dos outros DCs. Sempre que um outro DC contiver informações mais atualizadas do que as que foram restauradas a partir do backup, estas informações serão replicadas para o DC onde foi feito o restore nonauthoritative. É o processo padrão de restore.

**Restore Authoritative (Com autoridade):** Esta é uma situação especial. Para ilustrar este tipo de restore, vou utilizar uma situação prática onde ele seria necessário. Imagine que, por engano, um administrador excluiu uma OU e todo o seu conteúdo. Esta informação (ou seja a informação de que a OU foi excluída) será replicada para os demais DCs do domínio. O efeito prático é que esta OU será excluída em todos os DCs do domínio. Você pode imaginar o seguinte: Basta restaurar a OU a partir do Backup e pronto, as informações da OU serão replicadas para os demais DCs e os dados serão recuperados. Nada disso. Ao restaurar a OU usando o método normal (Nonauthoritative), os dados da OU serão considerados mais antigos do que a informação de que não existe a OU. Quando houver a replicação entre o DC onde foi feito o restore da OU e qualquer outro DC do domínio, o que irá acontecer é que a OU será novamente excluída e não enviada para os outros DCs, pois a informação de que ela foi excluída, é mais recente do que os dados da OU. Com o uso de um restore Authoritative é possível recuperar esta informação. Nesta situação, o administrador utiliza o comando Ntdsutil para fazer um restore Authoritative (Com autoridade) da OU que foi excluída. Fazer um

restore authoritative significa alterar o número de série dos dados que estão sendo restaurados, de tal maneira que eles sejam considerados as atualizações mais recentes em relação a mesma informação que está nos demais DCs do domínio. Com isso, quando houver a replicação entre o DC onde foi feito o restore e os demais DCs, os dados da OU serão considerados mais recentes e a OU e todo o seu conteúdo será replicada para os demais DCs. O efeito prático é que os dados da OU serão recuperados.

Quem tem permissão para fazer o backup do estado do sistema? Para fazer o backup ou um restore do tipo nonauthoritative, o usuário deve ter as seguintes permissões e direitos de usuário:

Para fazer o backup do estado do sistema, o usuário deve pertencer ao grupo Backup Operators (Oper. de cópia) ou ao grupo Local do domínio Administrators (Administradores).

Para fazer o restore do estado do sistema, o usuário deve pertencer ao grupo Local do domínio Administrators (Administradores).

Com base no que foi exposto, verificamos que estão corretas as afirmativas III e IV, o que torna verdadeira a alternativa “a”.

**Questão 35:** Você é o responsável pela administração das impressoras da rede da empresa. A empresa utiliza apenas impressoras Laser Coloridas, de alta velocidade e resolução. As impressoras são controladas e compartilhadas a partir de três servidores de impressão: IMPSRV01, IMPSRV02 e IMPSRV03. IMPSRV01 está instalado na matriz em São Paulo. IMPSRV02 está instalado na filial no Rio de Janeiro e IMPSRV03 na filial em Porto Alegre. Um usuário em cada localidade, inclusive na matriz, deve ter permissão para gerenciar a fila de impressão, excluindo, se necessário, inclusive os documentos enviados por outros usuários, aumentando a prioridade de impressão de alguns documentos e assim por diante. Somente você, como administrador da rede, deve ter permissão para compartilhar impressoras, alterar as suas propriedades e, inclusive, excluir impressoras. Qual o nível de permissão que deve ser configurado para o usuário responsável pelo gerenciamento da fila de impressão em cada unidade?

- a) Imprimir
- b) Gerenciar Documentos
- c) Gerenciar Impressoras
- d) Controle Total
- e) Gerenciar Fila

Resposta certa: b

**Comentários:** Assim como é possível atribuir permissões para uma pasta compartilhada, é possível definir permissões de acesso para uma impressora compartilhada na rede. As permissões definem quais os usuários que podem utilizar a impressora e qual o nível de permissão de cada um. Existem três níveis de permissão de impressão, conforme descrito a seguir:

**Imprimir:** Permite ao usuário Imprimir documentos, pausar, reiniciar e continuar a impressão dos documentos por ele enviados para a impressora, conectar-se à impressora através da rede. Normalmente atribuída para aqueles usuários que simplesmente precisam enviar documentos para a impressora.

**Gerenciar documentos:** Todas as permissões de Imprimir, mais Controlar a impressão de todos os documentos e também pausar, reiniciar e continuar a impressão de qualquer documento enviado por qualquer usuário. Normalmente atribuída para aquele usuário que administra a impressora, resolvendo problemas de impressão, mas sem permissões para alterar propriedades e permissões da impressora.

**Gerenciar impressoras:** Todas as permissões de Imprimir e Gerenciar documentos, mais cancelar a impressão de todos os documentos pendentes, compartilhar a impressora, alterar as propriedades da impressora, eliminar a impressora e alterar as permissões de impressão. Normalmente atribuída a um usuário que deve ter poderes completos sobre a impressora, inclusive podendo removê-la do sistema.

É importante salientarmos, que as permissões para o uso da impressora tem efeito tanto localmente, quanto para o acesso através da rede. Além disso caso um usuário pertença a mais de um grupo que possui permissões para a impressora, a sua permissão efetiva é a soma das permissões de todos os grupos aos quais o usuário pertence. Também é importante lembrar que uma permissão Negar tem prioridade sobre Permitir. Por exemplo se o usuário jsilva pertence aos grupos Contabilidade e Marketing. O grupo Contabilidade possui permissão Permitir Imprimir, já o grupo Marketing tem permissão Negar Imprimir. Então a permissão efetiva do usuário jsilva será Negar Imprimir.

Pela descrição dos níveis de permissão podemos ver que a permissão que o usuário precisa, para gerenciar a fila de documentos é: Gerenciar documentos. Não existe a permissão Gerenciar fila. Por isso a resposta correta é a letra b.

**Questão 36:** Você é o Administrador de uma rede com servidores baseados no Windows Server 2003 Server e no Active Directory. A rede é formada por um único domínio: abc.com. Você é o responsável por definir a política de backup para três servidores: SRV01, SRV02 e SRV03. Estes servidores são Members Server do domínio abc.com e são utilizados, exclusivamente, para compartilhamento de arquivos. Nenhum outro sistema e/ou serviço está instalado nestes servidores. Como parte da política de Backup, você optou por fazer o Backup apenas dos dados dos usuários. Em caso de problemas com a instalação do Windows Server 2003 nestes servidores, você irá reinstalar o Windows Server 2003 e restaurar os dados dos usuários a partir do Backup. O horário normal de expediente é de segunda a sexta-feira. Os usuários não têm acesso aos dados nos finais de semana. As regras para a política de Backup são as seguintes:

- I. Deve ser feito, pelo menos, um backup semanal completo, de todos os dados, independente dos arquivos terem sido ou não alterados desde o último Backup.
- II. Você deve fazer o backup da menor quantidade de informação possível para a restauração dos dados.
- III. A política de backup deve permitir que o restore dos dados seja feito utilizando-se, no máximo, duas fitas.

Das estratégias de Backup descritas a seguir, qual a que atende as regras definidas pela política de Backup/Restore da empresa?

- a) Backup Normal no Sábado ou Domingo.  
Backup do tipo Cópia de segunda a sexta-feira.
- b) Backup Normal no Sábado ou Domingo  
Backup do tipo Incremental de segunda a sexta-feira.
- c) Backup Normal no Sábado ou Domingo  
Backup do tipo Diferencial de segunda a sexta-feira.
- d) Backup Normal todos os dias.
- e) Backup do tipo Cópia, todos os dias.

**Resposta certa: c**

**Comentários:** Esta questão testa, basicamente, o conhecimento do candidato em relação aos tipos de backup disponíveis no Windows Server 2003. A seguir apresento uma descrição dos tipos de backup disponíveis no Windows Server 2003:

No Windows Server 2003 podemos utilizar os seguintes tipos de backup:

Normal (Normal): Com este tipo de backup todos os arquivos são copiados, toda vez que o backup for executado, independentemente de os arquivos terem sido alterados ou não. Os arquivos são marcados como tendo sido feito o backup, ou seja, o atributo de arquivamento é desmarcado. Cada arquivo tem um atributo que pode ser marcado ou desmarcado. Este atributo serve para informar ao Windows Server 2003 se o arquivo foi ou não modificado desde o último backup normal. A principal vantagem do backup normal é a facilidade para fazer a restauração dos arquivos, quando necessário. Com o backup do tipo normal, para restaurar os dados, você precisa apenas do último backup normal que foi criado. A desvantagem é o tamanho do backup e o tempo para execução. Em cada execução do backup, todos os arquivos e pastas serão copiados, independentemente de terem sido alterados ou não. Geralmente, o backup normal é executado quando você cria um conjunto de backup pela primeira vez. Nos backup subsequentes é comum a utilização de outros tipos de backup, conforme descreverei logo a seguir. Por isso que nesta questão, descartamos o uso de um backup normal todos os dias, pois se fizéssemos isso, não estaríamos respeitando a diretiva que pede para que seja feito o backup do menor volume de informações possível.

Copy (Cópia): Backup que copia todos os arquivos selecionados, mas não marca cada arquivo como tendo sofrido backup (em outras palavras, o atributo de arquivamento não é desmarcado). É idêntico ao backup Normal, com a diferença de que os arquivos não são marcados como tendo sido copiados. A cópia é útil caso você queira fazer backup de arquivos entre os backups normal e incremental (veja descrição do backup incremental logo a seguir), pois ela não afeta essas outras operações de backup ou quando você precisa fazer uma cópia extra dos dados para enviar para um filial da empresa ou para manter a cópia armazenada em um local seguro. Por isso que nesta questão, descartamos o uso de um backup do tipo Cópia todos os dias, pois se fizéssemos isso, não estaríamos respeitando a diretiva que pede para que seja feito o backup do menor volume de informações possível.

Incremental (Incremental): Este tipo de backup copia somente os arquivos criados ou alterados desde o último backup normal ou desde o último backup incremental. Os arquivos copiados para o backup são marcados (ou seja, o atributo de arquivamento é desmarcado). Se você utilizar uma combinação de backups normais e incrementais para restaurar os seus dados, será preciso ter o último backup normal e todos os conjuntos de backups incrementais feitos após este backup normal e restaurá-los na seqüência correta. A grande vantagem do backup incremental é que ele reduz o tempo necessário para a execução do backup, pois somente é feita a cópia dos arquivos que foram criados ou modificados desde o último backup normal ou incremental. A grande desvantagem é que para fazer a restauração é necessário o último backup normal e todos os backups incrementais subsequentes. Os backups incrementais devem ser restaurados na seqüência cronológica em que foram criados. Além disso, se um dos backups incrementais apresentar problemas, não será possível restaurar os dados até o ponto do último backup incremental. Nesta questão específica, não pode ser utilizado o backup Incremental, pois para fazer o restore, usando uma combinação de backup normal e incremental, você deve restaurar o último backup normal e todos os backups incrementais subsequentes, na ordem em que foram feitos. A política de backup da empresa afirma que devem ser utilizadas, no máximo, duas fitas para fazer o restore. Com isso descartamos o backup incremental.

Differential (Diferencial): Este tipo de backup faz a cópia de todos os arquivos criados ou alterados desde o último backup normal ou incremental. Os arquivos que sofreram backup não são marcados como tal (ou seja, o atributo de arquivamento não é desmarcado). Com isso cada backup diferencial, copia todos os arquivos que foram modificados desde o último backup normal (ou incremental, caso algum tenha sido feito). Se você estiver executando uma combinação de backups normal e diferencial, a restauração de arquivos e pastas exigirá que você tenha o último backup normal e o último backup diferencial. A restauração é mais rápida do que quando você usa backups incrementais, pois somente é necessário o último backup diferencial, porém cada backup diferencial passa a ser maior, pois contém a cópia de todos os arquivos criados ou modificados desde o último backup normal ou incremental. Nesta questão específica, este é o tipo de backup ser utilizado, pois para fazer o restore, usando uma combinação de backup normal e diferencial,

você deve restaurar o último backup normal e somente o último backup diferencial, ou seja, no máximo serão necessários dois backups, que é exatamente o que pede a política de backup/restore da empresa.

Daily (Diário): Este tipo de backup copia todos os arquivos selecionados que forem alterados no dia de execução do backup diário. Os arquivos que sofreram backup não são marcados como tal (ou seja, o atributo de arquivamento não é desmarcado). Não é um tipo muito utilizado. Pode ser utilizado em conjunto com backups do tipo normal e incremental.

O tipo ou tipos de backup que estão sendo utilizados, definem as estratégias de restauração (restore) que serão utilizadas, em caso de perda dos dados originais. A estratégia a ser utilizada depende do volume de dados e do valor dos dados a serem protegidos. Por exemplo, para um usuário doméstico que não tem um grande volume de dados, pode ser suficiente uma estratégia de backup normal todos os dias. Já para os servidores com dados de missão crítica da sua empresa, toda proteção adicional é bem vinda.

**Questão 37:** Você é o Administrador de uma rede baseada no Windows Server 2003 e no Active Directory. O servidor SRV045 utiliza uma configuração de RAID-5, formada pela combinação de volumes em cinco discos dinâmicos. Desde o início da manhã os usuários vem reclamando de lentidão no acesso aos dados contidos no volume RAID-5 do servidor SRV045, volume este que é montado para os usuários, via logon de script, como sendo o drive S:. Você faz o logon como Administrador no console do servidor SRV045 e abre o console Gerenciamento do computador e acessa as configurações de discos do servidor. O status do volume RAID-5 está como Falha de redundância e o status de um dos discos está como Off-line. O nome do disco está como Ausente. Um ícone (X) aparece no modo de exibição gráfico do disco. Quais os passos para corrigir o volume RAID-5 que está apresentando problemas?

- a) 1. Faça o logon como Administrador ou como membro do grupo Administradores.  
2. Certifique-se de que o disco físico esteja ligado, conectado à fonte de energia e conectado ao computador. Se necessário, ligue ou reinstale o disco físico.  
3. Clique com o botão direito do mouse no disco ausente ou off-line e, em seguida, clique em Reativar disco.
- b) 1. Faça o logon como membro do grupo Oper. de Servidores.  
2. Certifique-se de que o disco físico esteja ligado, conectado à fonte de energia e conectado ao computador. Se necessário, ligue ou reinstale o disco físico.  
3. Clique com o botão direito do mouse no disco ausente ou off-line e, em seguida, clique em Reativar disco.
- c) 1. Faça o logon como Administrador ou como membro do grupo Administradores.  
2. Substitua o disco rígido.  
3. Clique com o botão direito do mouse no disco ausente ou off-line e, em seguida, clique em Reativar disco.
- d) Exclua o volume RAID-5.  
Recrie o volume.
- e) Exclua o volume RAID-5.  
Recrie o volume.  
Restaure os dados a partir do Backup.

**Resposta certa: a**

**Comentários:** Neste exemplo, por algum motivo, um dos discos do volume RAID-5 está apresentando o Status Off-line. Quando um disco está com o Status Off-line não é preciso substituí-lo. A primeira tentativa que deve ser feita é a

de Reativar o disco. Somente se não for possível reativar o disco é que deve-se partir para a substituição do disco. Para o exemplo da questão, primeiro você deve fazer o logon com uma conta com permissão de Administrador. O próximo passo é tentar reativar o disco. Não é preciso excluir o volume RAID-5. Com isso ficamos com a alternativa “a”

Mesmo que você tenha que substituir um disco, não será preciso recriar o volume. No evento de ter que substituir um disco defeituoso, o qual faz parte do RAID-5, após a substituição do disco, você deve fazer o logon como Administrador. Certifique-se de que o disco físico esteja ligado, conectado à fonte de energia e conectado ao computador. Se necessário, ligue ou reinstale o disco físico. Clique com o botão direito do mouse no disco ausente ou off-line e, em seguida, clique em Reativar disco. Para substituir uma região do disco no volume RAID-5, você precisa ter um disco dinâmico com espaço não alocado que seja, pelo menos, tão grande quanto a região a ser reparada. Se você não tiver um disco dinâmico com espaço suficiente não alocado, o comando Reparar volume não estará disponível. (Para verificar se você tem espaço suficiente, clique no disco, clique em Propriedades e veja o tamanho em Espaço não alocado. Esse tamanho pode ser um pouco menor do que o mostrado nos modos de exibição de lista e gráfico).

Quando um membro de um volume RAID-5 tem uma falha grave (como perda de energia ou uma falha total do disco rígido), ele se torna um órfão. Se isso acontecer, você poderá regenerar os dados para o membro órfão a partir dos demais membros do volume RAID-5.

Se a falha do volume RAID-5 ocorrer devido a uma falta de energia ou falha em fiação de um único dispositivo, você poderá regenerar os dados dentro do membro órfão do volume RAID-5, assim que as condições do hardware sejam restauradas.

O volume RAID-5 não exibirá o status Íntegro no Gerenciamento de disco até que a regeneração tenha terminado.

**Questão 38:** Em relação às permissões NTFS não é correta a seguinte afirmação:

- a) As permissões NTFS são cumulativas, ou seja, se um usuário pertencer a mais de um grupo, a sua permissão efetiva será a soma das permissões de todos os grupos.
- b) Negar tem precedência sobre qualquer outra permissão.
- c) As permissões de arquivos tem precedência sobre as permissões de pastas.
- d) É possível desabilitar o mecanismo de herança das permissões NTFS.
- e) Se um usuário retirar todas as permissões de uma pasta ou arquivo, esta pasta estará definitivamente inacessível, mesmo para o Administrador do sistema.

**Resposta certa: e**

**Comentários:** Todas as afirmativas estão corretas com exceção da letra e. As permissões NTFS são cumulativas, negar tem precedência sobre qualquer outra permissão, as permissões de arquivos que tem precedência sobre as permissões de pasta e também é possível desabilitar o mecanismo de herança. A letra e está errada porque mesmo que um usuário retire todas as permissões de uma pasta ou arquivo, o Administrador ainda poderá usar o recurso de “Take Ownership”, descrito na Questão 13 deste simulado.

**Questão 39:** O usuário jsilva pertence aos seguintes grupos: Gerentes, Técnicos e Marketing. O usuário jsilva precisa ter acessos somente de leitura nos documentos do Word que estão em uma pasta compartilhada, no servidor \\SRV01\\worddocs. O usuário deve ter permissão somente de leitura, quer ele esteja acessando a pasta worddocs através da rede ou localmente logado no servidor SRV01.

As permissões NTFS e de compartilhamento desta pasta e o seu conteúdo, estão configuradas da seguinte maneira:

- ◆ Permissões NTFS:

- ◆ Gerentes: Leitura e alteração
- ◆ Técnicos: Leitura
- ◆ Marketing: Acesso total
- ◆ Permissões de Compartilhamento:

  - ◆ Gerentes: Leitura
  - ◆ Técnicos: Leitura
  - ◆ Marketing: Leitura

O que deve ser alterado para que o usuário jsilva não possa alterar os documentos desta pasta, mas sim somente ler o conteúdo dos documentos, quer seja através da rede, quer seja acessando localmente no servidor SRV01?

- a) Atribua a permissão NTFS Negar Leitura a conta jsilva.
- b) Retire o usuário jsilva do grupo Gerentes.
- c) Retire o usuário jsilva do grupo Marketing.
- d) Define permissão de leitura para a conta jsilva.
- e) Retire o usuário jsilva do grupo Gerentes e também do grupo Marketing.

**Resposta certa: e**

**Comentários:** Para responder corretamente esta questão, o usuário deve lembrar de algumas regras básicas das permissões NTFS, quando o usuário pertence a mais de um grupo:

- ◆ A permissão efetiva é a soma das permissões de todos os grupos aos quais o usuário pertence.
- ◆ Negar tem precedência sobre qualquer outra permissão.

Também é importante lembrar que quando existem diferenças entre as permissões NTFS e as permissões de Compartilhamento, vale a mais restritiva. Neste caso a permissão mais restritiva é a de compartilhamento que é somente Leitura. Neste caso o usuário jsilva, quando acessando através da rede, terá somente leitura. Não esqueça que as permissões de compartilhamento somente tem efeito para o acesso através da rede. Se o usuário jsilva fizer o logon no servidor SRV01 e acessar a pasta worddocs localmente, valerão apenas as permissões NTFS. Neste último caso, acessando localmente, o usuário jsilva teria permissão Controle Total na pasta worddocs. Por isso devemos retirá-lo dos grupos Gerentes e Marketing para que, localmente, ele também tenha permissão somente de leitura.

**Questão 40:** Considere as afirmações a seguir em relação ao Terminal Services, no Windows Server 2003:

- I. Suporte automático à impressora local: O Terminal Services pode adicionar e reconectar automaticamente impressoras conectadas aos clientes de Serviços de terminal. Ou seja, mesmo conectado ao servidor, via Terminal Services, o cliente poderá imprimir na impressora localizada localmente na sua estação de trabalho.
- II. É possível fazer o redirecionamento de área de transferência Os usuários podem recortar e colar entre programas que estão sendo executados no computador local e no Terminal server.
- III. Integração com Usuários e grupos locais e Usuários e computadores do Active Directory do Windows Server 2003. Os administradores podem criar contas para os usuários dos Serviços de terminal da mesma forma que criam contas para os usuários do Windows Server 2003. Há campos extras para especificar informações específicas aos serviços de terminal, como caminho de perfil e pasta base de Serviços de terminal.
- IV. Criptografia: Os vários níveis de criptografia permitem que os administradores criptografem todos ou alguns dados transmitidos entre o Windows Server 2003 e os clientes de Serviços de terminal em três níveis diferentes

(baixo, médio ou alto), dependendo das necessidades de segurança. Além disso, o processo de logon dos Serviços de terminal inclui recursos para alterar a senha, desbloquear a área de trabalho e desbloquear a proteção de tela. O processo de logon é criptografado, garantindo a transferência segura do nome do usuário e senha. Os Serviços de terminal oferecem suporte à criptografia de 40 bits e 128 bits (disponível apenas nos Estados Unidos e no Canadá) entre o servidor e o cliente.

- V. Tempo limite de sessão configurável: Os administradores podem reduzir o uso de recursos do servidor ao configurar tempo limite de sessão. Os administradores podem especificar a duração de uma sessão ativa e o tempo em que a sessão pode permanecer ociosa no servidor.

Estão incorretas as seguintes afirmativas:

- a) I, III e V
- b) I e IV
- c) I, II, III e IV
- d) I, II, III
- e) Nenhuma, pois todas as afirmações estão corretas.

Resposta certa: e

**Comentários:** Todas as afirmações estão corretas, pois descrevem recursos realmente disponíveis no Terminal Services.

**Questão 41:** Você é o Administrador da rede da empresa, a qual é baseada no Windows Server 2003 Server e no Active Directory. As estações de trabalho da rede são baseadas no Windows XP Professional e no Windows 2000 Professional. Você deve implementar um conjunto de três pastas compartilhadas no servidor SRV01. Uma das pastas conterá documentos de uso público e deverá ser compartilhada como Pub. Uma segunda pasta conterá apenas arquivos de instalação de programas e deverá ser compartilhada como Programs. A terceira pasta conterá documentos sobre as finanças da empresa. Esta terceira pasta deve ser compartilhada de tal maneira que ele não possa ser exibida usando o comando \\SRV01 ou através da opção Meus locais de rede. Dos nomes de compartilhamento a seguir, qual pode ser utilizado para atender ao requisito solicitado?

- a) Finan#
- b) \$Finan
- c) Finan\$
- d) Finan@
- e) Finan\*

Resposta certa: c

**Comentários:** Esta questão um detalhe bastante simples, porém bem importante. Você pode criar os chamados Compartilhamentos Ocultos. Um compartilhamento Oculto não é exibido quando você executa o comando \\Nome\_do\_Computador e também não é exibido quando você acessa o computador através da opção Meus locais de rede. Para tornar um compartilhamento oculto, basta utilizar o caractere \$, como último caractere do nome do compartilhamento. Com isso ficamos com a alternativa C, ou seja, o nome do compartilhamento deve ser Finan\$.

**Questão 42:** Você é o administrador de uma rede baseada no Windows Server 2003 Server e no Active Directory. A rede é formada por um único domínio e todos os servidores estão baseados no Windows Server 2003. Atualmente você está implementando um processo de descentralização da administração de alguns recursos da rede. O usuário jsilva será o responsável por administrar o compartilhamento Docs, no servidor SRVFILES01. O usuário jsilva deve

ter permissão para alterar as permissões NTFS nas pastas e arquivos do compartilhamento Docs. Qual nível de permissão deve ser atribuído ao usuário jsilva, de tal maneira que ele possa alterar as permissões nas pastas e arquivos do compartilhamento Docs?

- a) Leitura, Alteração e Gravação
- b) Alteração e Gravação
- c) Leitura e Permissão Desviar pasta/Executar arquivo
- d) Alteração, Gravação e Ler atributos
- e) Controle Total

Resposta certa: e

**Comentários:** Dos níveis de permissão listados nas alternativas, o único nível de permissão que possibilita ao usuário, alterar as permissões de pastas e arquivos é a permissão Controle total. Ao invés de Controle total, poderia ser utilizado o nível Alterar permissões, porém este não foi citado na questão. A seguir apresento um resumo sobre os níveis de permissões NTFS disponíveis e as respectivas permissões associadas a cada nível.

**Traverse Folder/Execute File (Permissão Desviar pasta/Executar arquivo):** Estas permissões são aplicadas a pastas e arquivos. Para as pastas, Desviar pasta permite ou nega o movimento através de pastas para acessar outros arquivos ou pastas, mesmo que o usuário não tenha permissões referentes às pastas desviadas (aplica-se somente a pastas). Por exemplo vamos supor que o usuário tem permissão na pasta C:\Documentos, não tem permissão na pasta C:\Documentos\Ofícios e tem na pasta C:\Documentos\Ofícios\2001. Neste caso, o usuário para chegar até a pasta 2001, terá que passar pela pasta Ofícios, para a qual ele não tem permissão. Para que o usuário possa passar pela pasta Ofício, o administrador deve atribuir-lhe a permissão Desviar pasta. Desviar pasta tem efeito apenas quando o grupo ou usuário não tem o direito de usuário Ignorar verificação com desvio no snap-in de diretivas de grupo. (Por padrão, o grupo Todos tem o direito de usuário Ignorar verificação com desvio.).

**Para os arquivos:** Execute File (Executar arquivo) permite ou nega a execução de arquivos de programa (aplica-se somente a arquivos). Ao definir a permissão Traverse Folder (Desviar Pasta) em uma pasta, você não está automaticamente definindo a permissão Executar arquivo em todos os arquivos dessa pasta.

**Permissão List Folder/Read Data (Listar Pasta/Ler Dados):** List Folder (Listar Pasta) permite ou nega a exibição de nomes de arquivos e subpastas dentro da pasta. Essa permissão afeta apenas o conteúdo da pasta em questão, não afetando o fato de a pasta na qual a permissão está sendo definida ser listada ou não. Aplica-se somente a pastas. Read Data (Ler Dados) permite ou nega a exibição de dados em arquivos (aplica-se somente a arquivos). Por exemplo, se o usuário tem permissão de Ler dados em um arquivo do Word, este usuário poderá abrir o arquivo, porém não poderá alterá-lo ou excluí-lo.

**Permissão Read Attributes (Ler Atributos):** Permite ou nega a exibição de atributos de um arquivo ou pasta, como os atributos somente leitura ou oculto. Os atributos são definidos pelo NTFS. Para acessar os atributos de uma pasta ou arquivo, clique com o botão direito do mouse na pasta/arquivo e, no menu que surge, dê um clique na opção Properties (Propriedades).

**Permissão Read Extended Attributes (Ler Atributos Estendidos):** Permite ou nega a exibição de atributos estendidos de um arquivo ou pasta. Os atributos estendidos são definidos por programas e podem variar de acordo com o programa.

**Permissão Create Files/Write Data (Criar Arquivos/Gravar Dados):** Criar arquivos permite ou nega a criação de arquivos dentro da pasta (aplica-se somente a pastas). Gravar dados permite ou nega as alterações no arquivo e a substituição de um conteúdo existente (aplica-se somente a arquivos). Esta permissão é mais conhecida por permissão de Escrita (ou Alteração).

Create Folders/Append Data (Permissão Criar Pastas/Acrecentar Dados): Criar pastas permite ou nega a criação de pastas dentro da pasta na qual a permissão foi definida (aplica-se somente a pastas). Acrecentar dados permite ou nega as alterações no final do arquivo, mas não a alteração, exclusão ou substituição de dados existentes (aplica-se somente a arquivos).

Permissão Write Attributes (Gravar Atributos): Permite ou nega a alteração de atributos de um arquivo ou pasta, como somente leitura ou oculto. Os atributos são definidos pelo NTFS. A permissão Gravar atributos não implica na criação ou exclusão de arquivos ou pastas, apenas inclui a permissão para efetuar alterações nos atributos de um arquivo ou de uma pasta.

Permissão Write Extended Attributes (Gravar Atributos Estendidos): Permite ou nega a alteração de atributos estendidos de um arquivo ou pasta. Os atributos estendidos são definidos por programas e podem variar de acordo com o programa. A permissão Gravar atributos estendidos não implica na criação ou exclusão de arquivos ou pastas, apenas inclui a permissão para efetuar alterações nos atributos de um arquivo ou de uma pasta

Permissão Delete Subfolders and Files (Excluir Subpastas e Arquivos): Permite ou nega a exclusão de subpastas e arquivos, mesmo que a permissão Excluir não tenha sido concedida na subpasta ou arquivo. (aplica-se a pastas). Por exemplo, se você não tem permissão de Excluir na pasta Documentos, mas tem permissão de Excluir em um arquivo memo.doc, que está na pasta Documentos, você conseguirá Excluir o documento memo.doc, pois as permissões de arquivo tem precedência sobre as permissões de pastas, quando conflitantes.

Permissão Delete (Excluir): Permite ou nega a exclusão da pasta e/ou arquivo. Se o usuário não tiver permissão de excluir em um arquivo ou pasta, ele ainda poderá excluir o arquivo ou pasta, se ele tiver permissão Delete Subfolders and Files (Excluir Subpastas e Arquivos) na pasta pai. Por exemplo, suponha uma pasta Documentos, na qual o usuário tem permissão Delete Subfolders and Files. Dentro da pasta Documentos tem a pasta Ofícios, na qual o usuário não tem permissão Delete. Mesmo assim ele poderá excluir a pasta Ofícios, pois ele tem permissão Delete Subfolders and Files na pasta Pai de Ofícios que é a pasta Documentos.

Permissão Read Permissions (Ler Permissões): Permite ou nega a leitura de permissões do arquivo ou pasta, como Controle total, Ler e Gravar. Se o usuário não tiver esta permissão, ele não poderá exibir a lista com as permissões definidas para um arquivo e/ou pasta.

Permissão Change Permissions (Alterar Permissões): Permite ou nega a alteração de permissões do arquivo ou pasta, como Controle total, Ler e Gravar. Esta é uma permissão “poderosa” e que deve ser utilizada com cuidado. Uma vez que o usuário tem permissão para Alterar permissões, ele pode perfeitamente atribuir Controle total para ele mesmo, ou seja, para a sua conta de usuário.

Permissão Take Ownership (Apropriar-se) : Permite ou nega a apropriação (tornar-se dono) do arquivo ou pasta. O proprietário de um arquivo ou pasta sempre pode alterar permissões, independentemente de qualquer permissão existente que proteja o arquivo ou pasta. O dono de um arquivo ou pasta, por padrão, é o usuário que cria o arquivo /pasta.

**Questão 43:** Considere as afirmações a seguir em relação as permissões NTFS:

- I. Permissões NTFS são cumulativas, isto é , se um usuário pertence a mais de um grupo, os quais tem diferentes níveis de permissão para um recurso, a permissão efetiva do usuário é a soma das permissões atribuídas aos grupos aos quais o usuário pertence.
- II. Permissões NTFS para um arquivo têm prioridade sobre permissões NTFS para pastas. Por exemplo se um usuário têm permissão NTFS de escrita em uma pasta, mas somente permissão NTFS de leitura para um arquivo dentro desta pasta, a sua permissão efetiva será somente a de leitura, pois a permissão para o arquivo tem prioridade sobre a permissão para a pasta.

- III. Negar uma permissão NTFS tem prioridade sobre permitir. Por exemplo, se um usuário pertence a dois grupos diferentes. Para um dos grupos foi dado permissão de leitura para um arquivo e para o outro grupo foi Negada a permissão de leitura, o usuário não terá o direito de leitura, pois Negar tem prioridade sobre Permitir.
- IV. Permissões NTFS são válidas tanto para acesso local, no computador onde as pastas e arquivos estão gravados, quanto para o acesso via uma pasta compartilhada na rede.
- V. No caso de diferenças entre as permissões NTFS resultantes e as permissões de compartilhamento resultantes, a permissão efetiva será a mais restritiva.

Estão corretas as seguintes afirmativas:

- a) I, II, III, IV e V
- b) I, II, III e V
- c) I, III, IV e V
- d) I, II, III e IV
- e) II, III e IV

Resposta certa: a

**Comentários:** Todas as afirmações estão corretas e descrevem o funcionamento das permissões NTFS. Este é um tópico que o candidato deve conhecer muito bem para o exame. Você deve conhecer como funciona o mecanismo de permissões, tanto permissões NTFS quanto permissões de compartilhamento

Ao criar um compartilhamento em uma pasta, por padrão o Windows Server 2003 atribui como permissão de compartilhamento Read (Somente Leitura) para o grupo Everyone (Todos), que conforme o nome sugere, significa qualquer usuário com acesso ao computador, seja localmente, seja pela rede. Ou seja, ao criar um compartilhamento, automaticamente será permitida a leitura em todo o conteúdo do compartilhamento para todos os usuários da rede. Esta situação já é um pouco melhor do que ocorria com o Windows 2000 Server, onde era definida, por padrão, permissão Full Control (Controle Total) para o grupo Everyone (Todos). Por isso ao criar um compartilhamento, o administrador já deve configurar as permissões necessárias, a menos que esteja sendo compartilhada uma pasta de domínio público, onde todos os usuários devam ter acesso de leitura em todos os arquivos e subpastas da pasta que está sendo compartilhada.

**Questão 44:** Você trabalha com Administrador de uma rede baseada no Windows Server 2003 e com Clientes utilizando o Windows 2000 Professional ou o Windows XP Professional. Como Administrador da rede você está implementando uma política de monitoramento do desempenho dos servidores da rede. Os dados são coletados e armazenados em um banco de dados para análise posterior. Os usuários passaram a reclamar de problemas de desempenho em um dos servidores de arquivos da rede - SRVFILES01. Você acessa o banco de dados de monitoramento de desempenho e faz pesquisas para obter o valor médio de alguns contadores que estão sendo monitorados, conforme indicado a seguir:

Memória\Available Bytes -> 650 MB

Physical Disk\Current Disk Queue Length -> 13,45 (valor médio)

**IMPORTANTE:** As permissões definem o que o usuário pode fazer com o conteúdo de uma pasta compartilhada, desde somente leitura, até um controle total sobre o conteúdo da pasta compartilhada. Porém as permissões de compartilhamento somente tem efeito se o acesso for feito pela rede. Se o usuário fizer o logon no computador onde está a pasta compartilhada e acessá-la localmente, através do drive C: (ou outro drive qualquer onde está a pasta compartilhada), as permissões de compartilhamento não serão verificadas e, portanto, não terão nenhum efeito. Para limitar o acesso, mesmo localmente, usa-se as permissões NTFS, as quais serão descritas mais adiante.

**Memory Memory\Pages/sec -> 1,25 (valor médio)**

**Processor\% Processor Time -> 35% (valor médio)**

Com base nos valores obtidos, o que você deve fazer para solucionar o problema de desempenho do servidor SRVFILES01?

- a) Adicionar mais memória RAM
- b) Substituir o sistema de discos por um sistema de maior velocidade
- c) Fazer um Upgrade do Processador
- d) Adicionar mais uma placa de rede
- e) Aumentar o tamanho do arquivo de paginação - PageFile.sys

Resposta certa: b

**NÃO ESQUEÇA:** Permissões de compartilhamento, não impedem o acesso ao conteúdo da pasta localmente, isto é, se um usuário fizer o logon no computador onde está a pasta compartilhada, o usuário terá acesso a todo o conteúdo da pasta, a menos que as Permissões NTFS estejam configurados de acordo. Permissões NTFS é assunto para daqui a pouco.

**Comentários:** Esta questão testa o conhecimento do candidato em relação aos valores limites para os principais contadores a serem monitorados em um Servidor com o Windows Server 2003. Dos contadores apresentados, o que está acima do limite é o contador Current Disk Queue Length (Comprimento atual da fila de disco). O limite sugerido para este contador é 2, ou seja, valores maiores do que 2 indicam problemas de desempenho com o sistema de discos. A seguir apresento uma lista dos valores limites sugeridos, para os principais contadores a serem monitorados:

**Disco físico\ % Tempo do disco -> 90%**

**Disco físico\ Comprimento atual da fila de disco -> 2**

**Memória Memória\ Bytes disponíveis -> Menos de 4 MB**

**Memória Memória\ Páginas por segundo -> 20**

**Arquivo de paginação Arquivo de paginação\ % Uso -> 99%**

**Processador Processador\ % Tempo do processador -> 85%**

**Questão 45:** Você é o responsável por implementar uma rede baseada no Windows Server 2003. A maioria das estações dos Clientes utilizarão o Windows 2000 Professional e algumas utilizarão o Windows 98 ou Windows Me. Você fez o projeto da rede, criando um único domínio baseado no Active Directory. Como serviço de resolução de Nomes você está utilizando o DNS. O servidor DNS está instalado no DC da matriz. As configurações do protocolo TCP/IP são fornecidas, automaticamente, para todas as estações clientes, utilizando um servidor DHCP devidamente configurado e autorizado no Active Directory. A sua rede é composta de um único domínio distribuído em diferentes localidades. Em cada localidade é instalado um servidor com o Windows Server 2003 e com o Active Directory e o serviço DHCP instalado. Os clientes com o Windows 98 informam que não estão conseguindo acessar recursos nos servidores de impressão e de arquivos do domínio. Você faz uma análise do problema e descobre que os clientes com o Windows 98 não estão conseguindo resolver o nome dos servidores. O que você deve fazer para que todos os clientes Windows 98, de todas as localidades, possam resolver normalmente o nome de todos os servidores da rede?

- a) Crie uma zona DNS secundária nos servidores das demais unidades.  
Configure esta zona como primária do DNS da matriz.
- b) Transforme a zona DNS do servidor da matriz em uma zona integrada com o Active Directory.
- c) Configure o DHCP das unidades para replicar com o servidor DHCP da matriz.
- d) Instale o WINS em, pelo menos, um servidor de cada unidade, inclusive na Matriz.  
Configure a replicação entre os servidores WINS.

Configure os servidores DHCP para fornecer o número IP do respectivo servidor WINS de cada localidade.

- e) Habilite o Forward no Servidor DNS da Matriz.

Resposta certa: d

**Comentários:** A chave para essa questão é saber que os clientes, anteriores ao Windows 2000 (Windows 95/98 ou Me), dependem do serviço WINS - Windows Internet Naming Services para a resolução de nomes. Estes clientes mais antigos não usam o DNS para a resolução de nomes da rede interna. No exemplo proposto, como não existe servidores WINS disponíveis, os clientes Windows 98/Me não conseguem resolver o nome dos servidores, por isso não conseguem se conectar aos recursos disponíveis nos servidores. Para que os clientes Windows 98/Me possam resolver os nomes da rede interna, você deve instalar um servidor WINS em cada localidade e configurar um esquema de replicação entre esses servidores. Se a replicação não for configurada, os clientes somente conseguirão resolver o nome dos servidores da própria localidade, usando para isso Broadcast. Após ter instalado os servidores WINS, você deve configurar o servidor DHCP para informar o número IP do servidor WINS para os clientes, durante a inicialização. Esta última etapa é fundamental, pois não adianta estar disponível o servidor WINS se o cliente não for configurado para utilizá-lo. Em resumo: “Em redes que possuem clientes com o Windows 2000 e também clientes com versões anteriores, como o Windows 95/98/Me, não basta o DNS, é preciso o WINS. O Windows XP utiliza o DNS para resolução de nomes.

Questão 46: Você é o Administrador de uma rede com servidores baseados no Windows Server 2003 Server e no Active Directory. Você está fazendo o planejamento em relação aos volumes e tipos de volumes a serem implementados nos servidores da rede. Considere as afirmações a seguir, em relação ao armazenamento básico e dinâmico no Windows Server 2003:

- I. **Armazenamento básico:** É o tipo de armazenamento que vem sendo utilizado desde a época do bom e velho (talvez não tão bom) MS-DOS. É utilizado por sistemas como o Windows 95, Windows 98, Windows NT Server 4.0 e Windows NT Workstation 4.0. 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”.
- II. É importante salientar que um disco somente pode ser configurado para um tipo de armazenamento. Não é possível, por exemplo, ter uma parte do disco configurada como armazenamento básico e o restante como armazenamento dinâmico.
- III. No armazenamento básico, o disco é dividido em partições. Uma partição é uma parte 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 prática se comportam como se fossem dois discos de 2GB independentes. Em um disco com armazenamento básico, é possível ter Partições primárias, partições estendidas e Drivers lógicos.
- IV. 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 disco dinâmico. Existem diferentes tipos de volumes. O tipo de volume a ser utilizado, é determinado por fatores tais 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 de comprometimento de um disco ou volume.

Estão corretas as seguintes afirmações:

- a) Nenhuma

- b) I, II e III
- c) I, II e IV
- d) I, II, III e IV
- e) IV

Resposta certa: d

**Comentários:** Esta questão descreve as características dos dois tipos de armazenamento disponíveis no Windows Server 2003: Disco Básico e Disco Dinâmico. Todas as afirmativas estão corretas e descrevem corretamente os tipos de armazenamento. Com isso ficamos com a alternativa D.

**Questão 47:** Você é o responsável por administrar o servidor SRV015, o qual é um Member Server do domínio abc.com.br. O servidor SRV015 atua como servidor de arquivos. Nesse servidor você criou um volume do tipo Stripe Set Sem Paridade (Striped Volume), a partir de espaços não alocados de cinco discos diferentes. Toda noite é feito um backup Normal de todos os dados do Stripe Set. Na segunda-feira você chega mais cedo ao serviço e observa que a luz de advertência de um dos discos que faz parte do Stripe Set está acessa. Em seguida você constata que o referido disco está com problemas e precisa ser substituído. O que você deve fazer para que o Stripe Set volte a estar disponível para os usuários da rede?

- a) Substitua o disco defeituoso.

Utilize o comando Examinar Discos Novamente (Rescan Disks).

Exclua o Stripe Set existente.

Crie um novo Stripe Set no qual é incluído espaço não alocado do novo disco.

Restaure o último Backup Normal.

- b) Substitua o disco defeituoso.

Utilize o comando Reconstruir Stripe Set.

- c) Substitua o disco defeituoso.

Utilize o comando Examinar Discos Novamente (Rescan Disks).

Restaure o último Backup Normal.

- d) Substitua o disco defeituoso.

Utilize o comando Examinar Discos Novamente (Rescan Disks).

Exclua o Stripe Set existente.

Crie um novo Stripe Set no qual é incluído espaço não alocado do novo disco.

- e) Substitua o disco defeituoso.

Utilize o comando Examinar Discos Novamente (Rescan Disks).

Crie um novo Stripe Set no qual é incluído espaço não alocado do novo disco.

Restaure o último Backup Normal.

Resposta certa: a

**Comentários:** Um Stripe Set sem paridade (Striped Volume) pode ser criado a partir de espaços não alocados, de igual tamanho, de no mínimo dois e no máximo 32 discos. O Windows preenche o espaço de cada disco simultaneamente. Com isso as informações são gravadas nos diversos discos ao mesmo tempo. Porém esse tipo de volume não fornece nenhuma tolerância à falhas, ou seja, se um dos discos que forma o Stripe Set apresentar problemas, todo o conteúdo gravado no Stripe Set estará inacessível e terá que ser restaurado do Backup. Na situação proposta você deve, primeiro, substituir o disco defeituoso, em seguida utilizar o comando Examinar Discos Novamente (Rescan Disks), para que

o Windows 2000 detecte o novo disco. Em seguida você deve excluir o Stripe Set existente, criá-lo novamente, agora já incluindo espaço do novo disco e em seguida restaurar os dados a partir do último backup Normal. Por isso a resposta correta é a letra “a”.

**Questão 48:** Você é o Administrador de uma rede baseada no Windows Server 2003 e no Active Directory. Todos os clientes são baseados no Windows XP Professional e estão configurados para utilizar o servidor DNS do domínio, para resolução de nomes. Você instalou uma impressora de rede, Laser, Colorida, de alta velocidade e qualidade, a qual será utilizada pelo departamento de Projeto e Design da empresa. Você atribuiu o endereço IP 10.10.5.150 para a impressora e o nome LaserCol05. Os usuários reclamam que não estão conseguindo acessar a nova impressora, usando os aplicativos do departamento de Projeto e Design. Você verifica as configurações destes aplicativos e observe que estes somente aceitam que seja configurada uma impressora, usando o nome da impressora e não o endereço IP. Esta impressora será utilizada por cerca de 250 usuários do departamento de Projeto e Design. Qual a maneira mais prática de fazer com que todos os usuários possam ter acesso a impressora usando o nome LaserCol05?

- a) Adicione a seguinte linha, ao arquivo hosts de todas as estações de trabalho que devem ter acesso à impressora:  
10.10.5.150 LaserCol05
  - b) Adicione a seguinte linha, ao arquivo hosts do servidor DNS:  
10.10.5.150 LaserCol05
  - c) No servidor DNS da rede, crie um registro do tipo A, associando o nome LaserCol05 com o IP 10.10.5.150
  - d) No servidor DNS da rede, crie um registro do tipo CNAME, associando o nome LaserCol05 com o IP 10.10.5.150
  - e) No servidor DNS da rede, crie um registro do tipo PTR, associando o nome LaserCol05 com o IP 10.10.5.150
- Resposta certa: c

**Comentários:** Esta questão testa os conhecimentos básicos do candidato em relação ao DNS. Embora o DNS não seja um tópico específico do programa oficial do Exame, a Microsoft poderá cobrar questões básicas do DNS, por considerá-las fundamentais para o candidato que pretende obter o MCSA ou MCSE-2003. O DNS é cobrado mais detalhadamente nos Exames 70-291, 70-292 e 70-296. Nesta questão, o primeiro ponto é que a configuração deve ser feita no servidor DNS e não no arquivo hosts. A opção de configurar o arquivo hosts de todas as estações de trabalho até iria funcionar, porém está longe de ser a maneira mais prática. Uma vez definido que deve ser utilizado o DNS, você tem que lembrar que o tipo de registro que associa um nome com um número IP é o registro do tipo A. Com isso ficamos com a alternativa C, ou seja, o administrador deve criar um registro do tipo A, no servidor DNS, associando o nome LaserCol05 com o respectivo IP: 10.10.5.150. Para mais detalhes sobre a instalação, configuração e administração do DNS, consulte o Capítulo 16 do seguinte livro: Windows Server 2003 – Curso Completo, 1568 páginas, publicado pela Editora Axcel Books.

**Questão 49:** Você é o Administrador de uma rede com servidores baseados no Windows Server 2003 Server e no Active Directory. A rede é formada por um único domínio, chamado ABC. Você utiliza a conta jpedro, a qual pertence ao grupo Admins. do Domínio. O usuário jsilva está logado no servidor SRV01 e está rodando uma aplicação financeira que é fundamental para o fechamento da contabilidade mensal da empresa. Esta aplicação ainda irá demorar cerca de 6 horas para concluir o seu trabalho e você não pode fazer o logoff do usuário jsilva, senão a aplicação deixará de rodar e a contabilidade não será fechada no tempo previsto. Porém você precisa rodar o console de Gerenciamento do Computador para fazer algumas configurações importantes, as quais também não podem ser adiadas. Você tenta fazer as configurações usando a conta do usuário jsilva, mas recebe uma mensagem de acesso negado. Você também não tem a opção de fazer o acesso via Terminal Services, pois por definição das políticas de segurança da empresa, este tipo de acesso está desabilitado em todos os servidores. O que você pode fazer para rodar o console Gerenciamento do computador e fazer as configurações necessárias, sem que seja necessário que o usuário jsilva tenha que fazer o logoff?

- a) Abra o console Gerenciamento do Computador via linha de comando.
- b) Atribua permissão Controle total para o grupo Todos, no atalho para o console Gerenciamento do computador.
- c) Utilize o recurso de Múltiplos logons do Windows Server 2003
- d) Abra a opção Ferramentas administrativas do Painel de Controle.  
Clique com o botão direito do mouse no console Gerenciamento do computador.  
No menu de opções que é exibido clique em Executar como...  
Na janela que é exibida, informe como nome de usuário jpaulo, informe a senha e no domínio digite ABC.
- e) Abra a opção Ferramentas administrativas do Painel de Controle.  
Clique com o botão direito do mouse no console Gerenciamento do computador.  
No menu de opções que é exibido clique em Executar como...  
Na janela que é exibida, informe como nome de usuário jpaulo, informe a senha e no domínio digite SRV01.

Resposta certa: d

**Comentários:** Esta questão testa um recurso bastante útil, que é a opção Executar como... O Windows Server 2003 não tem a opção de Múltiplos logons, como tem o Windows XP Professional. Com isso, somente um usuário poderá estar logado, diretamente no console do servidor, por vez. Via Terminal Services a história é outra. Via Terminal Services, o número de usuários que pode estar logado remotamente é definido pelo número de licenças de acesso instaladas no servidor. Muito bem, na situação descrita na questão, o Administrador não pode fazer o logoff da conta jsilva, senão a aplicação financeira será interrompida e o usuário jsilva não tem as permissões necessárias para fazer as configurações desejadas. Neste caso, o Administrador usa o recurso Executar Como, para abrir o console Gerenciamento do computador, usando o recurso Executar como..., recurso este que permite ao administrador executar um programa no contexto da sua conta de Administrador, sem ter que efetuar o logoff do usuário atual. Com isso ficamos com a alternativa D. A seguir mais alguns detalhes sobre o recurso Executar como...

Usar o comando Executar como para iniciar um programa como administrador:

No Windows Explorer, clique no programa, ferramenta Microsoft Management Console (MMC), ou no item do Painel de controle que você deseja abrir.

Pressione SHIFT e clique com o botão direito do mouse no programa e, em seguida, clique em Executar como.

Clique em Executar o programa usando o seguinte usuário.

Digite o nome de usuário, a senha e o domínio da conta de administrador que você deseja utilizar.

**Observações:** Se você desejar usar a conta Administrador no seu computador, no campo Domínio, digite o nome do computador. Se você desejar executar como um administrador de domínio, em Domínio, digite o nome do domínio. Em Nome de usuário, Senha e Domínio, você pode digitar até 256 caracteres em cada campo. O comando Executar como permite executar programas (\*.exe), consoles do MMC salvos (\*.msc), atalhos para programas e consoles do MMC salvos, além de itens do Painel de controle. Você pode executá-los como um administrador enquanto tiver efetuado logon em seu computador como um membro de um outro grupo, como grupo Usuários ou Usuários avançados.

É possível definir uma propriedade nos atalhos para programas e consoles do MMC, de forma que você sempre seja solicitado a apresentar credenciais alternativas ao utilizar o atalho. Para definir a propriedade, clique com o botão direito do mouse no atalho, clique em Propriedades e, em seguida, clique em Executar como usuário diferente.

O comando Executar como pode ser utilizado para iniciar qualquer programa, console do MMC ou item do Painel de controle, desde que os seguintes requisitos sejam atendidos:

Você forneça a conta de usuário e as informações sobre senha apropriadas.

A conta de usuário possa efetuar logon no computador.

O programa, console do MMC ou item do Painel de controle estejam disponíveis no sistema e para a conta de usuário.

O comando Executar como é geralmente utilizado para executar programas como um administrador, apesar de não estar limitado a contas de administrador. Qualquer usuário com várias contas pode utilizar o comando Executar como para executar um programa, console do MMC ou item do Painel de controle com credenciais alternativas.

Se você tentar iniciar um programa, console do MMC ou item do Painel de controle a partir de um local da rede usando Executar como, ele pode falhar, pois as credenciais usadas para a conexão com o compartilhamento de rede são diferentes das credenciais usadas para iniciar o programa. As credenciais usadas para executar o programa podem não dar acesso ao mesmo compartilhamento de rede.

O comando Executar como e o Serviço de logon secundário aceitam apenas autenticação por senha. Se as diretivas exigirem que seja feito logon com cartão inteligente para contas especiais ou para todos os usuários, o comando Executar como não irá funcionar.

**Questão 50:** Você é o administrador de uma rede baseada no Windows Server 2003 e no Active Directory. Todos os clientes são baseados no Windows XP Professional. Você é o administrador responsável pelas políticas de segurança da empresa. Você está avaliando a possibilidade de utilizar a criptografia do próprio Windows. Considere as afirmativas a seguir em relação a criptografia do Windows:

- I. Somente arquivos e pastas em volumes NTFS podem ser criptografados.
- II. As pastas e os arquivos compactados não podem ser criptografados. Se o usuário marcar um arquivo ou pasta para criptografia, ele será descompactado e vice-versa.
- III. Se você mover arquivos descriptografados para uma pasta criptografada, esses arquivos serão automaticamente criptografados na nova pasta. No entanto, a operação inversa não descriptografa automaticamente os arquivos. Nesse caso, é necessário descriptografar manualmente os arquivos. Os arquivos marcados com o atributo Sistema não podem ser criptografados, bem como os arquivos da pasta raiz do sistema, isto é C:\ ou D:\ e assim por diante.
- IV. Criptografar um arquivo ou uma pasta não protege contra exclusão ou listagem de arquivos ou pastas. Qualquer pessoa com permissões NTFS adequadas pode excluir ou listar pastas ou arquivos criptografados. A proteção da criptografia é contra o acesso ao conteúdo dos arquivos, ou seja, somente o usuário que criptografou o arquivo terá acesso. Para proteção contra listagem e exclusão recomenda-se o uso do EFS em combinação com permissões NTFS, utilizando as permissões NTFS para impedir que outros usuários possam excluir e até mesmo listar os arquivos que estão em um pasta criptografada.
- V. Você pode criptografar ou descriptografar pastas e arquivos localizados em um computador remoto ativado para criptografia remota. No entanto, se você abrir o arquivo criptografado através da rede, os dados transmitidos na rede através desse processo não serão criptografados. Outros protocolos, como (SSL/TLS) ou IP Seguro (IPSec), devem ser usados para criptografar dados durante a transmissão através da rede.

---

**IMPORTANTE:** Alguns itens, como o Windows Explorer, a pasta Impressoras e os itens da área de trabalho, são iniciados indiretamente pelo Windows 2000. Esses itens não podem ser iniciados com o comando Executar como.

---

**NOTA:** Você também pode usar o comando runas na linha Executar ou em um prompt de comando.

---

Estão corretas as seguintes afirmativas:

- a) Todas
- b) I, II, III e IV
- c) II, III, IV e V
- d) III, IV e V
- e) II, III e IV

Resposta certa: a

**Comentários:** Todas as afirmativas estão corretas e descrevem características do sistema de criptografia (EFS - Encrypted File System) do Windows Server 2003.

**Questão 51:** Você é o Administrador da rede da sua empresa, a qual tem servidores baseados no Windows 2000 Server e Windows Server 2003. A rede é composta de um único domínio: abc.com.br. Você participa da equipe que está definindo a política de recuperação à desastres para os servidores da sua rede. Uma das exigências é que seja possível acessar as partições/volumes do servidor, tanto formatados com FAT como com NTFS, mesmo que o Windows 2000 Server esteja com problemas para reiniciar. Você gostaria de acessar as partições/volumes e usar comandos para desabilitar serviços e/ou drivers que estejam com problemas, bem como copiar arquivos de e/ou para as partições/volumes. Qual comando você deve executar, em cada servidor, para atender esse item da política de recuperação à desastres?

- a) Execute o comando setup/recovery
- b) Execute o comando setup/cmdcons
- c) Execute o comando i386/cmdcons
- d) Execute o comando winnt/cmdcons
- e) Execute o comando winnt32/cmdcons

Resposta certa: e

**Comentários:** Para que você possa acessar as partições/volumes de um servidor, mesmo quando o Windows não está conseguindo inicializar normalmente, você precisa inicializar o servidor no modo Console de Recuperação. O modo Console de Recuperação é parecido com o antigo modo MS-SOS. Nesse modo estão disponíveis comandos para habilitar e/ou desabilitar serviços e drivers, também podemos copiar arquivos do disco rígido para o disquete ou vice-versa. O Console de Recuperação não é instalado por padrão, quando o Windows 2000 Server ou o Windows Server 2003 são instalados. Você pode instalar o console de recuperação usando o comando winnt32/cmdcons. O comando winnt32 está disponível na pasta i386 do CD de instalação do Windows 2000 Server e do Windows Server 2003.

**Questão 52:** Você é o Administrador de uma rede formada por um único domínio: abc.com. Todos os servidores são baseados no Windows Server 2003. Como parte da política de segurança da empresa você precisa definir as propriedades dos logs de todos os DCs do domínio. Você deseja definir propriedades tais como tamanho máximo, política de retenção (definir se eventos mais antigos serão descartados ou não quando o espaço máximo for atingido) e outras características. Qual a maneira mais prática para implementar esta exigência da política de segurança da empresa?

- a) Crie um script WSH o qual define as características dos Logs de Auditoria.  
Associe este Script com o grupo Admins. do Domínio.
- b) Crie um script WSH o qual define as características dos Logs de Auditoria.  
Associe este Script com cada uma das contas pertencentes ao grupo Admins. do Domínio.

- c) Use o console Visualizador de Eventos para se conectar com cada DC do domínio e configurar as propriedades de cada um dos logs.
- d) Use o console Gerenciamento do computador para se conectar com cada DC do domínio e configurar as propriedades de cada um dos logs.
- e) Crie uma nova GPO chamada Configura DCs e associe esta GPO com a OU Domain Controllers. Na GPO Configura DCs, configure as propriedades a serem aplicadas aos logs.

Resposta certa: e

**Comentários:** Esta questão testa os conhecimentos básicos do candidato em relação ao recurso de GPOs. Via GPO é possível configurar diversas opções do Windows Server 2003, dentre as quais, as propriedades dos logs de auditoria. Nesta questão, a maneira mais fácil para implementar as configurações desejadas, em todos os DCs do domínio, é criar um GPO e associá-la a OU Domain Controllers. As configurações necessárias são feitas na GPO e depois serão aplicadas a todos os DCs do domínio, pois as contas de todos os DCs, por padrão, estão contidas na OU Domain Controllers. Com isso ficamos com a alternativa E.:

**Questão 53:** Considere as afirmativas a seguir sobre o DNS no Windows Server 2003:

- I. Alterações somente podem ser feitas em zonas primárias.
- II. Para uma transmissão segura de informações entre zonas, você deve utilizar zonas integradas com o Active Directory.
- III. As atualizações dinâmicas são configuradas a nível de servidor DNS, ou seja, todas as zonas de um servidor DNS tem a mesma configuração: Ou estão com as atualizações dinâmicas habilitadas ou estão com as atualizações dinâmicas desabilitadas.
- IV. Podem ser criadas duas ou mais zonas primárias para um mesmo domínio.
- V. Uma zona pode conter informações sobre um ou mais domínio.

Estão corretas as seguintes afirmativas:

- a) I e II
- b) I, II e III
- c) I, II e IV
- d) III, IV e V
- e) I, II e V

Resposta certa: e

**Comentários:** Esta questão testa os conhecimentos do candidato em relação as características do DNS, no Windows Server 2003. A alternativa III é falsa, pois a configuração de Atualizações Dinâmicas pode ser configurada individualmente, em cada zona de um Servidor DNS. A alternativa IV também é falsa, pois somente uma zona primária pode ser criada para cada domínio. Uma alternativa que pode causar confusão ou dúvidas é a V, porém ela está absolutamente correta, ou seja, em uma única zona é possível ter informações sobre mais de um domínio. Com isso ficamos com a letra E, ou seja, estão corretas as afirmativas I, II e V.

**Questão 54:** Você é o administrador de uma rede baseada no Windows Server 2003 e no Active Directory. A rede é formada por três domínios: abc.com, vendas.abc.com e producao.abc.com. Cada domínio tem, no mínimo, dois DCs instalados. Você precisa instalar um novo DC no domínio vendas.abc.com. Quais os passos necessários para criação deste novo DC no domínio vendas.abc.com?

- a) Instalar o Windows Server 2003 em um novo servidor como Member Server. Fazer o logon com uma conta do grupo Domain Admins do domínio vendas.abc.com Configurar o servidor para fazer parte do domínio.
- b) Instalar o Windows Server 2003 em um novo servidor como Member Server. Fazer o logon com uma conta do grupo Domain Admins do domínio vendas.abc.com. Rodar o comando DCPROMO para promover o Member Server a DC.
- c) Fazer o logon com uma conta do grupo Domain Admins do domínio vendas.abc.com. Instalar o Windows Server 2003 em um novo servidor como DC.
- d) Fazer o logon com uma conta do grupo Domain Admins do domínio abc.com. Instalar o Windows Server 2003 em um novo servidor como DC.
- e) Instalar o Windows Server 2003 em um novo servidor como Member Server. Fazer o logon com uma conta do grupo Domain Admins do domínio vendas.abc.com. Rodar o comando winnt32 /promo para promover o Member Server a DC.

Resposta certa: b

**Comentários:** Não é possível instalar o Windows Server 2003 criando diretamente um DC. Primeiro você instala o Windows Server 2003 normalmente. Concluída a instalação, você terá um Member Server, caso o servidor tenha sido configurado para fazer parte do domínio, durante a instalação ou um Stand alone Server, caso o servidor não tenha sido configurado para fazer parte do domínio, durante a instalação. Para instalar o Active Directory, promovendo o servidor a DC, você utiliza o comando dcpromo. Para promover o Member Server a DC, você deve estar logado com uma conta com permissão de Administrador, ou seja, pertencente ao grupo Domain Admins (Administradores do Domínio) do domínio vendas.abc.com. Com isso ficamos com a alternativa b.

**Questão 55:** Você é o responsável pela administração da rede da empresa. A rede é baseada no Windows Server 2003 e no Active Directory. Você implementou o SUS, para fazer a atualização automática do Windows Server 2003 em cerca de 100 Servidores da rede. O SUS foi instalado com sucesso no servidor SRVSUS01 e os clientes foram configurados com sucesso para utilizar o servidor SUS. A atualização automática vem funcionando normalmente, durante os últimos dois meses, sendo que o SUS faz a sincronização e o download automático a partir do site Windows Update e os demais servidores, recebem as atualizações a partir do servidor SRVSUS01. Na última semana, você ficou sabendo pela Internet, sobre uma nova atualização crítica de segurança para o Windows Server 2003. Imediatamente você tenta acessar a página de administração do SUS, para aprovar esta atualização, de tal forma que ela seja aplicada aos servidores da rede. Ao tentar acessar a página de administração do SUS, você recebe uma mensagem de erro. Você tenta acessar a página padrão do IIS no servidor SRVSUS01 e também não consegue. O que você deve fazer para normalizar o funcionamento do SUS, sem interromper a execução de outros serviços que estão rodando no servidor SRVSUS01?

- a) Parar e Reiniciar todos os serviços relacionados ao IIS
- b) Reiniciar o serviço de FTP
- c) Parar e Reiniciar o serviço de NETLOGON
- d) Forçar uma sincronização imediata do SUS
- e) Forçar uma atualização automática do SUS

Resposta certa: a

**Comentários:** Esta questão testa se o candidato sabe que o SUS é basicamente um site que é instalado em um servidor IIS. Ou seja, todo o funcionamento do SUS depende do IIS. Se houver problemas com os serviços do IIS, é provável que a causa sejam os serviços do IIS. Nesta questão, a solução é parar e reiniciar todos os serviços relacionados ao IIS. Com isso deverá normalizar o funcionamento do SUS. Com isso ficamos com a alternativa a.

**Questão 56:** Você é o administrador de uma estação de trabalho com o Windows Server 2003 instalado. Você tem um conjunto de atalhos e configurações que devem ser aplicados apenas aos novos usuários que fizerem o logon na estação de trabalho, ou seja, aqueles usuários que estão logando pela primeira vez na estação, para os quais ainda não existia uma Profile na estação. Qual profile você deve modificar?

- a) All Users
- b) Administrador
- c) Users
- d) Default User
- e) New Users

**Resposta certa: d**

**Comentários:** Esta questão testa, basicamente, o conhecimento do candidato em relação ao Conceito de Profile. Atalhos e configurações que devem estar disponíveis para todos os usuários, devem ser feitas na Profile All Users. Atalhos e configurações que devem estar disponíveis apenas para novos usuários que façam o logon na estação de trabalho, devem ser feitos na profile Default User. Com isso ficamos com a alternativa D.

**Questão 57:** Você é o Administrador de uma rede com servidores baseados no Windows Server 2003 e no Active Directory. A rede é formada por um único domínio: abc.com. A WAN da empresa é formada pela rede local da matriz em SP e pelas redes locais das filiais em SC, RS e PR. Você está em fase de implementação da rede e gostaria de limitar o número de usuários com permissões de Administrador em todos os recursos do domínio, ou seja, você quer reduzir o número de usuários que serão incluídos no grupo Domain Admins. Porém você gostaria de ter usuários com permissão para gerenciar recursos tais como contas de usuários e computadores em cada uma das redes locais. Por exemplo, você gostaria de permitir que um usuário da matriz em SP possa gerenciar recursos apenas para os usuários, servidores e recursos da rede local de SP. Que tipo de objeto do Active Directory você pode utilizar para implementar a solução proposta?

- a) Unidades Organizacionais
- b) Group Policy Objects
- c) Diretivas de IPSec
- d) Diretivas locais de segurança
- e) Grupos de distribuição

**Resposta certa: a**

**Comentários:** O conceito de Unidade organizacional foi introduzido no Windows 2000 Server, juntamente com o Active Directory e veio para solucionar um problema sério de Administração existente no Windows NT Server 4.0. Conceito este que, evidentemente, também está presente no Windows Server 2003.

Com o NT Server 4.0, não havia como atribuir permissões de acesso apenas em uma parte do domínio. Ou você atribuía permissões de Administrador no domínio inteiro ou não tinha como atribuir permissões de administrador para um usuário apenas para parte dos recursos do domínio. Imagine uma empresa que tem uma rede, com filiais em todos os estados brasileiros. No nosso exemplo, o domínio é composto pelas redes das filiais do RS, SC, PR e SP. Com o NT Server 4.0, você não teria como definir que um usuário tivesse permissões de Administrador somente nos servidores

da filial do RS. Uma vez que você atribuía permissões de Administrador, o usuário teria estas permissões em todos os recursos do domínio. No nosso exemplo, o usuário seria Administrador nos servidores e em todos os recursos das filiais do RS, SC, PR e SP, ou seja, em todos os servidores do domínio.

Esta situação gerava inconvenientes (e noites de sono perdidas) muito sérios. Era comum a situação onde um domínio tinha 10 ou mais contas de usuários com permissão de Administrador. Ora, eram 10 ou mais contas com permissões total em todos os servidores do domínio. Nada bom.

Com a disponibilidade de Unidades Organizacionais, a partir do Windows 2000 Server, este problema foi minimizado. Agora você pode criar, dentro do domínio, várias Unidades organizacionais. Em seguida você desloca para dentro de cada unidade organizacional, as contas de usuários, grupos e computadores, de acordo com critérios geográficos ou funcionais. Em seguida você pode delegar tarefas administrativas a nível de Unidade organizacional (OU – Organizational Unit).

**Questão 58:** Em relação ao recurso de GPOs não é correta a seguinte afirmação:

- a) Com o recurso de GPOs é possível configurar a redireção de pastas. O administrador pode configurar uma GPO para que pastas tais como Meus documentos e Minhas imagens sejam redirecionadas para uma pasta compartilhada em um servidor da rede da empresa. Com isso os dados do usuário passam a estar disponíveis no servidor e poderão ser acessados de qualquer estação de trabalho da rede, na qual o usuário faça o logon. Além disso, com os dados no servidor, é possível criar e implementar uma política de backup centralizada.
- b) Com o recurso de GPO é possível gerenciar centralizadamente, configurações definidas na registry do Windows, com base em templates de administração (Administrative Templates). As GPOs criam arquivos com definições da registry. Estes arquivos são carregados e aplicados na estação de trabalho do usuário, nas partes referentes a configuração de Usuários e configuração de Computador da registry. As configurações de usuário são carregadas na opção HKEY\_CURRENT\_USER (HKCU), da registry. As configurações de computador são carregadas na opção HKEY\_LOCAL\_MACHINE (HKLM), da registry. A idéia é relativamente simples. Ao invés de ter que configurar estas opções em cada estação de trabalho, o administrador cria elas centralizadamente, usando GPOs. Durante o logon, o Windows aplica as configurações definidas na GPO.
- c) As GPOs inclui configurações que são aplicadas a nível de usuário (ou seja, em qualquer estação de trabalho que o usuário faça o logon, as políticas associadas a sua conta de usuário serão aplicadas) e a nível de computador (ou seja, qualquer usuário que faça o logon no computador terá as políticas de computador aplicadas). Por exemplo, se o administrador definiu uma política de usuário para o grupo do usuário jsilva, de tal maneira que o menu Run (Executar) não deva estar disponível para este grupo. Em qualquer estação de trabalho que o jsilva fizer o logon, o menu Run não estará disponível. Agora imagine que o administrador configurou uma política de computador, para o grupo de computadores da seção de contabilidade, definindo que o menu Run (Executar) não deve estar disponível nestes computadores. Qualquer usuário que faça o logon em um dos computadores da seção de contabilidade, não terá o menu Run sendo exibido, independentemente dos grupos aos quais pertença o usuário, uma vez que a política está sendo aplicada ao computador (independentemente do usuário que esteja utilizando-o).
- d) As configurações feitas via GPO são aplicadas para usuários, computadores, member servers e DCs, são aplicadas a computadores executando Windows 2000 (Server ou Professional), Windows XP ou Windows Server 2003. São também aplicadas para versões mais antigas do Windows, tais como Windows 95/98/Me e NT 4.0, o recurso de GPO não é aplicado, permitindo que o Administrador configure uma ampla variedade de clientes, usando diferentes versões do Windows..
- e) O recurso de Group Policy Objects (GPO) é de “enorme” utilidade para o administrador. Com o uso de GPO o administrador pode definir as configurações de vários elementos da estação de trabalho do usuário, como por

exemplo os programas que estarão disponíveis, os atalhos do menu Iniciar que estarão disponíveis, configurações de Internet, de rede e assim por diante. Por exemplo, o administrador pode configurar, via GPO, quais grupos de usuários deverão ter acesso ao menu Run (Executar) e quais não terão, pode configurar a página inicial do Internet Explorer para um grupo de usuários ou para toda a empresa, pode fazer configurações de Proxy e por aí vai. São milhares (literalmente “milhares”) de opções de configurações que estão disponíveis via GPO.

**Resposta certa: d**

**Comentários:** Todas as afirmativas estão corretas com exceção da letra d. O recurso de GPOs não se aplica a versões mais antigas do Windows, tais como o Windows 95/98/Me. Todas as demais alternativas, com exceção da letra d, descrevem as características e capacidades do recurso de GPOs.

**Questão 59:** O usuário jsilva pertence aos seguintes grupos: Gerentes, Técnicos e Marketing. O usuário jsilva precisa ter acessos somente de leitura e alteração nos documentos do Word que estão em uma pasta compartilhada, no servidor \\SRV01\worddocs. O usuário deve ter permissão somente de leitura e alteração, sem ter permissão de exclusão e alteração das permissões, quer ele esteja acessando a pasta worddocs através da rede ou localmente logado no servidor SRV01.

As permissões NTFS e de compartilhamento desta pasta e o seu conteúdo, estão configuradas da seguinte maneira:

- ◆ Permissões NTFS:
  - ◆ Gerentes: Leitura e alteração
  - ◆ Técnicos: Leitura
  - ◆ Marketing: Leitura
- ◆ Permissões de Compartilhamento:
  - ◆ Gerentes: Leitura
  - ◆ Técnicos: Leitura e Alteração
  - ◆ Marketing: Leitura

O que deve ser alterado para que o usuário jsilva tenha somente as permissões de leitura e alteração, quer seja para acesso através da rede, quer seja acessando localmente no servidor SRV01?

- a) Atribua a permissão NTFS Negar Leitura a conta jsilva.
- b) Nada precisa ser feito.
- c) Retire o usuário jsilva do grupo Marketing.
- d) Define permissão de leitura para a conta jsilva.
- e) Retire o usuário jsilva do grupo Gerentes e também do grupo Marketing.

**Resposta certa: b**

**Comentários:** Para responder corretamente esta questão, o usuário deve lembrar de algumas regras básicas das permissões NTFS, quando o usuário pertence a mais de um grupo:

- ◆ A permissão efetiva é a soma das permissões de todos os grupos aos quais o usuário pertence.
- ◆ Negar tem precedência sobre qualquer outra permissão.
- ◆ Também é importante lembrar que quando existem diferenças entre as permissões NTFS e as permissões de Compartilhamento, vale a mais restritiva. Neste caso a permissão mais restritiva é a de compartilhamento que é somente Leitura. Neste caso a permissão efetiva NTFS é Leitura e alteração e a permissão efetiva de compartilhamento é Leitura e Alteração. Combinando as duas, evidentemente, resulta em leitura e alteração, ou seja, o usuário jsilva já tem o nível de permissão exigido pela questão. Com isso nada precisa ser feito.

Não esqueça que as permissões de compartilhamento somente tem efeito para o acesso através da rede. Se o usuário jsilva fizer o logon no servidor SRV01 e acessar a pasta worddocs localmente, valerão apenas as permissões NTFS.

**Questão 60:** Considere as afirmações a seguir em relação aos tipos e escopos de grupos de usuários, no Windows Server 2003:

- I. **Grupos de segurança:** Normalmente utilizados para atribuir permissões de acesso aos recursos da rede. Por exemplo, ao criar um grupo Contabilidade (que conterá todas as contas dos funcionários do departamento de contabilidade) o qual será utilizado para atribuir permissões de acesso a uma pasta compartilhada, devo criar este grupo como sendo do tipo Grupo de segurança. Um grupo de segurança também pode ser utilizado como um grupo de distribuição, embora essa não seja uma situação muito comum. Esses grupos, assim como as contas de usuários são armazenados no Banco de dados do Active Directory.
- II. **Grupos de distribuição:** São utilizados para funções não relacionadas com segurança (não relacionadas a atribuição de permissões). Normalmente são utilizados em conjunto com servidores de e-mail, tais como o Exchange 2000, para o envio de e-mail para um grupo de usuários. Uma das utilizações típicas para um Grupo de distribuição é o envio de mensagens de e-mail para um grupo de usuários de uma só vez. Somente programas que foram programados para trabalhar com o Active Directory, poderão utilizar Grupos de distribuição (como é o caso do Exchange 2000 citado anteriormente). Provavelmente as novas versões dos principais sistemas de correio eletrônico estarão habilitadas para trabalhar com o Active Directory. Não é possível utilizar grupos de distribuição para funções relacionadas com segurança.
- III. **Grupos universais (Universal group):** Como o próprio nome sugere são grupos que podem ser utilizados em qualquer parte de um domínio ou da árvore de domínios e podem conter como membros, grupos e usuários de quaisquer domínios. Pode conter: Contas de usuários, outros grupos universais, e grupos globais de qualquer domínio. Pode ser membro de: Grupos locais de qualquer domínio ou grupos universais de qualquer domínio. Pode receber permissões para recursos localizados em qualquer domínio. Um domínio baseado no Active Directory pode estar em diferentes modos de funcionalidade (Windows 2000 Nativo, Misto ou Windows Server 2003). Para cada modo existem diferentes possibilidades em relação aos grupos Universais: Quando o nível de funcionalidade do Domínio está configurado como Windows 2000 Nativo ou Windows Server 2003, os seguintes elementos podem ser incluídos como membros de um grupo universal: Usuários, grupos Globais e grupos Universais de qualquer domínio da floresta. Quando o nível de funcionalidade do Domínio está configurado como Windows 2000 Misto, não é possível criar grupos Universais. Quando o nível de funcionalidade do Domínio está configurado como Windows 2000 Nativo ou Windows Server 2003, um grupo Universal pode ser colocado como membro de um outro grupo Universal e permissões podem ser atribuídas em qualquer domínio. Um grupo pode ser convertido de Universal para Global ou de Universal para Local do domínio. Nos dois casos esta conversão somente pode ser feita se o grupo Universal não tiver como um de seus membros, outro grupo Universal.
- IV. **Grupo global:** Um grupo Global é “global” quanto aos locais onde ele pode receber permissões de acesso, ou seja, um grupo Global pode receber permissões de acesso em recursos (pastas compartilhadas, impressoras, etc) de qualquer domínio. Pode conter: Contas de usuários e grupos globais do mesmo domínio, ou seja, somente pode conter membros do domínio no qual o grupo é criado. Pode ser membro de: Grupos universais e Grupos locais, de qualquer domínio. Grupos globais do mesmo domínio. Pode receber permissões para recursos localizados em qualquer domínio. Um domínio baseado no Active Directory pode estar em diferentes modos (Windows 2000 Nativo, Misto ou Windows Server 2003). Para cada modo existem diferentes possibilidades em relação aos grupos Globais: Quando o nível de funcionalidade do Domínio está configurado como Windows 2000 Nativo ou Windows Server 2003, os seguintes elementos podem ser incluídos como membros de um grupo Global: contas de

usuários e grupos globais do mesmo domínio. Por exemplo, se você cria um grupo global chamado WebUsers, no domínio abc.com.br, este grupo poderá conter como membros, grupos globais do domínio abc.com.br e usuários do domínio abc.com.br. Quando o nível de funcionalidade do Domínio está configurado como Windows 2000 Misto, somente contas de usuários do próprio domínio é que podem ser membros de um grupo Global. Por exemplo, se você cria um grupo global chamado WebUsers, no domínio abc.com.br e este domínio está no modo Misto, então somente contas de usuários do domínio abc.com.br é que poderão ser membros do grupo WebUsers. Um grupo pode ser convertido de Global para Universal, desde que o grupo Global não seja membro de nenhum outro grupo Global.

- V. **Grupos locais (Domain local group):** São grupos que somente podem receber permissões para os recursos do domínio onde foram criados, porém podem ter como membros, grupos e usuários de outros domínios. Pode conter membros de qualquer domínio. Somente pode receber permissões para recursos em servidores do domínio no qual o grupo foi criado. Pode conter: Contas de usuários, grupos universais e grupos globais de qualquer domínio. Outros grupos Locais do próprio domínio. Pode ser membro de: Grupos locais do próprio domínio. Um domínio baseado no Active Directory pode estar em diferentes modos (Windows 2000 Nativo, Misto ou Windows Server 2003). Para cada modo existem diferentes possibilidades em relação aos grupos Globais: Quando o nível de funcionalidade do Domínio está configurado como Windows 2000 Nativo ou Windows Server 2003, os seguintes elementos podem ser incluídos como membros de um grupo Local: contas de usuários, grupos universais e grupos globais de qualquer domínio. Outros grupos locais do próprio domínio. Um grupo pode ser convertido de Local para Universal, desde que o grupo não tenha como seu membro um outro grupo Local.

Estão corretas as seguintes afirmativas:

- a) Todas
- b) I e II
- c) III, IV e V
- d) II, III, IV e V
- e) I, II e III

**Resposta certa:** a

**Comentários:** Todas as afirmações estão corretas e descrevem os tipos e escopos de grupos de usuários, disponíveis no Windows Server 2003.

## Conclusão

Muito bem amigo leitor. Aqui encerro minha contribuição para ajudá-lo na batalha para o Exame 70-290. Recomendo que você estude e revise cuidadosamente os conceitos apresentados neste livro e procure aprofundar os seus estudos usando a Ajuda do Windows Server 2003, os endereços indicados neste site e outras fontes de estudo que você possa ter acesso.

Este manual foi projetado para ajudá-lo a obter aprovação no Exame 70-290. Os assuntos abordados foram baseados no programa Oficial da Microsoft. Estude com atenção os tópicos apresentados neste manual, releia mais algumas vezes o resumo do Capítulo 14 e o simulado deste capítulo e não deixe de consultar os sites indicados ao longo de todo o livro.

É o meu mais sincero desejo que este livro possa ajudá-lo em sua caminhada rumo ao MCSE-2003.

Agradeço imensamente por ter adquirido e estudado este livro. É meu mais sincero desejo que você seja aprovado em mais este exame. Não deixe de enviar suas sugestões e críticas para o meu email: [webmaster@juliobattisti.com.br](mailto:webmaster@juliobattisti.com.br).