UNIDADE 3

CONTEÚDOS

- História dos sistemas operativos servidores Windows
- Objectives do Windows Server
- Características e componentes do Windows Server 2003
- Terminologia de redes da Microsoft
- Planeamento da instalação
- Partições
- *Hardware* e *software*
- Processo de instalação
- Ferramentas de administração
- Administração rápida
- *Active Directory*
- Contas e grupos de utilizadores
- Perfis de utilizador
- Políticas de grupo e de sistema
- *Home folder* / Pasta raiz
- *Logon scripts*
- Gestão do servidor
- TCP/IP
- DHCP
- Gestão de licenças
- Monitorização e optimização
- Cópias de segurança
- Segurança de discos
- Auditoria do servidor
- Gestão de energia
- Gestão dos clientes da rede

SISTEMA OPERATIVO WINDOWS SERVER

OBJECTIVOS

- Conhecer o enquadramento histórico do Windows Server e ser capaz de o relacionar com outras versões, nomeadamente o Windows NT.
- Conhecer os principais objectivos, características e novidades do sistema operativo.
- Conhecer a terminologia de redes da Microsoft.
- Ser capaz de planear a instalação de um servidor com o Windows Server 2003 e saber fazer as escolhas das partições adequadas, do *hardware* e do *software* necessários.
- Conhecer o processo de instalação do Windows Server 2003, escolhendo o modo mais adequado.
- Ser capaz de administrar um servidor com o Windows Server 2003.
- Saber utilizar diversas ferramentas de administração.
- Conseguir instalar o *Active Directory* e criar contas e grupos de utilizadores.
- Saber gerir perfis de utilizador, políticas de grupo e de utilizador.
- Ser capaz de instalar, configurar e/ou administrar os diversos serviços do sistema Windows Server 2003.
- Ter noção da importância dos *backups* no sistema Windows Server 2003.
- Ser capaz de activar a segurança adequada ao nível dos discos.
- Saber analisar o estado do sistema recorrendo às ferramentas apropriadas.
- Conseguir gerir a energia do sistema.
- Ser capaz de ligar ao servidor clientes de diversos sistemas operativos para postos de trabalho da Microsoft.
- Saber aceder remotamente ao sistema, configurando-o de modo correcto.

PLANIFICAÇÃO ANUAL

UNIDADES	SUBUNIDADES	OBJECTIVOS	CONTEÚDOS	ESTRATÉGIAS/ ACTIVIDADES
3. SISTEMA OPERATIVO WINDOWS 2003 SERVER	1. Introdução ao Windows Server	• Conhecer o enquadramento histórico do Windows Server e ser capaz de o relacionar com outras versões, nomeadamente o Windows NT. • Conhecer os principais objectivos, características e novidades do sistema operativo. • Conhecer a terminologia de redes da Microsoft.	• História do Windows. • Objectivos do Windows Server. • Características e componentes do Windows 2003 Server. • Terminologia de redes da Microsoft.	• Visualização de pequenos documentários ou minifilmes. • Simulações de laboratório (de quebras de segurança, por exemplo). • Ilustrações de diferentes tipos de redes. • Recurso a sistemas operativos para ilustrar o TCP/IP. • Apresentação de tipologias de redes de computadores. • Realização de debates. • Organização de colóquios.
	2. Instalação e configuração do Windows Server 2003	• Ser capaz de planear a instalação de um servidor de Windows e saber fazer as escolhas das partições adequadas, do *hardware* e do *software* necessários. • Conhecer o processo de instalação do Windows, escolhendo o modo mais adequado.	• Planeamento da instalação. • Partições. • *Hardware* e *software*. • Processo de instalação.	
	3. Administração e serviços do Windows Server 2003	• Ser capaz de administrar um servidor de Windows. • Saber utilizar diversas ferramentas de administração. • Conseguir instalar o *Active Directory* e criar contas e grupos de utilizadores. • Saber gerir perfis de utilizador, políticas de grupo e de utilizador. • Ser capaz de instalar, configurar e/ou administrar os diversos serviços do sistema.	• Ferramentas de administração. • Administração rápida. • *Active Directory*. • Contas e grupos de utilizadores. • Perfis de utilizador. • Políticas de grupo e de sistema. • *Logon scripts*. • Gestão do servidor. • TCP/IP. • HCP. • Gestão de licenças. • Monitorização e optimização.	
	4. Trabalho em rede com Windows Server 2003	• Ter noção da importância dos *backups* no sistema. • Ser capaz de activar a segurança adequada ao nível dos discos. • Saber analisar o estado do sistema recorrendo às ferramentas apropriadas. • Conseguir gerir a energia do sistema. • Ser capaz de ligar ao servidor clientes de diversos sistemas operativos da Microsoft.	• Cópias de segurança. • Segurança de discos. • Auditoria do servidor. • Gestão de energia. • Gestão dos clientes da rede.	

ÍNDICE

ÍNDICE

ÍNDICE

ÍNDICE

1. Introdução ao Windows Server

1.1. História do Windows

Ao longo dos anos, a Microsoft tem desenvolvido diversos sistemas operativos, tanto para postos de trabalho como para servidores. Na disciplina de Tecnologias Informáticas do 10.º Ano foram estudados alguns dos **sistemas operativos para postos de trabalho**, que passamos a relembrar.

Sistemas operativos para postos de trabalho desenvolvidos pela Microsoft

MS-DOS

O MS-DOS (*Microsoft Disk Operating System*), ou DOS, foi comercializado pela Microsoft para equipar os **primeiros microprocessadores da Intel de 8 e 16 bit**, e depois desenvolvido para o primeiro IBM PC, em 1981. Este sistema operativo não podia executar mais do que um programa em simultâneo, não permitindo que outros programas invadissem o espaço de memória, pois provocariam falhas no funcionamento. Não nos podemos esquecer que o MS-DOS só trabalhava com 640 kB de memória RAM.

O MS-DOS teve influências do UNIX, nomeadamente nos comandos de gestão e de navegação entre directorias, que são muito idênticos aos do UNIX, mas, no geral, o funcionamento é muito diferente, pois o MS-DOS **não suporta multitarefa, não tem interface gráfica incorporada, é monoutilizador, não incorpora sistema de segurança, não inclui ligação em rede e não suporta multiprocessamento** (funcionalidades incluídas no UNIX, praticamente desde as primeiras versões).

A última versão do MS-DOS foi a 6.22, lançada em 1994. No entanto, e apesar das suas grandes limitações, ainda hoje é possível encontrar pessoas a usar o MS-DOS, dado a grande quantidade de programas existentes para o mesmo e pelo facto de ainda se encontrarem situações onde não é possível, ou tornar-se financeiramente inviável, conseguir-se um programa compatível com os sistemas operativos mais actuais.

Windows 3.11

Verificado o sucesso do MacOs – sistema operativo com interface gráfica com o utilizador (GUI) –, a Microsoft começou a executar as primeiras versões do Windows, que foram desenvolvidas até à versão **Windows 3.11**, em 1994; estas **não eram**, no entanto, **consideradas sistemas operativos**, mas **programas** que **corriam sobre o MS-DOS** e que colocavam os microprocessadores da Intel (a partir dos 80386DX) a trabalhar em modo protegido. Pelo facto de se trabalhar com o MS-DOS, estes programas só conseguiam trabalhar com 16 bit de dados de cada vez, não podendo, assim, tirar partido das capacidades de processamento de 32 bit do microprocessador Intel 80386 e superiores. Não devemos esquecer que as versões do Windows 3.11 (e as anteriores) utilizavam **multitarefa cooperativa**, e, deste modo, não podiam executar mais do que um programa em simultâneo e o bloqueamento de um dos programas provocaria uma falha em todo o sistema.

Windows 95, 98 e Me

Entre 1993 e 1995, a Microsoft foi desenvolvendo um sistema operativo que trabalhava com 32 bit, com interface gráfica com o utilizador (GUI) integrada e que dava ainda a possibilidade de trabalhar em rede e de suportar multitarefa preemptiva. A versão que surgiu nos finais de 1995 designou-se **Windows 95** e, neste caso, pode-se dizer que se tratava, de facto, de **um sistema operativo e não de uma aplicação**. Outras características para o seu sucesso foram a compatibilidade com a maioria dos programas feitos para o MS-DOS e vir pré-instalado de fábrica em milhões de microcomputadores. Este sistema operativo foi actualizado em 1997 – **Windows 95 OSR2** – e esta versão já suportava a gestão dos discos rígidos de FAT16 e de FAT32, cuja vantagem era poder-se trabalhar com partições superiores a 2 Gbyte.

O **Windows 98**, lançado em 1998, ofereceu maior estabilidade, melhor conectividade com a Internet e *drives* para novos periféricos (ex.: DVD-ROM). No espaço de apenas um ano, esta versão foi actualizada para **Windows 98 SE** (Segunda Edição).

O **Windows Me (Millenium Edition)** foi lançado nos finais de 2000. O lançamento do Windows XP Home, que utiliza a tecnologia do Windows NT, substituiu o Windows Me e assistimos ao **fim dos sistemas operativos que derivaram do MS-DOS** (fim da tecnologia Windows 9x), como podemos analisar pelo esquema seguinte:

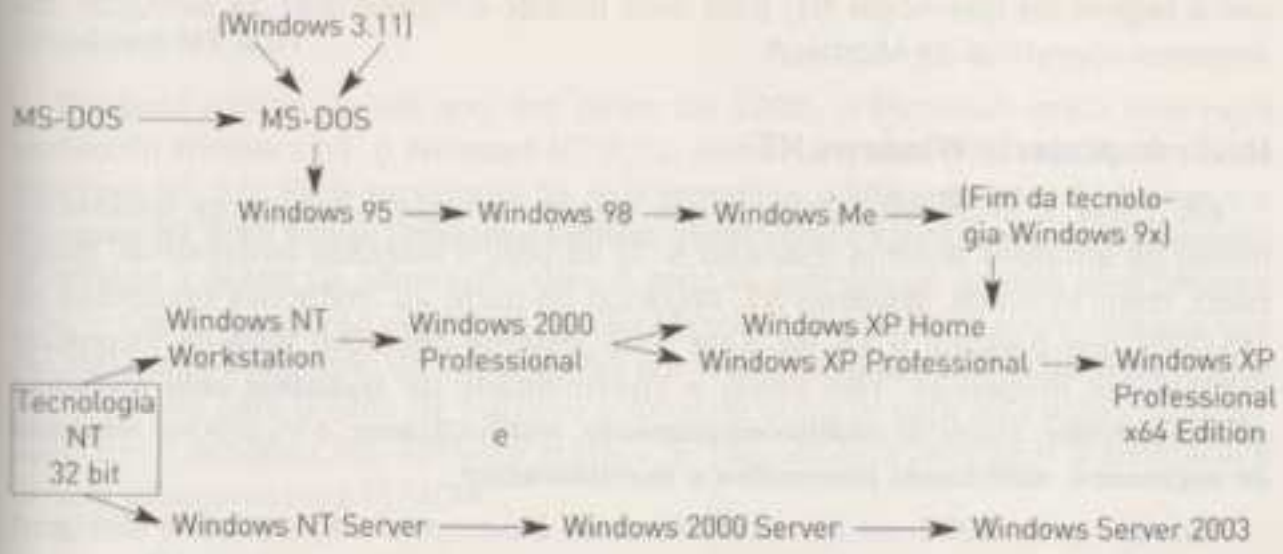

Fig. 3.1 Esquema da evolução dos sistemas operativos da Microsoft

Windows NT, 2000 e XP

O Windows NT, querendo NT significar Nova Tecnologia (*New Tecnology*), foi desenvolvido pela Microsoft nos finais dos anos 80. Tratava-se, então, de um sistema operativo já a 32 bit, indicado para o mercado empresarial. Por um lado, este sistema operativo pretendia substituir o MS-DOS e o Windows 9x, por outro lado, pretendia também lançar uma versão para postos de trabalho, o **Windows NT Workstation**, e outra versão para computadores servidores (**Windows NT Server**).

O Windows NT evoluiu das primeiras versões, Windows NT 3.1, 3.4, 3.51, até à última versão Windows NT 4.0.

Em 2000 surgiu o Windows 2000 – que mais não é do que uma evolução do Windows NT –, na versão **Windows 2000 Professional** (a evolução do Windows NT Workstation para postos de trabalho) e na versão **Windows 2000 Server** (para postos servidores de rede).

Com a versão Windows 2000 Professional, a Microsoft anunciou que iria substituir por completo as versões para postos de trabalho de clientes domésticos, o Windows 95 e 98, mas tal não aconteceu.

Foi apenas nos finais de 2001, com o lançamento do **Windows XP Home Edition** (versão para sistemas operativos para postos de trabalho domésticos), que a Microsoft terminou com os sistemas operativos Windows 95, 98 e Me; com o lançamento do **Windows XP Professional** (para postos de trabalho empresariais), a Microsoft substituiu o Windows 2000 Professional. As duas versões provinham da tecnologia NT.

Em 25 de Abril de 2005, a Microsoft lançou a versão final do seu novo sistema operativo para microprocessadores a 64 bit, designado **Windows XP Professional x64 Edition**.

A versão servidora, conhecida por **Windows Server 2003**, surgiu em 2003 e substituiu o Windows 2000 Server.

Sistemas operativos para servidores desenvolvidos pela Microsoft

Antes mesmo de começar com a explicação deste ponto, convém dar a conhecer a origem da tecnologia NT, para uma melhor compreensão da evolução dos sistemas operativos da Microsoft.

Inicio do projecto Windows NT

Em 1988, a Microsoft formou o que viria a tornar-se a equipa de desenvolvimento de um novo sistema operativo a 32 bit para o mercado empresarial, designado, como já vimos, **Windows NT**, deixando de parte as limitações existentes no MS-DOS, que trabalha a 16 bit. Este novo sistema operativo teria de incorporar tecnologias modernas, tais como a possibilidade de **trabalhar com sistemas cliente-servidor**, suportar **multiprocessamento, multiutilizador**, e incorporar **sistemas de segurança, multitarefa preemptiva e *multithreading***.

Em Agosto de 1991, na *Microsoft Windows Developers Conference*, a Microsoft demonstrou a implementação do seu novo sistema operativo Windows NT.

Windows NT 3.1

Em Julho de 1993, a Microsoft lançou o **Windows NT 3.1 Advanced Server**, para servidores, e o **Windows NT 3.1**, para postos de trabalho empresariais. Estes abriram um novo caminho na capacidade dos sistemas operativos da Microsoft, na sua performance e na sua confiança, através de uma variedade de características, entre as quais se destacam a arquitectura *microkernel*, o suporte a microprocessadores da Intel ou compatíveis x86, um pouco mais tarde, o suporte a microprocessadores Alpha, gestor de multitarefa preeemptiva, suporte de aplicativo Wind32®, suporte para DOS, versões 16 bit do Windows, aplicações OS/2 e POSIX, segurança de servidor de domínio, serviços de ficheiros e de impressão e sistemas de ficheiros NTFS (*Windows NT File System*).

O Windows NT 3.1 manteve a consistência com o Windows 3.1 a nível de ambiente gráfico, dado que, na época, muitos utilizadores usavam, em postos de trabalho domésticos, a versão do Windows 3.1.

Windows NT 3.5

O Windows NT 3.5, com o nome de código "Daytona", foi lançado em 6 de Setembro de 1994 e tinha três versões diferentes. Duas eram para servidores de rede: o **Windows NT 3.5 Server** e, com capacidades acrescidas, o **Windows NT 3.5 Server Enterprise Edition**. A terceira versão foi proposta para postos de trabalho e era designada **Windows NT 3.5 Workstation**, que limitava o número de tarefas simultâneas em rede. As interfaces destas versões do Windows NT 3.5 eram iguais à do **Windows 3.1** para postos de trabalho. Os utilizadores deixaram de ter o ecrã preto de iniciação, como no MS-DOS, e, em seu lugar, surgiu um ecrã de iniciação gráfico.

O Windows NT 3.5 Workstation dava suporte ao padrão de elementos gráficos OpenGL, que ajudava a activar aplicativos de topo de linha poderosos para desenvolvimento de *software*, engenharia, análise financeira, fins científicos e tarefas de importância crítica da empresa.

Estas versões foram construídas sobre as rugosidades e a estabilidade da versão Windows NT 3.1, para aumentar a velocidade, reduzir o tamanho e fornecer maior conectividade com outros sistemas, nomeadamente ambientes Novell NetWare e UNIX. Todas as versões incluíam características para utilizadores com destreza limitada ou com diminuição de audição.

Windows NT 3.51

Passado menos de um ano, em Junho de 1995, a Microsoft lança uma nova versão do Windows NT, o Windows NT 3.51. Foram lançadas três versões como no Windows NT 3.5. Para servidores de rede tínhamos o **Windows NT 3.51 Server** e o **Windows NT 3.51 Server Enterprise Edition**; estas versões incluíam uma ferramenta destinada a ajudar os administradores a gerir as licenças de acesso para clientes (CAL – *Client Access Licences*) da família Microsoft BackOffice® e um utilitário que permitia uma instalação do Windows 95 por rede. O **Windows NT 3.51 Workstation** era a versão para postos de trabalho e fornecia suporte para aplicações compatíveis com o Windows 95, *software* popular de fax, um ecrã WinLogon substituível e *drivers* adicionais para PCMCIA.

Windows NT 4.0

Em Julho de 1996, a Microsoft lançou o Windows NT 4.0, composto por versões servidoras e uma para postos de trabalho.

Nas versões servidoras foram lançadas várias versões diferentes: uma versão-base, designada **Windows NT 4.0 Server**; o **Windows NT 4.0 Server Enterprise Edition**, que era uma versão com capacidades superiores à versão-base, para suportar situações mais exigentes em redes de grande porte; o **Windows NT Server 4.0 Terminal Server Edition**, que incluía o serviço de *terminal service* que possibilitava correr aplicações no próprio servidor em vez dos clientes, isto é, nos clientes eram visualizados ecrãs das aplicações que estavam realmente a ser processadas no servidor, e, por fim, o **Windows Small Business Server**, ou simplesmente **SBS**, sendo a última versão a SBS 4.5. Esta última versão era destinada a servidores de rede de pequenas e médias empresas, pois estava limitada em número de utilizadores. Só era permitido ter um servidor da Microsoft numa rede, mas com a vantagem de incorporar diversos serviços de rede que estavam excluídos nas versões anteriores e que tinham de ser adquiridas à parte, com custos acres-

cidos, tais como, entre outros, servidor de base de dados SQL Server, partilha de acesso à Internet, partilha de *modem* e servidor de correio electrónico Exchange Server. A versão para postos de trabalho empresariais era a versão **Windows NT 4.0 Wokstation**.

O **Windows NT Server** e **Workstation 4.0** acarretaram facilidades na utilização e na gestão, maior taxa de transmissão da rede e um conjunto completo de ferramentas para desenvolvimento e gestão de intranets. O Windows NT Server 4.0 incluía a versão 2.2 do Microsoft Internet Information Server e a versão 1.1 de criação e ferramentas de gestão de *websites* da Microsoft FrontPage®. O lançamento do Windows NT Workstation incluía a popular interface do utilizador do Windows 95 e o suporte interno de trabalho na Net (*networking*), fornecendo acesso seguro e fácil à Internet e às intranets colectivas. Todas as versões servidoras incluíam serviços mais rápidos de ficheiros e de impressão, suporte a aplicativos mais robusto, recursos de comunicação baseados em padrões e, tanto as versões servidoras como a de posto de trabalho, utilizavam uma interface gráfica semelhante à do Windows 95.

Desde a introdução original do Windows NT 4.0, o produto evoluiu através de vários pacotes de serviço, designados "*service pack*", e um pacote opcional, adicionando e integrando funcionalidades de chave-pública (*public key*) e de autoridade certificada (*certificate authority*), suporte de *smart card*, melhorias na escalabilidade de multiprocessamento simétrico (SMP), capacidade de *clustering*, suporte a modelos de objectos componentes (COM), características de *streaming media* e muitas tecnologias de servidores e de *browsers* relevantes à Internet.

A 27 de Outubro de 1998, a Microsoft anunciou que o Windows NT passará a ser conhecido apenas como Windows, retirando o "NT" na próxima versão, que veio a chamar-se, então, apenas Windows 2000.

Windows 2000

A 17 de Fevereiro de 2000, a Microsoft lançou o Windows 2000, que veio substituir o Windows NT 4.0. Esta nova versão foi mais do que uma mera evolução; o Windows 2000 inclui recursos avançados, como gestão centralizada baseada em políticas com novas tecnologias, como a gestão Microsoft *IntelliMirror* e o serviço Microsoft *Active Directory* e gestão de sistemas de ficheiros NTFS versão 5, que possibilita a gestão de quotas em disco. Em todas as versões, o ambiente gráfico permaneceu quase o mesmo, quando comparado com o do Windows 98. A implementação e a gestão tornaram-se mais simples e rápidas e levaram muitas organizações a migrar para o Windows 2000.

O **Windows 2000 Professional** era a versão para postos de trabalho que acabaria por substituir o Windows NT 4.0 Workstation.

Foram lançadas 4 versões para servidores de rede:

- **Windows 2000 Server** – versão-base que substituiu o Windows NT 4.0 Server; utilizada para equipar pequenos e médios servidores.
- **Windows 2000 Advanced Server** – substituiu o Windows NT 4.0 Server Enterprise Edition, que, em termos genéricos, se destina a equipar servidores de departamentos com necessidades de prestações superiores à versão-base.
- **Windows 2000 Datacenter Server** – a versão servidora mais poderosa até então desenvolvida pela Microsoft, com a finalidade de equipar *clusters* de servidores

de grande porte, correndo aplicações complexas, sistemas cliente-servidor, elevada capacidade de comunicação e de grande fluxo de dados. Esta versão não existia na versão NT 4.0 e veio colmatar a inexistência de um produto servidor para sistemas de grande porte por parte da Microsoft.

Para informação mais detalhada, encontra-se na tabela 3.1 uma comparação dos serviços disponibilizados pelas diversas versões da família Windows 2000 Server.

	Windows 2000 Server	Windows 2000 Advanced Server	Windows 2000 Datacenter Server*
N.º máximo de CPU	4	8	32
Memória máxima	4 GB	8 GB	32 GB
Servidor de ficheiros e impressoras	x	x	x
Internet Information Services (IIS) 5.0	x	x	x
Application Services	x	x	x
Networking and Communications Services	x	x	x
Active Directory	x	x	x
Terminal Services	x	x	x
Suporte Kerberos e PKI	x	x	x
COM+	x	x	x
Failover Clustering		x	x
Balanceamento de rede		x	x
Process Control Manager			x
WinSock Direct			x
Windows Datacenter Program			x

Tabela 3.1 Comparação dos serviços disponibilizados pelas diferentes versões da família Windows 2000 Server.

- **Small Business Server 2000**, ou simplesmente **SBS 2000**, é uma solução para pequenas e médias empresas, concebida para suportar um máximo de 50 clientes, e veio substituir o Small Business Server 4.5.

O Small Business Server 2000 inclui, para além dos serviços do Windows 2000 Server, outros serviços que na versão-base (Windows 2000 Server) têm de ser adquiridos à parte, acarretando custos adicionais. Desses serviços destacamos o servidor de base de dados (SQL Server 2000), o servidor de correio electrónico (Exchange Server 2000), a nova versão de acesso partilhado à Internet através de um *proxy* e *firewall* designado *Microsoft Internet Security and Acceleration Server 2000* (*ISA Server 2000*) – que veio substituir o anterior *Proxy Server* –, a partilha de fax, partilha de *modem* e facilidade na administração, devido à imple-

mentação de uma configuração integrada onde é possível instalar e configurar o sistema operativo, todos os componentes de aplicações e actualizações, entre outros.

Windows Server 2003

Em 24 de Abril de 2003, a Microsoft lançou o Windows Server 2003, que veio substituir o Windows 2000 Server.

O **Windows XP Professional** é a versão para postos de trabalho substituto do Windows 2000 Professional, lançado em 2001. As versões servidoras mantiveram o ambiente gráfico utilizado no Windows XP Professional.

Foram lançadas diversas versões para servidores de rede, das quais passamos a destacar:

- **Windows Server 2003** – versão-base que substituiu o Windows 2000 Server e que se destina a equipar servidores de pequena ou média dimensão. Para uma pequena ou média empresa, com um número da ordem de algumas dezenas de clientes, esta será, normalmente, a versão que melhor se adapta, excepto em situações específicas. Esta versão vai ser utilizada para a instalação do Windows Server 2003, conteúdo a estudar mais à frente.

  A versão 2003 Standard inclui, entre outras características, serviços de partilha de ficheiros e impressoras, validação de utilizadores com o *Active Directory*, partilha de acesso à Internet, *firewall*, serviços para MacOS que equipam os Macintosh, sistema de ficheiros distribuídos (*Distributed File System*), suporte a rede privada virtual VPN (*Virtual Private Network*), serviço de fax, *Intellimirror*, serviços de terminal (*Terminal Services*), *Windows Media Services*, serviços de instalação remota (RIS), linha de comandos do WMI (*Windows Management Instrumentation*) e suporte para *framework*.NET. Esta versão suporta somente processadores a 32 bit da Intel ou compatíveis, 4 processadores para multiprocessamento simétrico e até 4 GB de memória RAM. Não existe versão para os processadores a 64 bit Intel Itanium.
- **Windows Server 2003 Enterprise Edition** – vem ocupar o lugar do Windows 2000 Advanced Server, e mantém as características da versão-base; contém ainda serviços de *clustering*, gestor de recursos de sistema do Windows WSRM (*Windows System Resource Manager*), infra-estrutura de chaves públicas, serviços de certificado e *Smart Cards*. Existem duas versões do Windows Server 2003 Enterprise Edition, uma para servidores com processadores a 32 bit da Intel ou compatíveis, e outra para servidores equipados com os processadores a 64 bit Intel Itanium. Esta última versão suporta até 8 processadores para multiprocessamento simétrico e 64 GB de memória RAM.
- **Windows Server 2003 Datacenter Server** – a versão mais poderosa e mais escalável; aqui também existem duas versões, uma para processadores a 32 bit da Intel ou compatíveis, e outra para os processadores de 64 bit Intel Itanium, que suporta até 64 processadores de multiprocessamento simétrico e 512 GB de memória RAM. O Windows Server 2003 Datacenter Server não inclui serviços de *firewall* e de partilha de acesso à Internet.
- **Windows Server 2003 Web Edition** – a versão mais reduzida a nível de características das versões servidoras do Windows Server 2003. Esta versão destina-se a servidores *Web* e suporta somente processadores a 32 bit da Intel ou compatíveis, 2 processadores para multiprocessamento simétrico e até 2 GB de memória RAM. Não existe versão para os processadores a 64 bit

Intel Itanium. Esta versão é limitada relativamente à versão-base, não inclui serviços de fax, serviços para MacOS que equipam os Macintosh, *Windows Media Services* ou serviço de *Terminal Services*, entre outros.

Para informação mais detalhada, encontra-se na tabela 3.2 uma comparação dos serviços disponibilizados pelas diversas versões da família Windows Server 2003.

Legenda: ■ = Funcionalidade incluída ◪ = Função parcialmente suportada □ = Funcionalidade não incluída

Funcionalidade	Standard Edition	Enterprise Edition	Datacenter Edition	Web Edition
Especificações de *hardware*				
Suporte de 64 bit para computadores baseados em Intel® Itanium™	□	■	■	□
Memória *Hot add* [1,2]	□	■	■	□
NUMA (Acesso Não Uniforme à Memória) [2]	□	■	■	□
Programa *Datacenter*	□	□	■	□
Até 2 GB de RAM	□	□	□	■
Até 4 GB de RAM	■	□	□	□
Até 32 GB de RAM	□	■	□	□
Até 64 GB de RAM [3]	□	◪	■	□
Até 512 GB de RAM [4]	□	□	◪	□
SMP de 2 processadores	□	□	□	■
SMP de 4 processadores	■	□	□	□
SMP de 8 processadores	□	■	□	□
SMP de 32 processadores	□	□	■	□
SMP de 64 processadores	□	□	■	□
Serviços de directório				
Active Directory	■	■	■	◪
Suporte para meta-serviços de directório (MMS)	□	■	■	□
Serviços de segurança				
Internet Connection Firewall	■	■	□	■
Infra-estrutura de chaves públicas, serviços de certificado e *Smart Cards*	◪	■	■	◪

(cont.)

(continuação)

Serviços de terminal				
Ambiente de trabalho remoto para a administração	■	■	■	■
Servidor de terminais	■	■	■	□
Directório de sessões do servidor de terminais	□	■	■	□
Tecnologias de *cluster*				
Balanceamento da carga de rede	■	■	■	■
Serviço de *cluster*	□	■	■	□
Serviços de comunicações e de rede				
Serviços de comunicações e de rede	■	■	■	◪
Internet Authentication Service (IAS)	■	■	■	□
Network Bridge	■	■	■	□
ICS (Partilha da ligação à Internet)	■	■	□	□
IPv6	■	■	■	■
Serviços de ficheiros e de impressão				
DFS (Sistema de ficheiros distribuído)	■	■	■	■
EFS (Sistema de ficheiros encriptado)	■	■	■	■
Restauração de cópias-sombra	■	■	■	■
Armazenamento amovível e remoto	■	■	■	□
Serviço de fax	■	■	■	□
Serviços de gestão				
IntelliMirror	■	■	■	◪
Serviços de gestão	■	■	■	◪
Linha de comandos do WMI (*Windows Management Instrumentation*)	■	■	■	■
Instalação remota do sistema operativo	■	■	■	■
RIS (Serviços de Instalação Remota)	■	■	■	□

(cont.)

(continuação)

WSRM (Gestor de Recursos de Sistema do Windows)	□	■	■	□
Serviços de aplicações .NET				
.NET Framework [1]	■	■	■	■
IIS (Serviços de Informação Internet) 6.0	■	■	■	■
ASP.NET 1	■	■	■	■
Serviços UDDI empresariais	■	■	■	□
Serviços de multimédia				
Windows Media™ Services	■	■	■	□

[1] Não é suportado nas versões de 64 bit do Windows Server 2003.

[2] Pode ser limitado por falta de suporte por *hardware* OEM.

[3] A versão de 32 bit do Datacenter Edition e a versão de 64 bit do Enterprise suportam até 64 GB de RAM.

[4] A versão de 64 bit do Datacenter Edition suporta até 512 GB de RAM.

Tabela 3.2 Comparação dos serviços disponibilizados pelas diferentes versões da família Windows Server 2003.

Existem ainda mais duas versões da família Windows Server 2003, designadas **Small Business Server 2003 Standard** e **Small Business Server 2003 Premium**. Estas duas versões vêm substituir a versão Small Business Server 2000, são aplicadas em servidores de pequenas empresas, para suportar, no máximo, 50 clientes, e mantêm as mesmas características encontradas na versão-base do Windows Server 2003, onde foram adicionados mais alguns serviços que passamos a destacar:

- **Small Business Server 2003 Standard**, ou simplesmente **SBS 2003 Standard** – a versão mais reduzida das versões SBS 2003 e que contém o Windows SharePoint Services, o Exchange Server 2003, o Microsoft Office Outlook 2003, o Microsoft Shared Fax Service, serviços de encaminhamento e acesso remoto (RRAS).
- **Small Business Server 2003 Premium** – contém os serviços da versão-base, com excepção dos serviços de encaminhamento e acesso remoto (RRAS) e inclui o ISA Server 2000, o SQL Server 2000 e o Microsoft Office FrontPage® 2003.

Na tabela 3.3 encontra-se informação mais detalhada sobre as funcionalidades existentes nas duas edições do Windows Small Business Server 2003.

Funcionalidade	Small Business Server 2003 Standard	Small Business Server 2003 Premium
Windows Server 2003	Mantém os serviços disponibilizados pelo Windows Server 2003.	Mantém os serviços disponibilizados pelo Windows Server 2003.
Windows SharePoint Services	Ambiente de comunicações e colaboração entre equipas.	Ambiente de comunicações e colaboração entre equipas.
Exchange Server 2003	Servidor de correio electrónico e colaboração. Microsoft Outlook® Web Access serve para aceder a correio electrónico pela *Web*.	Servidor de correio electrónico e colaboração. Microsoft Outlook® Web Access serve para aceder a correio electrónico pela *Web*.
Microsoft Office Outlook 2003	Um local central que serve de cliente de correio electrónico, calendários, contactos e outras informações pessoais e de grupo.	Um local central que serve de cliente de correio electrónico, calendários, contactos e outras informações pessoais e de grupo.
Microsoft Shared Fax Service	Serviço de partilha de envio e recepção de faxes. Recepção de faxes através do SharePoint, correio electrónico ou impressora.	Serviço de partilha de envio e recepção de faxes. Recepção de faxes através do SharePoint, correio electrónico ou impressora.
Serviços de encaminhamento e acesso remoto (RRAS)	Tecnologia para ajudar a proteger as ligações à Internet.	Excluído.
ISA Server 2000 (Internet Security Acceleration Server)	Excluído.	Serviços de *firewall* (protecção de ligações à Internet) e *cache web*.
SQL Server 2000	Excluído.	Serviço de base de dados relacionais.
Microsoft Office FrontPage® 2003	Excluído.	Ferramentas para o desenvolvimento de *websites* ou a criação de soluções personalizadas para o Windows SharePoint Services.

Tabela 3.3 Comparação de funcionalidades do Small Business Server 2003 Standard e Premium.

Para terminar esta abordagem sobre as características e as funcionalidades das várias versões do Windows NT, 2000 e 2003, podem-se observar, na figura 3.2, as datas desde o início do projecto Windows NT até ao Windows Server 2003, e, na tabela 3.4, uma lista de versões lançadas do Windows NT, 2000 e 2003.

Fig. 3.2 Datas de lançamento das versões servidoras da Microsoft

	Versão 3.1	Versão 3.5	Versão 3.51	Versão 4.0	Versão 2000	Versão 2003
Versão para postos de trabalho	Windows NT 3.1 Workstation	Windows NT 3.5 Workstation	Windows NT 3.51 Workstation	Windows NT 4.0 Workstation	Windows 2000 Professional	Windows XP Home Edition e Professional
		Windows NT 3.5 Server	Windows NT 3.51 Server	Windows NT 4.0 Server	Windows 2000 Server	Windows Server 2003 Standard Edition
	Windows NT 3.1 Advanced Server	Windows NT 3.5 Server Enterprise Edition	Windows NT 3.51 Server Enterprise Edition	Windows NT 4.0 Server Enterprise Edition	Windows 2000 Advanced Server	Windows Server 2003 Enterprise Edition 32 bit e 64 bit
					Windows 2000 Datacenter Server	Windows Server 2003 Datacenter Edition
Versões para servidores				Small Business Server 4.5	Small Business Server 2000	Small Business Server 2003 Standard Small Business Server 2003 Premium
				Windows NT Server 4.0 Terminal Server Edition		
						Windows Server 2003 Web Edition

Tabela 3.4 Versões lançadas do Windows NT, 2000 e 2003.

1.2. Objectivos do Windows Server

Introdução

A Microsoft pretendia, com o Windows NT, atingir um conjunto tão ambicioso de objectivos que a equipa, liderada por Dave Cutler, viu-se forçada a adiar por várias vezes o lançamento do produto, pela complexidade da tarefa. Na brincadeira, a concorrência chegou mesmo a "traduzir" a sigla NT por *Nice Try* ou *Not There*, significando 'boa tentativa' ou 'inexistente'.

Vamos analisar os principais objectivos que se pretendiam atingir com o Windows NT, que serviu de base ao Windows 2000 Server e ao Windows Server 2003.

Compatibilidade

O Windows NT já vinha de base com suporte para vários ambientes de rede, contava também com suporte para diversos tipos de aplicações (ex.: MS-DOS, Windows 3.x, OS/2 1.x e POSIX) e até já integrava suporte para dois tipos de formatação importantes: **FAT** – que era usada pelo DOS (da Microsoft) e pelo HPFS no OS/2 (da IBM) – e **NTFS**. Tanto o Windows 2000 como o Windows Server 2003 utilizam ainda suporte para FAT32 e NTFS versão 5.

Escalabilidade

É possível fazer-se multiprocessamento simétrico, beneficiando de computadores com vários processadores, através das diversas versões do Windows Server ou das versões para postos de trabalho (Windows 2000 Professional e Windows XP Professional). O Windows Server 2003 Standard Edition, por exemplo, pode tirar partido de computadores com até quatro processadores, a versão Advanced Server pode chegar aos oito processadores; a versão Datacenter Server para processadores 32 bit da Intel ou compatíveis suporta até trinta e dois processadores, enquanto que a versão para processadores de 64 bit Intel Itanium suporta até sessenta e quatro processadores de multiprocessamento simétrico, mas, por outro lado, a versão Web Edition já só inclui suporte para dois processadores. Estes números reduzem-se significativamente quando se analisam as versões pessoais, como o Windows NT Workstation, o Windows 2000 Professional ou o Windows XP Professional, que apenas suportam até dois processadores. As versões do Windows para o mercado doméstico, casos do Windows 95, 98, Me e XP Home Edition, têm suporte para apenas um processador e ignoram quaisquer outros que possam existir.

Deste modo, a escalabilidade do Windows Server 2003 torna-se vantajosa, no sentido de permitir a uma empresa crescer ao seu ritmo, podendo fazer actualizações no servidor de rede sempre que precisar, sem ter de mudar o sistema operativo do servidor.

Segurança

Desde o início que a segurança foi uma prioridade. A segurança, tanto do Windows Server 2003 como do sistema de ficheiros NTFS (*NT File System*), obedece à norma de segurança C-2 definida pelo NCSC (*National Computer Security Council*), uma divisão da Agência Nacional de Segurança dos Estados Unidos. Este nível de segurança, implementada por *software* no Windows Server 2003, permite, por exemplo:

- limitar o acesso a um determinado documento;
- fazer a auditoria de acontecimentos (saber quando e que utilizadores fizeram *login*, quem acedeu a um determinado ficheiro, etc.);
- identificar e autenticar os utilizadores (através de um nome (*login*) e de uma *password*);
- evitar que determinados conteúdos ou ficheiros criados por um utilizador ou por um processo e posteriormente libertados, ou seja, apagados, sejam reutilizados por outros utilizadores ou processos.

Alguns dos processos do Windows Server 2003 não só estão de acordo com a norma C-2, como, inclusivamente, obedecem à norma B-2, que ainda é mais restritiva. Além de se seguirem todas estas normas de segurança, deve ainda existir uma *password* de acesso ao servidor e, para a segurança ser considerada total, o servidor deve encontrar-se num local inacessível a estranhos e ter as unidades de disquetes desactivadas; a informação nos discos dos PC deve ser guardada no servidor e devem, regularmente, ser feitos *backups* das informações guardadas.

Processamento distribuído

É possível integrar em rede servidores Windows Server 2003 com muitos outros servidores diferentes. Para além de ter um suporte para rede ao nível do sistema operativo, o Windows Server 2003 também assegura algumas funcionalidades de rede, como *Named Pipes*, *Remote Procedure Calls* (RPC) e *Windows Sockets*.

Vejamos um exemplo: se for realizado um pedido de processamento a um determinado servidor, ele poderá ser reencaminhado para outro que esteja com mais disponibilidade; assim, as cargas são distribuídas pelos servidores, diminuindo o tempo de processamento global.

Robustez

A arquitectura robusta do Windows Server 2003 evita que, sempre que uma determinada aplicação bloquear, as outras aplicações bloqueiem. Isto deve-se ao facto de existirem áreas de memória protegidas para as aplicações.

Fiabilidade

O Windows Server 2003 é considerado um sistema operativo seguro, na medida em que, muito raramente, problemas de *hardware* podem ser a causa de perdas irrecuperáveis de dados, devido aos seus diversos mecanismos de salvaguarda dos mesmos.

Extensibilidade

O Windows Server 2003, pela sua forma modular, permite acrescentar, de um modo bastante simples, serviços (módulos) ao sistema operativo, tornando-o assim muito mais flexível.

Portabilidade

Os primeiros sistemas operativos do Windows NT corriam em computadores com processadores Alpha e Intel de 32 bit. O Windows 2000 e o Windows Server 2003 só correm em processadores da família Intel e compatíveis, embora algumas versões especiais de Windows Server 2003 suportem apenas os novos processadores Itanium de 64 bit da Intel.

1.3. Características técnicas do Windows Server 2003

Introdução

Servindo-se das características técnicas do Windows NT 4.0, o Windows Server 2003 consegue integrar as mais recentes tecnologias. A existência de uma HAL (*Hardware Abstraction Layer* – camada de abstracção do *hardware*) facilita o porte do Windows Server 2003 para outros ambientes, visto o *hardware* ser apenas acedido a partir do núcleo (*kernel*) do sistema operativo, de alguns tipos de *device drivers* e da HAL.

Vejamos mais algumas características do Windows Server 2003.

Arquitectura cliente/servidor

Não é fácil resumir em poucas linhas tudo o que há a dizer sobre arquitecturas cliente/servidor. Podemos, muito resumidamente, definir um sistema cliente/servidor como aquele em que há um ou mais computadores (servidores) responsáveis por satisfazer pedidos dos clientes. Vejamos um exemplo: um servidor com o

Windows Server 2003 tem uma base de dados de SQL Server e pretende-se realizar uma pesquisa à dita base de dados. Acontece que o cliente faz o pedido e a pesquisa é realizada pelo servidor; o resultado é transmitido ao cliente que fez o pedido.

Multitarefa (*multitasking*) ou multiprocessamento (*multiprocessing*)

Multitarefa é uma tecnologia que permite a um sistema operativo executar mais do que uma tarefa em simultâneo, no mesmo sistema. O número de aplicações que um sistema operativo pode correr simultaneamente e a performance do sistema quando as está a correr depende da quantidade de memória do sistema.

Multiprocessamento é uma tecnologia que permite a um sistema operativo usar múltiplos processadores em simultâneo, para melhorar a performance e reduzir o tempo de processamento.

No caso do Windows Server 2003, este consegue gerir vários processadores em simultâneo e, quando apenas existe um processador, o sistema operativo Windows Server 2003 consegue controlar a gestão dos programas que estão a ser utilizados, definindo prioridades.

Multithreading

Este termo refere a capacidade de uma tarefa, que se encontra em execução, dar origem a uma subtarefa, que, por sua vez, irá disputar tempo de processador com as restantes tarefas em execução no sistema, ou seja, a subtarefa lançada permite à tarefa principal continuar, evitando deste modo tempo de espera. Com o uso de *threads*, aplicações servidoras podem responder em simultâneo a pedidos de diversos clientes, evitando que pedidos mais imediatos tenham de esperar pela resposta a outros pedidos mais demorados, o que, no caso de servidores de rede, como o Windows Server 2003, é bastante importante.

Segurança da informação

Como já vimos, é possível atribuir permissões no acesso a ficheiros, controlando, deste modo, o acesso à informação contida nos mesmos. Também já mencionámos o facto de problemas no *hardware* não significarem, necessariamente, perda de informação, desde que haja ferramentas de cópias de segurança (*backup*) realizadas periodicamente. Felizmente, tanto o Windows Server 2003 como o Windows XP Professional incluem essas ferramentas, e não só. O Windows Server 2003 conta também com um suporte para RAID (*Redundant Array of Independent Disks* – conjunto redundante de discos independentes).

O Windows Server 2003 inclui suporte a vários sistemas de RAID. Aqui destacamos o *Disk Mirroring* (RAID 1), em que os dados armazenados num disco são copiados para um segundo disco, que se torna uma réplica exacta do primeiro, ou seja, o segundo disco é um espelho do primeiro. Apesar de se desperdiçar 50% de espaço em termos de disco, é muito útil quando surge um defeito num disco ou haja necessidade de se trocar os discos por outros de maior capacidade. Para a implementação deste tipo de RAID são necessários, pelo menos, dois discos rígidos.

Tentando minorar este desperdício de utilização de espaço, o Windows Server 2003 inclui, também contido já no próprio *software* do sistema operativo, algo chamado suporte para o *Disk Stripping* com Paridade (RAID 5), em que existe uma

determinada quantidade de discos (no mínimo três) e um dos discos contém informação de paridade relativamente aos restantes, desperdiçando, assim, menos espaço quando comparado à utilização do *Disk Mirroring*. É possível implementar estes dois tipos de RAID, tanto por meio de utilização de *software* como por *hardware*. O Windows NT Server, o 2000 Server e o Server 2003 implementam estes sistemas de RAID por *software*, com a vantagem a nível de custos, dado que só é necessário adquirir dois discos rígidos. Esta solução, apesar de ser financeiramente mais acessível relativamente à implementação por *hardware*, tem a desvantagem de ser mais lenta e de não se poder trocar um disco danificado por um novo sem ter de desligar o servidor.

Para além destes sistemas de RAID, existem outros que serão analisados mais à frente, no ponto 4 (Segurança do Windows Server 2003 – Segurança de discos), mas apenas estes são tolerantes a falhas (*fault-tolerant*).

Ambiente de trabalho

A versão Windows NT Server 4.0 adoptou uma interface gráfica próxima da utilizada no Windows 95, enquanto que o Windows 2000 e o Windows Me contavam com uma versão melhorada a nível gráfico da interface utilizada pelo Windows 98. No caso do Windows Server 2003, a interface adoptada baseou-se na do Windows XP, embora conte com algumas pequenas diferenças, nomeadamente no **Painel de controlo** ou mesmo no modo de dispor e arrumar as diversas ferramentas.

1.4. Novas características e componentes do Windows Server 2003

Introdução

Neste ponto pretende-se fazer uma breve abordagem de alguns dos mais importantes termos e tecnologias adoptados no Windows Server 2003 e que não foram mencionados no ponto anterior.

Active Directory (AD)

O *Active Directory* é uma das grandes novidades no Windows 2000 e no 2003, quando comparado com o Windows NT, alterando radicalmente tudo o que se refere à administração e gestão de rede. O *Active Directory* é uma espécie de arquivo de informação do sistema e respectivos serviços de acesso, ou seja, uma base de dados de toda a informação que possa dizer respeito à comunicação ou administração, a utilizadores ou aos seus direitos, a grupos (ou *group policies*), a permissões, a domínios, a *sites*, a diversas aplicações e a muitas outras informações que se queiram acrescentar. O *Active Directory* suporta protocolos de autenticação, como o *Kerberor* 5, o *Securs*, o *Sockets Layer* 3 (SS2) e o certificador X.509.

A um servidor que esteja a utilizar o Windows 2000 Server ou o Windows Server 2003 com o *Active Directory* dá-se o nome de *Domain Controller* – **Controlador de domínio.**

No Windows NT Server só era possível promover e despromover o *Domain Controller*, ou até mesmo ser transferido do domínio onde tem funções de controlador de domínio, caso fosse reinstalado novamente o sistema operativo. No Windows

2000 Server e no Windows Server 2003 esta situação foi alterada e deixaram de ser necessárias mais reinstalações do sistema operativo para realizar estas tarefas.

Alguns controladores de domínio têm, entre outras funções, de autenticar o *Logon* no sistema por parte dos utilizadores e serviços.

Um facto importante no que concerne ao *Active Directory* é a possibilidade de se configurar a replicação entre *Domain Controller*, com base na noção de *site*, sendo a informação replicada com maior simplicidade e transparência, facilitando a criação e a manutenção de WAN, que no Windows NT eram difíceis de gerir.

Sistemas de ficheiros distribuídos (DFS – *Distributed File System*)

Muitas vezes, um servidor não é mais do que um servidor de ficheiros que podem ser acedidos por vários utilizadores: colocam-se os ficheiros num conjunto de pastas (*folders*) que, após o processo de partilha, podem ser acedidos localmente, tendo em atenção algumas questões, como permissões de acesso, métodos de acesso, especificações das operações, etc.

O DFS foi integrado, pela primeira vez, no sistema operativo no Windows 2000 Server e, recentemente, no Windows Server 2003. No Windows NT 4.0, o DFS foi adicionado com o lançamento do *Service Pack 3*.

Esta tecnologia é, basicamente, um serviço de partilha de recursos parecido com os *shares* tradicionais, mas mais eficaz, isto é, as pastas partilhadas não estão num único servidor específico. Na prática, pode ocorrer que, ao gravar um ficheiro, ele seja copiado para outras pastas de outros servidores, aumentando assim a redundância do sistema; caso falhe um servidor, é possível gravar o ficheiro ou ir lê-lo, visto que ele será copiado ou lido de outro servidor. Outra vantagem deste sistema reside no facto de, caso exista excesso de carga num servidor, o ficheiro que se pretende gravar ou ler poder ser gravado ou lido noutro servidor, libertando o servidor com carga em excesso.

Apesar do aumento de desempenho, existe a desvantagem da necessidade de redireccionar a ligação das partilhas em todos os servidores, pois parte dos ficheiros são movidos para os novos servidores, aumentando a complexidade na gestão deste sistema.

Versão 5 da NTFS

Esta versão melhorada do formato NTFS representa a melhor alternativa ao sistema FAT. A versão 5 da NTFS permite, ao Windows 2000 Server e ao Windows Server 2003, controlar e limitar o espaço em disco ocupado por cada utilizador e indexar o conteúdo dos discos (melhorando pesquisas de ficheiros e de conteúdos). Além disso, tornou-se possível encriptar ficheiros automaticamente, barrando o seu acesso a quaisquer elementos estranhos.

IntelliMirror

Não é fácil explicar o que significa IntelliMirror. Talvez a melhor forma de o fazer seja entender o IntelliMirror como designando um grupo de elementos que são factores fundamentais na diminuição do custo total de propriedade (TCO) da qual fazem parte. Falamos de *Windows Installer*, *Remote Install*, *Offline Folders*, *Group Policies* e *Roaming User Profiles*.

Serviços de terminal (*Terminal services*)

Estes serviços permitem-nos (através da utilização de um computador e de uma simples *workstation*) correr programas num servidor remotamente, como se estivéssemos em frente ao mesmo. Este conceito de trabalho já se encontrava incluído no Windows 2000 Server como componente opcional. O servidor que corre o *Terminal services* aceita ligações feitas através de um cliente de terminal, que, depois de estabelecer a ligação inicial (sobre TCP/IP), inicia uma sessão que corre totalmente no servidor, tal como se o utilizador estivesse a usar o teclado e o rato daquele computador. No fundo, trata-se de uma recuperação da filosofia dos *mainframes* e dos primeiros sistemas **Unix**, em que um servidor central com altas capacidades de processamento servia terminais sem essa mesma capacidade.

Este serviço é muito útil na implementação de trabalho remoto, onde a largura de banda disponibilizada entre o servidor e o posto de trabalho é reduzida. Deste modo, todo o processamento é realizado no servidor, o posto de trabalho envia os comandos do teclado e do rato e recebe no ecrã o resultado do que se passa nessa secção do servidor. Outra implementação deste tipo de serviço surge em redes em que os postos de trabalho tenham pouco poder de processamento ou se queira reutilizar postos de trabalho mais antigos (com pouco poder de processamento) e que consigam correr aplicações mais recentes. Isto é possível se as aplicações correrem num servidor ou num conjunto de servidores de modo a libertarem os postos de trabalho do processamento mais pesado. Nesta solução, a manutenção será feita no servidor, facilitando a manutenção dos postos de trabalho. A grande desvantagem deve-se à necessidade de se ter um servidor ou conjunto de servidores que suportem este acréscimo de processamento.

Consola de gestão da Microsoft – MMC (*Microsoft Management Console*)

Ao utilizar o Windows 2000 Server e o Windows Server 2003 verificamos que, quando comparadas ao Windows NT, as ferramentas de administração não só são bastante diferentes, como passaram a ser acedidas através da MMC, que mais não é do que uma consola de administração. A MMC permite aos administradores escolherem os grupos de ferramentas que mais se adequam às suas necessidades.

Plug and Play

A norma *Plug and Play* é uma das tecnologias suportadas pelo Windows 2000 Server e melhorada no Windows Server 2003 que reconhece e configura automaticamente os dispositivos (ex.: *hardware*) compatíveis com a norma, tornando-se desnecessário o moroso processo de configuração manual (que tinha de ser feito com o Windows NT).

DNS Dinâmico (DDNS – *Dynamic Domain Name System*)

O serviço DNS/DDNS tem como objectivo básico traduzir nomes para endereços IP. Ao contrário dos tradicionais servidores DNS (*Domain Name System*), onde é necessário realizar manualmente o registo dos nomes dos domínios e os respectivos endereços IP, o Windows 2000 Server e o Windows Server 2003 têm um DNS com um "D" a mais, um "D" de dinâmico, que faz o registo automaticamente e evita longos e cansativos trabalhos de configuração, visto que cada cliente, por si, pode registar-se no servidor DNS (desde que seja um cliente que suporta registos dinâmicos).

Comando *Runas*

Normalmente, cada utilizador pode ligar-se em vários computadores ou em todos os computadores da rede. No entanto, visto nem todos os utilizadores terem os mesmos direitos de acesso e devido às políticas de segurança, tornava-se necessário um *logoff* do utilizador, sempre que este não tinha direitos de acesso a uma determinada estação, e um *logon* do utilizador que tinha esses direitos.

Com o Windows Server 2003 isto torna-se desnecessário, pois este sistema operativo já conta com o comando *Runas* (se tivermos em atenção o som do comando "*run [us]*", verificamos que significa "corre-nos"). Ao accionar/correr este comando, um utilizador com mais direitos de acesso (digamos, um utilizador de nível superior) pode executar programas em computadores onde esteja "logado" um utilizador corrente, sem ser necessário aplicar o *logoff* do utilizador corrente, ou mesmo o *logon* do utilizador com os direitos de acesso.

1.5. Terminologia de redes da Microsoft

A Microsoft, ao implementar o *Active Directory* (AD) no Windows 2000 Server, veio alterar a terminologia adoptada até então para redes. O Windows Server 2003 manteve estas novas nomenclaturas. Vamos abordar algumas das novas terminologias adoptadas pela Microsoft para redes.

Grupos de trabalho (*Workgroups*)

A Microsoft lançou o **Windows for Workgroups** (versões 3.1 e 3.11) com a intenção de permitir, mesmo a uma empresa de menores dimensões, uma ligação em rede sem a necessidade de adquirir qualquer *hardware* e *software* extra. Ou seja, este produto tornava possível que qualquer posto de trabalho pudesse ser usado, simultaneamente, como mini-servidor, permitindo a partilha de pastas e impressoras por todos os utilizadores ligados em rede. A este tipo de rede sem um servidor dá-se o nome de ponto a ponto (*peer-to-peer*) e o termo usado pela Microsoft é *workgroup*.

Domínio

O primeiro servidor que funciona como *Domain Controller* (DC) é a parte dominante do domínio. Um domínio surge logo após a instalação do primeiro servidor DC. Dependentes do servidor DC (que manterá o *Active Directory*) podem adicionar-se outros servidores e *workstations*, definir-se utilizadores e grupos, proceder à validação dos utilizadores, instalar periféricos, etc. Assim, domínio pode também ser descrito como um conjunto de redes em que existe um servidor responsável pela segurança da rede, relativa à validação das contas dos utilizadores, ou seja, a certificação de que um determinado utilizador é mesmo quem diz ser. Esta validação é feita através de um processo de identificação, que passa pela necessidade da utilização de uma *password*, associada ao nome do utilizador. No caso do Windows Server 2003, o nome de domínio não pode ser apenas uma única palavra ou um nome NetBIOS, terá de ser uma entrada DNS. Imaginemos que a empresa ESCOLA escolhe "escola" como nome do domínio; este passaria a ser **escola.com** ou **escola.pt** ou **escola**. qualquer outra terminação de DNS. Normalmente, uma rede com um só domínio é apenas instalada em empresas pequenas e/ou simples. Empresas com maiores dimensões tendem a utilizar redes com mais de um domínio, ou seja, uma árvore (ou floresta).

Domain Controller (DC), *Standalone Server* e *Member Server*

Pode dizer-se que, tanto o *Domain Controller*, como o *Standalone Server* ou o *Member Server*, são nomes atribuídos pela Microsoft a três tipos de servidores de rede.

Uma rede do tipo domínio precisa de, pelo menos, um servidor, o ***Domain Controller***, ou seja, o controlador de domínio – que contém o directório do sistema (ver *Active Directory*, no ponto 1.4). Qualquer rede que não tenha, no mínimo, um *Domain Controller* será, como ainda nos lembramos, um grupo de trabalho ou *workgroup*.

O DC, para além de controlar a segurança dentro de um domínio, como, por exemplo, validando contas de utilizadores, ou seja, proceder à autenticação dos utilizadores em rede, faz também o que um *Standalone Server* ou um *Member Server* fazem.

Se os servidores estiverem integrados num domínio já existente, então pode dizer-se que são ***Member Servers***, isto é, são servidores que, não sendo controladores de domínio, são apenas membros do domínio. Como tal, reconhecem os seus utilizadores, grupos e recursos, são capazes de partilhar os próprios recursos (sistema de correio electrónico, impressoras, ficheiros, etc.) com os utilizadores e ainda têm acesso ao directório, mas não validam os *logons* dos utilizadores, nem dão informação sobre o domínio.

Um ***Standalone Server***, como o próprio nome indica, é um servidor que "está sozinho" – *stand alone*, ou seja, é um computador que corre o Windows 2000 Server ou o Windows Server 2003 e, como tal, pode aderir a um grupo de trabalho ou até mesmo criar um, mas não faz parte de um domínio.

Assim sendo, um servidor Windows Server 2003, sem o *Active Directory*, pode ser um *Member Server*, se pertencer a algum domínio, ou um *Standalone Server*, caso pertença a um grupo de trabalho.

Estações de trabalho (*Workstations*)

Normalmente, uma rede é constituída por vários postos de trabalho ligados entre si ou a um servidor. Chamamos posto ou estação de trabalho ao computador que é usado por alguém para trabalhar (*in loco*).

Servidores

Basicamente, um servidor é um computador que disponibiliza serviços numa rede, como, por exemplo: a partilha de impressoras, a disponibilização de espaço em disco ou a validação de utilizadores. O Windows Server 2003 oferece, para além dos mencionados, servidores de bases de dados, como o **SQL Server** ou o **Oracle**, serviço de correio electrónico, como o **Exchange Server**, serviço *World Wide Web* (WWW), como o ***Internet Information Services Web*** (IIS) ou o **APACHE**, entre outros.

Caso se queira proceder à identificação do papel dos servidores, basta ir a **Meus locais na rede** (*My Network Places*), no Windows 2000 Server e no Windows Server 2003, clicar com o botão direito sobre um computador, seleccionar **Propriedades** (*Properties*) no menu e fazer a verificação na respectiva janela.

Dependendo do sistema operativo e do *software* servidor de rede utilizados num computador-servidor, este pode ser, ou não, o que se chama 'dedicado'. Um servidor dedicado é aquele com o qual podemos trabalhar de modo interactivo, ou seja, utilizá-lo não só como servidor, mas também, simultaneamente, como

cliente. Um exemplo de um servidor dedicado pode ser a Novell NetWare 3.12 (e versões seguintes), visto o Windows Server 2003 estar optimizado para servidor de rede e, como tal, não implementar servidores dedicados (podendo, no entanto, ser usado como posto de trabalho). Sendo assim, não convém instalar este sistema operativo num computador-servidor que será usado como posto ou estação de trabalho; nestes casos é preferível instalar o Windows XP Professional.

Unidades organizacionais (*Organizational units*)

A utilização de unidades organizacionais permite dividir um domínio em várias unidades, estas em vários níveis, ou seja, uma *Organizational unit* pode conter outras *Organizational units*. Podemos definir, para cada uma das *Organizational units* criadas, políticas de grupo e esquemas de segurança, facilitando, deste modo, a administração e a delegação de poderes.

Árvores (*Trees*)

Reparemos na figura:

Fig. 3.3 Esquema de implementação de uma árvore composta por quatro domínios. Neste exemplo existe um domínio de topo, que interliga todos os domínios; pode ser possível partilhar recursos entre os utilizadores dos quatro domínios.

Tal como foi já mencionado, organizações com maiores dimensões e, principalmente, se geograficamente distribuídas, necessitam, normalmente, de uma planificação mais estruturada e organizada, que é mais facilmente obtida através de um conjunto de domínios hierarquizados em árvore, a partir de um domínio de raiz, ou seja, de topo. Assim sendo, uma árvore é um conjunto de um ou mais domínios de um *site*. Torna-se, então, necessário criar um domínio de raiz (um DC – *Domain Controller*), como, por exemplo, **escola.com**, para se poder criar uma árvore (que partilha um AC) com domínios-filhos ou 'ramificações', que, no caso do exemplo, poderiam ser **aveiro.escola.com**, **sjm.escola.com** e **porto.escola.com**. Cada domínio pode ser visto como uma entidade administrativa, mas é possível gerir, desde que autorizado, o domínio de raiz e fazer com que as modificações aí efectuadas se reflictam também nas ramificações desse domínio. Deste modo, pode dizer-se que, numa árvore, todas as "ramificações" constituintes dessa árvore (domínios) estão interligadas de modo bidireccional, sendo que cada domínio dá acesso aos seus recursos a cada um dos outros. A árvore ainda pode ser mais complexa, em que cada subdomínio poderá, por sua vez, ter domínios-filhos, como, por exemplo, **norte.aveiro.escola.com** e **sul.aveiro.escola.com**.

Obrigatoriamente, o domínio de topo tem de ser o primeiro a ser instalado.

Florestas (*Forests*)

Como facilmente se pode deduzir, as florestas são sistemas de múltiplos domínios, consistindo numa partilha de recursos. Uma floresta é, assim, por defi-

nição, um conjunto de árvores associadas, cada uma delas com o seu domínio de raiz, com um nome diferente dos usados nas outras árvores da floresta. Isto não significa que entre as várias árvores exista automaticamente uma relação de confiança bidireccional, embora seja possível obtê-la manualmente, caso se configure o primeiro DC do domínio **ministerio.com** de modo a aderir à floresta existente que inclui o domínio **escola.com** servidor. Assim, é possível estabelecer uma ligação entre **ministerio.com** e **escola.com** e partilhar recursos entre os domínios da mesma árvore. Neste caso, temos uma floresta constituída por duas árvores (ver figura 3.4). Na prática, esta situação pode ocorrer quando duas organizações se fundem, por exemplo, na compra de uma empresa por outra, e em que haja necessidade de partilhar recursos entre as duas florestas, formando uma única floresta.

Caso não se faça a adesão do primeiro DC do domínio **ministerio.com** à floresta existente que contém o domínio **escola.com** (ver figura 3.4), temos duas florestas e duas árvores.

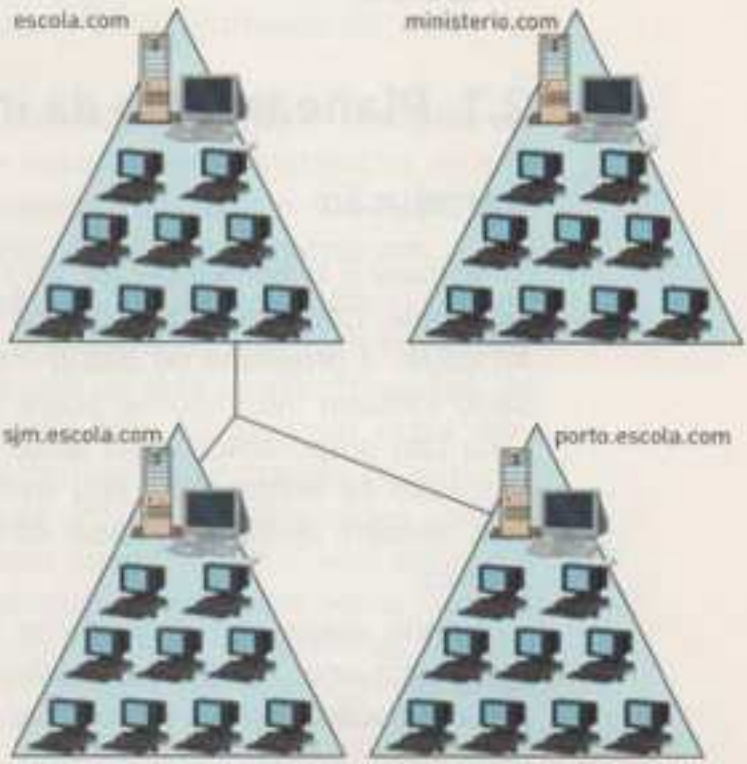

Fig. 3.4 Esquema de uma floresta formada por duas árvores, caso haja inserção da floresta que contém o domínio **ministerio.com** na floresta que contém o domínio **escola.com**. Caso não haja esta inserção, estamos perante duas florestas e duas árvores.

Utilizadores e respectivas contas (contas de acesso)

Podemos controlar o acesso a um recurso por meio de uma *password* ou, então, por meio de predefinição de regras de identificação para cada utilizador.

No Windows 2000 Server e no Windows Server 2003, a segurança obriga à existência de contas de utilizador. Um utilizador, ao aceder ao sistema, tem de o fazer através de uma conta. Cada conta inclui um nome do utilizador, uma palavra-chave (*password*) e diversos atributos definidos pelo sistema.

Grupos de utilizadores

Ao criar um grupo de utilizadores, o que se pretende é juntar certos utilizadores num grupo, para assim poder configurar, de uma só vez, opções que dizem respeito a todos os utilizadores desse grupo. Deste modo, um grupo de utilizadores pode conter muitos utilizadores. No entanto, isto não significa que, a partir do momento em que um utilizador pertence a um grupo, não pode pertencer a mais nenhum. Pelo contrário, um utilizador pode pertencer a vários grupos de utilizadores.

Devem criar-se grupos de utilizadores de acordo com a utilização que se pretende que venham a ter, como, por exemplo, agrupar utilizadores que pertencem a uma determinada secção numa organização. Por fim, se uma organização assim o entender, pode ainda dividir os grupos de utilizadores em vários tipos, como, por exemplo: grupo de utilizadores da contabilidade; grupo de utilizadores dos serviços administrativos; grupo de utilizadores do Porto, etc.

2. Instalação e configuração do Windows Server 2003

2.1. Planeamento da instalação

Introdução

Instalar o Windows Server 2003 requer alguma preparação, devido à sua complexidade. Complexidade significa opções, e opções necessitam de planeamento. Ao correr o programa de *setup* (configuração) do Windows Server 2003, é necessário fornecer informações sobre como instalar e configurar o sistema operativo. Uma boa preparação prévia ajuda a evitar alguns problemas e dúvidas durante o processo de instalação. Uma compreensão das opções de configuração disponíveis também ajuda a certificar se temos um sistema operativo devidamente configurado.

Sendo assim, antes de iniciar a instalação, deve-se verificar se temos tudo o que precisamos, através da elaboração de uma *checklist* (lista de verificação) de pré-instalação, como o exemplo que se segue.

	Lista de verificação de pré-instalação
✓	Fazer *backups* (cópias de segurança) dos dados – caso se planeie instalar o servidor num computador que já tenha ficheiros com dados.
✓	Determinar qual o sistema operativo a instalar.
✓	Verificar se o *hardware* vai de encontro aos requisitos mínimos necessários.
✓	Identificar os requisitos recomendados pelo sistema operativo.
✓	Verificar se o *hardware* é suportado / compatível – ver se consta da lista HCL.
✓	Verificar o espaço disponível no disco rígido (2 GB ou mais).
✓	Determinar as opções de partição de disco.
✓	Seleccionar o sistema de ficheiro para a partição do Windows Server 2003 – formatar a partição com NTFS, a não ser que se necessite de uma configuração *dual boot*.
✓	Seleccionar o modo de licenciamento para o Windows Server 2003 (*Per Server* ou *Per Seat*).
✓	Determinar se o servidor vai ficar a funcionar como novo *Domain Controller* DC, ou como *Domain Controller* pertencente a um domínio já existente, ou como nova árvore em floresta existente, ou como *Member Server* (juntar-nos a um domínio já existente), ou como *Standalone Server* (juntar-nos a um grupo de trabalho já existente).
✓	Determinar nome de domínio ou de grupo de trabalho (*workgroup*).
✓	Criar *password* para a conta do administrador do sistema operativo.
✓	Criar *password* da conta do administrador do domínio.

Tabela 3.5 Lista de verificação de pré-instalação

Modos de instalação

Nas versões servidoras Windows Server 2003 e Windows 2000 Server, bem como nas versões de posto de trabalho Windows 2000 Professional e XP, os modos de instalação podem-se subdividir em dois:

- **Instalação assistida por computador** (não automática), onde o operador vai respondendo às questões colocadas pelo assistente de instalação do sistema operativo. Esta opção é a tradicionalmente utilizada e é interessante quando temos de instalar um número reduzido de sistemas operativos;
- **Instalação não assistida (*unattended install*)** (instalação automática) é, simplesmente, um método de providenciar as respostas às questões colocadas durante o processo de instalação, antes mesmo de elas serem colocadas, de modo a automatizar o processo de instalação. Não há qualquer outra diferença na instalação propriamente dita. Mas porque necessitamos de automatizar? Normalmente, a automatização é mais útil em grandes redes onde é frequentemente necessário instalar o sistema operativo em muitos computadores. Ao automatizar estas instalações poupam-se inúmeras horas que, de outro modo, seriam gastas em frente à consola. Outro benefício de instalações não assistidas é que estas podem ser corridas por pessoas não especializadas neste tipo de tarefa.

A Microsoft providencia três ferramentas diferentes para tornar possíveis as instalações não assistidas:

- **usar Sysprep** (*using Sysprep*);
- **instalações por *script*** (*scripting installations*);
- **usar serviços de instalação remota** (*using remote installation services*).

Sysprep – é uma ferramenta criada para implantar em múltiplos computadores o Windows Server 2003, o Windows 2000 Server, o Windows 2000 Professional e o XP.

Muitas empresas preferem criar primeiro um computador que se parece exactamente com aquilo que eles querem que todos os seus computadores pareçam. Depois criam centenas de duplicados exactos daquele computador protótipo, "clonando" o disco duro do protótipo, e criando, rapidamente, com este processo, centenas de computadores *desktop* ou servidores prontos-a-trabalhar. Isto consegue-se usando uma ferramenta chamada **Sysprep**.

Normalmente, instala-se o sistema operativo, com as configurações pretendidas, no disco rígido de um computador – que vamos designar por "mestre". Com auxílio do **setupmgr.exe** que acompanha o **Sysprep**, definem-se quais os parâmetros que serão predefinidos e quais os que terão de se introduzir; estas configurações são guardadas num ficheiro de texto. O **Sysprep** vai associar o ficheiro de texto criado à instalação do sistema operativo já realizada e, depois, terá de se desligar o computador. O disco será duplicado com o auxílio de um programa adequado para o efeito, como, por exemplo, o **Ghost** ou o **Partimage**. A "imagem-mestra" criada é utilizada para ser instalada nos outros computadores. Logo no primeiro arranque do sistema operativo, após a instalação da imagem, será

Fig. 3.5 Aspecto geral do arranque do **setupmgr.exe**

necessário responder apenas a algumas questões previamente seleccionadas, facilitando grandemente todo o processo de instalação. O **Sysprep** encontra-se na directoria **\support\tools** e é necessário extraí-lo do ficheiro **deploy.cab**.

Fig. 3.6 Criar novo ficheiro de configuração.

Fig. 3.7 Selecção da criação de novo ficheiro

Fig. 3.8 Escolha da versão do sistema operativo

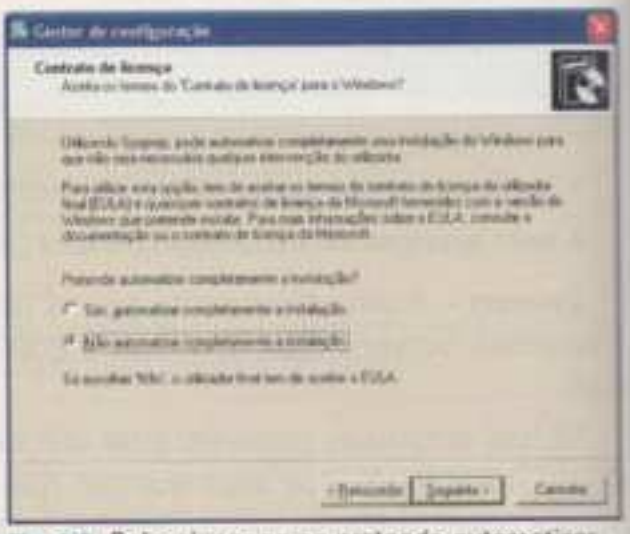

Fig. 3.9 Seleccionar se se pretende automatizar, ou não, a instalação.

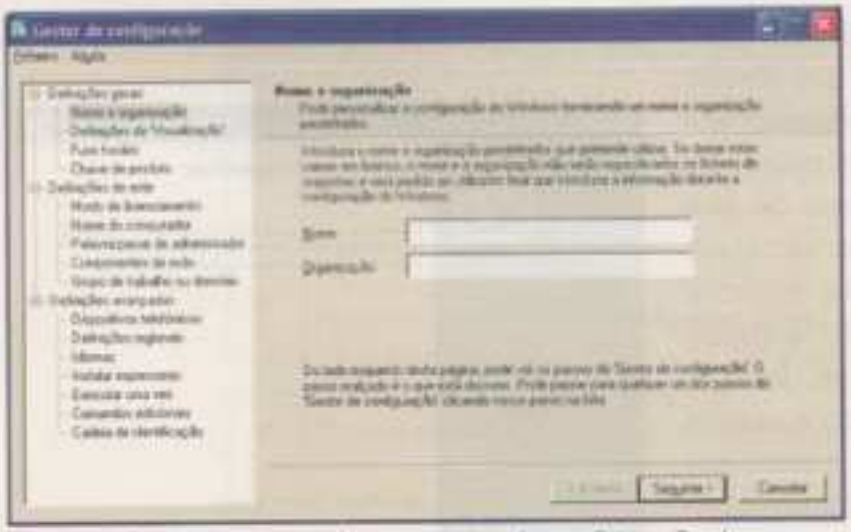

Fig. 3.10 Campos a preencher no gestor de configuração do **setupmgr.exe**.

Fig. 3.11 Aspecto geral do **sysprep.exe**, onde será feita a associação ao ficheiro de texto configurado pelo **setupmgr.exe**.

Scripting – na sua forma mais simples, um *script* é apenas um ficheiro que pré-responde a todas as questões que o *setup* coloca – como se deve chamar ao computador, qual é o teu nome, qual é o valor do ID do produto, este tipo de coisas. Então, o que tem de se aprender com esta ferramenta? Em primeiro lugar, tem de se aprender a linguagem dos *scripts*; tal como a maioria das "coisas de computador", os *scripts* têm uma sintaxe específica, que teremos de seguir, ou então não funcionam. No Windows Server 2003, a Microsoft facilitou o trabalho de escrita do *script*, no qual incluíram um programa que faz algumas perguntas e depois gera um *script*. Este *script* é apenas um *script* básico, que depois terá de ser modificado, adicionando algumas linhas para o tornar útil.

Instalação remota (RIS) – tudo o que um bom *script* faz é evitar que se responda a questões enquanto se corre o processo de instalação, mas existe um senão: primeiro terá de se conseguir iniciar o processo de instalação. Vamos analisar ferramentas que simplificam o método de se iniciar o processo de entrega, no novo computador, de todos os ficheiros de início de instalação do sistema operativo.

A forma mais simples de iniciar a configuração é colocar um CD na *drive* de CD-ROM do computador e depois fazer o arranque a partir do CD. Mas como fornecer o *script*? Pode-se colocar o *script* numa disquete, mas quem é que quer andar por aí com um CD-ROM e, além disso, o que acontece se pretendermos utilizar mais do que o sistema operativo? Com o Windows NT4, era necessário criar uma partilha de rede que contivesse todos os ficheiros de instalação do NT e depois tinha de se utilizar um processo de ligar o computador, sem nenhum sistema operativo instalado no seu disco duro, à rede (*network*).

Mais uma vez, o Windows Server 2003 (e o 2000) simplifica esta tarefa com uma ferramenta chamada RIS (*Remote Installation Services*) – serviços de instalação remota. Com o RIS, podem-se guardar ficheiros de instalação e *scripts* pré-construídos do Windows 2000, do XP e do Server 2003, num servidor designado **servidor RIS**. O RIS elimina a necessidade de nos questionarmos sobre como iremos conseguir que o nosso novo computador se ligue à rede. Os novos computadores suportam o arranque através da placa de rede do computador chamada PXE, o *Preeboot Execution Environment* (o ambiente de execução de pré-arranque). Se o computador não for compatível com o PXE, não há problema, pois o RIS pode gerar uma disquete genérica que permitirá que a maioria dos computadores e alguns portáteis se liguem a um servidor RIS, sem necessidade de ter um suporte PXE instalado (*built-in PXE support*).

Um servidor RIS pode distribuir Windows Server 2003, Windows 2000 Server, Windows 2000 Professional e XP.

Ficheiros de instalação

Os ficheiros de instalação encontram-se na directoria **\I386** do CD-ROM do Windows Server 2003, tal como acontece com o Windows 2000 Server e com o Windows NT Server.

Se estivermos a fazer uma instalação a partir de um computador já com um sistema operativo instalado, como o Windows 9x, o Windows NT, o Windows 2000 ou o Windows XP (Professional ou Home Edition), deve-se correr o programa **WINNT32.EXE**, que se encontra na directoria (*folder*) **\I386**. Caso o sistema operativo instalado seja o MS-DOS, deve-se correr o **WINNT.EXE**, que está localizado na mesma directoria.

Caso seja feito um arranque por CD-ROM, não é necessário escolher o executável de arranque, pois a configuração será lançada automaticamente.

Se a intenção é fazer uma actualização (*upgrade*), então convém saber que uma actualização de um sistema operativo Windows para o Windows Server 2003 só é possível a partir do Windows NT 4.0 Server ou do Windows 2000 Server e, para tal, deve-se correr o programa **WINNT32.EXE**, que se encontra na directoria (folder) **\i386**.

Papel dos servidores

É necessário dedicar algum cuidado no que concerne ao papel dos servidores, devido às diferenças existentes entre o Windows Server 2003 e o Windows 2000 Server relativamente ao Windows NT Server, principalmente no que diz respeito a instalação em redes mistas.

Aconselha-se a rever o capítulo 1.5, para um refrescar da informação sobre o papel dos servidores.

Deste modo, os servidores podem ter o papel de:

Controladores de domínio (*Domain Controllers*): a definição deste papel atribuído ao servidor já foi dada no ponto 1.5. Basta apenas, talvez, acrescentar que, caso se pretenda ter um servidor DC, não é obrigatório configurar o servidor como DC no processo de instalação do Windows Server 2003 e do Windows 2000 Server. Após a instalação do sistema operativo, um servidor pode ser convertido em *Domain Controller* por meio do utilitário **dcpromo.exe**. Um servidor que corra o Windows Server 2003 ou o Windows 2000 Server pode até deixar de desempenhar o papel de controlador de domínio ou ser transferido para outro domínio ou rede sem necessidade de reinstalar o sistema operativo, como acontecia no Windows NT Server. Um DC também é responsável pelo controlo de segurança dentro de um domínio e procede à autenticação dos utilizadores em rede.

O Windows Server 2003 e o Windows 2000 Server podem ser configurados a funcionar como:

Fig. 3.12 Servidor que funciona como *Domain Controller* único e pertencente ao topo da floresta.

- **Novo *Domain Controller***. Este servidor irá funcionar como servidor de topo da floresta e como único *Domain Controller* da floresta, dado que, quando se promove este servidor a *Domain Controller*, ainda não existirá nenhuma floresta.

- ***Domain Controller* pertencente a um domínio já existente**. Este servidor fica com uma cópia do AD do *Domain Controller* já existente. Se o primeiro servidor estiver em baixo (desligado), o novo servidor poderá, por exemplo, continuar a validar os utilizadores. Na prática, o segundo servidor não fica com uma réplica exacta do AD do primeiro servidor, mas este ponto será focado mais à frente.

Fig. 3.13 O Servidor 2 ficou a pertencer ao domínio já existente no Servidor 1.

- **Nova árvore em floresta existente**. Nesta situação já tem de existir uma floresta criada e, pelo menos, um *Domain Controller*. É possível criar um novo domínio totalmente autónomo do outro DC (já criado anteriormente) na floresta existente, embora se consiga ter acesso aos recursos do anterior domínio, dado que este novo vai ser criado dentro da floresta já existente.
- ***Member Servers*** – são servidores que estão associados a um domínio já existente, ou seja, são apenas membros do domínio, mas não são controladores de domínio. Um servidor configurado como *Member Server* reconhece os utilizadores, grupos e recursos do *Domain Controller*, podendo ainda disponibilizar os seus próprios recursos utilizadores existentes no *Domain Controller*.
- ***Standalone Server*** – são servidores que podem aderir a um grupo de trabalho existente ou até mesmo criar um, mas não fazem parte de um domínio e também não contêm o AD.

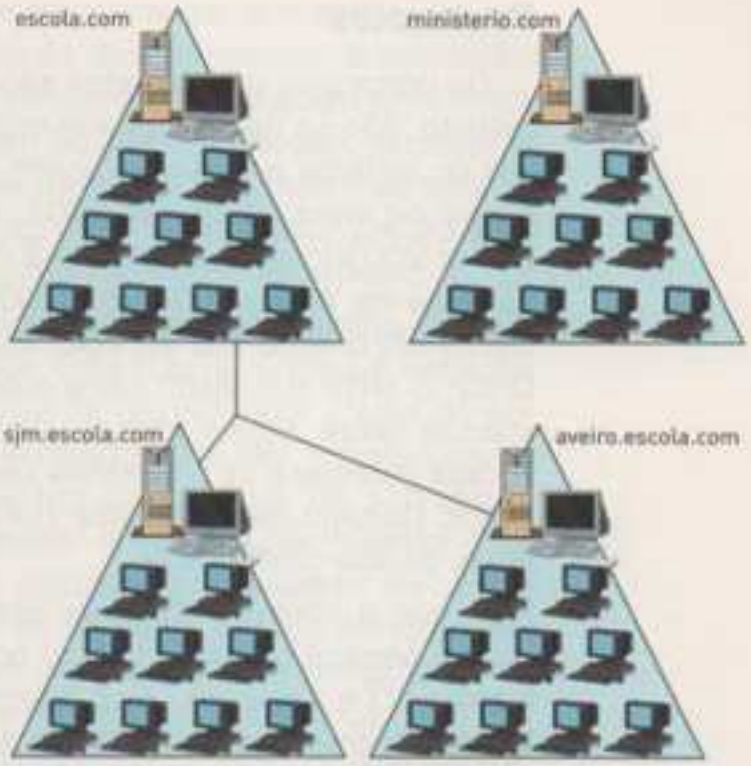

Fig. 3.14 **Esquema de implementação de nova árvore composta por quatro domínios.** Neste exemplo foi criado um novo domínio **ministerio.com**, que pertence à floresta já existente que contém o domínio **escola.com**.

Para **determinar o papel de um servidor** (Windows Server 2003 e Windows 2000 Server), basta ir à janela **Os meus locais na rede** (*My Network Places*), clicar com o botão direito do rato sobre um computador, ir ao menu, seleccionar a janela **Propriedades** (*Properties*) e fazer a verificação.

Em alternativa à obtenção da mesma informação, podem seguir-se os seguintes passos:

- ir ao menu **Start/Run**, digitar **cmd** e clicar em **OK**;
- no *command prompt*, executar o comando **net accounts**;
- verificar o *status* que surge na linha *Computer Role*.

Domínios, árvores e florestas

Mais uma vez se aconselha a reler a informação contida no capítulo 1.5. desta unidade, para recordar as diferenças entre um domínio, uma árvore e uma floresta.

Um **domínio** Microsoft existe a partir do momento em que se instale o primeiro DC do domínio. Os servidores DC que correrem com Windows Server 2003 e Windows 2000 Server conseguem trocar entre si actualizações do directório, processo chamado ***Multimaster Replication***. Normalmente, uma rede com um só domínio é apenas instalada em empresas pequenas e/ou simples, enquanto que empresas com maior projecção preferem utilizar redes com mais de um domínio, ou seja, uma árvore (ou floresta).

Uma **árvore** é um conjunto de domínios colocados de forma hierárquica, a partir de um domínio de raiz (um DC).

Uma **floresta** é um sistema de vários domínios (um conjunto de árvores associadas) que partilham recursos.

Protocolos

Os protocolos mais usados são o NetBEUI, o NWLink (IPX/SPX) e o TCP/IP. No entanto, não se devem instalar múltiplos protocolos, a não ser que as características do sistema assim o obriguem a fazer. Não é muito difícil optar pelo protocolo a usar no Windows Server 2003, uma vez que o único protocolo que o Windows Server 2003 instala por defeito é o TCP/IP e, além do mais, a grande maioria dos serviços do Windows Server 2003 é dependente do protocolo TCP/IP, nomeadamente em relação aos serviços usados na Internet, como, por exemplo, o DNS, o DHCP, o HTTP e o MAIL, entre outros. Configurar o TCP/IP requer alguns conhecimentos sobre alguns tópicos – o que é um endereço IP, um *subnet mask*, um *default gateway* e se preferimos usar um servidor DNS (para principiantes) ou usar DHCP. Convém saber do que trata toda esta informação sobre este protocolo, antes da sua configuração.

O que é novo no Windows Server 2003 é que este sistema operativo nem sequer oferece o NetBEUI como opção de protocolo, ficando-se apenas pelos protocolos IPX e AppleTalk como alternativas ao TCP/IP. O NetBEUI está disponível no CD do Windows Server 2003, na directoria **\valueadd\msft\net\netbeui**, mas para o encontrar é preciso procurar com alguma atenção!

O uso do IPX/SPX em simultâneo com o TCP/IP é necessário quando se pretende que um cliente de uma rede Microsoft aceda a um servidor NetWare de modo transparente, isto é, poder aceder ao servidor NetWare como se estivesse a aceder ao Windows Server 2003 ou ao Windows 2000 Server.

Tipos de licença

Existem dois tipos de licença, que devem ser bem distinguidos, para evitar problemas posteriores e, por vezes, dispendiosos: **licenças de utilização dos sistemas operativos** e **licenças de cliente**:

- **Licença de utilização dos sistemas operativos** – esta licença vem em conjunto com um sistema operativo (SO) adquirido legalmente e até serve de prova de compra, por exemplo, com o Windows 9x, o NT Workstation, o 2000 Professional ou o XP Professional. Esta licença permite instalar e usar o sistema operativo adquirido.

Por cada Windows Server 2003 instalado é necessária a compra de uma licença de servidor.

Quando se trata de um servidor onde existem computadores-clientes que se ligam a ele para acederem aos ficheiros e bases de dados, entre outros recursos partilhados, é necessário adquirir, para cada cliente, não só uma licença de utilização do SO, como também uma **licença de acesso cliente**, chamada **CAL** (*Client Access Licence*), que autoriza o SO a ser cliente do servidor.

O Windows Server 2003 permite ter dois modos de licenciamento dos clientes (CAL), licenciamento *per server* e *per seat*.

- **Licença *per server*** – além da licença de utilização do sistema operativo que cada computador-cliente tem de ter, é necessária outra licença de acesso cliente (CAL) para aceder ao servidor. Neste tipo de licenciamento, o servidor deve ter um número de licenças igual ou superior ao número de clientes ligados em simultâneo ao servidor. Por exemplo, se tivermos uma rede com um servidor e 50 computadores e se, no máximo, estiverem 30 clientes ligados em simultâneo ao servidor, apenas será necessário adquirir 30 licenças de acesso

cliente. Este licenciamento adequa-se mais a empresas que têm apenas um servidor ou que trabalhem por turnos. Se tivermos dois servidores, é necessário contabilizar para cada um o número máximo de clientes que acedem em simultâneo a cada servidor. Por exemplo, se existirem 30 clientes a aceder, simultaneamente, ao servidor 1 e, noutro momento, os mesmo 30 acederem ao servidor 2, é necessário adquirir 30 + 30 licenças CAL. Têm de ser adquiridas 30 licenças CAL por cada servidor, visto as licenças serem aplicadas ao servidor.

- **Licença *per seat*** – este tipo de licença difere da anterior pelo motivo de cada ligação cliente-servidor requerer uma licença. Este tipo de licença é necessária por computador-cliente e não por utilizador. Se um utilizador aceder ao servidor através de um portátil, quando se encontra fora das instalações da empresa, e, em outra altura, através de um computador de secretária, quando se encontra no interior das instalações, então são necessárias duas licenças CAL, uma por cada PC. Caso este utilizador queira aceder de casa a partir do seu computador particular, terá de ter outra licença (neste caso, uma terceira licença). Em contrapartida, se um determinado computador for partilhado por 3 utilizadores, apenas temos de adquirir uma licença.
  Esta licença CAL permite a qualquer pessoa que esteja num computador aceder a qualquer um dos servidores, independentemente do número de domínios que o sistema contenha.

Exemplo 1:

Vamos imaginar que se têm 4 servidores, 20 empregados e 35 computadores *workstation* (20 computadores de secretária e 15 portáteis). Neste exemplo existem mais computadores do que pessoas, devido aos portáteis e aos computadores de acesso geral. O objectivo é que todos os 20 empregados possam aceder a qualquer servidor em qualquer altura. Com licenças ***per server*** seria necessário comprar 20 licenças CAL para cada servidor, ou seja, 80 CAL no total. Com licenças ***per seat***, bastaria uma licença CAL para cada uma das 35 máquinas. Neste caso, seriam necessárias 35 CAL (uma por computador). Neste exemplo, o licenciamento *per seat* ganha vantagem.

Exemplo 2:

A empresa é composta por um servidor e 100 computadores-clientes, mas sabe-se que, no máximo, só 20 computadores-clientes estarão a aceder ao servidor. Com o licenciamento *per server*, basta adquirir, no máximo, 20 licenças, enquanto que no licenciamento *per seat* seriam necessárias 100 licenças, uma por cada computador que aceda ao servidor.

- Se formos **clientes da Internet** e se acedermos a serviços de HTTP e FTP do servidor, não é necessário adquirir licenças CAL, mas existe um senão: se existirem páginas WWW (*World Wide Web*) a aceder a uma base de dados SQL Server, já é necessário ter uma licença de acesso ilimitado e, se acedermos via Internet ao servidor e executarmos o *logon* no servidor para acedermos a ficheiros ou impressoras, então também necessitaremos de uma licença CAL.

Sistemas *multi-boot*

Sistema *multi-boot* ou *dual-boot* significa que, no arranque do Windows Server 2003, surge um menu onde constam os sistemas operativos instalados nesse computador e é possível seleccionar, entre eles, aquele que se pretende utilizar. Assim, no mesmo computador podem estar instalados, simultaneamente, o Windows Server 2003, como também o DOS e o Windows 95, por exemplo (o DOS terá de ser insta-

lado sempre antes do Windows 2000/NT ou do Server 2003). É claro que os sistemas operativos não correm todos em simultâneo, mas sim alternadamente, consoante a opção feita no arranque. Este sistema pode tornar-se útil, por exemplo, se depararmos com *software* que só é compatível com um ou outro sistema operativo.

Esta situação é útil num laboratório de uma sala de aula, ou em casa, quando se pretende utilizar o mesmo computador para se instalar diversos sistemas operativos, com vista à realização de testes de instalação e de configuração, sem necessidade de custos adicionais a nível de *hardware*.

Caso se pretenda instalar um servidor para funcionar a tempo inteiro como servidor numa determinada organização, não se deve optar por instalar diversos sistemas operativos; um servidor deve estar permanentemente ligado para que esteja sempre disponível, sem que haja a preocupação de o ligar ou desligar.

Nome do computador e do domínio

Parece algo sem importância, mas é uma boa ideia planear os nomes a usar nos servidores. É fácil lembrarmo-nos de nomes como "escritório", "produção", ou "nome_da_empresa", quando se tem uma pequena rede local (LAN), mas, quando se começa a ter mais do que aquela meia-dúzia de servidores, começa a tornar-se difícil recordar quem é o quê. O truque está na simplicidade, mas também no aspecto prático. Convém dedicar algum tempo a este assunto, pois, embora seja fácil alterar posteriormente o nome do servidor, não é tão fácil alterar as centenas ou as milhares de *workstations* de utilizadores que estão ligadas a ele. Daí a importância não só da escolha do nome de cada computador, como também do nome do domínio a que o computador pertencerá. Ao instalar o Windows Server 2003 ou o Windows 2000 Server tem de se atribuir um nome de domínio NetBIOS; este nome pode ter até 15 caracteres, para que seja compatível ao mesmo tempo com o Windows NT Server, de outro modo não é possível a integração deste último com o Windows Server 2003 ou o Windows 2000 Server. O nome NetBIOS é visto por todos os sistemas operativos da Microsoft.

Se, mais tarde, o servidor for promovido a *Domain Controller*, então também se torna necessário indicar o nome de domínio DNS. No caso do Windows Server 2003 ou do Windows 2000 Server, o nome de domínio não pode ser apenas uma única palavra ou um nome NetBIOS, terá de ser uma entrada DNS, como, por exemplo, *escola.com*.

Nomes de domínios DNS

Normalmente, uma rede com um só domínio é apenas instalada em empresas pequenas e/ou simples. Empresas com maiores dimensões tendem a utilizar redes com mais de um domínio, por exemplo, uma floresta composta por diversas árvores. No entanto, o nome de domínio só adquire mais relevância quando o servidor é convertido em DC, após a instalação do Windows Server 2003 ou do Windows 2000 Server. Mas, como já foi dito, alterar um nome posteriormente à instalação do servidor pode tornar-se bastante complicado, devido ao *Active Directory* já instalado e às *workstations* que já se encontram no sistema.

Caso a máquina esteja ligada directamente à Internet, tem de se registar o nome do domínio antes da promoção a DC. Numa organização em que exista um domínio, por exemplo, **escola.com** e um ou mais subdomínios, por exemplo **norte.escola.com** e **sul.escola.com**, só é necessário registar o primeiro domínio.

Configuração do TCP/IP

Para configurar o TCP/IP é importante que se compreenda o seu funcionamento. Para formar uma ligação em rede de vários computadores, de modo que possam trocar entre si informações, cada computador tem de estar identificado com um endereço, ao qual se dá o nome de endereço IP. Uma parte do endereço IP de cada computador identifica-o na rede (*Host ID* – identificador do computador ou de qualquer componente da rede com endereço IP) e uma outra parte identifica a rede a que o mesmo pertence (*Network ID* – identificador da rede). Todos os computadores da rede devem ter um endereço IP com o mesmo *Network ID* e cada cliente (*host*) deve ter um *Host ID* diferente. Para começar, é necessário escolher o endereço IP e a *subnet mask* a usar pelo servidor.

Como se sabe, um endereço IP consiste num conjunto de quatro bytes separados por pontos, não podendo o 1.º byte ser 127 nem maior que 223, nem ser zero.

O *subnet mask* indica qual a secção do endereço IP que representa a *Network ID* e qual a que identifica o *Host ID*. Sendo assim, é necessário não só configurar um endereço IP para cada computador, como também se torna imperativo informar o sistema sobre a parte do endereço que representa a identificação da rede, e isto é feito através da especificação de uma *subnet mask*.

Se o computador pertencer a uma rede local privada, então a escolha de qualquer endereço IP e de qualquer *subnet mask* é possível, visto a rede nunca chegar a interagir com uma rede pública, tipo Internet.

No caso de os computadores estarem ligados à Internet (rede pública), então é necessário solicitar ao ISP o endereço ou a gama de endereços que podem ser usados.

Na nossa instalação vai-se utilizar o servidor numa rede local, pelo que não é obrigatório respeitar as classes de endereços IP utilizadas na Internet. O nosso servidor vai ser instalado com IP fixo, com endereço classe C 192.168.1.1 e com *subnet mask* 255.255.255.0. Na nossa rede podem existir 254 *host*.

Para informação mais detalhada deve ser feita uma revisão à Unidade 2, sobre endereços IP.

2.2. Partições

Particionamento e formatação

Uma partição de disco é uma forma de dividir o disco de modo a que cada secção funcione como uma unidade separada. Ao criar partições num disco, está-se a dividir o disco em uma ou em mais áreas, que podem ser formatadas para uso por um sistema de ficheiros, como o FAT (*File Allocated Table*) ou o sistema de ficheiros NTFS, por exemplo.

Há, então, que decidir que tipo de utilização se pretende dar ao servidor, para, a partir daí, se decidir a quantidade e os tamanhos necessários para cada partição a criar. Talvez a longo prazo se torne mais conveniente ter os dados numa partição e o sistema noutra. Nesse caso, apenas se necessita de espaço suficiente para o SO com alguma folga, sugerindo-se talvez um mínimo de 4 GB de partição. Caso se pretenda também usar serviços de instalação remota, convém deixar de parte uma grande partição apenas para este fim. Para todos os efeitos, é sempre aconselhável ter um disco com a máxima capacidade existente no mercado.

Se seleccionarmos uma nova partição durante o processo de configuração (*setup*), deve-se criar e medir apenas a partição na qual se irá instalar o Windows Server 2003. Após a instalação do Windows Server 2003, deve usar-se o *Disk Management* para particionar o restante espaço no disco duro. Isto significa que, se a instalação do Windows Server 2003 for feita através de CD-ROM, o programa de *setup* inicial permite fazer o particionamento e a formatação durante a instalação. Assim sendo, ao fazer uma nova instalação por meio de um CD, o programa de configuração (*setup program*) examina o disco duro para determinar a configuração existente, e oferece as seguintes opções:

- **Uma nova partição num disco duro não particionado.** Se o disco duro não estiver particionado, pode-se criar e decidir o tamanho da partição do Windows Server 2003.
- **Uma nova partição num disco duro particionado.** Se o disco duro estiver particionado, mas conta com espaço não particionado suficiente no disco, pode-se criar a partição para Windows Server 2003 no espaço não particionado.
- **Instalar em partição existente.** Se o disco duro já conta com uma partição suficientemente grande, pode-se instalar o Windows Server 2003 nessa partição. Se já existe um sistema operativo na partição existente, efectuar uma nova instalação significa instalá-la por cima da existente, apagando-a.
- **Apagar uma partição existente.** Se um disco duro tem uma partição existente, pode-se apagá-la para criar mais espaço de disco não particionado para a partição do Windows Server 2003. Ao apagar qualquer partição existente, apaga-se igualmente quaisquer dados que nela possam estar guardados.

Caso se pretenda particionar o disco antes da instalação, é possível fazê-lo através do programa **fdisk** do DOS e, depois, podem-se formatar as partições criadas com o comando **format**.

Seja como for, antes de qualquer instalação do Windows Server 2003, é necessário decidir qual o esquema de partições a usar.

Após ter criado a partição sobre a qual se irá instalar o Windows Server 2003, o processo de configuração permite seleccionar o sistema de ficheiro com o qual formatar a partição.

O Windows Server 2003 suporta os seguintes sistemas de ficheiros (*file system*):

- **NTFS** (*NT File System*) versão 5 – sistema de ficheiros mais fiável (suporta nível de segurança C-2) e recente. Com bom desempenho num disco grande, é o sistema de ficheiros recomendado*.

Atenção: o Windows Server 2003, o Windows XP, o Windows 2000 e o Windows NT são os únicos sistemas operativos que podem aceder a dados num disco duro local

---

* O **NTFS** é o sistema de ficheiros recomendado para o Windows Server 2003, o Windows XP e o Windows 2000, que, nestes casos, é a versão 5. Deve usar-se NTFS (5) em partições que requerem:
- **Segurança a nível de ficheiros e pastas** – o NTFS permite controlar o acesso aos ficheiros e às pastas.
- **Compressão de ficheiros** – o NTFS comprime os ficheiros para criar mais espaço de armazenamento.
- **Gestão de quotas de disco** – o NTFS permite controlar a utilização do disco, utilizador por utilizador.
- **Encriptação de ficheiros** – o NTFS permite que se encriptem dados de ficheiros de modo transparente.
- **Gestão de ficheiros duplicados**.
- **Maior velocidade** – conseguida em partições com mais de 400 megabytes (a instalação básica do Windows Server 2003 exige, pelo menos, 900 megabytes).
- **Instalação do *Active Directory*** – necessita do NTFS pelo menos numa partição.

Obs.: No Windows Server 2003, no Windows XP e no Windows 2000, o NTFS é a versão 5; no entanto, o Windows NT não tem capacidade para tirar partido das novas características do NTFS 5.
Deve evitar-se instalar vários sistemas operativos numa mesma partição, devido a alguns problemas e erros de software que possam surgir. O melhor é instalar cada sistema operativo numa partição diferente.
Para informações mais detalhadas sobre sistemas de ficheiros, consultar o manual de TI do 10.º ano, no ponto 4.3.2.

que é formatado com NTFS; não permite aceder às partições a partir de DOS, por exemplo. Caso se pretenda instalar o Windows 2000 ou o Windows Server 2003, mas também instalar ou manter uma instalação existente do Windows NT, convém que este tenha o Service Pack 4 instalado e, além disso, convém sempre que o Windows 2000, ou o Windows XP, ou o Windows Server 2003 seja o último a ser instalado.

- **FAT 32** – sistema de ficheiros que apareceu com a segunda versão do Windows 95 (versão OSR/2 ou posterior); é uma evolução do FAT 16, usado pela família Windows 9x, Windows 200x, Windows XP e Linux (mas não é suportado pelo Windows NT). É utilizado em discos de maiores dimensões, oferece maior segurança (cria cópias de segurança do sector de arranque – *boot sector*) e melhor aproveitamento do espaço útil em disco (consegue criar *clusters* de pequenas dimensões – 4 kB).
- **FAT** ou **FAT 16** (*File Allocation Table*) – sistema de ficheiros mais antigo (usado no MS-DOS, no Windows 3.x e no 95, por exemplo) e simples; é bom para discos pequenos e com boa compatibilidade.

Deve optar-se pela formatação com FAT caso se necessite aceder às partições a partir de DOS ou se o sistema correr com o Windows 95. Este tipo de formatação não suporta partições com tamanho superior a 2 GB.

Há também sistemas de ficheiros em discos que podem ser lidos pelo Windows Server 2003, mas que não podem ser usados para formatar discos rígidos:

– **CDFS** (*Compact Disk File System*) – sistema de ficheiros usado em CD-ROM;

– **UDF** (*Universal Disk Format*) – sistema de ficheiros usado em DVD.

Conversão para NTFS

Caso se inicie uma instalação do Windows 2000 ou do Windows Server 2003 num computador que já conta com discos particionados em formato NTFS, então estas partições serão automaticamente convertidas em NTFS 5; se tivermos um servidor criado numa *drive* FAT, há sempre a opção de converter posteriormente este sistema de ficheiros para NTFS, bastando para tal abrir uma linha de comando e digitar **convert c: /fs:ntfs.**, onde "**c:**" é o volume que se pretende converter. Mas como, depois, não há regresso possível para FAT, convém ter a certeza que se pretende mesmo converter o FAT para NTFS. Para se obter mais informações do comando **Convert**, deve-se escrever na linha de comandos **help convert**.

```
C:\>convert c: /fs:ntfs
```

Fig. 3.15 Linha de comandos com o comando **Convert**

```
C:\>help convert
Converte volumes de FAT em NTFS.

CONVERT volume /FS:NTFS [/V] [/CvtArea:nomefich] [/NoSecurity] [/X]

 volume        Especifica a letra de unidade (seguida de dois pontos),
               o ponto de montagem ou o nome do volume.
 /FS:NTFS      Especifica que o volume deve ser convertido em NTFS.
 /V            Especifica que CONVERT deve ser executado em modo
               verboso.
 /CvtArea:nomefich
               Especifica um ficheiro contínuo no directório raiz como
               marcador de posição para ficheiros de sistema NTFS.
 /NoSecurity   Especifica que as definições de segurança dos ficheiros
               e directórios convertidos sejam acessíveis a todos.
 /X            Obriga o volume a desmontar primeiro se for necessário.
               Todos os identificadores abertos para este volume serão
               inválidos.
```

Fig. 3.16 Manual do comando **Convert**

Partições *Boot* e *System*

Há dois grandes grupos de ficheiros de sistemas, que são o ***system files*** – ficheiros de SO instalados no directório **\windows**, para o caso do Windows Server 2003, e no directório **\winnt**, no caso de ser Windows 2000 Server e/ou NT Server – e o ***boot files*** – ficheiros usados para arranque, com menu para selecção do SO a usar. Assim sendo, fazer um *boot* em vários sistemas operativos não é mais do que arrancar com diferentes sistemas operativos num mesmo computador. Há que ter em atenção, no entanto, que, ao arrancar com um determinado sistema operativo, apenas estarão disponíveis os serviços instalados nesse mesmo sistema operativo. Uma configuração *dual boot* permite, então, escolher entre dois ou mais sistemas operativos, cada vez que se reinicie o computador.

Resumindo, partições *boot* (*boot partition*) contêm os ficheiros de *boot* (tipicamente em **c:**) e partições *system* (*system partition*) contêm os ficheiros de sistema.

Normalmente, não se iria formatar a partição na qual reside o Windows Server 2003 com FAT ou FAT 32, a não ser que se necessitasse de uma configuração *dual boot*.

Nota: Num servidor que está a trabalhar a nível prático, não é usual ter-se mais que um sistema operativo instalado. Um servidor deve estar sempre ligado para estar sempre disponível.

2.3. *Hardware*

Requisitos do servidor

Os requisitos de *hardware* para a instalação do Windows Server 2003 ou do Windows 2000 Server dependem das versões utilizadas e podem ser divididas em:

- **Requisitos mínimos** – representam o *hardware* obrigatório para se conseguir instalar o sistema operativo.
- **Requisitos recomendados** – representam o *hardware* que se deve utilizar para se conseguir um funcionamento adequado do servidor. Os requisitos recomendados ou reais variam consoante a configuração do sistema e as aplicações e funcionalidades que se escolheram para instalar.
- **Requisitos máximos** – indicam qual o *hardware* máximo que cada versão do sistema operativo suporta: acima destes valores, o sistema operativo não reconhece o *hardware*.

Na **tabela 3.6** encontram-se os requisitos mínimos e recomendados para executar o Windows Server 2003, o Standard Edition, o Enterprise Edition, o Datacenter Edition e o Web Edition, e na **tabela 3.7** para as versões Small Business Server 2003 Standard Edition e Premium Edition.

Requisitos do sistema operativo Windows Server 2003				
Requisito	**Standard Edition**	**Enterprise Edition**	**Datacenter Edition**	**Web Edition**
Velocidade mínima da CPU	133 MHz	133 MHz para computadores baseados em x86 733 MHz para computadores baseados em Itanium*	400 MHz para computadores baseados em x86 733 MHz para computadores baseados em Itanium*	133 MHz
Velocidade recomendada da CPU	550 MHz ou superior, de preferência	733 MHz ou superior, de preferência	733 MHz ou superior, de preferência	550 MHz ou superior, de preferência
Mínimo de RAM	128 MB	128 MB	512 MB	128 MB
Mínimo recomendado de RAM	256 MB	256 MB	1 GB	256 MB
Máximo de RAM	4 GB	32 GB para computadores baseados em x86 64 GB para computadores baseados em Itanium*	64 GB para computadores baseados em x86 512 GB para computadores baseados em Itanium*	2 GB
Suporte de multiprocessador	Até 4	Até 8	Mínimo de 8 necessário; máximo de 32	Até 2
Espaço em disco para a configuração	1,5 GB	1,5 GB para computadores baseados em x86 2,0 GB para computadores baseados em Itanium*	1,5 GB para computadores baseados em x86 2,0 GB para computadores baseados em Itanium*	1,5 GB
Drive	No mínimo, leitor de CD-ROM, de preferência leitor de DVD-ROM e leitor de disquetes.	No mínimo, leitor de CD-ROM, de preferência leitor de DVD-ROM e leitor de disquetes.	No mínimo, leitor de CD-ROM, de preferência leitor de DVD-ROM e leitor de disquetes.	No mínimo, leitor de CD-ROM, de preferência leitor de DVD-ROM e leitor de disquetes.
Monitor e placa gráfica	No mínimo, VGA ou *hardware* que suporte o redireccionamento. De preferência, monitor e placa gráfica Super VGA (800 × 600) ou de resolução superior.	No mínimo, VGA ou *hardware* que suporte o redireccionamento. De preferência, monitor e placa gráfica Super VGA (800 × 600) ou de resolução superior.	No mínimo, VGA ou *hardware* que suporte o redireccionamento. De preferência, monitor e placa gráfica Super VGA (800 × 600) ou de resolução superior.	No mínimo, VGA ou *hardware* que suporte o redireccionamento. De preferência, monitor e placa gráfica Super VGA (800 × 600) ou de resolução superior.
Outros dispositivos	- Teclado e rato ou dispositivo apontador compatível. - 1 placa de interface de rede Ethernet, de preferência 2 placas de rede que suportem arranque por rede *"Preboot Execution Environment (PXE) Standard."*	- Teclado e rato ou dispositivo apontador compatível. - 1 placa de interface de rede Ethernet, de preferência 2 placas de rede que suportem arranque por rede *"Preboot Execution Environment (PXE) Standard."*	- Teclado e rato ou dispositivo apontador compatível - 1 placa de interface de rede Ethernet, de preferência 2 placas de rede que suportem arranque por rede *"Preboot Execution Environment (PXE) Standard."*	- Teclado e rato ou dispositivo apontador compatível. - 1 placa de interface de rede Ethernet, de preferência 2 placas de rede que suportem arranque por rede *"Preboot Execution Environment (PXE) Standard."*

*Importante: As versões de 64 bit do Windows Server 2003 Enterprise Edition e do Windows Server 2003 Datacenter Edition só são compatíveis com os sistemas baseados em Intel Itanium de 64 bit. Não podem ser instaladas correctamente em sistemas de 32 bit.

Tabela 3.6 Lista de requisitos mínimos, recomendados e máximos da família Windows Server 2003

Requisitos do sistema operativo Windows Small Business Server 2003		
Requisito	**Standard Edition**	**Premium Edition**
Velocidade mínima da CPU	300 MHz	300 MHz
Velocidade recomendada da CPU	550 MHz ou superior, de preferência	550 MHz ou mais rápido
Mínimo de RAM	256 MB	256 MB
Mínimo recomendado de RAM	384 MB ou superior	512 MB ou superior
Máximo de RAM	4 GB	4 GB
Suporte de multiprocessador	Até 4	Até 4
Espaço em disco para a configuração	4 GB de espaço disponível no disco rígido*	5 GB de espaço disponível no disco rígido* (são apenas necessários 2 GB, se actualizar a partir do Small Business Server 2000)
Drive	No mínimo, leitor de CD-ROM. De preferência, leitor de DVD-ROM e leitor de disquetes.	No mínimo, leitor de CD-ROM. De preferência, leitor de DVD-ROM e leitor de disquetes.
Monitor e placa gráfica	No mínimo, VGA ou *hardware* que suporte o redireccionamento. De preferência, monitor e placa gráfica Super VGA (800 × 600) ou de resolução superior.	No mínimo, VGA ou *hardware* que suporte o redireccionamento. De preferência, monitor e placa gráfica Super VGA (800 × 600) ou de resolução superior.
Outros dispositivos	- Teclado e rato ou dispositivo apontador compatível. - *Hardware* que suporte o redireccionamento da consola. - 1 placa de interface de rede Ethernet; de preferência 2 placas de rede que suportem arranque por rede "*Preboot Execution Environment (PXE) Standard.*"	- Teclado e rato ou dispositivo apontador compatível. - *Hardware* que suporte o redireccionamento da consola. - 1 placa de interface de rede Ethernet; de preferência 2 placas de rede que suportem arranque por rede "*Preboot Execution Environment (PXE) standard.*"
Itens e serviços adicionais necessários para o acesso à Internet e rede	- Algumas funcionalidades do servidor requerem o acesso à Internet e o pagamento de uma taxa em separado a um fornecedor de serviços, podendo aplicar-se encargos telefónicos locais e/ou de longa distância. - Ligação à Internet de banda larga ou por *modem* de alta velocidade. - Fax *modem* de classe 1 dedicado para utilizar o serviço de fax.	- Algumas funcionalidades do servidor requerem o acesso à Internet e o pagamento de uma taxa em separado a um fornecedor de serviços, podendo aplicar-se encargos telefónicos locais e/ou de longa distância. - Ligação à Internet de banda larga ou por *modem* de alta velocidade. - Fax *modem* de classe 1 dedicado para utilizar o serviço de fax.

*Os requisitos reais variam consoante a configuração do sistema e as aplicações e funcionalidades que se escolheram para instalar. Poderá ser necessário espaço disponível adicional no disco rígido, se a instalação for realizada através de uma rede.

Tabela 3.7 Lista de requisitos mínimos, recomendados e máximos da família Small Business Server 2003

Os requisitos recomendados variam consoante a aplicação que se dá ao servidor, pelo que, idealmente, deve-se utilizar o melhor processador possível e a máxima memória RAM. Nos discos rígidos deve-se utilizar, de preferência, discos SCSI e respectivas controladoras (*Ultra Wide*, se possível). Quanto ao espaço do disco, quanto maior, melhor! Nestas coisas, mais vale ter espaço livre a mais do que faltar mais tarde.

Claro que isto é válido desde que não se esqueçam os requisitos máximos suportados pelo Windows Server 2003 e restantes versões, e os custos que pode acarretar uma escolha demasiado sobredimensionada do servidor.

HCL

Verificar se todo o *hardware* a instalar está na HCL (*Hardware Compatibility List*) – lista em que a Microsoft coloca todo o *hardware* que é reconhecido como suportando Windows Server 2003 – o *hardware* que funciona seguramente com o Windows Server 2003. Esta lista é fornecida com o produto em manual próprio e também se encontra no CD-ROM do Windows Server 2003 e do Windows 2000 Server (na pasta **\support/**, ficheiro ***hcl.txt***), bem como na respectiva página do *site* da Microsoft na Internet (http://www.microsoft.com/hcl/default.asp).

Isto não significa, obrigatoriamente, que não existam outras peças de *hardware*, com qualidade, no mercado, que não funcionem à mesma, apesar de não constarem da tal lista. Em situações como esta, deve-se verificar se os *drivers* funcionam; se isto acontecer, é porque o *hardware* é compatível.

Arquitectura do disco

Como já foi referido nos requisitos, aconselham-se discos SCSI e respectivas controladoras, *Ultra Wide*, de preferência, de modo a garantir um bom desempenho do computador-servidor. Podem existir discos IDE e SCSI num mesmo servidor, embora, nestes casos, se devam escolher os discos e as controladoras mais rápidos e repartir os ficheiros mais usados por discos independentes.

Mirrors (Espelho)

Um *mirror*, ou espelho, de um disco ou partição, mais não é do que uma duplicação do disco e partição, em que o segundo disco é uma cópia fiel do primeiro. Caso um dos discos avarie, o outro continua a trabalhar sem que os utilizadores notem paragem do servidor. Após a detecção, é possível retirar o disco avariado, retirando, ou seja, "partindo" o *mirror* dos discos e, depois, colocar um novo disco e fazer novamente o *mirror* do disco, em que será feita uma cópia integral para o novo disco.

Fig. 3.17 Espelho de discos

Este tipo de opção é interessante na altura de substituir os discos existentes no servidor por outros de maior capacidade, sem ter de reinstalar o sistema operativo.

2.4. Software

O coração de um computador é o seu sistema operativo: o *software* que controla o seu *hardware*. Como o nome indica, o sistema operativo opera o computador. É ele que carrega aplicações para a memória do computador, corre essas aplicações e controla os dispositivos periféricos, como discos e impressoras, e serve de interface com os utilizadores.

Drivers da controladora de disco

Os *drivers* para as mais importantes controladoras de disco encontram-se no *software* de configuração (*setup*). Se, porventura, surgirem alguns problemas de reconhecimento dos mesmos, é sempre bom ter por perto uma disquete que contenha esses *drivers*, para os carregar sempre que necessário, durante o processo inicial de instalação (ecrã azul – tecla **F6**).

Fig. 3.18 Seleccionar **F6** para se escolher os *drivers* das novas controladoras.

Fig. 3.19 Seleccionar a disquete com o *driver* da nova controladora.

Disk cache (*Cache* de disco)

O sistema intitulado *Disk cache* deve ser activado no caso de se pretender fazer uma instalação a partir do DOS ou do Windows 3.1., antes mesmo de se iniciar a instalação, para aumentar a velocidade de carregamento dos ficheiros de instalação. Para configurar o SMARTDRIVE, basta digitar o comando **SMARTDRV.EXE 8192**, no ficheiro ***autoexec.bat***, e reiniciar o computador.

Setup Disks

A maneira mais rápida de instalar o Windows Server 2003 e o Windows 2000 Server é, como já foi dito, através do CD de instalação, principalmente se o disco não estiver formatado ou particionado. Mas imagine-se o caso de o computador não permitir um arranque através do CD-ROM. Neste caso, com o **Windows 2000 Server** tem-se a possibilidade de se proceder à instalação por meio de um conjunto de quatro disquetes de arranque – os *setup disks* – que contêm o *software* de instalação e permitem iniciar a instalação ou uma reparação, acedendo ao CD-ROM depois de efectuado o carregamento dos respectivos *drivers*.

Caso não se tenham essas disquetes, que, normalmente, vêm no CD-ROM de instalação do Windows 2000 Server, não é caso para desespero! Estas disquetes, chamadas *setup boot disk* e *setup disk* 2, 3 e 4, podem ser criadas executando-se o seguinte comando (sendo **d:** a *drive* que contém o CD de instalação):

d:\bootdisk\makeboot.exe a:

Depois é só colocar a primeira disquete (*setup boot disk*) na *drive* de disquetes e ligar o computador.

Atenção: Antes de criar as disquetes, convém ter a certeza que elas estão formatadas, e deve-se configurar a BIOS do computador para realizar o arranque pela *drive* de disquetes.

No **Windows Server 2003** não existe esta possibilidade de se criar as disquetes de arranque. Se pretendermos arrancar por disquetes, temos de as criar a partir do CD-ROM de instalação do Windows 2000 Server, ou utilizar uma disquete de arranque do Windows 98 que contenha os *drivers* do leitor de CD-ROM, para que este seja reconhecido, ou, ainda, com uma disquete de MS-DOS com os *drivers* do leitor de CD-ROM.

Serviços a instalar

Os serviços disponibilizados pelo SO Windows Server 2003 ou pelo Windows 2000 Server são *software* com várias funções e muitas tarefas úteis e específicas. No entanto, no processo de instalação devem apenas instalar-se aqueles serviços essenciais para a instalação, de modo a evitar possíveis complicações. Qualquer outro serviço poderá ser instalado posteriormente, através do ícone **Adicionar/Remover Programas**.

Software aplicacional

Software aplicacional são todas as aplicações que terão de ser reinstaladas após a instalação (e não *upgrade*) do Windows Server 2003 ou do Windows 2000 Server, dado que as aplicações registam informação relevante no *registry*, pelo que não estarão convenientemente configuradas após a instalação do SO.

Executáveis de instalação

Pode iniciar-se a instalação do Windows Server 2003 ou do Windows 2000 Server por meio de um dos seguintes comandos:

- **winnt.exe** – executável de 16 bit que inicia a instalação a partir do DOS, Windows 3.1 ou do Windows for Workgroups;
- **winnt32.exe** – executável de 32 bit que inicia a instalação a partir do Windows NT, do Windows 9x ou de uma versão do Windows 2000 previamente instalada.

É claro que, ao iniciar uma instalação por meio do CD-ROM ou a partir do arranque com os *setup disks* criados a partir do CD-ROM de instalação do Windows 2000 Server, não é necessário escolher um dos executáveis, visto o *setup* se iniciar automaticamente.

2.5. Processo de instalação

Modos de arranque

Por modos de arranque entendem-se os vários processos que podem ser usados para dar início à instalação do Windows Server 2003 e do Windows 2000 Server. Então, pode-se arrancar:

- **a partir do CD-ROM**. Neste caso, basta configurar o BIOS, colocar o CD na respectiva *drive* e arrancar com o computador. A vantagem consiste em se poder iniciar a instalação mesmo que o disco não esteja particionado ou formatado;
- **a partir do CD-ROM, sobre o Windows 9x/NT/2000 Professional/XP**. Neste caso, basta colocar o CD na *drive* e seleccionar a opção de instalação;
- **com disquetes e depois partir do CD-ROM**. Esta situação (ver *Setup disks*) é útil quando o computador não consegue arrancar a partir do CD-ROM. Então, coloca-se a primeira disquete de instalação na *drive* **a:** e o CD na *drive* de CD-ROM.
  No Windows 2000 Server, estas disquetes podem ser criadas a partir do CD-ROM do sistema operativo (já analisado anteriormente).
  O CD-ROM do Windows Server 2003 não inclui a possibilidade de se criar disquetes de arranque, mas pode-se utilizar uma disquete de arranque do MS-DOS com os *drivers* do leitor de CD e arrancar com o ficheiro **d:\i386\winnt.exe**, sendo **d:** a *drive* do CD-ROM;
- **a partir de um *share* na rede**. Com este modo é possível iniciar a instalação através de uma ligação, em rede, a um servidor que tenha uma cópia dos ficheiros de instalação (em pasta partilhada) ou um CD-ROM;
- **a partir de uma cópia residente no disco**. Este modo é útil por reduzir o tempo total da instalação, bastando para isso copiar o conteúdo da pasta (*folder*) **\i386** para uma partição do disco.

Tipos de instalação

Pode-se instalar o Windows Server 2003 de várias maneiras e há múltiplas opções e requisitos de sistema para cada método de instalação.

- **Instalar um novo sistema operativo**, ou seja, fazer a instalação num servidor que nada tem instalado.
- Fazer a **instalação num computador que já tenha um sistema operativo Microsoft instalado**. A instalação do Windows Server 2003 seria realizada numa partição ou num disco que não tenha nenhum sistema operativo já instalado. Assim, no arranque do computador, é possível optar pelo sistema operativo a arrancar.
- Fazer a **instalação a partir de uma actualização** (*upgrade*) de um servidor que já tenha instalado o Windows 2000 Server ou o Windows NT 4.0 Server.

Antes de iniciar a instalação, falta ainda obter a **licença** do sistema operativo. No caso do Windows Server 2003, é necessário comprar um CD-ROM com o sistema operativo, que, por sua vez, inclui o respectivo número de licença. À semelhança do Windows XP, a Microsoft tenta combater a pirataria utilizando uma protecção adicional e, além do número de série, é necessário **activar o produto**, para que este funcione. Esta activação é feita automaticamente, caso se possua Internet, ou via telefone para a Microsoft. Em ambos os casos é verificado se o número de série do Windows não foi já "activado" noutro computador, pois, caso isso aconteça, o Windows Server 2003 **não funciona**.

Outro detalhe relacionado com esta **chave de activação** é que ela está associada ao *hardware* do computador. Portanto, não é aconselhável fazer uma "instalação para experiência" num computador, antes de realizar qualquer *upgrade* de *hardware* (para evitar ter de telefonar para a Microsoft uma segunda vez). Claro que é possível experimentar a instalação do Windows Server 2003 numa outra máquina, mas sem que se proceda à activação do mesmo, já que a Microsoft dá 30 dias para o activar. Mas o melhor que se tem a fazer é proceder à instalação, em definitivo, na máquina desejada, já com todas as "peças" instaladas e *upgrades* de *hardware* efectuados.

Início da instalação

Como já foi referido, existem diferentes maneiras de se iniciar uma instalação de um servidor Windows Server 2003.

Vamos abordar duas opções distintas de iniciar a instalação do Windows Server 2003.

1.ª opção – vamos iniciar a instalação do Windows Server 2003 a partir de um computador com o Windows XP Professional já instalado. O novo sistema operativo será instalado numa nova partição a criar durante a instalação. Esta opção poderá ser interessante, caso se utilize um computador do laboratório da sala de aula ou um computador de casa, em que o objectivo é estudar e experimentar a instalação e o funcionamento do Windows Server 2003.

2.ª opção – a segunda instalação será realizada através de CD-ROM, num computador sem nenhum sistema operativo instalado e sem nenhuma partição criada no disco. Como já vimos, com acesso a um CD-ROM instalado no servidor, basta entrar no programa de configuração do BIOS, seleccionar esta opção, colocar o CD do Windows 2003, reiniciar o computador e esperar que a instalação corra automaticamente.

Este tipo de instalação é designada **instalação limpa** e é utilizada na instalação de servidores que estão a funcionar a "tempo inteiro" como servidores. Um servidor deve estar sempre ligado, para estar sempre disponível.

Instalação

Finalmente, vamos começar a instalar o Windows Server 2003 (versão portuguesa).

Mãos à obra...

1.ª opção de instalação

Instalação realizada a partir do CD-ROM, com o Windows XP Professional Português já instalado e com espaço em disco para se criar uma nova partição. A instalação será assistida pelo instalador.

Vamos ligar o computador e aguardar que o Windows XP Professional arranque completamente. De seguida, introduz-se o CD-ROM do Windows Server 2003 no leitor de CD e aguarda-se que o arranque da instalação inicie automaticamente. Caso isto não aconteça, deve-se abrir o CD-ROM e clicar duas vezes sobre **setup.exe**, que se encontra na raiz do CD-ROM, e aparece a janela da figura 3.20.

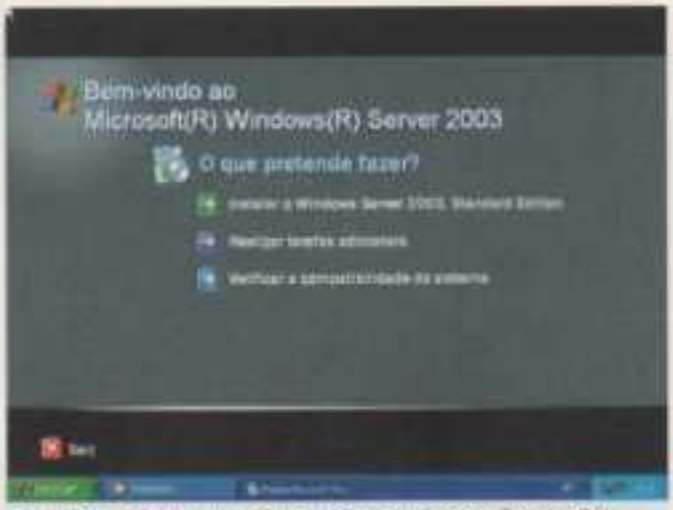

Fig. 3.20 Menu que surge após a inserção do CD-ROM de instalação do Windows Server 2003.

Fig. 3.21 Clicar em **OK** para realizar nova instalação.

A terceira opção, **Verificar a compatibilidade do sistema**, serve para fazer um diagnóstico ao computador. Seleccionada esta opção, pode-se escolher entre visitar o *site* da Microsoft ou verificar automaticamente a compatibilidade do sistema operativo.

Feito o diagnóstico, e estando certos de que se deseja instalar o Windows Server 2003, clica-se na opção **Instalar o Windows Server 2003, Standard Edition**, e salta-se para o ecrã da figura 3.21.

Neste tipo de instalação, a sequência de arranque do BIOS da placa-mãe do computador não precisa de estar configurada para arrancar pelo leitor de CD-ROM.

Fig. 3.22 Seleccionar **Seguinte** para realizar nova instalação.

Outra opção de arranque pode ser feita clicando duas vezes no ficheiro **d:/i386/WINNT32.EXE**, e surge também a janela da figura 3.21.

Como se está a instalar o Windows Server 2003 a partir do Windows XP Professional, não é possível realizar a actualização do sistema operativo; assim, pressiona-se o botão **OK**, para continuar.

Clicar em **Seguinte**, para continuar com a nova instalação (não é possível realizar uma actualização).

Após a indicação de nova instalação, há que "ler" o contrato do uso do Windows Server 2003 e, caso se concorde com ele, escolher **Aceito este contrato** e, depois, clicar em **Seguinte**.

Imediatamente após a aceitação do contrato, temos de introduzir o número de série do Windows Server 2003 (e, como já foi mencionado, para além deste número de série, vai ser igualmente necessário, no final, um código de activação).

Fig. 3.23 Contrato da licença do Windows Server 2003

Fig. 3.24 Inserir número de série do Windows Server 2003.

Segue-se o quadro das opções de instalação. Em **Seleccione o idioma principal e a região que pretende utilizar** devem seleccionar-se o idioma e o país que se quer em primeiro lugar (idioma e país predefinido). No nosso caso, a escolha é **Português (Portugal)**.

Fig. 3.25 Selecção do idioma e do país

Caso se tenha escolhido **Opções avançadas**, na figura 3.25, pode-se indicar a pasta de origem e a de destino, ou seja, pode-se indicar o disco e a pasta em que se encontra o CD-ROM de instalação do Windows Server 2003, e o disco e a pasta em que o Windows Server 2003 vai ser instalado.

Nesta janela (fig. 3.26) é ainda possível seleccionar (forçar) a cópia dos ficheiros de instalação que se encontram no CD-ROM, para o disco rígido – **Copiar todos os ficheiros de instalação do CD do programa de configuração** –, o que ocupa mais espaço em disco, mas é conveniente para que não seja necessário estar sempre a introduzir o CD de instalação.

Na outra opção **Quero escolher a letra da unidade de instalação e a partição durante o programa de configuração**, pode-se escolher a partição do disco antes de iniciar a configuração propriamente dita.

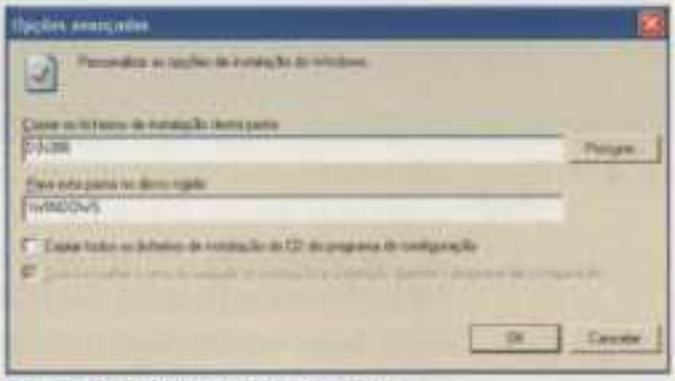

Fig. 3.26 Menu **Opções avançadas**

Na figura 3.27, seleccionar **Opções de acessibilidade** permite activar o **Microsoft Magnifier** durante a instalação. Surgirá uma janela separada e ampliada, para utilizadores com problemas de visão.

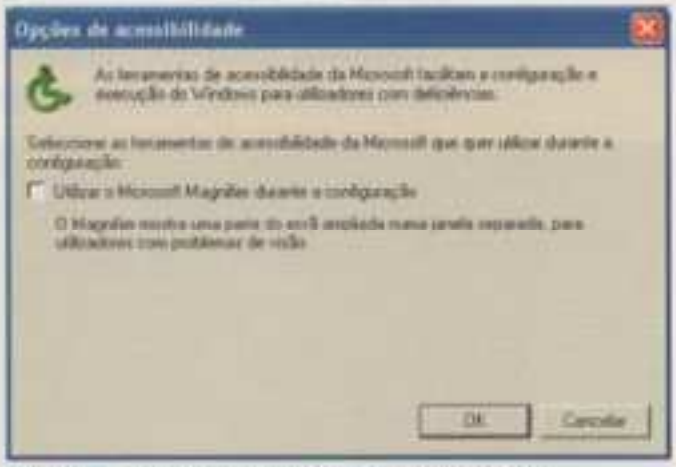

Fig. 3.27 Menu das **Opções de acessibilidade**

Voltando à figura 3.25, pressiona-se o botão **Seguinte** para continuar com a instalação.

Na próxima etapa é-nos questionado se desejamos que o programa de instalação procure eventuais actualizações do produto no *site* da Microsoft – **Sim, transferir os ficheiros de configuração actualizados (recomendado)**. Caso não se pretenda consultar o *site* da Microsoft, deve-se escolher **Não, ignorar este passo e continuar a instalar o Windows** e, logo após, **Seguinte**.

Fig. 3.28 Actualização do *software* a partir do *site* da Microsoft.

Segue-se, finalmente, o processo de instalação, que começa por um reinício do sistema. Reiniciado o computador, surgem os tradicionais ecrãs que indicam o progresso da instalação dos componentes; este processo demora uns longos minutos (tempo que difere de computador para computador).

Fig. 3.29 Evolução do tempo que falta para terminar a instalação.

Fig. 3.30 O computador vai reiniciar pela primeira vez.

No arranque do computador, caso seja solicitado, deve-se optar por arrancar pelo disco e não pelo CD-ROM; constata-se que foi instalado um menu que possibilita seleccionar se queremos arrancar com o Windows XP Professional, ou com o programa de configuração do Windows Server 2003 Standard Edition, opção 1 – **Microsoft Windows XP Professional**, e opção 2 – **Programa de configuração do Windows Server 2003, Standard Edition**, respectivamente.

Opta-se pela 2.ª opção – **Programa de configuração do Windows Server 2003, Standard Edition**, e inicia-se o processo de configuração.

Fig. 3.31 Menu de selecção do sistema operativo

Fig. 3.32 Início do processo de configuração do Windows

Vamos terminar esta opção de instalação e começar com uma segunda – **arranque por CD-ROM**. A partir deste ponto, as duas opções de instalação convergem, pelo que podemos prosseguir com a instalação na figura 3.38.

2.ª opção de instalação

Instalação do Windows Server 2003 realizada a partir de um computador sem nenhum sistema operativo instalado e sem partições criadas no disco. O arranque é realizado pelo CD-ROM e a instalação é assistida pelo instalador.

Normalmente, a instalação do Windows Server 2003 é feita por meio de um CD-ROM e é instalado num computador totalmente "limpo", isto é, sem nenhum sistema operativo instalado e sem nenhuma partição criada no disco.

Durante a instalação do Windows Server 2003, o **assistente de configuração** solicita que se realizem algumas selecções e que se forneçam determinadas informações. As seguintes descrições dos ecrãs do assistente, bem como as informações que estes pedem, deverão servir de exemplo e de ajuda.

Ao efectuar uma nova instalação, tem de se **introduzir o CD-ROM** com o sistema operativo do Windows Server 2003 no leitor de CD-ROM, e **reiniciar o computador.**

Se o computador estiver configurado para que a sequência de arranque seja pelo CD-ROM, a instalação iniciar-se-á automaticamente, senão terá de se proceder às seguintes alterações no BIOS do computador:

Arranque a partir do CD-ROM

A sequência de arranque do BIOS, geralmente, está configurada para começar por ler a disquete e o disco, isto é, numa primeira fase, deve tentar-se arrancar pela disquete e, numa segunda fase (e apenas se a primeira falhar), pelo disco rígido. Neste caso, interessa arrancar na seguinte sequência: CD-ROM, disco, disquete. Em primeiro lugar deve estar o CD-ROM, porque é aqui que se vai colocar o CD com o sistema operativo. Para proceder a esta configuração, no arranque do computador deve-se entrar para o *software* de configuração do BIOS. Existem diversas formas para entrar neste *software* e que variam de computador para computador, mas, geralmente, isto pode ser efectuado pressionando a tecla **Escape** ou **F1** ou **F2** ou **Delete**, no arranque do PC.

Depois de se entrar no *software* do BIOS, deve-se encontrar a opção da sequência de arranque. Esta opção difere, mais uma vez, de fabricante para fabricante, mas, vulgarmente, está presente sob a designação de *Boot sequence*. Depois de se ter colocado o CD-ROM no primeiro lugar dessa opção, deve-se gravar, sair e reiniciar o computador.

Fig. 3.33 Aspecto geral do menu principal do BIOS. Este menu varia consoante o modelo de *board* e fabricante.

Fig. 3.34 Aspecto geral do menu do BIOS, onde se pode alterar a sequência de arranque.

Em *boards* mais recentes, geralmente não é necessário alterar as configurações no BIOS para se forçar o arranque por CD-ROM. Logo após o arranque do computador surge, na parte inferior do ecrã, uma indicação da tecla que se deve pressionar para activar a opção de escolha de arranque. Normalmente, deve-se seleccionar a tecla **ESC**, ou **F8**, ou **F10**, ou **F12**, ou outra. Esta situação depende da placa-mãe utilizada.

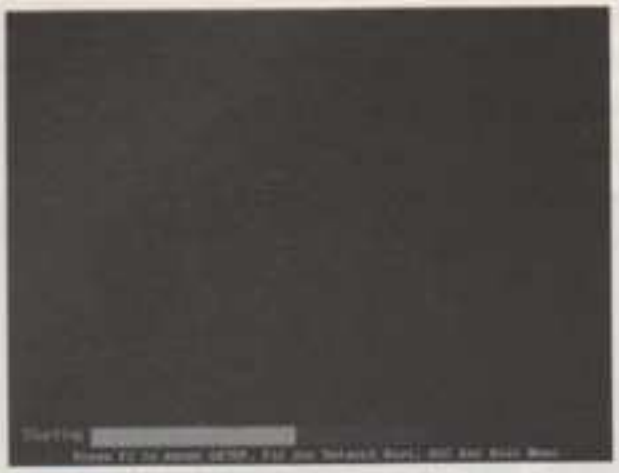

Fig. 3.35 Seleccionar **ESC** para activar o menu de escolha de dispositivo de arranque.

Fig. 3.36 Selecção de arranque a partir do CD-ROM

Após a selecção de arranque do computador através do CD-ROM, poderá ser necessário carregar em **ENTER** para arrancar.

Fig. 3.37 Caso seja necessário, pressionar **Enter** para não se arrancar por outra *drive* que não seja o CD-ROM.

O arranque da instalação e da configuração do sistema operativo será realizado por *autorun* do CD-ROM e apresenta o ecrã da figura 3.38.

NOTA:

A partir deste ponto, a configuração da instalação segue os mesmos procedimentos da opção 1 (ver figura 3.32).

Logo após o arranque, e no caso do computador ter alguma controladora SCSI ou controladora RAID em que seja necessário instalar um *driver* próprio e que não venha no CD-ROM do Windows Server 2003, deve-se pressionar **F6** no instante em que aparece, em rodapé, a informação **Prima F6 para instalar um controlador SCSI ou RAID de terceiros** (figura 3.38). Caso se pretenda seleccionar esta opção, tem de se agir rapidamente, pois ela aparece no ecrã durante poucos segundos.

Se a tecla **F6** não for pressionada, o processo de instalação continua e surge uma nova opção em rodapé: **Prima F2 para executar a "Recuperação automática do sistema" (ASR)**. Esta opção tem utilidade caso já se tenha instalado o sistema operativo no computador e o computador deixou de funcionar. Se, previamente, se tivesse criado uma disquete de recuperação, poder-se-ia utilizá-la nesta altura para recuperar o sistema.

Fig. 3.38 Início do processo de configuração do Windows

Fig. 3.39 Clicar em **F2** para executar a "Recuperação automática do sistema" (ASR).

Numa instalação corrente, não há necessidade de escolher a opção anterior. Não seleccionando nenhuma opção, obtém-se o ecrã da figura 3.40, com três opções:

- **Para configurar agora o Windows prima ENTER.**
- **Para reparar ou recuperar uma instalação do Windows, prima R.**
- **Para sair do programa de configuração sem instalar o Windows, prima F3.**

Para continuar a instalação, escolhe-se a primeira opção, pressionando **Enter**.

Aparece o contrato, que deve ser lido, e, no caso de se concordar com o mesmo, premir a tecla **F8** para continuar a instalação (figura 3.41).

Fig. 3.40 Ecrã **Bem-vindo ao programa de configuração**

Fig. 3.41 Aceitar contrato da licença do Windows.

Instalação das partições

Nesta fase da instalação existem algumas diferenças entre a 1.ª e a 2.ª opções de instalação.

Na 1.ª opção já existia uma partição criada, onde se encontrava instalado o Windows XP Professional. Nesta situação é necessário criar uma nova partição no espaço livre do disco, para que se possa instalar o Windows Server 2003.

Na 2.ª opção (a actual), não existe nenhuma partição criada, pelo que é obrigatório criar uma partição.

A partição pode ser criada seleccionando a opção **C**.

Em caso de esquecimento, convém reavivar a memória sobre partições. Este assunto foi abordado na subunidade 2.2.

Neste exemplo temos somente 6134 MB livres no disco para instalar o Windows Server 2003, pelo que estamos com pouco mais do que o espaço mínimo necessário. Quanto mais espaço disponível, melhor.

Fig. 3.42 Selecciona opção para criar nova partição.

Vamos seleccionar o tamanho máximo disponível e pressionar **Enter**, para criar a partição (figura 3.43).

Se o tamanho da partição estiver correcta, prime-se novamente **Enter**, para instalar.

Fig. 3.43 Escolha do tamanho da partição a criar.

Fig. 3.44 Instalar participação.

É necessário formatar a partição onde se vai instalar o sistema operativo. O sistema de ficheiros a usar vai ser o NTFS.

Temos duas opções para criar partições NTFS.

Na opção **Formatar a partição utilizando o sistema de ficheiros NTFS (Rápido)**, a partição é criada em NTFS, mas não é realizada uma análise ao disco. Esta opção é substancialmente mais rápida do que a que se segue.

Na opção **Formatar a partição utilizando o sistema de ficheiros NTFS**, o disco é formatado em NTFS e é feita uma verificação ao disco. Caso seja a primeira formatação, convém utilizar esta opção para verificar se é detectado algum defeito no disco.

Vamos prosseguir a criação da partição escolhendo esta última opção e pressionando **Enter**.

A formatação vai ser realizada e surge uma barra a indicar a percentagem de formatação já realizada. Temos de aguardar uns bons minutos.

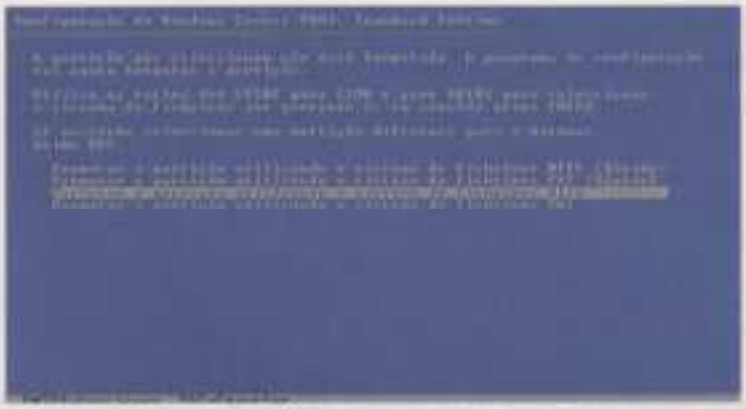

Fig. 3.45 Selecção do formato a utilizar.

Fig. 3.46 Formatação em curso. É visualizada a percentagem de formatação realizada.

Com a formatação terminada, vai dar-se início à cópia dos ficheiros na partição criada, e, mais uma vez, há que aguardar uns bons minutos.

No final da cópia dos ficheiros, o computador vai reiniciar.

Fig. 3.47 Cópia dos ficheiros para o disco rígido.

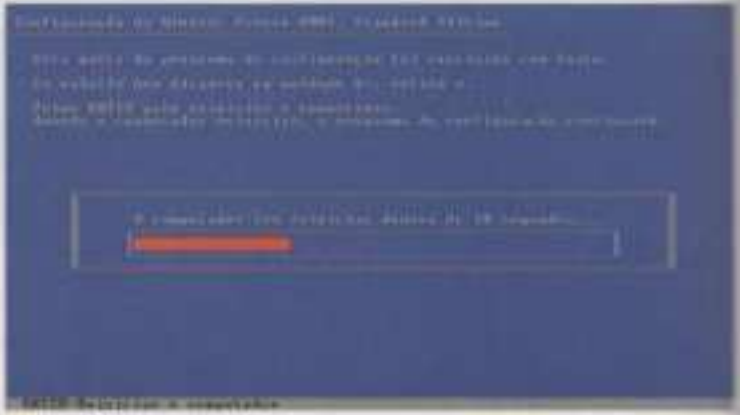

Fig. 3.48 O computador vai reiniciar.

Caso a instalação tenha sido feita a partir da 1.ª opção, esta seria a segunda vez que o servidor iria reiniciar, enquanto que, pela 2.ª opção, será a primeira vez que reinicia.

Fig. 3.49 Arranque do computador

Após o arranque, o processo de instalação continua, e é necessário aguardar mais uns minutos...

Fig. 3.50 Ecrã após arranque do computador. A instalação prossegue.

Fig. 3.51 Continuação da instalação

No ecrã **Opções regionais e de idioma**, deve seleccionar-se a língua que se está a utilizar, **português**, para que o teclado fique bem configurado.

Na figura 3.52, seleccionando a opção **Personalizar**, temos acesso às configurações regionais (moeda, data, hora, numeração, entre outras).

Fig. 3.52 Opções regionais e de idioma

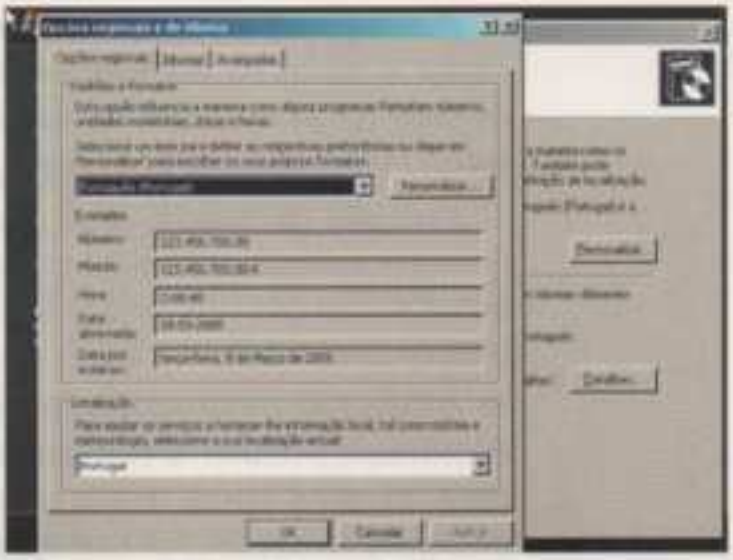

Fig. 3.53 Configuração das opções regionais

Voltando ao ecrã da figura 3.52 e seleccionando a opção **Detalhes**, temos acesso às configurações do idioma do teclado. Como a versão utilizada é a portuguesa, o teclado português é instalado por defeito. Se houver necessidade de adicionar um teclado com as configurações de outro país, deve ir-se ao novo ecrã, pressionar **Adicionar** e seleccionar o novo teclado.

Feitas as alterações, deve escolher-se **Aplicar** no ecrã da figura 3.54 e pressionar **Seguinte** no ecrã da figura 3.52.

Continuando a instalação, é necessário colocar o nome do utilizador e da empresa na qual fica registada a licença do Windows Server 2003, e, logo após, pressionar **Seguinte** (figura 3.55).

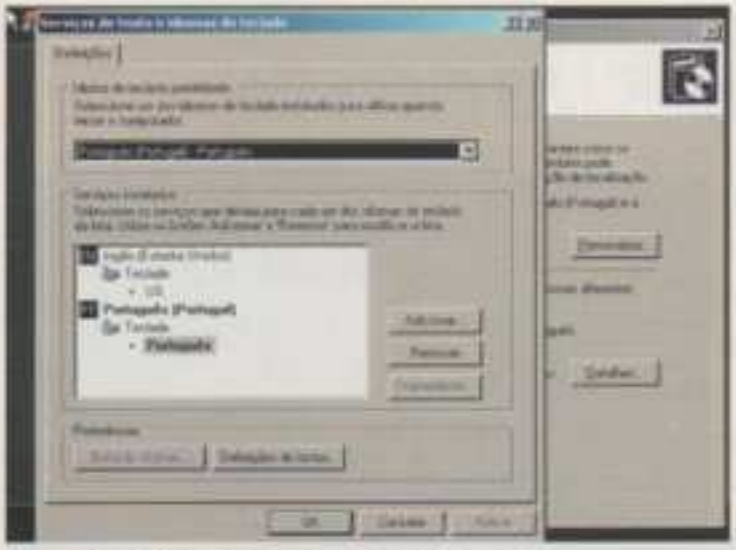

Fig. 3.54 Selecção do idioma do teclado

Fig. 3.55 Introdução do nome do utilizador e da empresa

Vai ser necessário introduzir a chave que acompanha o CD-ROM do Windows Server 2003 Standard Edition. Na 1.ª opção de instalação, esta seria a segunda vez que a chave teria de ser introduzida, enquanto que, na 2.ª opção de instalação, se trata da primeira vez.

Após a introdução da chave, se, ao clicar em **Seguinte**, surgir uma mensagem de erro, deve-se verificar se não houve engano na introdução da chave (figura 3.56).

A chave foi introduzida correctamente. A fase que se segue serve para seleccionar o modo de licenciamento. Antes da escolha do modo de licenciamento, deve-se recordar o que foi estudado na subunidade **2.1. Planeamento da instalação**, no ponto **Tipos de licença**.

Em caso de dúvida, deve ser escolhida a **licença por servidor** (*per server*) e deve ser indicado o número de licenças de cliente (CAL) que se possui. Podem-se adquirir licenças adicionais de cliente e, nesta opção, deve colocar-se a soma total de licenças (figura 3.57).

O modo de licenciamento **Por dispositivo ou por utilizador** (*per seat*) só deve ser escolhido se houver a certeza absoluta do que se está a fazer, dado que não é possível, mais tarde, mudar de modo de licenciamento. O contrário é possível – mudar do modo de licenciamento de **licença por servidor** para licenciamento **Por dispositivo ou por utilizador**.

Fig. 3.56 Introdução da chave do Windows Server 2003 Standard Edition

Fig. 3.57 Selecção do modo de licenciamento

No ecrã da figura 3.58 introduz-se o nome do computador e a palavra-chave do administrador, que terá de ser introduzida duas vezes, para garantir que não há enganos (esta palavra-chave deve ser guardada em local seguro e deve-se também verificar se foram utilizadas letras maiúsculas ou minúsculas).

No Windows Server 2003 é exigida a palavra-chave do administrador, pois este utilizador é que irá ter permissão para fazer todas as alterações ao sistema operativo. Para o trabalho corrente, mais adiante vão ser criados outros utilizadores com permissões limitadas, para aumentar a segurança do sistema operativo. Deve-se ainda criar um utilizador com permissões de administrador, que será o utilizador usado para administrar o sistema. O utilizador "administrador" deve ser utilizado o menos possível, para que não seja usado indevidamente.

Para prosseguir com a instalação, escolher **Seguinte**.

ATENÇÃO: Se a versão utilizada do Windows Server 2003 for a inglesa, o utilizador administrador chama-se ***administrator***.

Se, após a introdução da palavra-chave do administrador, aparecer a janela da figura 3.59, é dada a indicação de que esta, por questões de segurança, não foi criada tendo em atenção os seguintes factores:

- deve ser composta por 6 caracteres ou mais;
- não pode conter os caracteres **Administrador** ou **Admin**;
- deve conter letras maiúsculas, minúsculas e números;
- não podem ser usados caracteres não alfanuméricos, por exemplo: #, &, ~, etc.

Por questões de segurança, deve-se optar por seleccionar **Não**, para se introduzir uma nova palavra-chave que respeite os factores mencionados anteriormente.

Se for escolhido **Sim**, a instalação vai prosseguir com a palavra-chave introduzida inicialmente.

Fig. 3.58 Introdução do nome do computador e da palavra-chave do administrador

Fig. 3.59 Possibilidade de introduzir nova palavra-passe do administrador para melhorar a segurança.

No passo seguinte, temos a possibilidade de ajustar o relógio existente na placa-mãe do computador. Podemos acertar a hora, a data e o fuso horário, seleccionando o meridiano de Greenwich.

Para continuar com a instalação, deve-se clicar em **Seguinte**.

Nesta fase da instalação pode-se fazer uma pausa, visto a instalação demorar um pouco até que solicite nova configuração.

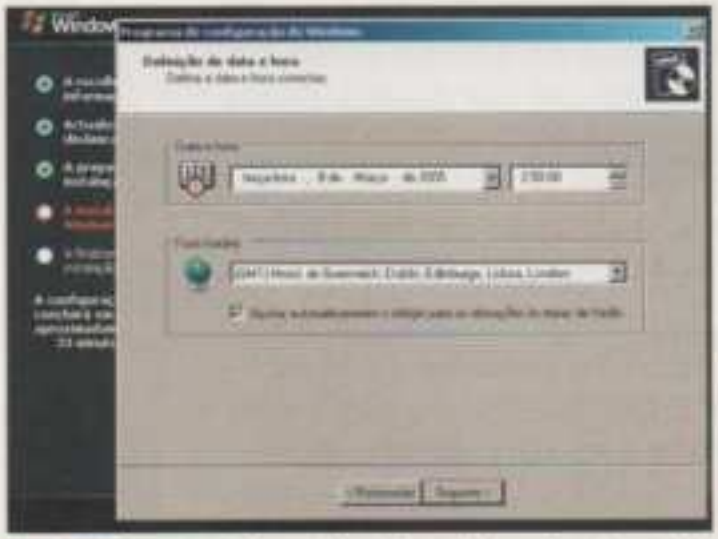

Fig. 3.60 Acerto da hora, da data e do fuso horário relativamente ao meridiano de Greenwich

Fig. 3.61 A instalação do Windows Server 2003 está em curso

Antes da instalação ter iniciado, foi introduzida, neste computador, uma placa de rede compatível com o Windows Server 2003. Se tudo correu bem, o sistema detecta e instala os *drivers* da placa de rede.

Nesta fase (figura 3.62) podemos optar por seleccionar:

- **Definições típicas**
- **Definições personalizadas**.

Na primeira opção, a instalação prossegue sem que se configure o protocolo TCP/IP (esta opção poderá ser realizada após a instalação do sistema operativo). A instalação continua no ecrã da figura 3.65.

Na segunda opção, temos a possibilidade de se configurar, nesta fase, o protocolo TCP/IP.

Neste exemplo, vamos optar por escolher a opção **Definições personalizadas** e clicar em **Seguinte**, para se configurar o protocolo TCP/IP.

Tendo em conta o que foi estudado na subunidade **2.1. Planeamento da instalação**, vamos configurar o nosso servidor com o endereço IP fixo **192.168.1.1** e com a máscara **255.255.255.0**. Neste caso, o endereço da rede é dado pelos 3 primeiros bytes – **192.168.1** –, enquanto que o último byte define o endereço de cada *host*. O endereço de rede é igual em todos os *hosts*, mas cada *host* tem de ter um endereço diferente.

- Endereço da nossa rede: **192.168.1**
- Endereço do nosso servidor: **1**

Fig. 3.62 Definições de rede

Os endereços disponíveis na nossa rede vão de 2 a 254 (o 0 e 255 não podem ser utilizados e o 1 vai ser ocupado pelo nosso servidor).

A configuração do endereço IP é realizada pressionando **TCP/IP (Protocolo Internet)** e, de seguida, **Propriedades** (figura 3.63).

Para se introduzir o endereço do nosso servidor, deve-se clicar em **Utilizar o seguinte endereço IP:**, para que os campos **Endereços IP** e **Máscara de sub-rede** fiquem activos (figura 3.64). Após a introdução do endereço e da máscara tem de se pressionar em **OK**, no ecrã que se segue, para se validar a introdução do endereço. Voltamos ao ecrã da figura 3.63 e, para continuar com a instalação, clica-se sobre **Seguinte**.

Fig. 3.63 Configuração do protocolo TCP/IP

Fig. 3.64 Introduzir o endereço IP fixo.

Para mais informação sobre a configuração do TCP/IP, deve-se consultar a subunidade **2.1. Planeamento da instalação**, no ponto **Protocolos**.

Na janela da figura 3.65 vamos atribuir, na primeira opção, o nome ao grupo de trabalho a que o nosso servidor vai pertencer na rede. O nosso servidor fica a funcionar como *Standalone Server*, isto é, o servidor vai pertencer a um grupo de trabalho existente e, no nosso caso, vai criar um novo grupo de trabalho, dado que ainda não foi introduzido nenhum computador na nossa rede.

Se existisse algum domínio na nossa rede, podíamos associar este servidor ao existente e ficava a funcionar como *Member Server*. Para isso ter-se-ia de escolher a segunda opção: **Sim, fazer este computador membro do seguinte domínio**.

Fig. 3.65 Selecção do grupo de trabalho ou domínio

Aconselha-se uma revisão à subunidade **2.1. Planeamento da instalação**, no ponto **Papel dos servidores.**

Após a introdução do grupo de trabalho, escolhe-se **Seguinte**, para continuar com a instalação.

A partir deste momento, pode-se fazer um novo intervalo, pois, mais uma vez, a instalação vai demorar um bom bocado. No fim da instalação, o computador reinicia automaticamente.

Fig. 3.66 Continuação da instalação do sistema operativo

Fig. 3.67 Instalação a terminar

Finalmente, o servidor termina a instalação e vai reiniciar automaticamente.

A instalação do sistema operativo pode ter terminado, mas, em termos de servidor, ainda há muito trabalho a realizar. O nosso servidor ainda não foi promovido a controlador de domínio (*Domain Controller* – DC).

Primeiro arranque

Fig. 3.68 Arranque do servidor após a instalação

Após uma longa espera, o computador vai arrancar pela primeira vez com o sistema operativo instalado.

Se a instalação foi realizada a partir da 1.ª opção, existirão dois sistemas operativos no mesmo computador, em partições diferentes (Windows XP Professional e Windows Server 2003). No arranque surgirá um menu a solicitar qual o sistema operativo que se pretende que arranque. Se o operador não seleccionar nenhum, por defeito arrancará, ao fim de alguns segundos, o Windows Server 2003. Se o operador usar as setas para

escolher o sistema operativo, o temporizador pára. O carregamento do sistema operativo só se efectuará caso se pressione **Enter**.

Se a instalação for realizada pela 2.ª opção, não aparece o menu indicado anteriormente e o Windows Server 2003 arranca automaticamente.

Primeiro *Logon*

Após o surgimento da janela **Bem-vindo ao Windows**, é necessário carregar em **CRTL+ALT+DEL**, para termos acesso à janela de **introduzir o nome do utilizador e a palavra-passe**.

Caso não se consiga entrar, deve-se verificar se o **Caps Lock** está activo, ou não, e ter cuidado com as letras maiúsculas e minúsculas; deve também verificar-se, novamente, se o nome do utilizador está correcto.

Não esquecer: se a versão do Windows Server 2003 for a inglesa, o nome do utilizador administrador é **Administrator**.

Fig. 3.69 Introdução do primeiro *Logon*

Fig. 3.70 Introdução do nome do utilizador e da palavra-passe

Depois de instalado o Windows Server 2003 Standard Edition, surge um novo ambiente de trabalho. A primeira imagem que aparece é a de um ecrã "limpinho", sem quaisquer ícones, a não ser o da **Reciclagem**, e uma janela com um gestor do servidor. No fundo aparece uma barra de ferramentas colorida que, aparentemente, nada tem de novo; à direita, os ícones das aplicações residentes; no centro, as aplicações abertas; e, à esquerda, o botão **Iniciar**.

Fig. 3.71 Ambiente de trabalho após conclusão da instalação do Windows Server 2003

Verificar se o *hardware* está correctamente instalado

Para se verificar se os *drivers* estão correctamente instalados, é necessário ir ao menu **Iniciar** e ao **Painel de controlo**. Dentro do **Painel de controlo**, selecciona-se **Sistema**.

Na janela **Propriedades do sistema**, selecciona-se o separador **Hardware**.

Fig. 3.72 Abrir **Sistema** no **Painel de controlo**.

Fig. 3.73 Janela **Propriedades do sistema** – separador **Hardware**

Fig. 3.74 Ecrã com o estado dos *drivers* do *hardware*

No separador **Hardware**, clica-se sobre **Gestor de dispositivos** e fica-se com um acesso a uma janela, idêntica à do Windows 9x, 2000 Professional, XP e Windows 2000 Server. Se surgir algum *driver* com um ponto de interrogação, de exclamação ou com um "x" a vermelho ou a amarelo, somos informados que o *driver* está mal instalado e que o *hardware* correspondente não funciona. **Para resolver este problema** deve-se verificar se o *hardware* está correctamente instalado (fisicamente) ou se os *drivers* estão correctos. Um *driver* de um determinado *hardware* pode funcionar no Windows XP, mas pode não trabalhar correctamente no Windows Server 2003. É necessário ter os *drivers* adequados para o sistema operativo a utilizar. O processo de instalação não diverge do do Windows XP, estudado no 10.º Ano.

Neste exemplo existe um controlador que não está bem instalado – **Controladores multimédia de áudio** –, visto encontrar-se um ponto de interrogação e de exclamação a indicar o defeito.

Registo do Windows Server 2003

Tal como acontece com a maioria dos sistemas operativos da Microsoft, também é possível, opcionalmente, fazer o registo do Windows Server 2003 por telefone, pelo envio de um impresso próprio preenchido que vem com o produto, ou *online*, via Internet. Este último método tem a vantagem de ser mais rápido e fácil de registar. No entanto, o Windows Server 2003 não fica por aí. Para além do registo mencionado, e no intuito de evitar possíveis piratarias, a Microsoft introduziu, já a partir do Windows e do Office XP, um novo método de activação. Para se activar o produto, este cria uma chave (*hash key*), que depois tem de ser enviada para a Microsoft. Através dessa chave, a Microsoft consegue verificar se o produto já fora activado em outras ocasiões ou não (baseado nas licenças adquiridas para

o produto), e, se tudo estiver legalmente em ordem, envia uma informação ao PC que está registado com o produto e esta informação é usada sempre que se reinicia o computador para verificação e confirmação do respectivo registo. Sempre que se procede a um *upgrade* em que se torna necessário activar novamente o Windows, é necessário avisar a Microsoft desta situação.

A Microsoft faculta-nos 30 dias para se proceder à activação do Windows Server 2003, permitindo poder decidir pela instalação do Windows Server 2003 num outro computador, por exemplo, ou, dada uma possível "lentidão", preferir fazer um *upgrade* (para um novo processador, por exemplo).

Vamos, então, ver como se regista o Windows Server.

O acesso à janela de activação é feito a partir do menu **Iniciar > Programas** e **Activar o Windows**.

Para fazer a activação, tudo o que se tem a fazer é seleccionar uma das opções da figura 3.76:

a) **Sim, activar o Windows através da Internet agora.**

b) **Sim, pretendo telefonar a um representante da assistência a clientes para activar o Windows.**

c) **Não, lembrar-me de activar a cópia do Windows periodicamente.**

Fig. 3.75 Chamar janela de activação do Windows.

Caso se opte por realizar a **activação do Windows pela Internet**, é necessário ter-se configurado o acesso à Internet.

Caso o campo seleccionado seja o primeiro da figura 3.76, vai surgir uma nova janela (figura 3.77), com duas opções:

a) **Sim, pretendo efectuar o registo e activar o Windows ao mesmo tempo.**

b) **Não, não pretendo efectuar o registo agora, quero apenas activar o Windows.**

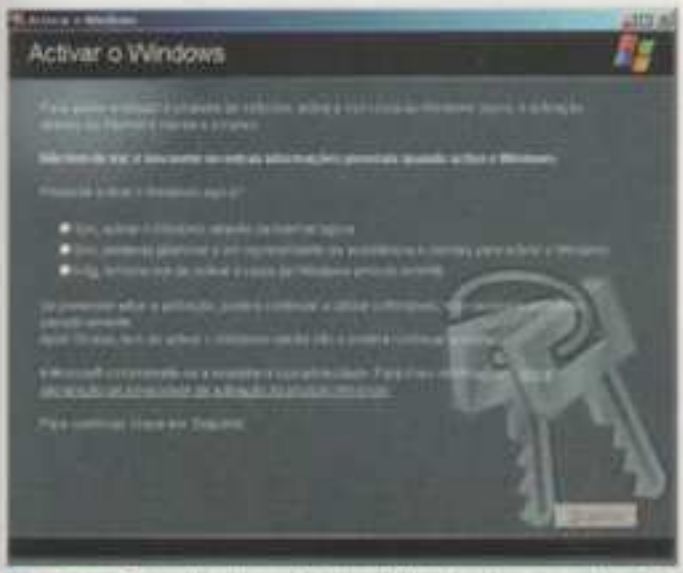

Fig. 3.76 Escolha do método utilizado para a activação do Windows

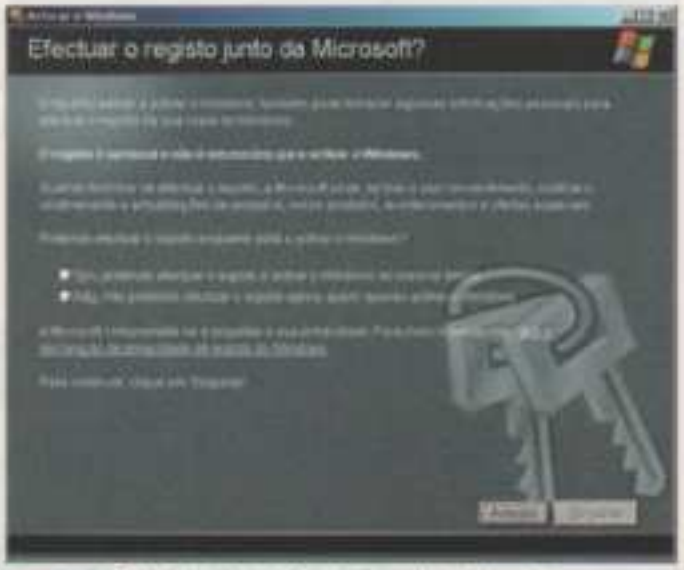

Fig. 3.77 Registo da activação pela Internet

A selecção do primeiro campo da figura 3.77 vai abrir uma nova janela, onde temos acesso à introdução dos nossos dados para o registo. Depois, basta pressionar **Seguinte** para ser feita a ligação à Internet, enviar os dados preenchidos no registo e fazer a activação do Windows.

Fig. 3.78 Preenchimento dos dados do registo do Windows

Se, na janela da figura 3.77, se optar por escolher o segundo campo, será realizada somente a activação do Windows via Internet.

Em ambas as situações é necessário ter o servidor configurado para ter acesso à Internet.

Voltando à janela da figura 3.76, pode-se realizar o registo e a **activação por telefone**. Para isto, selecciona-se o segundo campo dessa janela: **Sim, pretendo telefonar a um representante da assistência a clientes para activar o Windows.**

Abre-se uma nova janela, onde vamos escolher o país (passo 1), que, no nosso caso, é Portugal. Automaticamente, no passo 2, surge o número de telefone para onde devemos ligar para solicitar o código de activação e, no passo 3, é gerado um código que teremos de fornecer via telefone. Com este código, a Microsoft fornecerá o código do ID, que será preenchido no passo 4. Ao fazer **Seguinte** será realizada a activação.

É necessário não esquecer que, se realizarmos nova instalação do sistema operativo, é gerado um novo código, logo, teremos de activar novamente o Windows.

Fig. 3.79 Activação do Windows por telefone

Fig. 3.80 Alterar chave do Windows.

Se, durante a instalação do Windows Server 2003, for erradamente introduzida a chave do Windows (ver figura 3.56), podemos introduzir o novo registo e, de seguida, activar o Windows. A realização desta tarefa pode ser efectuada clicando em **Alterar chave de produto**, na figura 3.79, colocar a nova chave na figura 3.80 e depois clicar em **Actualizar**.

Caso se opte por não realizar a activação do Windows, pode-se seleccionar o último campo da janela da figura 3.76 e clicar em **Seguinte**. Com esta opção, o sistema operativo vai-nos informando dos dias que faltam para realizarmos a activação.

Pode-se ir adiando a activação, mas a mesma terá de ser feita no **prazo máximo de trinta dias.**

Em caso de dúvidas, encontra-se tudo explicado na **Ajuda** do Windows. Para aceder à **Ajuda**, deve pressionar-se o botão que tem um ponto de interrogação. É

aconselhável que se consulte a **Ajuda**, nem que seja para verificar como é interactiva, pois o botão vai assumindo outros ecrãs/imagens e vai circulando pelo ecrã, até ao ponto onde se deseja obter ajuda.

Promoção a *Domain Controller*

Ponto da situação: Após a instalação do sistema operativo, este ficou a funcionar como *Standalone Server*, isto é, o servidor passou a pertencer a um grupo de trabalho existente e, no nosso caso, criou um novo grupo de trabalho, dado que ainda não foi introduzido nenhum computador na nossa rede.

Para que o servidor tenha o papel de controlador de domínio (*Domain Controller*), vamos ter de o promover, ou seja, configurar o servidor para que este fique a funcionar como servidor de topo da floresta e como único *Domain Controller* da floresta, dado que, quando se promover este servidor a *Domain Controller*, ainda não existirá nenhuma floresta.

Aconselha-se uma revisão da subunidade 2.1. **Planeamento da instalação**, no ponto **Papel dos servidores**.

Ao instalar o servidor como o primeiro controlador de domínio de um domínio, este vai ser configurado não só como controlador de domínio (DC), mas também como servidor DDNS. Esta é uma das razões pela qual é necessária a utilização do TCP/IP.

A promoção do servidor a controlador de domínio (DC) exige a instalação do *Active Directory*. A instalação do *Active Directory* só é possível se for instalado num volume que esteja formatado em NTFS V5.

O início da instalação do *Active Directory* é executado a partir da caixa de diálogo **Executar**, correndo o comando **dcpromo.exe**. O acesso a esta caixa de diálogo pode ser realizado a partir do menu **Iniciar** e, depois, seleccionar **Executar**.

Executar comando **dcpromo.exe** para se iniciar a instalação do *Active Directory*. Se for escrito somente **dcpromo**, o processo de instalação também é iniciado.

Fig. 3.81 Acesso à caixa de diálogo **Executar**

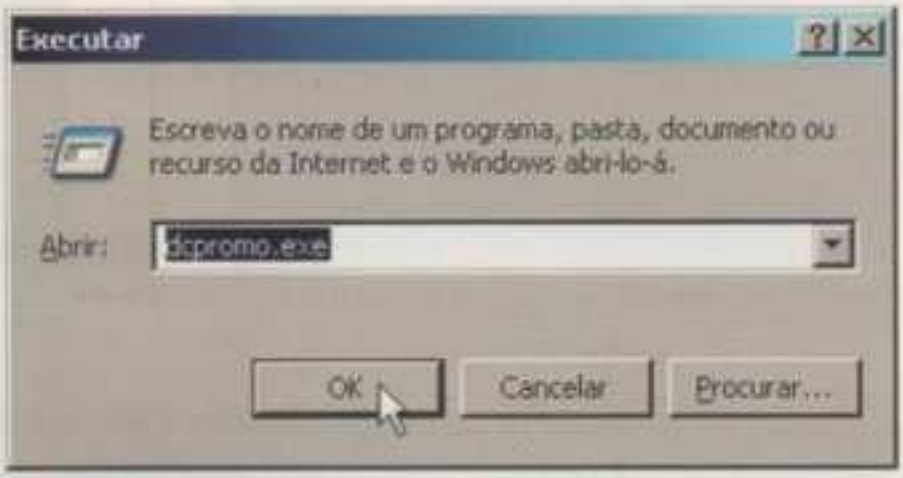

Fig. 3.82 Executar comando **dcpromo.exe**.

Surge uma caixa de diálogo a dar-nos as boas-vindas à instalação do *Active Directory*. Para se prosseguir com a instalação, deve-se clicar em **Seguinte**.

Fig. 3.83 Início do Assistente de instalação do Active Directory

Na janela que se segue, surge um quadro que nos informa das incompatibilidades existentes das versões mais antigas do Windows com os domínios criados pelo Windows Server 2003.

As versões do Windows 95 e do Windows NT 4.0, com *Service Pack* 3 ou inferior, não conseguirão ligar-se ao domínio ou obter recursos do mesmo.

Basicamente, as versões do Windows 95 e do Windows NT 4.0, com SP3 ou inferior, não têm, por defeito, encriptação das palavras-passe, e, por questões de segurança, um domínio criado pelo Windows Server 2003 só aceita palavras-passe encriptadas. Para obter mais informação sobre a incompatibilidade, deve-se clicar em **Ajuda de compatibilidade** e, para continuar com a instalação, deve-se clicar sobre **Seguinte**, na janela da figura 3.84.

Fig. 3.84 Indicação de incompatibilidades

Fig. 3.85 Ajuda sobre compatibilidade com sistemas operativos mais antigos

Na caixa de diálogo da figura 3.86, podemos seleccionar:

- **Controlador de domínio para um novo domínio**
- **Controlador de domínio adicional para um domínio existente**

Vamos seleccionar a primeira opção, para criar um novo domínio, uma nova árvore e uma nova floresta. Este servidor será o primeiro controlador de domínio (DC) do novo domínio. Após a selecção deve-se pressionar **Seguinte**, para continuar.

Na nova janela (figura 3.87), temos de escolher a primeira opção, para se criar o **domínio numa nova floresta**, e escolher **Seguinte**, para continuar com a instalação.

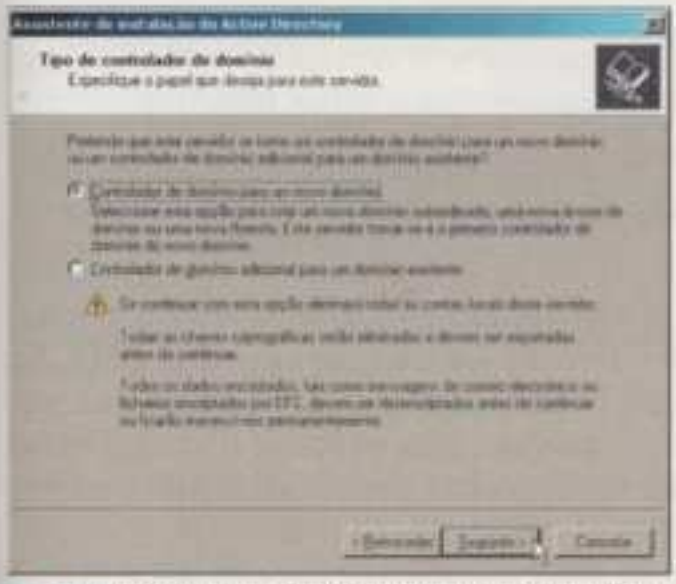

Fig. 3.86 Escolha do tipo de controlador de domínio (DC)

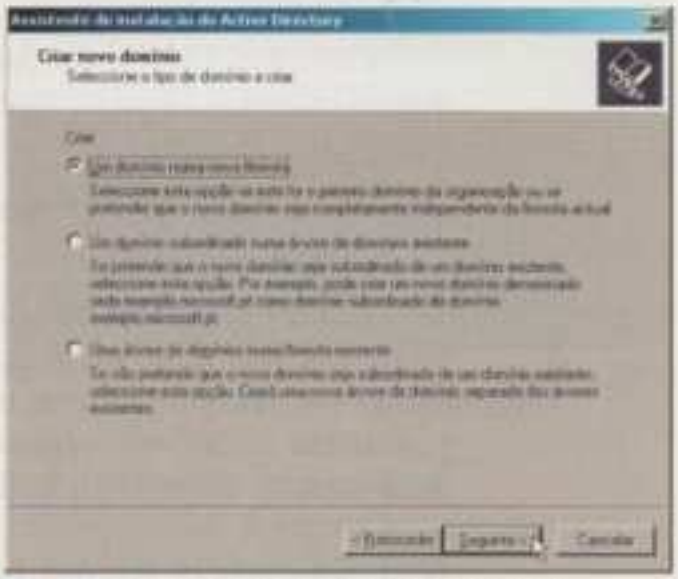

Fig. 3.87 Selecção do tipo de domínio a criar

O DNS faz parte do *Active Directory*, pelo que este serviço tem de estar instalado localmente ou noutro servidor da rede. Se existir um só servidor na rede, como é o nosso caso, temos de optar pela segunda opção para se instalar e configurar o DNS neste servidor (figura 3.88).

O passo que se segue serve para introduzir o nome de DNS do novo domínio (figura 3.89). Se o nosso servidor estivesse ligado directamente à rede Internet, o nome do domínio tinha de ser previamente registado na FCCN (Fundação para a Computação Científica Nacional), caso o domínio fosse do tipo **.pt**. Se o domínio foi do tipo **.com** ou **.net**, etc., o registo tinha de ser realizado na IbterNIC ou na *Network Solutions* ou em outra instituição equivalente.

Como o nosso servidor não está ligado directamente à Internet, mas somente à nossa rede local (LAN), não é necessário registar o nome do domínio.

Após a introdução do nome do domínio, vamos seleccionar **Seguinte**, para continuar com a instalação.

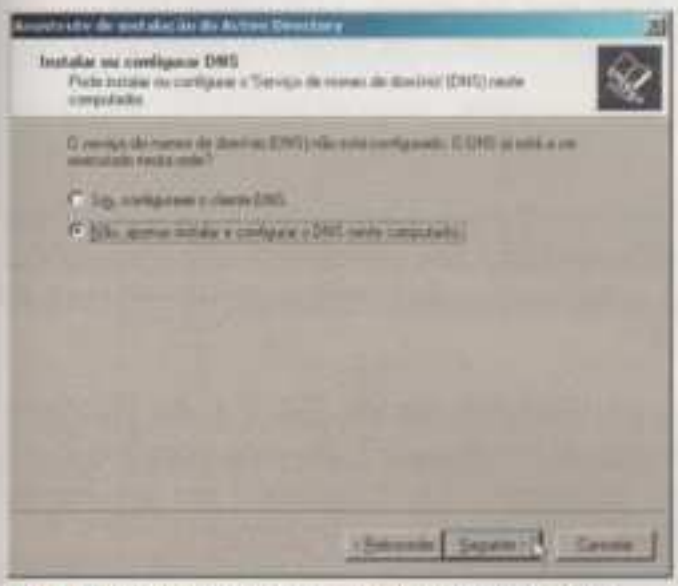

Fig. 3.88 Configuração e instalação do novo DNS

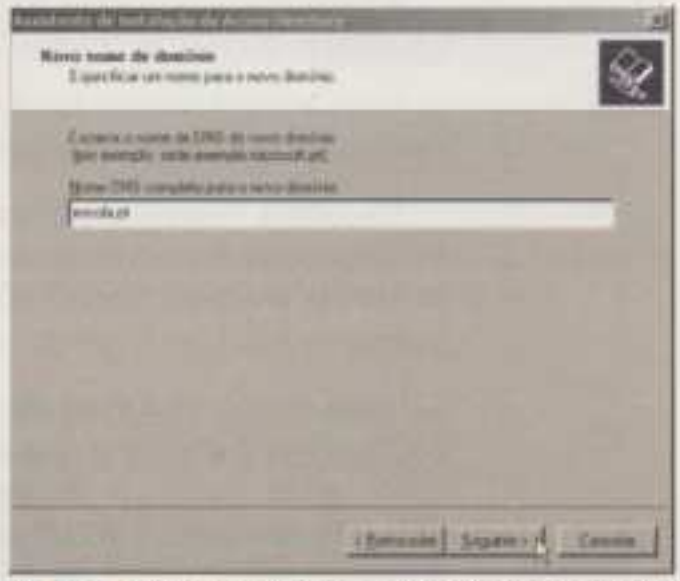

Fig. 3.89 Especificação do nome de DNS do novo domínio

Após a conclusão da instalação do nome do domínio, devemos introduzir o nome NetBIOS (figura 3.90). Este nome tem de ser introduzido para que as versões mais antigas do Windows, do Windows 98, do Windows Millenium consigam interligar-se com o *Active Directory*. O nome NetBIOS serve para garantir a compatibilidade com este tipo de clientes, que utilizam o nome NetBIOS para identificar o *Active Directory*.

Os clientes com o Windows 2000 Professional e o Windows XP Professional podem utilizar o nome de DNS para se interligarem com o *Active Directory*.

O nome escolhido vai ser "ESCOLA", mas poderia ser outro diferente do seleccionado no nome de DNS **escola.pt**. Após a introdução do nome NetBIOS, pressionar **Seguinte**, para continuar.

O questionário prossegue. Agora é obrigatório indicar o caminho onde é armazenada a base de dados do *Active Directory* e os ficheiros de registo. No nosso exemplo, só temos uma partição criada, pelo que as duas pastas são guardadas no mesmo volume. Caso seja possível, aconselha-se a utilizar estas duas pastas em discos separados, para se garantir mais fiabilidade e performance.

Para continuar, clicar sobre **Seguinte**.

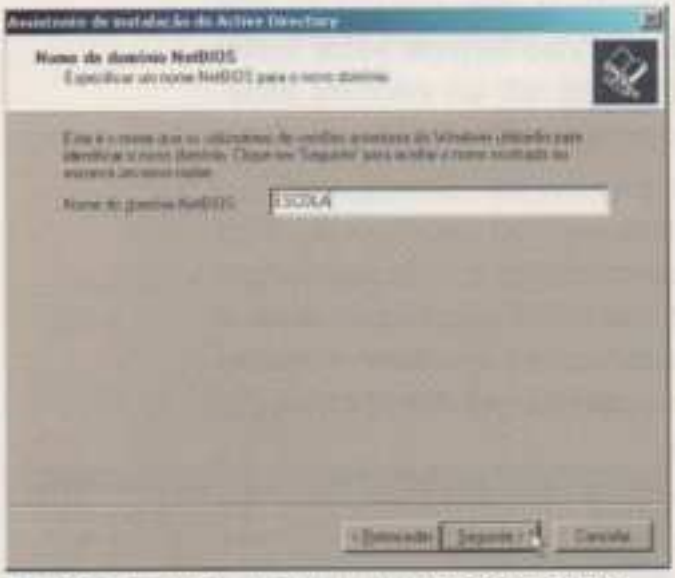

Fig. 3.90 Especificação do nome NetBIOS do novo domínio

Fig. 3.91 Localização das pastas da base de dados e dos ficheiros de registo

A localização da pasta **SYSVOL** é o passo que se segue. Esta pasta tem de ser localizada, obrigatoriamente, numa partição formatada em NTFS V5 (figura 3.92).

Após a selecção da localização da pasta **SYSVOL**, deve-se clicar em **Seguinte**, para continuar com a instalação.

Na janela **Permissões** (figura 3.93), vamos escolher a segunda opção, para que os programas de servidor corram apenas nos sistemas operativos Windows 2000 Server ou Windows Server 2003. Somente os utilizadores autenticados no domínio podem ler informação do domínio.

Dado que o esquema de segurança do Windows Server 2003 e do Windows 2000 Server é diferente das versões servidoras Windows NT, deve-se escolher a primeira opção. Assim, é possível correr os programas que funcionam em servidores NT ou em servidores Windows 2000 Server e Windows Server 2003.

Seleccionar a segunda opção e clicar **Seguinte**, para continuar.

Fig. 3.92 Localização da pasta SYSVOL

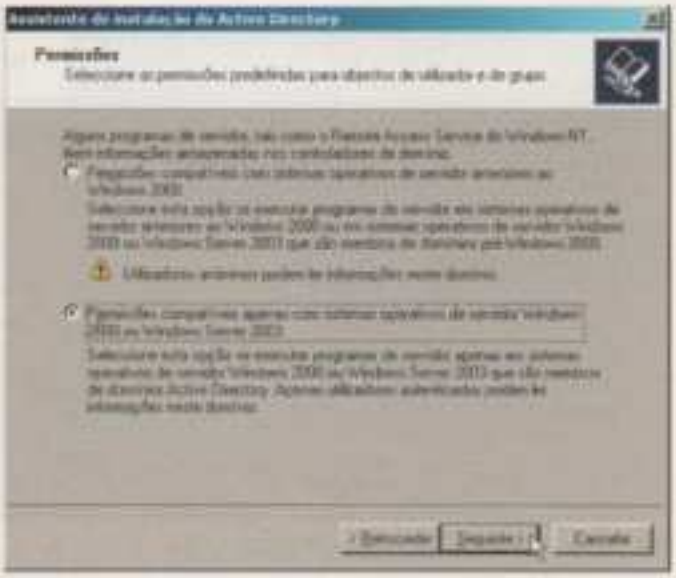

Fig. 3.93 Selecção das permissões predefinidas para objectos de utilizadores e de grupo

Na nova janela que se segue (figura 3.94), temos de introduzir uma palavra-passe do administrador do *Active Directory*. Esta palavra-passe é necessária quando o servidor for iniciado em **Modo de restauro dos serviços de directório**. Esta palavra-passe é diferente da palavra-passe utilizada para o administrador do sistema operativo. É necessário guardar as duas palavras-passe. Para mais informação, clicar em **Ajuda do Active Directory**.

Após a introdução da palavra-passe, a instalação prossegue seleccionando **Seguinte**.

Na janela **Resumo** surge um resumo das configurações escolhidas para a instalação do *Active Directory*. Se alguma opção estiver errada, podemos recuar na instalação pressionando **Retroceder**. Se tudo estiver de acordo com o pretendido, clica-se em **Seguinte**, para se instalar o *Active Directory*.

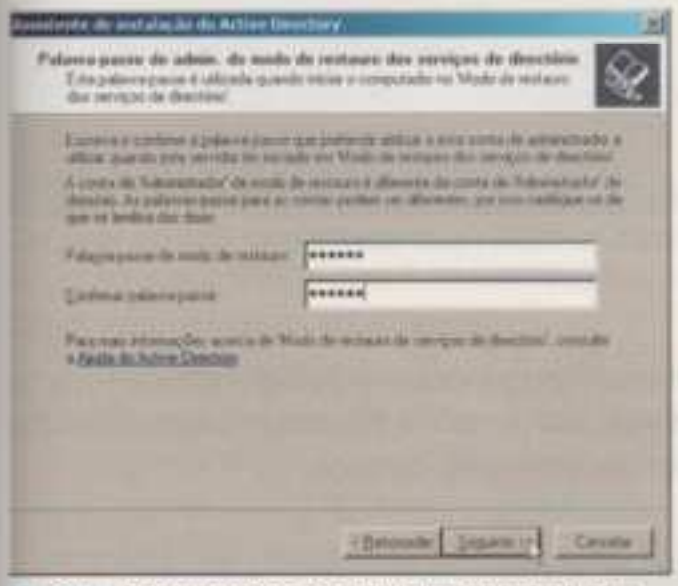

Fig. 3.94 Palavra-passe do administrador do *Active Directory*

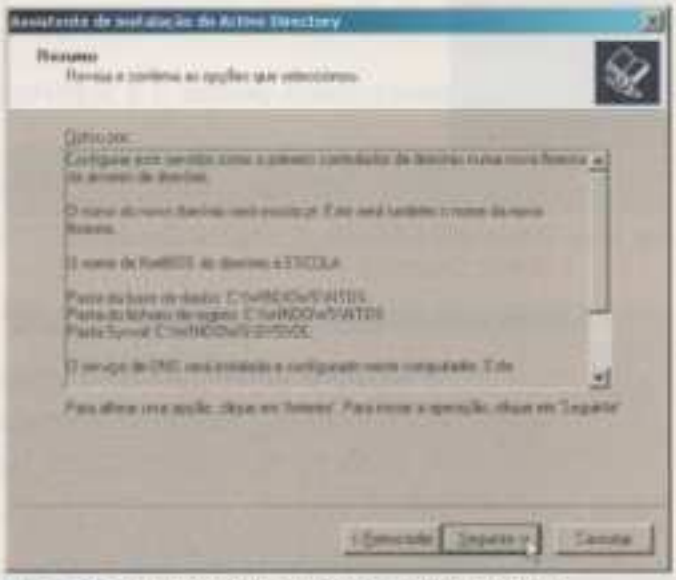

Fig. 3.95 Resumo das opções seleccionadas

A partir desta fase dá-se início à instalação do *Active Directory*. O processo de instalação é um pouco demorado, pelo que temos de esperar pela sua conclusão.

A instalação do *Active Directory* prossegue automaticamente, mas não nos podemos esquecer de colocar no leitor de CD o CD-ROM do Windows Server 2003 Standard Edition.

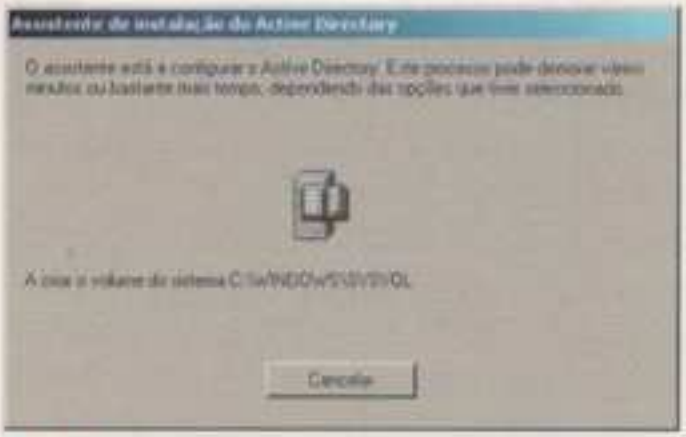

Fig. 3.96 *Active Directory* a instalar.

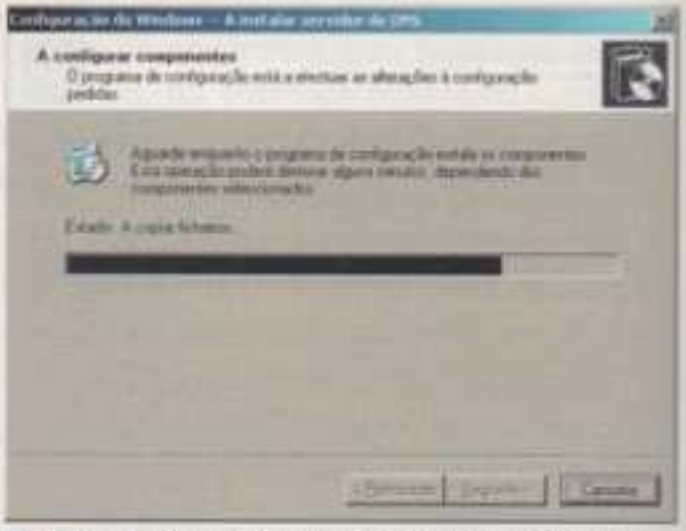

Fig. 3.97 A copiar ficheiros durante a instalação do *Active Directory*.

No fim da instalação do *Active Directory*, aparece a janela da figura 3.98, a indicar que a instalação decorreu correctamente. A conclusão da mesma é feita clicando em **Concluir**.

No final da instalação do *Active Directory*, convém reiniciar o computador. Para isto, deve-se pressionar **Reiniciar agora**.

Fig. 3.98 Resumo da conclusão da instalação do *Active Directory*

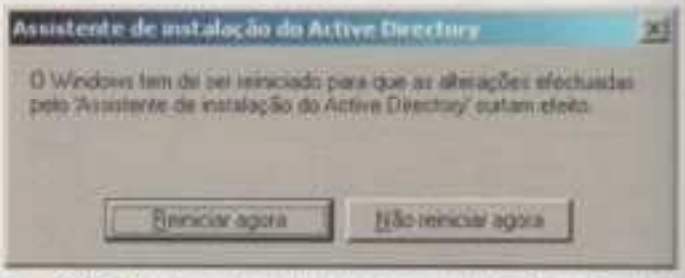

Fig. 3.99 Ordem para reiniciar o computador após instalação do *Active Directory*

Após o arranque do computador, o nosso servidor tem o *Active Directory* instalado. A partir deste momento, o nosso servidor passa a funcionar como servidor de topo da floresta e como único *Domain Controller* da floresta.

Despromoção de *Domain Controller*

Ponto da situação: Após a instalação do *Active Directory*, no ponto anterior, o servidor está a funcionar como controlador de domínio (DC). Pode-se voltar à fase inicial, isto é, despromovê-lo para que fique a funcionar como *Standalone Server* – para pertencer a um grupo de trabalho existente ou, caso não exista ainda nenhum grupo na rede, para que seja criado um novo grupo de trabalho.

O início da despromoção é executado pelo comando **dcpromo.exe**.

O comando pode ser chamado a partir da caixa de diálogo **Executar**, que, por sua vez, é chamada a partir do menu **Iniciar** e, depois, **Executar**.

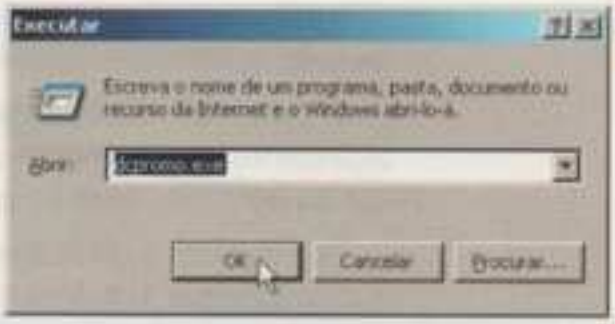

Fig. 3.100 Chamar o assistente de configuração do *Active Directory*.

> No Windows Server NT só era possível mudar o papel do servidor reinstalando novamente todo o sistema operativo.

Aparece-nos, de seguida, uma caixa de diálogo a dar as boas-vindas à remoção do *Active Directory*. Para se prosseguir com a remoção deve-se escolher **Seguinte**.

O assistente pára e somos informados de que o controlador de domínio é um servidor de **Catálogo global** – *Global Catalog*. Um servidor que seja um *Global Catalog* contém toda a informação do domínio (contas e permissões de utilizadores e grupos, entre outras).

A remoção continua, se pressionarmos em **OK**.

Fig. 3.101 Assistente de instalação do *Active Directory*

Fig. 3.102 Informação de que o servidor é um **Catálogo global** – *Global Catalog*.

Na figura 3.103, temos de escolher a opção **Este servidor é o último controlador de domínio dentro do domínio**.

É necessário ter a certeza de que pretendemos eliminar o *Active Directory*; se dermos ordem para remover o *Active Directory* – e como este é o último servidor do nosso domínio e é um *Global Catalog* – serão eliminados os seguintes dados:

- os computadores que pertencem a este domínio deixam de poder iniciar sessões no domínio ou aceder a quaisquer serviços do domínio;
- todas as contas de utilizadores e grupos serão eliminadas;
- todas as chaves criptográficas neste domínio serão eliminadas;
- todos os dados encriptados, tais como mensagens de correio electrónico ou ficheiros encriptados por EFS, devem ser desencriptados antes de continuar ou ficarão permanentemente inacessíveis.

Fig. 3.103 Selecção de que se pretende remover o último controlador de domínio.

Após a selecção da opção **Este servidor é o último controlador de domínio dentro do domínio**, pode-se continuar com a remoção do *Active Directory* clicando em **Seguinte**.

A caixa de diálogo da figura 3.104 indica-nos que, se pretendermos que o assistente remova todas as partições de directório de aplicações deste controlador de domínio, deve-se pressionar em **Seguinte**.

Por questões de segurança, o assistente pára novamente e força a escolha da opção **Eliminar todas as partições de directório de aplicações neste controlador de domínio**. Esta opção obriga-nos a reflectir se pretendemos realmente remover o *Active Directory*.

Fig. 3.104 Indicação de partições do controlador de domínio

Fig. 3.105 Ordem de confirmação para despromover o *Active Directory*

O assistente prossegue, mas não sem antes nos obrigar a introduzir a palavra-passe do administrador do sistema operativo. Esta opção é compreensível, pois, de outro modo, qualquer pessoa com acesso ao servidor poderia eliminar o *Active Directory* inadvertidamente, causando graves danos ao nosso servidor.

A remoção do *Active Directory* prossegue após a introdução da palavra-passe por duas vezes e pressionando em **Seguinte**.

Após a introdução da palavra-passe do administrador do sistema operativo, devemos verificar, na janela **Resumo**, se as opções seleccionadas estão correctas. Caso seja necessário rever alguma opção, seleccionamos a opção **Retroceder**; caso contrário, e se estiver tudo correcto, escolhemos a opção **Seguinte**.

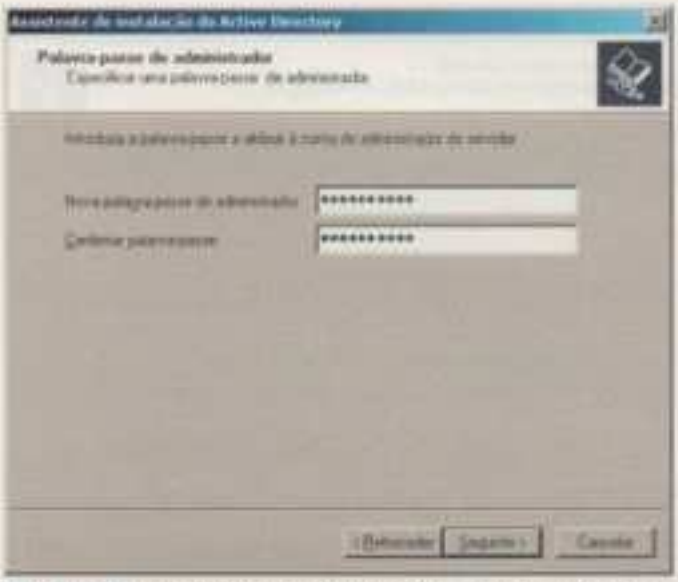

Fig. 3.106 Inserir palavra-passe do administrador do sistema operativo.

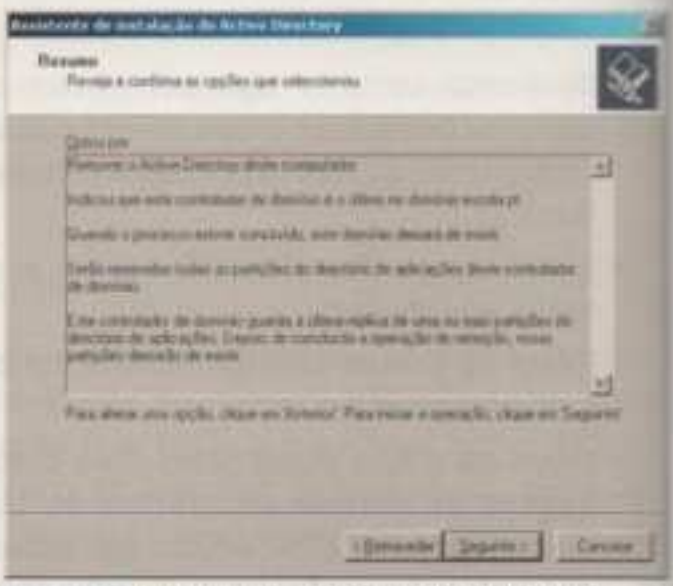

Fig. 3.107 Resumo das opções seleccionadas para a remoção do *Active Directory*

Após a verificação das opções seleccionadas para a remoção do AD, esta operação começa realmente a ser executada quando clicarmos em **Seguinte**.

Esta fase é demorada; há que aguardar que a remoção do AD termine.

Quando a remoção do AD terminar, surge uma janela a indicar que a remoção do *Active Directory* terminou correctamente.

A conclusão da remoção termina seleccionando **Concluir**.

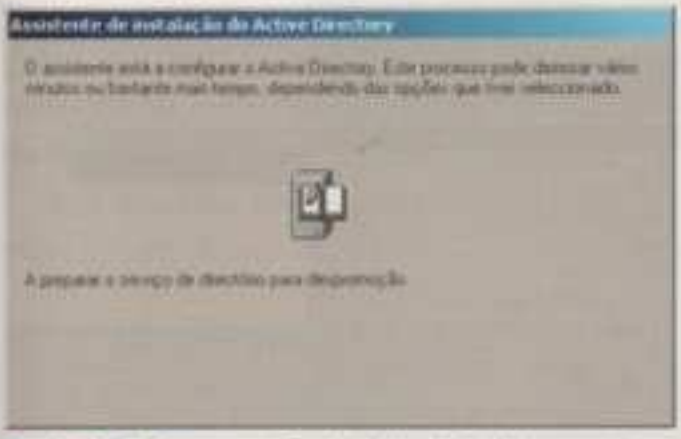

Fig. 3.108 Despromoção do *Active Directory* em execução

Fig. 3.109 Conclusão da despromoção do *Active Directory*

No final da remoção do *Active Directory*, convém reiniciar o computador e, para isto, deve-se clicar em **Reiniciar agora**.

Após o arranque do computador, o nosso servidor passa a funcionar como *Standalone Server*. No nosso caso, como não existe nenhum grupo na rede, o servidor cria um novo grupo de trabalho.

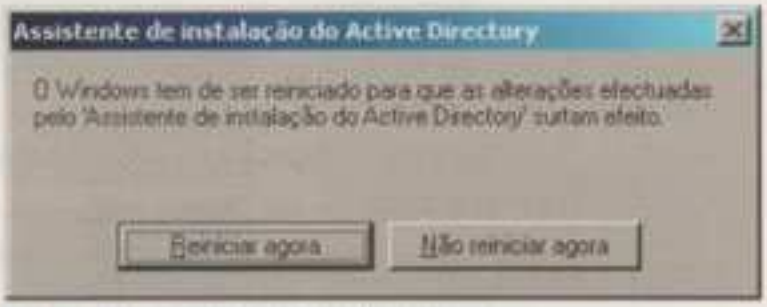

Fig. 3.110 Reiniciar o computador.

Configuração de servidores adicionais

Neste ponto vamos estudar como configurar um servidor para que funcione nos diversos tipos de papel que pode desempenhar numa rede.

> Para refrescar a memória, aconselha-se uma revisão da subunidade **2.1. Planeamento da instalação**, no ponto **Papel dos servidores**, e da subunidade **1.5. Terminologia de redes da Microsoft**.

Standalone Server – são servidores que pertencem a um grupo de trabalho. Após a despromoção do AD, o nosso servidor encontra-se configurado a funcionar como *Standalone Server*.

Member Servers – são servidores que estão associados a um domínio já existente, ou seja, são apenas membros do domínio, mas não são controladores de domínio.

Antes de configurarmos o nosso servidor como *Member Server*, a partir do servidor a funcionar como *Standalone Server*, é necessário inserir o endereço IP do servidor de domínio no DNS do nosso servidor.

Configuração do nosso servidor como cliente de DNS

Vamos partir do princípio que já existe um servidor a funcionar como controlador de domínio. O servidor tem como endereço IP **192.168.1.254** e nome de DNS **sala.com**.

O início da configuração do nosso servidor como cliente de DNS é executado desde o menu **Iniciar** > **Painel de controlo** > **Ligações de rede** e, por fim, **Ligação de área local**.

Fig. 3.111 Acesso à **Ligação de área local**

Na janela **Ligação de área local estado** (figura 3.112) escolhemos **Propriedades**.

Na nova janela **Propriedades de ligação de área local** (figura 3.113) escolhemos **TCP/IP (Protocolo Internet)** e depois **Propriedades**.

Finalmente, estamos na janela de configuração do cliente de DNS (figura 3.114). Em **Servidor de DNS preferido** vamos colocar o endereço IP do servidor que é controlador de domínio. Para validar as configurações, pressionamos em **OK**.

Após a inserção do endereço DNS, voltamos à janela da figura 3.113 e selecionamos novamente **OK** e, finalmente, na janela da figura 3.112, escolhemos **Fechar**.

Fig. 3.112 Janela **Ligação de área local estado**

Fig. 3.113 Janela **Propriedades de ligação de área local**

Fig. 3.114 Inserir endereço DNS.

Neste momento estamos prontos a configurar o nosso servidor, para que este funcione como *Member Server*. Não esquecer que, inicialmente, o nosso servidor estava a funcionar como *Standalone Server*. A instalação é realizada indo ao menu **Iniciar** > **Painel de controlo** e **Sistema**.

Na janela **Propriedades do sistema** (figura 3.116), vamos ao separador **Nome do computador** e escolhemos **Alterar**.

Nesta fase, o nosso servidor pertence ao grupo de trabalho **WORKGROUP**. Para que seja membro de um domínio seleccionamos **Membro de Domínio**.

Fig. 3.115 Acesso à janela **Sistema**

Em **Membro de Domínio** vamos inserir o nome DNS do servidor que é DC na nossa rede (figura 3.118).

Fig. 3.116 Separador **Nome do computador** da janela **Propriedades do sistema**

Fig. 3.117 Janela de configuração do servidor a membro de um domínio

Fig. 3.118 Janela de configuração do servidor a membro de um domínio

Após clicarmos em **OK**, o nosso servidor vai aparecer numa caixa de diálogo **Bem-vindo ao domínio**. A partir deste momento, o nosso servidor é membro do novo domínio.

Novo *Domain Controller* – este servidor irá funcionar como único *Domain Controller* da floresta e como servidor de topo da floresta.

Este tipo de papel de servidor já foi estudado nesta subunidade e pode ser analisado novamente a partir da figura 3.81.

***Domain Controller* pertencente a um domínio já existente** – este servidor fica com uma cópia do AD do *Domain Controller* já existente. Se o primeiro servidor estiver em baixo (desligado), o novo servidor poderá, por exemplo, continuar a validar os utilizadores. Na prática, o segundo servidor não fica com uma réplica exacta do AD do primeiro servidor. Para se entender melhor esta situação, devem ser analisados os *Global Catalog*, que, no entanto, não serão alvo de estudo neste ano lectivo.

Nesta situação, devemos configurar o nosso servidor como cliente de DNS do servidor que contém o DC.

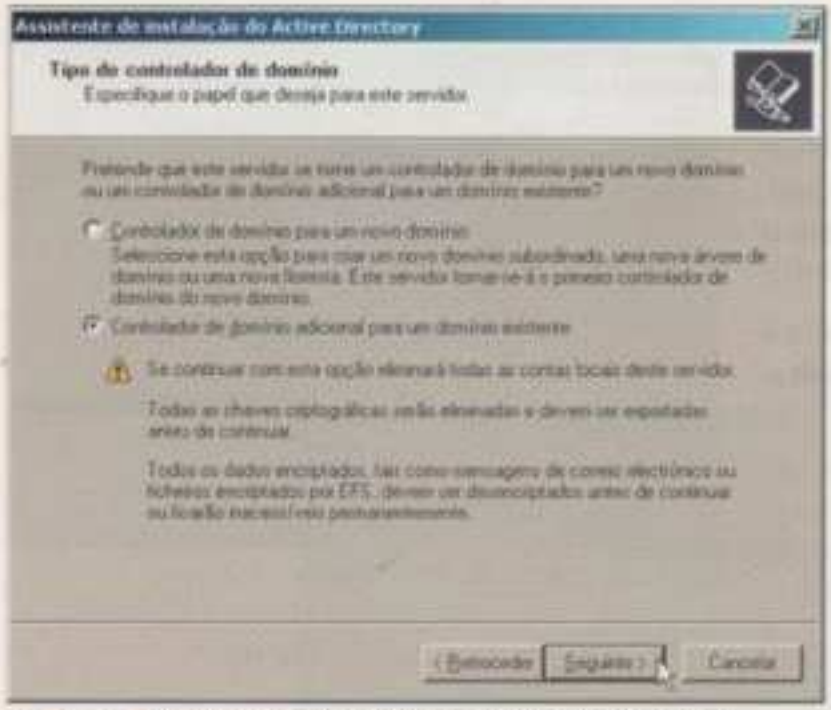

Fig. 3.119 Escolha do tipo de controlador de domínio (DC)
NOTA: Esta janela pode ser encontrada na figura 3.86, na **Promoção a *Domain Controller***, no ponto anterior desta subunidade.

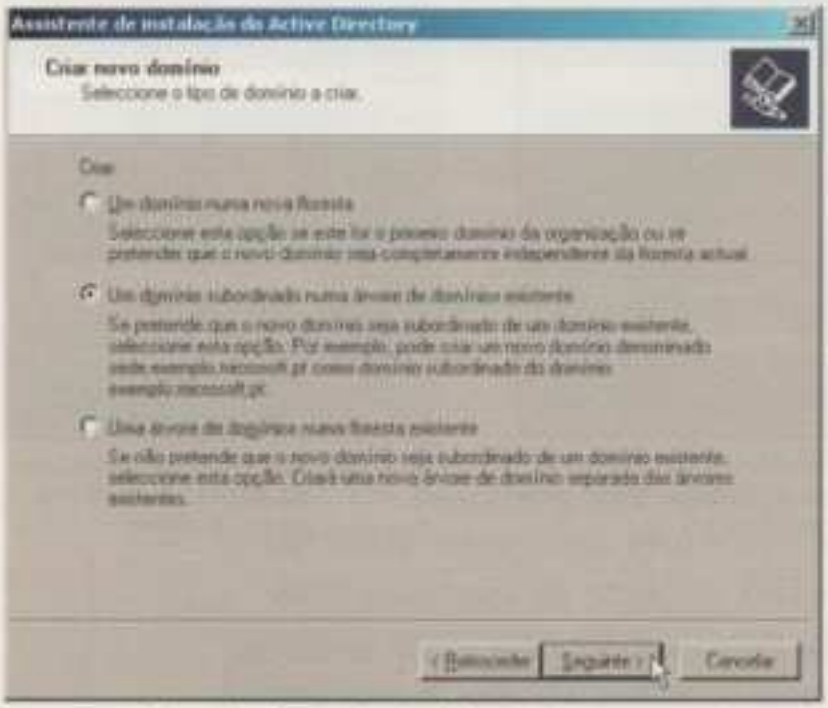

Fig. 3.120 Selecção do tipo de domínio a criar
NOTA: Esta janela pode ser encontrada na figura 3.87, na **Promoção a *Domain Controller***, no ponto anterior desta subunidade.

A configuração é feita a partir da figura 3.119, onde vamos escolher a segunda opção – **Controlador de domínio adicional para um domínio existente** – e, depois, seleccionar **Seguinte**, para prosseguir com a instalação.

Nova árvore em floresta existente. Nesta situação tem de já existir uma floresta criada e deve existir, pelo menos, um *Domain Controller*. É possível adicionar um novo domínio totalmente autónomo do outro DC (já criado anteriormente) à floresta existente, embora se consiga ter acesso aos recursos do anterior domínio, dado que o novo vai ser criado dentro da floresta já existente.

Antes de configurarmos o nosso servidor, temos de configurá-lo como cliente de DNS do servidor que contém o DC.

Na janela **Criar novo domínio**, temos de escolher a segunda opção, para criarmos uma nova árvore na floresta já existente, e depois seleccionar **Seguinte**, para continuar com a instalação.

Se o servidor que contém o DC principal tiver o nome de DNS **sala.com**, será formado um novo domínio, criado pelo nosso servidor, que vai ser subordinado do existente. Podemos atribuir ao nosso servidor o nome de DNS **laboratorio.sala.com**.

3. Administração e serviços do Windows Server 2003

3.1. Ferramentas de administração

A preferência dada, pelos administradores de rede, a um servidor Windows Server 2003 deve-se, principalmente, à sua fácil gestão, assim como à sua interface amigável e ao modo de funcionamento gráfico, que torna o trabalho de gestão de rede muito mais agradável. Além do referido, há ainda que relembrar as variadas ferramentas de administração de rede e do servidor que constituem parte do Windows Server 2003, destacando-se, entre elas, por exemplo, as ferramentas que constam

do *software* do BackOffice ou do *software* de *backups*, as ferramentas de gestão de discos rígidos, de utilizadores e de acessos, de servidores e de postos de trabalho.

As ferramentas de administração encontram-se no menu **Iniciar** (*Start*) > **Ferramentas administrativas** (*Administrative Tools*). No menu **Ferramentas administrativas** estão as ferramentas, após uma instalação por defeito, ou então todas aquelas que se optou por ter e que podem até ter sido instaladas após a instalação original.

Toda esta variedade de ferramentas conta com uma interface intuitiva, interligação e interacção com o SO e, entre as próprias ferramentas ou com outros programas, gestão centralizada (por exemplo, através da **Gestão de computadores** – *Computer Management* – ou do **Visualizador de eventos** – *Event Viewer*), gestão a partir de um posto de trabalho e o uso de **Serviços de Terminal** (*Terminal Services*), entre outros.

Fig. 3.121 **Ferramentas administrativas**

3.2. Administração rápida

Introdução

Como já foi dito, um servidor Windows Server 2003 é um dos favoritos do momento pela facilidade de administração. Para uma maior rapidez e facilidade de utilização de um administrador de rede, existem os chamados *wizards* (assistentes), que servem para ajudar nas tarefas das respectivas ferramentas a que estão associados.

Por exemplo, para configurar o servidor (ferramenta *Configure Your Server*) existem uns *wizards* que permitem à ferramenta **Configurar o servidor** implementar um modelo de gestão centralizada, através da qual se pode aceder às ferramentas de administração. Os *wizards* da ferramenta **Configurar o servidor**, por exemplo, contam ainda com várias outras funções, como gerir o servidor de ficheiros, criar filas de impressão, configurar e instalar os serviços da rede, instalar componentes e instalar e gerir serviços *Web* e de *media*, entre outros, tudo com o intuito de poupar tempo, pela facilidade da realização das tarefas de um administrador de rede. No entanto, mesmo que estes *wizards* associados à ferramenta **Configurar o servidor** façam quase tudo o que as respectivas ferramentas de administração fazem, nem todos os *wizards* fazem tudo o que seria possível fazer com a ferramenta que lhe está associada.

Gestão de ficheiros e directórios

É fácil gerir ficheiros e directórios, devido à possibilidade da sua partilha em rede entre os utilizadores. Para se poder partilhar ficheiros é necessário configurar esta funcionalidade. Para tal deve-se:

Ir ao menu **Iniciar** (*Start*) > **Ferramentas administrativas** (*Administrative Tools*) > **Assistente para configurar o servidor** (*Configure Your Server Wizard*).

A instalação prossegue clicando em **Seguinte** (*Next*).

No ecrã **Passos preliminares** (*Preliminary Steps*) da figura 3.124, deve-se pressionar em **Seguinte** (*Next*), para continuar e aguardar enquanto o assistente detecta as definições da rede.

Fig. 3.122 Lançamento do **Assistente para configurar o servidor**

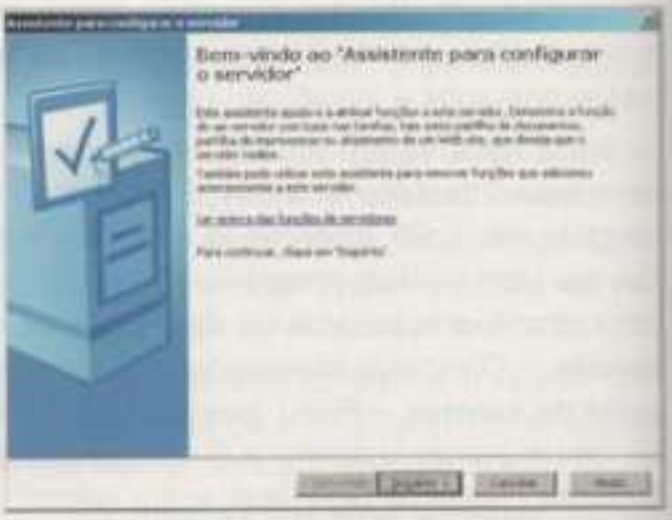

Fig. 3.123 Início do **Assistente para configuração o servidor**

Fig. 3.124 Recomendações antes de continuar com a instalação.

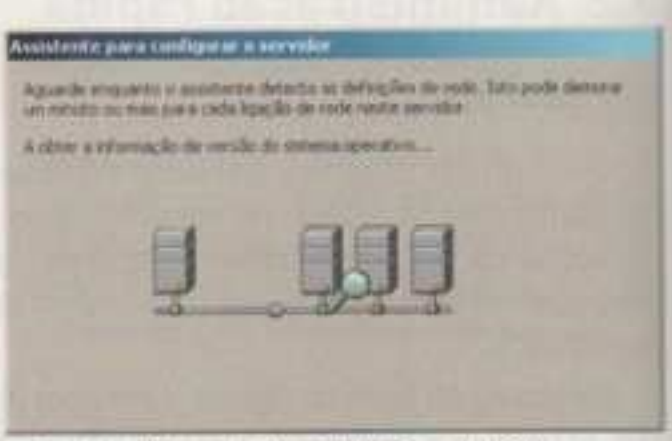

Fig. 3.125 Detecção das definições da rede

No ecrã **Opções de configuração** (*Configuration Options*), como a finalidade é criar um servidor de ficheiros, vamos seleccionar **Configuração personalizada** (*Custom Configuration*) e clicar em **Seguinte** (*Next*), para avançar.

No novo ecrã (figura 3.126), vamos seleccionar a opção **Servidor de ficheiros** (*File Server*) e clicar em **Seguinte** (*Next*).

No ecrã da figura 3.127, é necessário indicar se pretendemos, ou não, atribuir uma quota de disco por defeito a todos os utilizadores. Neste caso, deve-se indicar o valor máximo de espaço de disco utilizado por defeito e o valor a partir do qual será dado um aviso ao utilizador.

Se, além dos avisos, pretendermos que ao utilizador seja negada a utilização de mais espaço em disco para além do permitido (*deny disk space to users exceeding disk space limit*), então deve-se também seleccionar essa opção.

Por fim, pode-se também optar por registar os seguintes eventos: sempre que o limite de espaço em disco é atingido e/ou sempre que um aviso é emitido.

Clicar em **Seguinte** (*Next*) após a selecção das opções pretendidas.

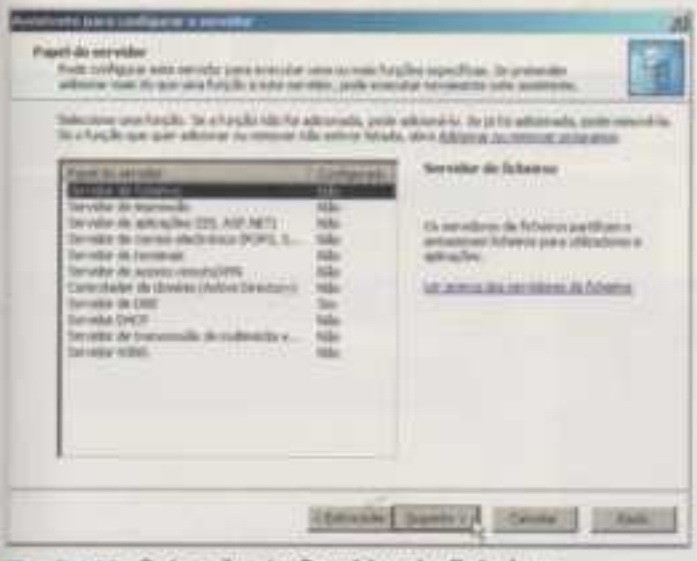

Fig. 3.126 Selecção de **Servidor de ficheiros**

Fig. 3.127 Ecrã **Gestão de quotas de disco de servidor de ficheiros**

Indicar se se pretende activar o serviço de indexação (figura 3.128). Este serviço efectua uma leitura dos conteúdos dos ficheiros partilhados e guarda os resultados numa base de dados para esse fim. Sempre que é feita uma pesquisa por palavra-chave, este serviço lista todos os ficheiros que contêm a tal palavra-chave. Sempre que um ficheiro sofre alterações, este volta a ser indexado, e, naturalmente, este procedimento acaba por prejudicar a performance do servidor.

Tomada a decisão, clicar em **Seguinte** (*Next*).

Surge, então, um ecrã com um resumo das decisões tomadas. Seleccionar **Seguinte** (*Next*), se estiver tudo em ordem, ou **Anterior** (*Back*), caso se pretenda alterar alguma selecção.

Clicar em **Seguinte** (*Next*), para continuar.

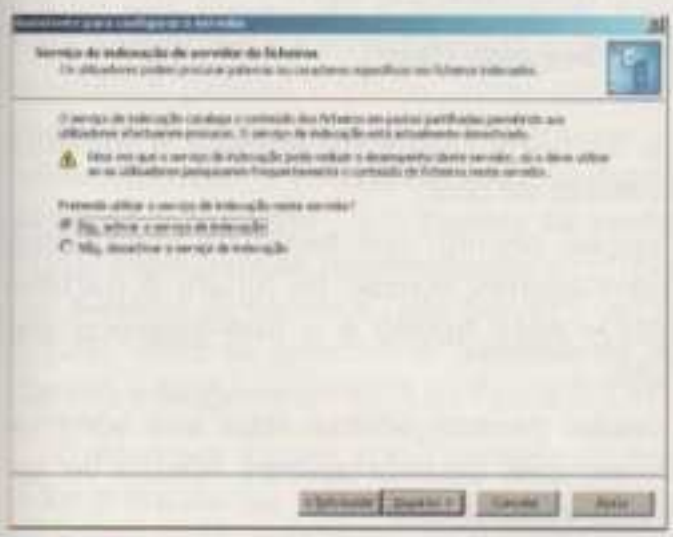

Fig. 3.128 Ecrã **Serviços de indexação do servidor de ficheiros**

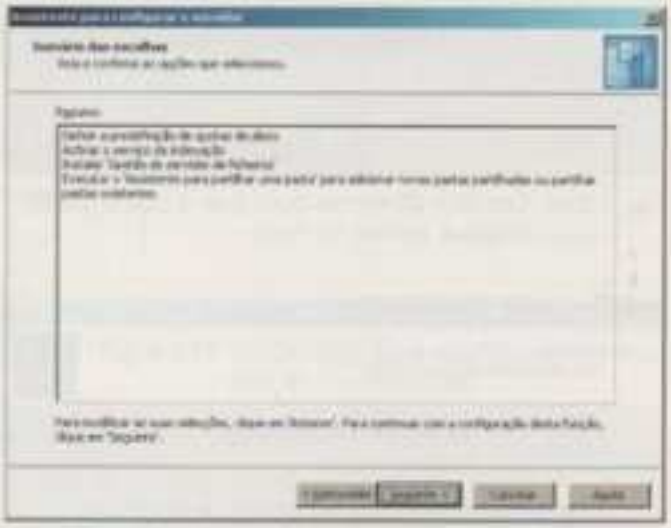

Fig. 3.129 Resumo das escolhas efectuadas

Nesta fase da configuração, vamos ter de aguardar para que as definições sejam aplicadas.

Finda a configuração do servidor de ficheiros, aparece um novo assistente (*wizard*) para a configuração da partilha e de direitos de acesso de directórios.

Clicar em **Seguinte** (*Next*).

Deve-se seleccionar a pasta a partilhar (usar o botão **Procurar** (*browse*)) e clicar em **Seguinte** (*Next*) (figura 3.131).

Fig. 3.130 Novo assistente para a configuração da partilha e de direitos

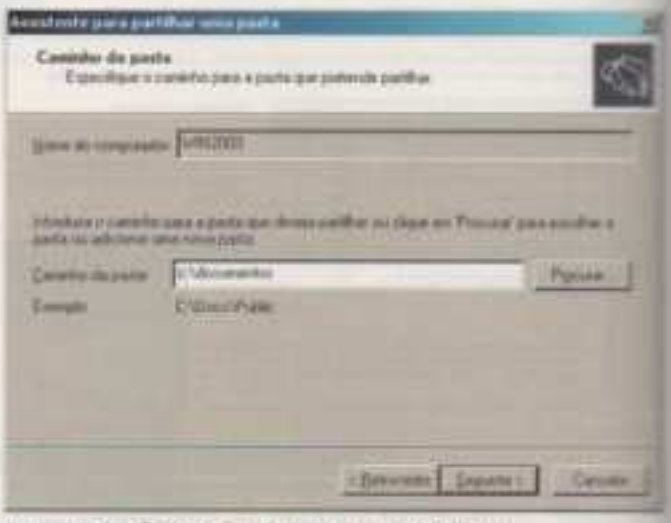

Fig. 3.131 Selecção da pasta a partilhar

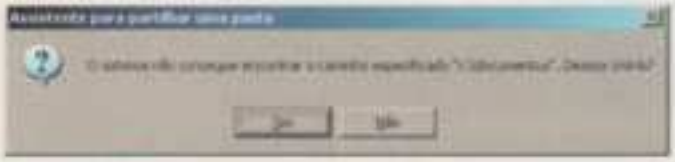

Fig. 3.132 Criar pasta que vai ser partilhada.

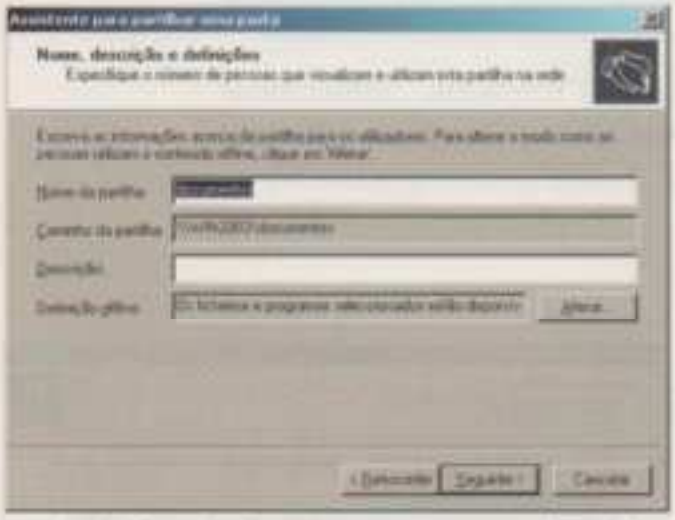

Fig. 3.133 Escolha do nome com que a pasta partilhada é visível na rede.

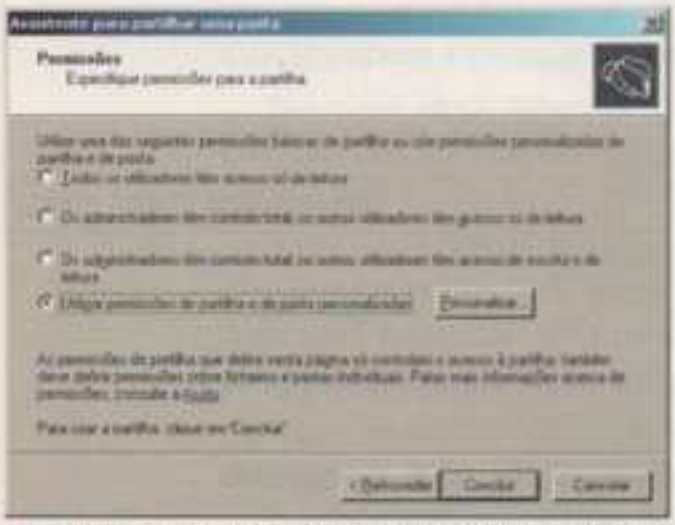

Fig. 3.134 Especificação das permissões de acesso à partilha

O assistente não encontra nenhuma pasta criada com o nome escolhido na figura anterior, pelo que, para o sistema criar uma pasta, é necessário clicar em **Sim** (*Yes*).

Indique o nome com que esta partilha será visível a partir da rede. Caso queira, pode ainda criar uma descrição da partilha, que será vista pelos clientes da rede que usem o Windows Explorer no modo de visualização **Detalhes**.

Neste campo é ainda possível optar por deixar o conteúdo da partilha disponível para um cliente em modo *offline* (desligado da rede).

Clicar em **Seguinte** (*Next*).

Defina as permissões de acesso à partilha (*share*) acabada de criar:

- **1.ª opção:** permitir que todos os utilizadores tenham apenas acesso de leitura à partilha criada – esta opção é a que aparece por defeito.
- **2.ª opção:** permitir acesso total aos administradores, mas permitir apenas acesso de leitura aos utilizadores.
- **3.ª opção:** permitir acesso total aos administradores, mas permitir apenas acesso de leitura e de escrita aos utilizadores.
- **4.ª opção:** caso se pretendam outras opções de segurança, seleccionar **Personalizar** (*Customize*).

Vamos escolher esta opção.

Defina os níveis de segurança e o tipo de acesso pretendidos para cada grupo de utilizadores da lista (**Adicionar** ou **Remover** grupos de utilizadores).

Seleccione **OK**.

Tendo concluído a administração de permissões sobre um *share*, surge a opção de podermos regressar ao início deste assistente e repetir a mesma operação sobre outra pasta. Para terminar, clique em **Fechar** (*Close*).

Fig. 3.135 Personalização dos direitos da partilha

Fig. 3.136 Fim do processo de partilha

Configuração de impressoras

Para que um servidor funcione como um servidor de impressão, este deve ter uma impressora instalada localmente que possa ser acedida pelos clientes da rede. Para tornar esta funcionalidade possível, teremos de repetir os passos comuns, referidos no início do subcapítulo anterior (**Iniciar** > **Programas** > **Ferramentas administrativas** > **Assistente para configurar o servidor** > **Seguinte** > **Seguinte** – em **Opções de configuração**, seleccionar **Configuração personalizada**) e, em vez de seleccionar **Servidor de ficheiros** (*File Server* – ver figuras 3.122 a 3.126), deve-se seleccionar **servidor de impressão** (*Print Server*) e **Seguinte** no ecrã da figura 3.137.

Fig. 3.137 Assistente para configurar o servidor de impressoras

O Windows Server 2003 contém *drivers* que têm de ser descarregados do servidor e instalados nos computadores-clientes, sempre que é feita a instalação da impressora de rede num cliente. Atendendo ao facto de os *drivers* poderem ser diferentes, dependendo do tipo de clientes que se tem na rede, torna-se necessário indicar, no ecrã da figura 3.138, se os clientes são apenas clientes Windows 2000/XP (opção 1), ou se são todos os tipos de clientes Windows (opção 2). Feita a opção, clicar em **Seguinte** (*Next*).

Após a leitura do sumário das escolhas efectuadas, podemos prosseguir com a instalação clicando em **Seguinte** (*Next*), ou, para alterar as opções, em **Retroceder** (*Back*).

Clicar em **Seguinte** (*Next*).

Fig. 3.138 Escolha dos controladores de impressoras

Fig. 3.139 Resumo das escolhas efectuadas

Na janela de boas-vindas do assistente de configuração de impressoras (figura 3.140), clicar em **Seguinte** (*Next*), para dar início à instalação da impressora.

A primeira opção diz respeito à instalação de uma impressora local ligada ao computador e, ao seleccionar esta opção, podemos ainda decidir se pretendemos que o assistente identifique e instale automaticamente a impressora (desde que compatível com a norma *Plug and Play*).

A segunda opção refere a instalação de uma impressora de rede ou partilhada por outro computador.

Feita a selecção pretendida (neste caso, opção 1), deve-se clicar em **Seguinte**.

Fig. 3.140 Assistente para instalação de impressoras

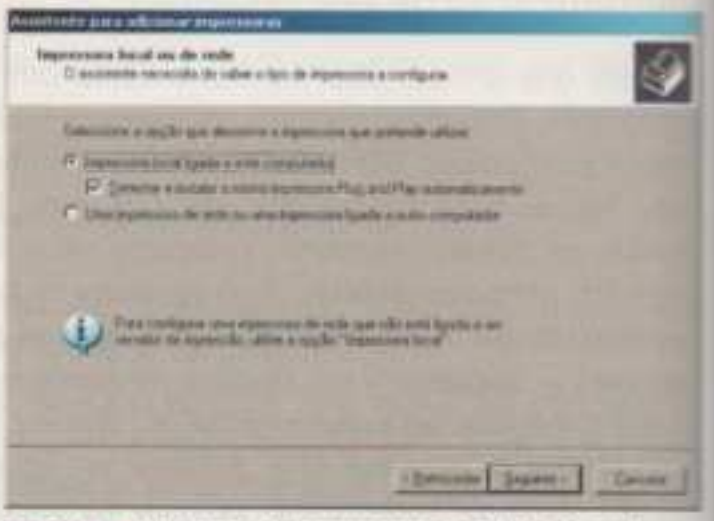

Fig. 3.141 Selecção de impressora local ou de rede

Caso não esteja nenhuma impressora ligada ao computador, ou se a impressora não for compatível com a norma *Plug and Play*, surge a mensagem da figura 3.142: **O assistente não conseguiu detectar quaisquer impressoras plug and play. Para instalar a impressora manualmente, clique em 'Seguinte'.**

Para continuar com a instalação, clicar em **Seguinte** (*Next*).

Escolher a porta à qual a impressora está ligada ou seleccionar **Criar uma nova porta**, no caso de se querer configurar uma impressora ligada à rede com periféricos adequados (figura 3.143).

Clicar em **Seguinte**.

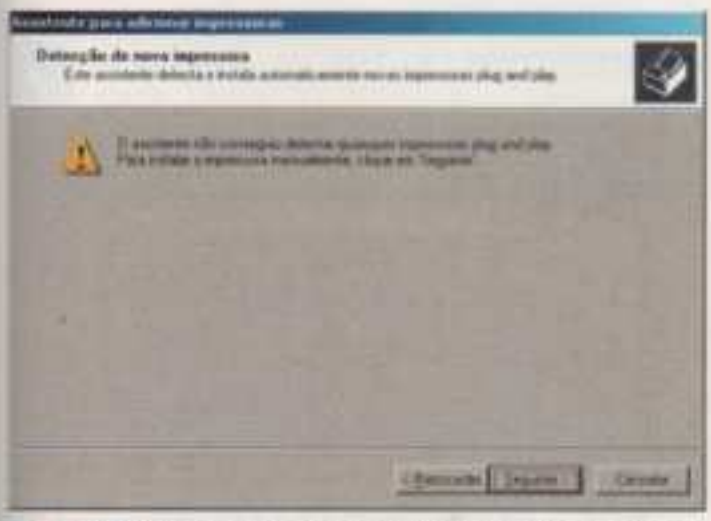

Fig. 3.142 Mensagem a informar que não existe impressora *Plug and Play* ligada.

Fig. 3.143 Escolha da porta a que a impressora está ligada.

Seleccionar o modelo e a marca da impressora que se pretende instalar.

No caso da impressora a instalar não constar da lista, então deve clicar-se em **Disco** (*Have Disk*) e seleccionar o sítio onde se encontram os *drivers* do *software* (fornecido pelo fabricante), ou então procurar os *drivers* na Internet, através do botão **Actualização do Windows** (*Windows Update*).

Verificar na HCL se o modelo da impressora pretendida é compatível com o Windows Server 2003.

Clicar em **Seguinte**.

Indicar o nome pelo qual a impressora é reconhecida.

Clicar em **Seguinte**.

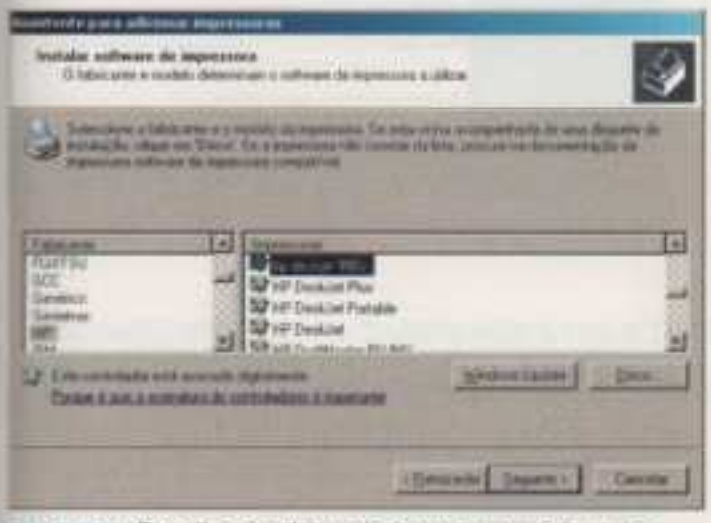

Fig. 3.144 Escolha do *driver* da impressora a instalar

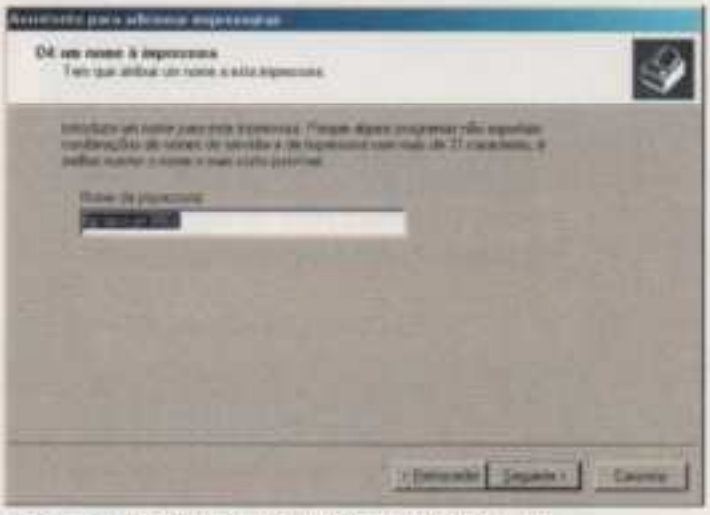

Fig. 3.145 Atribuição de nome à impressora

Indicar se pretende que a impressora local seja partilhada através da rede. Em caso afirmativo, indicar o nome dado ao *share* da impressora, que passará a ser visível para todos os clientes da rede.

Clicar em **Seguinte**.

Indicar uma descrição da localização física da impressora e, opcionalmente, algum comentário que se considere pertinente sobre as suas características ou capacidades, por exemplo.

Clicar em **Seguinte**.

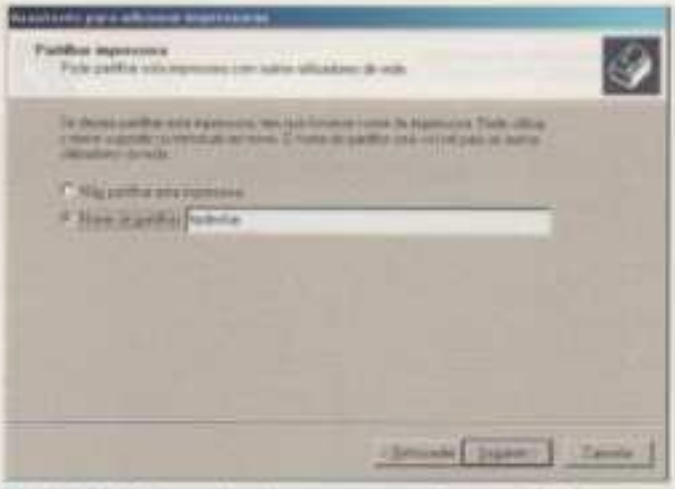

Fig. 3.146 Nome da impressora pelo qual é vista na rede.

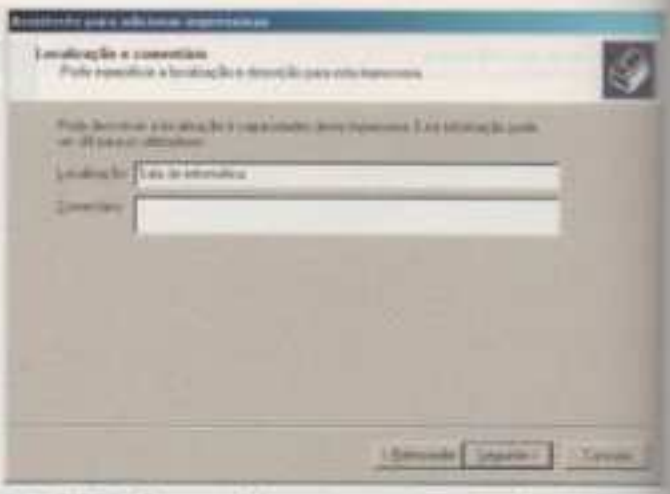

Fig. 3.147 Comentários sobre a localização física da impressora

Convém aceitar a impressão de uma página de teste, para saber se a impressora está correctamente instalada.

Clicar em **Seguinte**.

Surge, então, um ecrã com um resumo a confirmar a correcta instalação da impressora e das suas características, como mostra o ecrã da figura 3.149.

Clicar em **Concluir** (*Finish*), para sair do assistente de configuração.

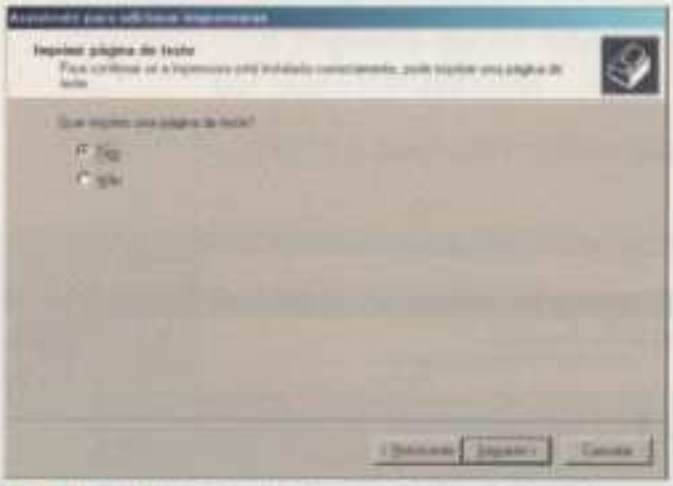

Fig. 3.148 Selecção de impressão de página de teste

Fig. 3.149 Fim do assistente de configuração

Os controladores da impressora estão a ser instalados. É necessário aguardar.

Após a instalação dos controladores da impressora, é imprimida uma página para teste. No final, devemos dizer se a impressão da página de teste foi realizada correctamente ou não.

Clicar em **OK**, para prosseguir.

Fig. 3.150 Instalação dos controladores da impressora

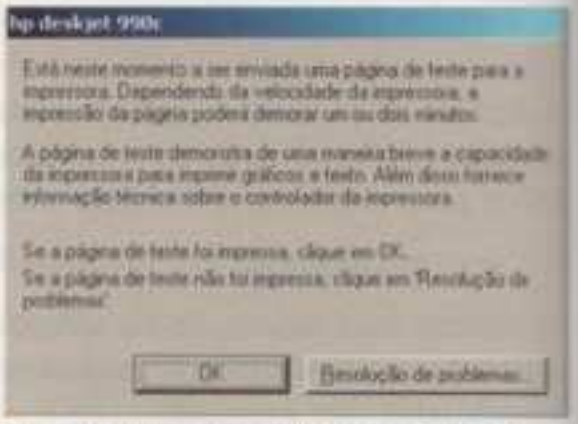

Fig. 3.151 Informação de que a página de teste está a ser imprimida.

Se no ecrã da figura 3.138 for seleccionada a opção 2, ou seja, a instalação de *drivers* para todos os tipos de clientes Windows, irá surgir um novo assistente de instalação dos controladores para as outras plataformas.

Clicar em **Seguinte** (*Next*).

Escolha o controlador da impressora a instalar no ecrã da figura 3.153. No caso da impressora a instalar não constar da lista, então deve clicar-se em **Disco** (*Have Disk*) e seleccionar o sítio onde se encontram os *drivers* do *software* (fornecido pelo fabricante), ou então procurar os *drivers* na Internet, através do botão **Actualização do Windows** (*Windows Update*).

Fig. 3.152 Assistente para adicionar controladores de impressora para outros clientes Windows

Clicar em **Seguinte**.

Seleccione os sistemas operativos e os processadores em que pretende instalar os controladores da impressora seleccionada no ecrã da figura 3.154. Para cada plataforma tem de ser instalado um controlador diferente.

Clicar em **Seguinte** (*Next*), para continuar.

Caso não existam os controladores no CD-ROM do Windows Server 2003, é necessário introduzir um CD-ROM com os controladores para cada sistema operativo anteriormente seleccionado.

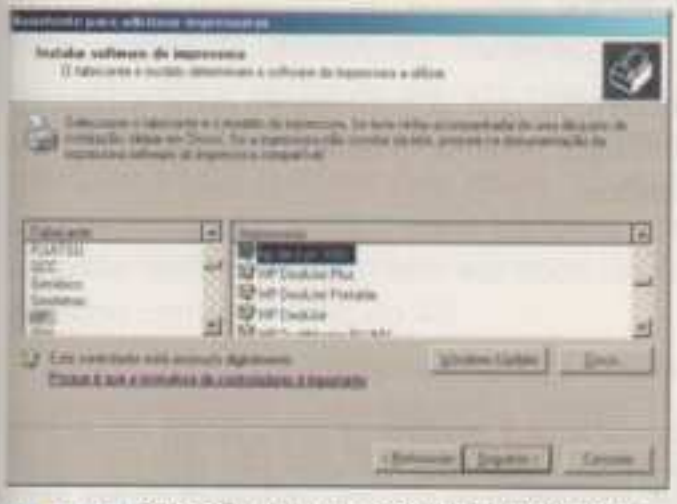

Fig. 3.153 Selecção do controlador da impressora a instalar

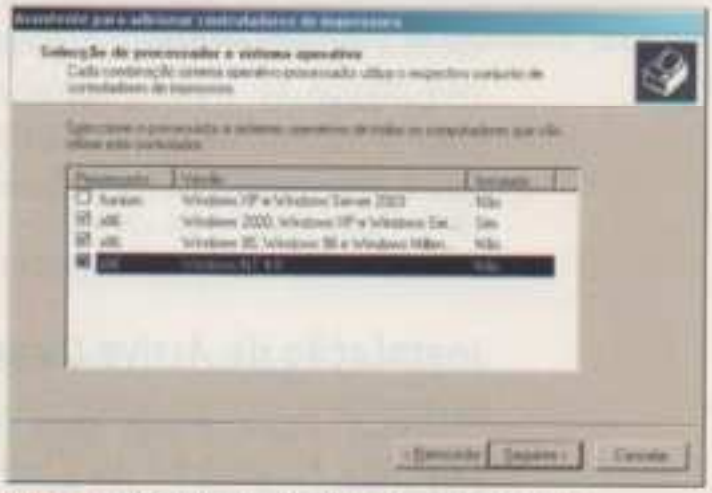

Fig. 3.154 Selecção das plataformas a instalar

Após a instalação dos controladores para cada plataforma anteriormente seleccionada, surge um ecrã com um resumo dos controladores instalados. Se não queremos instalar mais nenhuma impressora, não seleccionamos a caixa **Reiniciar o assis. para adicionar outro contr. de impressora**. Para fechar o assistente, pressionamos **Concluir**.

Surge, então, um ecrã a confirmar a correcta instalação da impressora para funcionar como servidor de impressão e as suas características.

Clicar em **Concluir** (*Finish*), para sair do assistente de configuração.

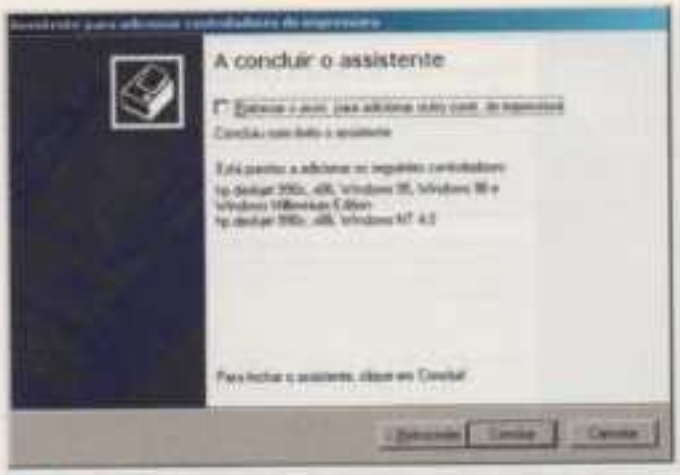

Fig. 3.155 Resumo da instalação dos controladores e conclusão do assistente

Fig. 3.156 Conclusão do assistente de configuração do servidor de impressão

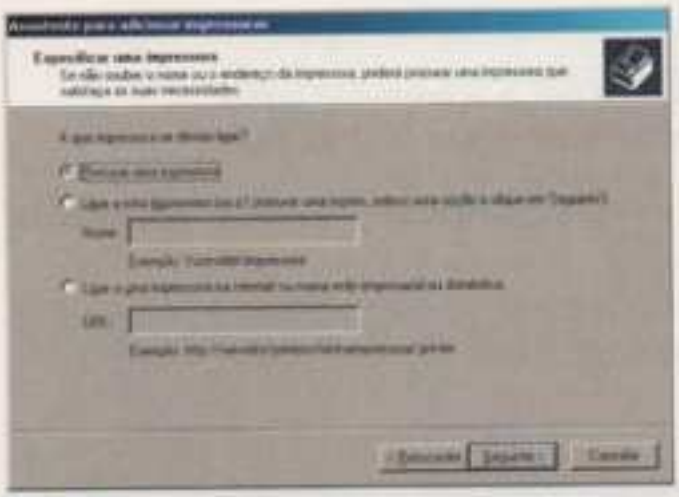

Fig. 3.157 Instalação de impressora de rede

No passo da figura 3.138, se tivéssemos escolhido a opção **Apenas para clientes Windows 2000 e Windows XP**, a instalação da impressora saltava do ecrã da figura 3.151 para a figura 3.156.

Nota: No caso de, em vez de se ter seleccionado a instalação de uma impressora local (ver figura 3.141), se tivesse optado pela opção 2 – **Instalação de uma impressora de rede**, então seria necessário indicar, em seguida, o nome da impressora ou o seu URL, ou então deixar que fosse localizada pelo *Active Directory*.

De seguida, há que decidir se pretendemos que a impressora seja a impressora *default* do Windows Server 2003 e surge, por fim, o ecrã com a indicação de que a impressora foi correctamente instalada.

Instalação do *Active Directory*

Nesta altura já não deve haver interrogações quanto à instalação do *Active Directory*. No entanto, para reavivar a memória, em caso de dúvidas, aconselha-se novamente a leitura do capítulo 2.5. desta unidade.

A instalação do *Active Directory* pode ser realizada executando o comando **dcpromo.exe** (ver figura 3.82), ou a partir do menu **Iniciar** > **Programas** > **Ferramentas administrativas** > **Assistente para configurar o servidor** > **Seguinte** > **Seguinte** – em **Opções de configuração**, seleccionar **Configuração personalizada** e, por fim, seleccionar **Controlador de domínio** (***Active Directory***) – ver figuras 3.122 a 3.126).

Na janela da figura 3.158, clica-se em **Seguinte** (*Next*), para continuar.

Aparece o sumário das escolhas efectuadas.

Clicar em **Seguinte** (*Next*), para prosseguir.

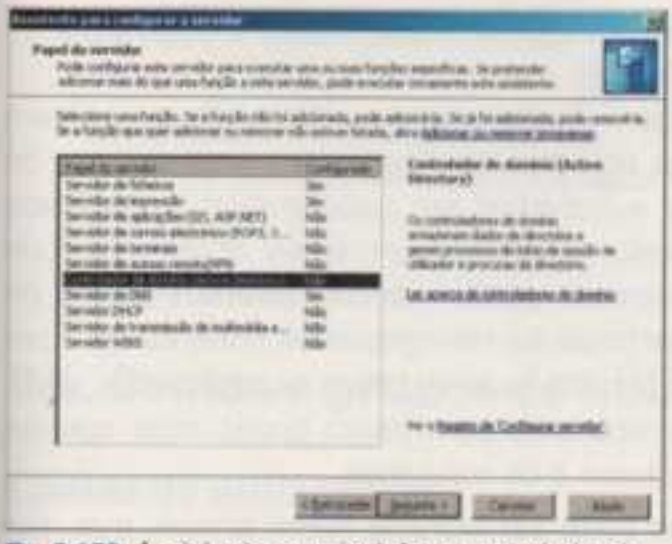

Fig. 3.158 Assistente para instalar o controlador de domínio (*Active Directory*)

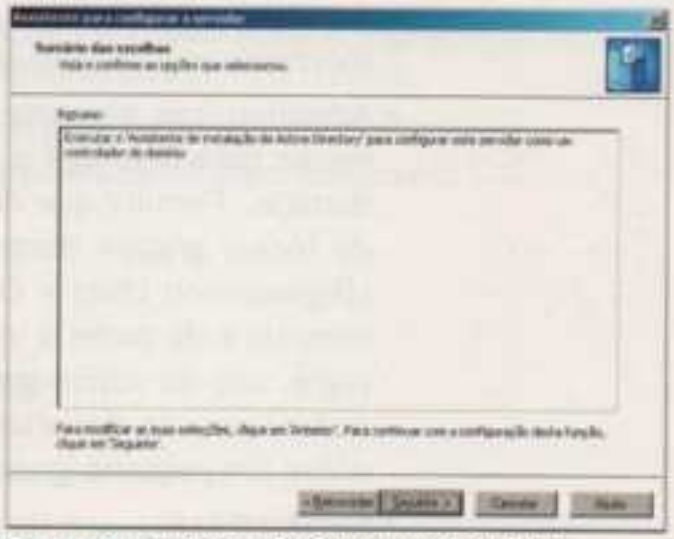

Fig. 3.159 Sumário das escolhas efectuadas

Surge uma caixa de diálogo a dar-nos as boas-vindas à instalação do *Active Directory*, igual à da figura 3.83. Para se prosseguir com a instalação do controlador de domínio deve-se clicar em **Seguinte**.

O restante processo de instalação e configuração é idêntico ao efectuado no capítulo 2.5.

3.3. *Active Directory*

Definições

Talvez a maneira mais fácil de definir o *Active Directory* (AD) seja chamar-lhe o serviço de directório do Windows Server 2003, com uma base de dados sobre informações de utilizadores, ficheiros, quaisquer objectos armazenados no directório (segundo a definição da sua classe e atributos/propriedades, de acordo com um conjunto de regras chamadas **Esquema** – *Scheme*) e, por exemplo, periféricos de rede; estas informações estão disponíveis tanto para administradores como para utilizadores, facilitando o trabalho a todos. No entanto, para que os clientes da rede tenham acesso aos serviços do *Active Directory*, eles têm de estar configurados como clientes do AD.

Um conceito de interesse no AD é o **Catálogo global** (*Global Catalog*), que conta com informações sobre todos os objectos do directório e que permite o acesso às mesmas aos utilizadores e administradores, não só sobre os próprios domínios, mas sobre qualquer um dos domínios na floresta. Como não podia deixar de ser, o servidor que o possui chama-se *Global Catalog Server* e, regra geral, este servidor é o primeiro controlador de domínio a ser configurado numa floresta.

Numa empresa com uma rede alargada, é de esperar que a complexidade do directório aumente, mas, para precaver situações deste tipo, o AD conta com um mecanismo de indexação e de pesquisa, que permite um acesso mais rápido e fácil aos recursos disponibilizados.

Vantagens do *Active Directory*

Embora já se tenham mencionado algumas das vantagens do AD, vamos tentar listar algumas das mais importantes:

- **Grande base de dados** – manter um índice de tudo o que se encontra no domínio, facilitando a pesquisa dos recursos.
- **Administração baseada em políticas** – implementar políticas de grupo com regras para restringir o acesso aos objectos do directório e aos recursos do domínio. Permitir que domínios se subdividam em subdomínios (capacidade de incluir grupos dentro de grupos), chamados unidades organizacionais (*Organization Units* – OU), nos quais se podem atribuir diversos pesos de controlo e de poder a indivíduos particulares (delegação de poderes que, por regra, são do administrador). Isto permite que se criem os chamados administradores de departamento – utilizadores com muito poder, mas apenas sobre um pequeno grupo de utilizadores e de máquinas.
- **Escalabilidade** – um domínio criado pode ser incluído numa árvore, que, por sua vez, faz parte de uma floresta.
- Domínios podem ser renomeados.
- **Permissões** – permitir que se criem utilizadores com diferentes níveis de permissões, desde contas de clientes quase sem poder algum até contas de utilizadores correntes com todo o poder de administrador ou apenas com algum desse poder.
- **Segurança da informação** – controlar o acesso dos utilizadores; estar a par de quem tem ou não tem autorização para usar a rede, através da manutenção de um serviço de autenticação.
- Providenciar um conjunto de servidores que funcionem como "servidores de autenticação" ou "servidores de *logon*", conhecidos como **Controladores de domínio** (*Domain Controllers*).
- Manter uma lista centralizada dos utilizadores e das *passwords*.
- **Extensibilidade** – capacidade de introduzir novas classes de objectos e de criar os próprios atributos ou de alterar atributos de objectos existentes.
- **Compatibilidade** – o AD conta com protocolos de acesso *standard*, que lhe permitem ser compatível com outros serviços, mais antigos, de directório.
- **Replicação (selectiva)** – na falha de um controlador de domínio (DC), qualquer outro pode desempenhar o papel do primeiro, através da replicação da informação entre os DC.
- **Integração com o DNS** – permite a "tradução" de endereços IP em nomes perceptíveis, sem haver necessidade da criação de uma tabela de conversão.

Ferramentas de administração do *Active Directory*

Além das ferramentas administrativas, o AD inclui nesse grupo alguns novos atalhos para as respectivas ferramentas, como, por exemplo:

- **Domínios e confianças do AD** – ferramenta que executa inúmeras tarefas administrativas, entre as quais:
  - a criação de relações de confiança entre domínios pertencentes a florestas diferentes ou com domínios NT;
  - passagem, no funcionamento de um domínio, do "modo misto" (garante compatibilidade com domínios Windows NT) para "modo nativo" (modo de funcionamento do Windows 2000/2003 e quando há certezas de não haver servidores NT na rede).

- **Serviços e locais (*sites*) do AD** – permite a criação de novos *sites* e migrar computadores entre eles; permite organizar a estrutura hierárquica de rede.
- **Computadores e utilizadores do AD** – permite criar e gerir objectos do directório, como os utilizadores, os grupos de utilizadores e as unidades organizacionais; permite gerir computadores.

3.4. Contas e grupos de utilizadores

Contas de utilizadores

As contas e os grupos de utilizadores podem variar mediante o tipo de servidor, dependendo se são servidores controladores de domínio, servidores membro ou servidores autónomos (*Standalone Server*). As contas de utilizadores destes dois últimos tipos de servidor, bem como do Windows NT Workstation, 2000 Professional e XP Professional, encontram-se guardadas em cada computador, numa base de dados chamada SAM – *Security Access Manager*, que, normalmente, se encontra localizada em **\Windows\system32\config**, dependendo do local onde se criou o directório da raiz do sistema (*system root directory*). Para um utilizador destes tipos de servidor entrar num domínio, ele terá de estar identificado, através de uma palavra-passe, por um controlador de domínio.

Num servidor que seja controlador de domínio (tem instalado o *Active Directory*), a segurança é controlada pelo *Active Directory*. O *Active Directory* guarda a informação de segurança num ficheiro designado NTDS.DIT, que se encontra, por defeito, em **Windows\NTDS**, embora se possa especificar um caminho diferente na rotina do DCPROMO. A base de dados NTDS.DIT guarda muito mais informação do que a base de dados SAM, chegando também a guardar informação sobre servidores e *workstations* (estações de trabalho), recursos, aplicações publicadas e políticas de segurança.

Sempre que são criadas contas de utilizadores, é-lhes automaticamente atribuído um identificador de segurança SID (*security identifier*), que é um número exclusivo que identifica uma conta. Os SID têm sido usados desde que começou o NT. O sistema não reconhece o nome do utilizador, mas sim o seu SID. As ID (identidades) do utilizador só lá estão para a interface humana. Os SID nunca são reutilizados; quando uma conta é apagada, o seu SID é apagado com ela. Um SID típico pode ter o seguinte aspecto:

S-1-5-21-1659004503-193565697-854245398-1002.

Os SID podem ser partidos em segmentos como este:

S-1-5-21-D1-D2-D3-RID

S-1-5- é apenas um prefixo *standard* (na realidade, o 1 é o número da versão, que não mudou desde o NT 3.1, e o 5 significa que o SID foi atribuído pelo NT); 21 também é um prefixo do NT; e D1, D2 e D3 são apenas números de 32 bit que são específicos para um domínio. Uma vez criado um domínio, são indicados os D1 até D3 e todos os SID daquele domínio passam a ter os mesmos três valores. Os RID significam identificadores relativos (*relative identifier*). O RID é a parte exclusiva de qualquer SID atribuído. Cada nova conta tem sempre

um número RID exclusivo/único, mesmo que o nome do utilizador ou outra informação seja a mesma de uma conta antiga. Deste modo, a nova conta não terá qualquer um dos direitos e permissões da conta antiga e a segurança é preservada.

Utilizadores e computadores do *Active Directory* – *Active Directory Users and Computers*

Active Directory Users and Computers é o nome dado à ferramenta de gestão de utilizadores, que se encontra disponível através do botão **Iniciar** (*Start*), depois **Ferramentas administrativas** (*Administrative Tools*) e, por fim, **Utilizadores e computadores do Active Directory** (*Active Directory Users and Computers*).

É esta ferramenta que possibilita, entre outras funções, por exemplo, a criação de contas de acesso (utilizadores) e de grupos (universais, globais e locais), o desbloqueamento de contas de acesso, alteração de propriedades de um utilizador e o envio de correio electrónico para utilizadores ou grupos. É também esta a ferramenta que é usada para gerir computadores ou até para usar "*templates* de utilizador", ou seja, "modelos de utilizador", pois esta ferramenta permite indicar que se quer criar um utilizador usando um outro como modelo.

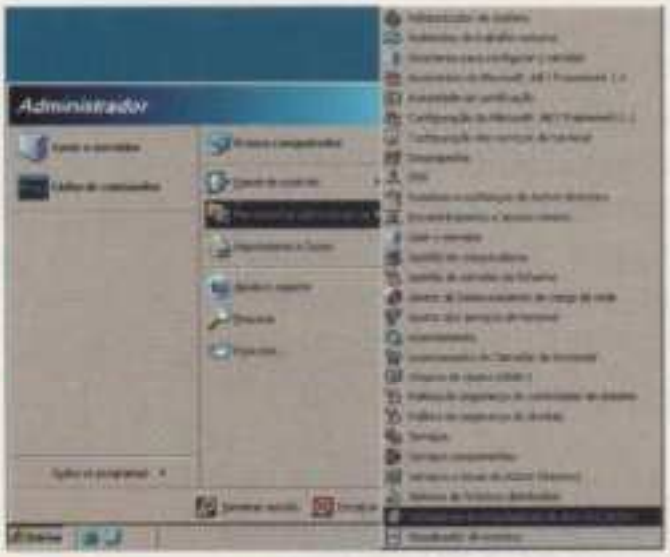

Fig. 3.160 Lançamento do gestor **Utilizadores e computadores do Active Directory**

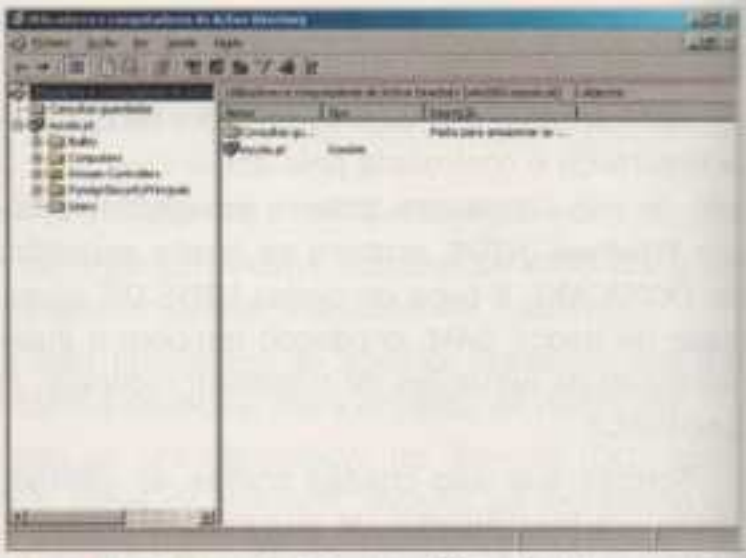

Fig. 3.161 Aspecto geral do gestor **Utilizadores e computadores do Active Directory**

Criação de contas de utilizadores

Para criar uma nova conta de acesso, ir ao gestor **Utilizadores e computadores do Active Directory** (*Active Directory Users and Computers*) e clicar com o botão direito do rato sobre o contentor onde se pretende criar o novo utilizador.

No menu que surge, escolher a opção **Novo** > **Utilizador** (*New* > *User*).

Indicar o nome próprio do utilizador, iniciais, apelido e nome completo.

Indicar o nome de *login* (no campo *logon*) para computadores que correm Windows 2000 e 2003 (composto pelo seu nome e pelo domínio, separados pelo símbolo @), e um nome usado para compatibilidade com sistemas anteriores ao Windows 2000 (NT/9x).

Clicar em **Seguinte** (*Next*).

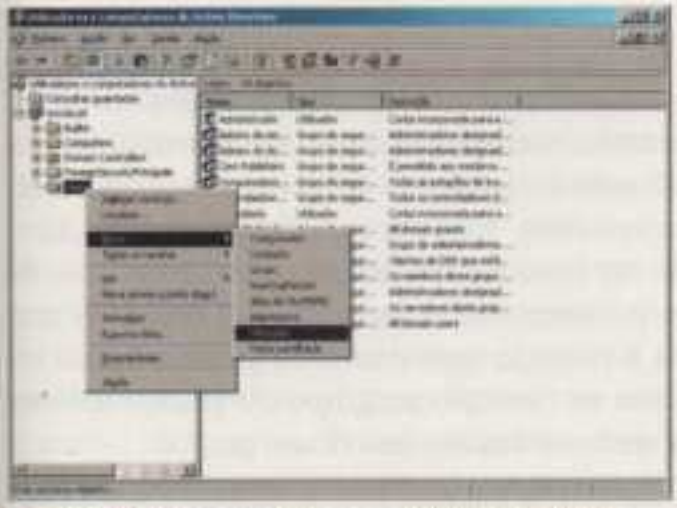

Fig. 3.162 Criação de um novo utilizador no *Active Directory*

Fig. 3.163 Janela de criação de um **Novo objecto – Utilizador**

Introduzir a palavra-passe (figura 3.164), e voltar a introduzi-la para confirmação.

Seleccionar uma das opções:

- o utilizador tem de mudar a palavra-passe no próximo início de sessão;
- o utilizador não pode alterar a palavra-passe;
- a palavra-passe nunca expira (nunca será necessário mudar de palavra-passe para a referida conta);
- conta desactivada (a conta não pode ser usada para acesso à rede, por não estar activa).

Clicar em **Seguinte** (*Next*), para prosseguir.

Verificar os dados apresentados no resumo da figura 3.165 (em caso de erros ou alterações, pressionar o botão **Retroceder**).

Clicar em **Concluir** (*Finish*).

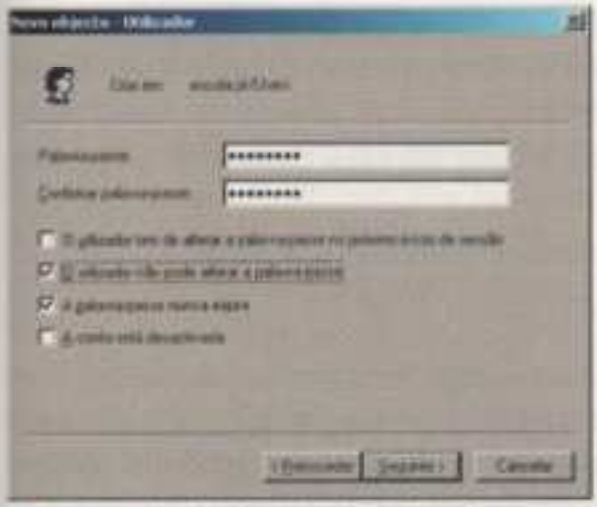

Fig. 3.164 Janela de atribuição da palavra-passe do utilizador

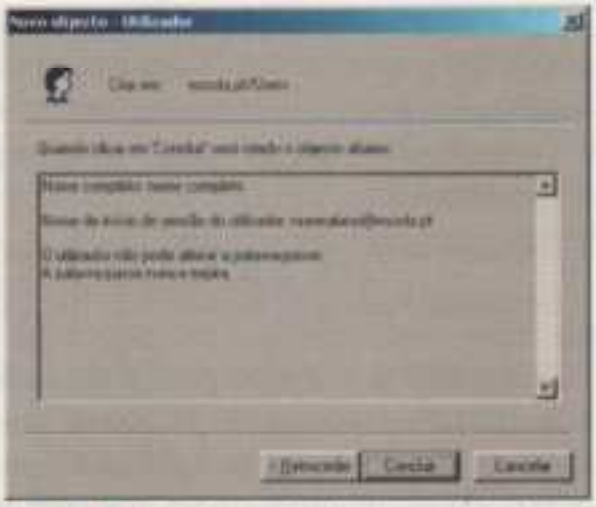

Fig. 3.165 Fim da criação do novo utilizador

A nova conta de utilizador está criada.

Como será explicado mais adiante, ainda neste capítulo, é possível criar *templates* (modelos) de utilizador por meio desta ferramenta, usando outro utilizador como modelo. O utilizador criado por meio deste processo acaba por ficar com a quase totalidade da informação – grupos de acesso, o *script* no momento do *login*, permissão, ou não, de alteração da palavra-passe, entre outros – da conta do primeiro utilizador. Através da utilização deste processo, facilitado por esta ferramenta, a criação de utilizadores com perfis semelhantes ou iguais acaba por se tornar muito mais produtiva.

Grupos de utilizadores

Um grupo de utilizadores, basicamente, não é mais do que reunir alguns utilizadores e geri-los em função das suas necessidades e características. Agrupar utilizadores facilita a atribuição de direitos para a realização de tarefas e de permissões para aceder a recursos, tais impressoras e pastas em rede. Este agrupar de utilizadores também facilita a tarefa de um administrador, no caso de um utilizador ter de mudar de departamento, por exemplo, pois, assim, o administrador apenas terá de ver a que grupo, ou grupos, o tal utilizador pertencia e mudá-lo para os novos grupos. Todas as permissões serão automaticamente perdidas em relação ao grupo ou grupos anteriores e novas permissões serão automaticamente atribuídas aos novos grupos.

Pode-se criar grupos de utilizadores para fins específicos e atribuir-lhes determinados direitos e permissões. Aos membros deste grupo criado pode, por sua vez, ser atribuída a capacidade de administrar outros grupos e objectos ou até mesmo unidades organizacionais inteiras. Grupos podem conter computadores, bem como utilizadores e outros grupos. Também podem ser usados como listas de distribuição de *e-mails*. Por tudo isto, é importante compreender os diferentes tipos de grupos que existem e como trabalhar com eles para delegar controlo, permitir acesso aos recursos necessários e configurar direitos.

Grupos universais, globais e locais

Onde é que eles são reconhecidos e o que podem conter? Estes são os assuntos principais que envolvem os grupos locais, locais de domínio (*domain local*), globais e universais. Uma vez que são usados para atribuir direitos e permissões, é necessário saber onde este *group membership* (admissão como membro do grupo) significa alguma coisa, onde é aceite.

Grupos universais

Um grupo universal pode fazer praticamente tudo. Os grupos universais só podem ser criados num *Domain Controller*, tal como os grupos globais e locais de domínio, mas com eles pode fazer-se o seguinte:

- colocar um grupo global de qualquer domínio na floresta dentro de um grupo universal;
- colocar um grupo universal dentro de qualquer tipo de grupo local;
- colocar um grupo universal dentro de outro grupo universal.

Finalmente, o grupo pelo qual estávamos à espera! Tal como as bonecas russas *matrioskas* (aquelas bonecas que se abrem e dentro da primeira boneca está outra e dentro daquela outra ainda e por aí fora), pode ter-se grupos universais dentro de grupos universais que, por sua vez, estão dentro de grupos universais...

Sendo assim, a pergunta que imediatamente nos vem à cabeça é: porque é que não usamos grupos universais para tudo e esquecemos os grupos locais de domínio e os grupos globais? Por dois motivos: primeiro, grupos universais só podem ser usados no Windows *server mode* ou no Windows 2000 *native mode* (modo nativo) – o que requer que todos os DC estejam a correr Windows Server 2003 ou Windows 2000 Server. Isto só é possível depois de se ter feito um *upgrade* de todos os *Domain Controllers* NT4 para Windows 2000 ou Server 2003; os *Domain Controllers* do NT4 não suportam grupos universais. Em segundo lugar, se usarmos apenas grupos universais, o catálogo global ficará demasiado cheio e pode tornar-se lenta a replicação de dados entre servidores que sejam *Global Catalog*.

Grupos globais

Este tipo de grupos só pode conter como membros outros grupos globais e contas de utilizadores do mesmo domínio e podem ser dadas permissões em qualquer domínio da floresta. No entanto, o *Active Directory* dá-lhes um pouco mais de poder – grupos globais podem existir dentro de outros grupos locais, desde que todos eles pertençam ao mesmo domínio. Pode-se colocar um grupo global dentro de um grupo local de qualquer domínio que confie (*trust*) no domínio do grupo global. Por isso, é possível colocar um grupo global num grupo local de um servidor-membro no mesmo domínio do grupo global ou dentro de um grupo local de qualquer outro domínio na floresta. Podemos pensar nos grupos globais como "grupos viajantes". São um ponto conveniente para juntar contas de utilizadores de domínio.

Grupos locais de domínio

Há, na realidade, duas facções de grupos locais de domínio: grupos locais de domínio inseridos (*built-in domain locals*) e outros grupos locais de domínio. Quando um servidor se torna um *Domain Controller*, os seus grupos locais de máquina tornam-se grupos locais de domínio e passam a estar no local de armazenamento inserido no *Active Directory*. Têm nomes familiares, como administradores, operadores de *backup* e operadores de impressoras. Há também novos grupos que foram criados com o domínio, como operadores de servidores (*Server Operator*) e operadores de contas (*Account Operator*). Estes grupos são parecidos com grupos locais de máquina, excepto no facto de todos os *Domain Controllers* num domínio partilharem a mesma base de dados de segurança. Por isso, cada *Domain Controller* terá os mesmos grupos locais e membros de grupo, como todos os restantes *Domain Controllers*. Se formos um membro de *Server Operators* num DC, então somos um membro de *Server Operators* em todos os DC. Estes grupos locais de domínio "inseridos" não podem ser movidos ou apagados e não podem tornar-se membros de outros grupos locais. Além disso, outros grupos locais não podem ser membros de grupos locais de domínio "inseridos".

Pelo que foi dito, **grupos globais** são grupos criados num *Domain Controller*, que podem conter como membros contas de utilizadores do domínio local e que podem ser colocados em qualquer grupo local, em qualquer máquina e em qualquer domínio dentro da floresta (ou em qualquer outro domínio que confia no domínio do grupo global). Por isso, se tivermos um grupo global criado no domínio A, e o domínio B confia no domínio A, então podemos colocar aquele grupo global em qualquer grupo local, em qualquer máquina, nos domínios A ou B.

Um **grupo local de domínio** age como um grupo global, exceptuando o facto de não poder ser usado fora do domínio. Pode-se apenas colocar um grupo local de domínio dentro dos grupos locais de máquinas dentro do mesmo domínio. Sendo assim, neste exemplo, um grupo local de domínio criado no domínio A poderia apenas ser colocado num grupo local numa máquina do domínio A. Vistas estas limitações, questiona-se o porquê da existência destes grupos locais de domínio.

Grupos locais básicos ou *machine local groups*

O grupo local básico, também chamado grupo local de máquina (*machine local group*), é o único tipo de grupo que pode ser criado nos servidores que tenham papel de *Standalone Server* ou como *member server*, no Windows NT Server, no Windows 2000 Server, no Windows Server 2003, no Windows NT Workstation ou no Windows 2000/XP Professional. No Windows 9x não existem grupos locais. Grupos locais são locais para as máquinas, ou seja, eles existem e são apenas válidos naquela *workstation* ou naquele servidor que não é um *Domain Controller*.

Um servidor *Standalone Server* Windows NT Workstation ou Windows 2000/XP Professional, que não é membro de um domínio, é como uma ilha sem conhecimento do mundo exterior, pois apenas reconhece os seus próprios grupos e utilizadores locais, ou seja, as permissões só podem ser dadas no próprio computador. Os grupos locais são os únicos a quem é dada permissão para aceder a recursos, e a sua admissão como membro é limitada a utilizadores locais. Quando, no entanto, a máquina se junta ao domínio, aquela ilha torna-se membro de um corpo de governação maior, como uma federação de ilhas. Pode ter contas de utilizadores locais, mas também pode aceitar contas de utilizadores criadas num *Domain Controller*.

Uma máquina usa os seus grupos locais para simplificar a administração. Imaginemos a seguinte situação: há um servidor com uma impressora e pretende-se controlar quem pode usar a impressora. Cria-se um grupo local, chamado "utilizadores de impressora" e dá-se ao grupo **utilizadores de impressora** permissão para imprimir nessa impressora. Mas como, inicialmente, não há ninguém nesse grupo, há que "povoá-lo". Talvez se queira deixar imprimir, nessa impressora, pessoas do domínio. Podiam inserir-se, uma a uma, as contas de utilizadores do domínio no grupo **utilizadores de impressora**, mas isto implicaria imenso trabalho; assim sendo, seria muito mais conveniente pegar num grupo que já contivesse aqueles utilizadores de domínio e colocar esse tal grupo no nosso grupo local. No entanto, um dos problemas é não se poder inserir grupos locais em grupos locais. Parece ser possível pegar no grupo A e colocá-lo, indiscriminadamente, dentro do grupo B, mas na realidade não o é. É por isto que os grupos locais são chamados grupos locais, para os diferenciar dos outros tipos de grupo.

A diferença entre este grupo e os outros tipos de grupos é que os últimos só podem ser criados em controladores de domínio. Assim sendo, um grupo local pode conter qualquer um dos três grupos "baseados em domínio" – os grupos globais, os locais de domínio (*domain local*) e os universais.

Outros factos sobre grupos

- Podem colocar-se contas de máquinas em grupos. Isto não era possível com o NT4.
- Há uma limitação, no *Active Directory* do Windows 2000 Server, que limita o tamanho de um grupo até, aproximadamente, 5000 membros.

Ao criar contas de grupos, tem-se ainda a opção de classificar um grupo como um grupo de segurança (*security group*) ou como um grupo de distribuição (*distribution group*).

O primeiro grupo é usado para questões de segurança, incluindo grupos e utilizadores aos quais são negadas, ou permitidas, permissões comuns aos seus elementos. Tal como as contas de utilizadores, os grupos de segurança têm números identificadores de segurança (SID) próprios. Há três grandes tipos de grupos de segurança: locais, globais e universais, ou, melhor, há quatro, se também incluirmos os locais de domínio. Como nos recordamos, a diferença entre um grupo local e um local de domínio é que o primeiro se encontra em servidores *Standalone Server* ou em servidores *Member Server* e Windows 2000 ou XP Professional, ou seja, não pertencem a *Domain Controllers*, enquanto que grupo local de domínio é um nome especial atribuído a um grupo local que existe num controlador de domínio (DC).

O segundo grupo não é um grupo de segurança, mas serve para criar grupos para listas de distribuição de mensagens. É mais fácil enviar correio electrónico (*e-mail*) aos alunos da turma do 11.º D, por exemplo, do que seleccionar individualmente, de uma lista, o nome de cada um dos alunos da turma.

Criação de grupos de utilizadores

Para criar um grupo de utilizadores é necessário, no ecrã da figura 3.166, ir ao gestor **Utilizadores e computadores do Active Directory** (*Active Directory Users and Computers*) e clicar com o botão direito do rato sobre o contentor onde pretendemos criar o grupo. No menu que surge, deve seleccionar-se a opção **Novo** > **Grupo** (*New* > *Group*).

Na janela que aparece (figura 3.167), deve inserir-se um nome para o grupo a ser utilizado pelo Windows Server 2003, um nome que garanta a compatibilidade com sistemas anteriores ao Windows 2000. De seguida selecciona-se o âmbito (*scope*) de grupo – local de domínio, global ou universal – e o tipo de grupo – segurança ou distribuição. Feito isto, clicar em **OK** e o grupo de utilizadores está criado.

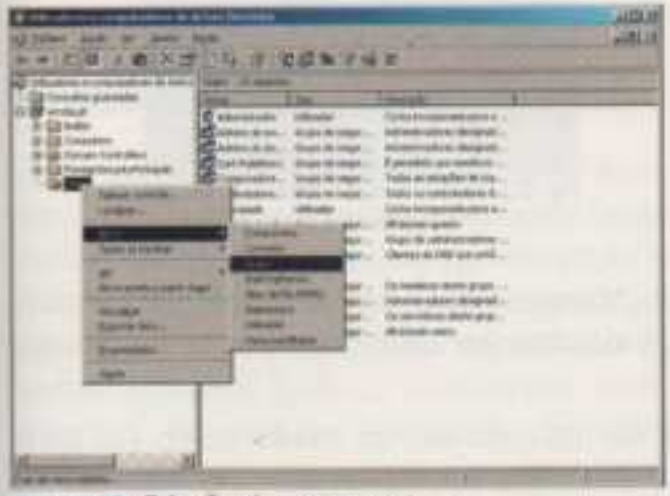

Fig. 3.166 Criação de um novo grupo

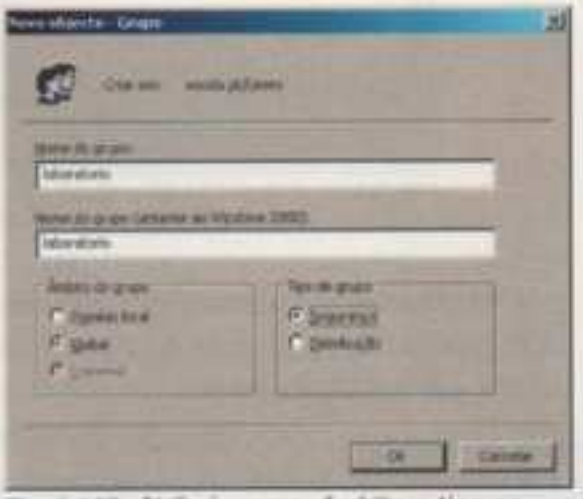

Fig. 3.167 Atribuir nome, âmbito e tipo ao novo grupo.

Caso se queira aceder a um maior leque de opções de configuração de um grupo, para além de apenas dar um nome ao grupo e de definir o seu âmbito e tipo, deve clicar-se com o botão direito do rato sobre o respectivo nome e, no menu, seleccionar a opção **Propriedades** (*Properties*), como mostra a figura 3.168.

No separador **Geral** (*General*), devemos indicar o nome usado em modo de compatibilidade (ambientes anteriores ao Windows 2000), uma descrição do grupo e o *e-mail*, para uma mais fácil identificação, bem como qualquer observação (**Notas**) que se considere pertinente registar. O âmbito e o tipo já se encontram seleccionados, devido aos passos anteriores à alteração das propriedades do grupo.

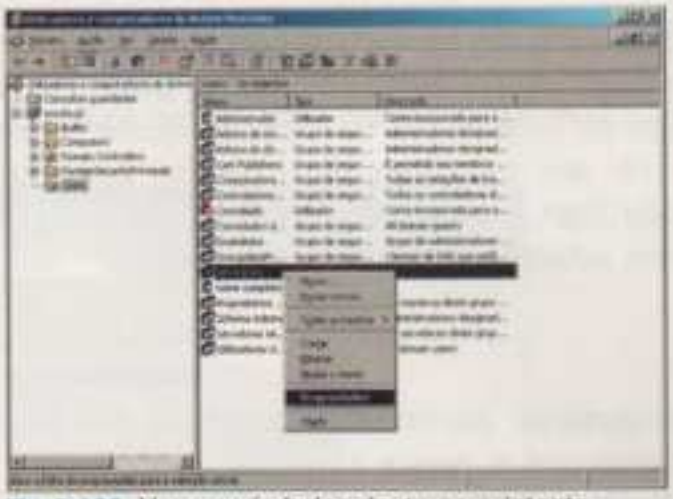

Fig. 3.168 Ver propriedades do grupo existente.

Fig. 3.169 Separador **Geral** das **Propriedades do grupo**

No separador **Membros** (*Members*) (figura 3.170) devemos atribuir utilizadores ao grupo e, para isto, deve pressionar-se o botão **Adicionar** (*Add*) e, baseado na lista que aparece, seleccionar os utilizadores pretendidos.

No separador **Membro de** (*Member of*) (figura 3.171) podemos optar pelos grupos locais ou universais em que pretendemos incluir o grupo criado, bastando para tal pressionar o botão **Adicionar** e seleccionar os grupos. A esta técnica dá-se o nome de *group nesting*, ou seja, encadeamento de grupos.

Fig. 3.170 Separador **Membros** das **Propriedades do grupo**

Fig. 3.171 Separador **Membro de** das **Propriedades do grupo**

Finalmente, no separador **Gerido por** (*Managed By*), definimos o responsável pela gestão do grupo, que, por defeito, é o administrador, mas que pode delegar poderes a outro utilizador.

Fig. 3.172 Separador **Gerido por** das **Propriedades do grupo**

A criação de grupos de utilizadores, do modo como foi apresentada, é apenas uma das duas formas existentes. Através do Windows Server 2003 é possível abrir um grupo e seleccionar os utilizadores que queremos que a ele pertençam (modelo apresentado), ou, então, pode-se seleccionar um utilizador e indicar todos os grupos a que queremos que a ele pertença. É claro que, para cada forma apresentada, os passos a seguir terão de ser inevitavelmente diferentes. No primeiro caso, há que começar pela criação de utilizadores, para que, posteriormente, ao criar um grupo, se possa aceder aos utilizadores e incluí-los no referido grupo. No segundo caso, o processo terá de seguir uma ordem "inversa". Se optarmos por indicar, utilizador por utilizador, quais os grupos a que cada um irá pertencer, então deveremos criar primeiro todos os grupos.

Para saber qual a melhor abordagem a fazer, talvez seja boa ideia começar por esquematizar em papel um levantamento do planeamento que se pretende fazer, até porque, se quisermos ter grupos de utilizadores com perfis iguais ou semelhantes, podemos e devemos recorrer aos *templates* do utilizador, para que os "utilizadores-modelo" estejam, desde logo, associados a grupos (assunto abordado na criação de utilizadores e mais adiante, ainda neste capítulo).

Domínios e *workgroups*

Ao trabalhar num ambiente tipo domínio, partimos do princípio que há muitos computadores a trabalhar em conjunto e, nesta situação, a segurança e a velocidade tornam-se prioritárias. Para um utilizador aceder à rede, este tem de ser validado por um *Domain Controller*, cuja função é verificar se as pessoas que se pretendem ligar à rede têm, ou não, autorização para o fazer. Caso o utilizador tenha permissão para trabalhar na rede, então o servidor *Domain Controller* passa essa informação e a do perfil do utilizador aos outros servidores

e postos de trabalho da rede. Qualquer utilizador ligado à rede, mas que não esteja validado e identificado perante o DC, é chamado **convidado** (*guest*), um desconhecido. Para que este desconhecido possa ser validado como membro do servidor, é necessário criar-lhe uma nova conta de utilizador. No caso de se tratar de uma empresa a trabalhar num ambiente *workgroup*, não haveria qualquer tipo de trabalho de gestão de rede para ligar o novo utilizador, o nosso desconhecido.

Num ambiente *workgroup*, normalmente, não há muitos computadores a trabalhar em conjunto e a segurança não é tida como uma prioridade. Como tal, qualquer utilizador "desconhecido" (não autorizado) não depara com grandes dificuldades em aceder à rede. O que se pretende com um *workgroup* está mais relacionado com a partilha de ficheiros, de impressoras, a partilha de acesso à Internet ou até troca de *e-mails* entre os computadores existentes.

Unidades organizacionais

As **unidades organizacionais** permitem fazer uma divisão de um domínio em várias unidades, como, por exemplo, uma divisão em vários departamentos. Cada unidade (departamento), nesta estrutura multinível, pode ter as suas próprias políticas de grupo e esquemas de segurança. Assim, cada unidade organizacional é uma espécie de "contentor" na estrutura do *Active Directory*, que se parece com pastas (*folders*) quando visualizado com ferramentas administrativas do *Active Directory*. Resumindo, unidades organizacionais são contentores que podem conter objectos – como contas de utilizadores ou de máquinas ou até mesmo outras unidades organizacionais – no *Active Directory*.

Aliás, ao criar uma conta de utilizador num domínio AD, pode-se escolher entre criar a conta directamente no domínio ou, então, criá-la dentro de uma daquelas coisas que se parecem com pastas e que se encontram naquele domínio.

Antes mesmo de se criar objectos para cada unidade, como grupos e utilizadores, convém planear a estrutura da unidade organizacional.

Para criar uma unidade organizacional deve-se clicar com o botão direito do rato sobre o ramo-pai, na árvore do AD onde se pretende incluí-la. No menu que surge, seleccionar **Novo** > **Unidade organizacional** (*New* > *Organizational Unit*), como mostra a figura 3.173.

De seguida, deve introduzir-se o nome da unidade organizacional e clicar em **OK**. Este passo deve ser repetido as vezes que forem necessárias até se obter a estrutura que se pretende. No final da criação da estrutura pretendida, a árvore terá um aspecto parecido com o da figura 3.174.

Fig. 3.173 Criação de uma **Unidade organizacional**

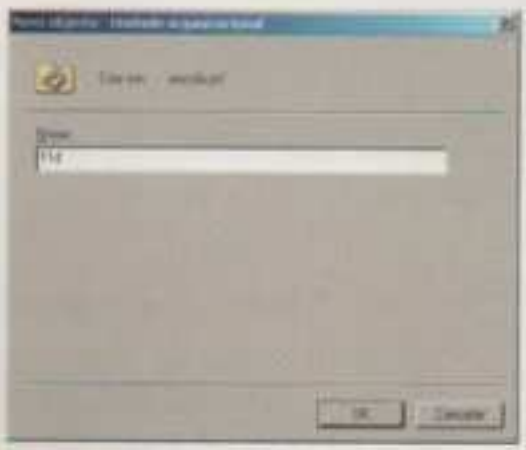

Fig. 3.174 Inserir nome na nova **Unidade organizacional**

Para povoar a árvore movem-se os objectos predefinidos pelo Windows Server 2003 para um dos contentores criados (por exemplo, "turmas"). Para o fazer, é necessário clicar com o botão direito sobre o nome do objecto e, no menu, seleccionar a opção **Mover** (*Move*).

Na janela da figura 3.176, basta seleccionar o contentor para o qual se pretende mover o objecto e repetir este passo as vezes que forem necessárias até se ter movido todos os objectos desejados.

O aspecto final da árvore do nosso domínio após termos movido o "contentor" **11d** para **turmas** é o seguinte:

Fig. 3.175 Mover "contentor" **11d**.

Fig. 3.176 Escolha do "contentor" para onde se vai mover o objecto.

Fig. 3.177 Aspecto final do "contentor" **turmas**

Criação e utilização de utilizadores-modelo

Fig. 3.178 Criação do utilizador-modelo

Como já foi referido, é possível criar *templates* de utilizador (modelos de utilizador) por meio da ferramenta **Utilizadores e computadores do Active Directory** (*Active Directory Users and Computers*), que está optimizada para este efeito, de modo a poupar trabalho. O modelo de utilizador criado acaba por ficar com a quase totalidade da informação da conta do primeiro utilizador.

Para definir utilizadores-modelo, ou seja, *templates* de utilizadores a serem usados na criação dos outros utilizadores, basta seguir os mesmos passos usados na criação de utilizadores:

- botão direito do rato sobre o contentor onde pretendemos criar o novo utilizador;
- escolher a opção **Novo** > **Utilizador-Modelo** (*New* > *Object User*);
- indicar o nome próprio do utilizador, iniciais, apelido e nome completo;
- indicar o nome de *login* (no campo *logon*) para computadores que correm Windows 2000 e 2003 (composto pelo seu nome e pelo domínio, separados pelo símbolo @) e um nome usado para compatibilidade com sistemas anteriores ao Windows 2000 (NT/9x);

- clicar em **Seguinte** (*Next*);
- introduzir a palavra-passe e voltar a introduzi-la para confirmação;
- seleccionar uma das opções apresentadas, de acordo com o que se pretende;
- clicar em **Seguinte** (*Next*);
- verificar os dados apresentados no resumo (em caso de erros ou alterações, pressionar o botão **Anterior**);
- Clicar em **Concluir** (*Finish*).

Como utilizar os utilizadores-modelo na criação de novos utilizadores?

Para criar utilizadores baseados no utilizador-modelo, basta, no ecrã da figura 3.180, seleccionar o utilizador na lista de utilizadores, clicar sobre ele com o botão direito do rato e, no menu que se apresenta, seleccionar a opção **Copiar** (*Copy*). Depois é só configurar os parâmetros (que ainda não estão preenchidos) que definem o utilizador.

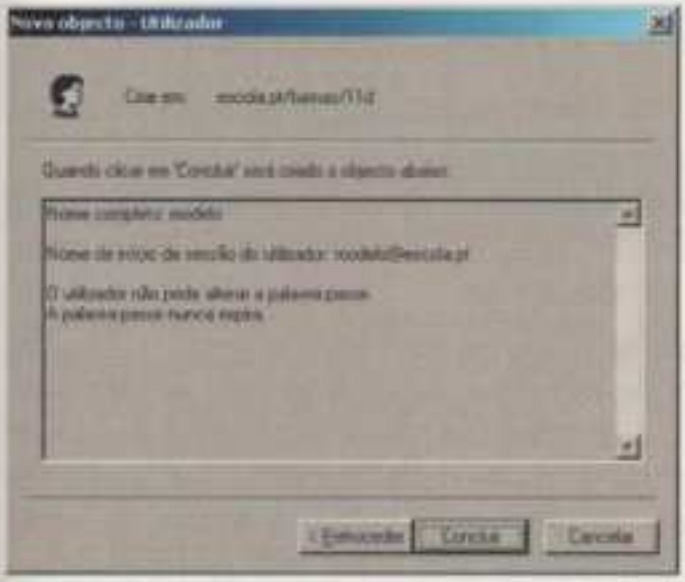

Fig. 3.179 Resumo da confirmação da conta do utilizador-modelo

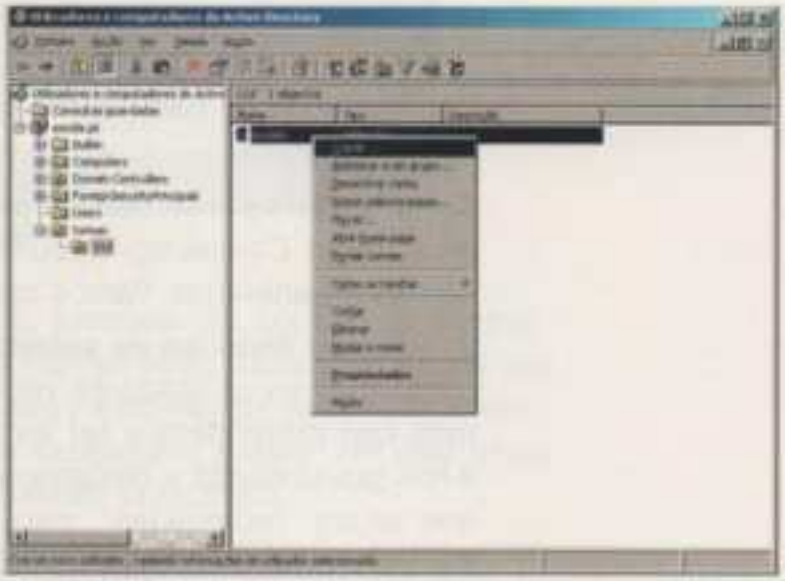

Fig. 3.180 Cópia de um utilizador-modelo

Definição da política para as contas de acesso

É possível definir uma política de utilização para as contas de acesso (utilizador), que, na realidade, não passa de um conjunto de propriedades, mais ou menos restritivas, aplicáveis a todas as contas e que permite harmonizar a nossa rede entre a segurança e a funcionalidade ou facilidade de utilização.

Para definir políticas de utilização de contas de acesso, devemos ir ao botão **Iniciar** (*Start*), depois **Ferramentas administrativas** (*Administrative Tools*) e, por fim, **Política de segurança do domínio** (*Domain Security Policy*).

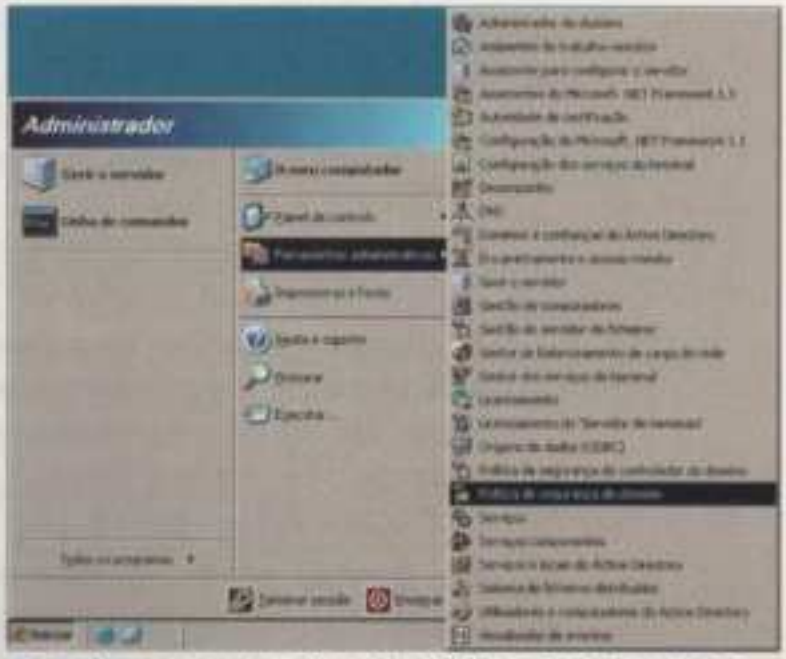

Fig. 3.181 Lançamento do gestor **Política de segurança do domínio**

- Na janela **Predefinições de segurança do domínio** (*Default Domain Security Settings*), clicamos em **Políticas de conta** (*Account Policies*) e seleccionamos **Política de palavras-passe** (*Password Policy*).

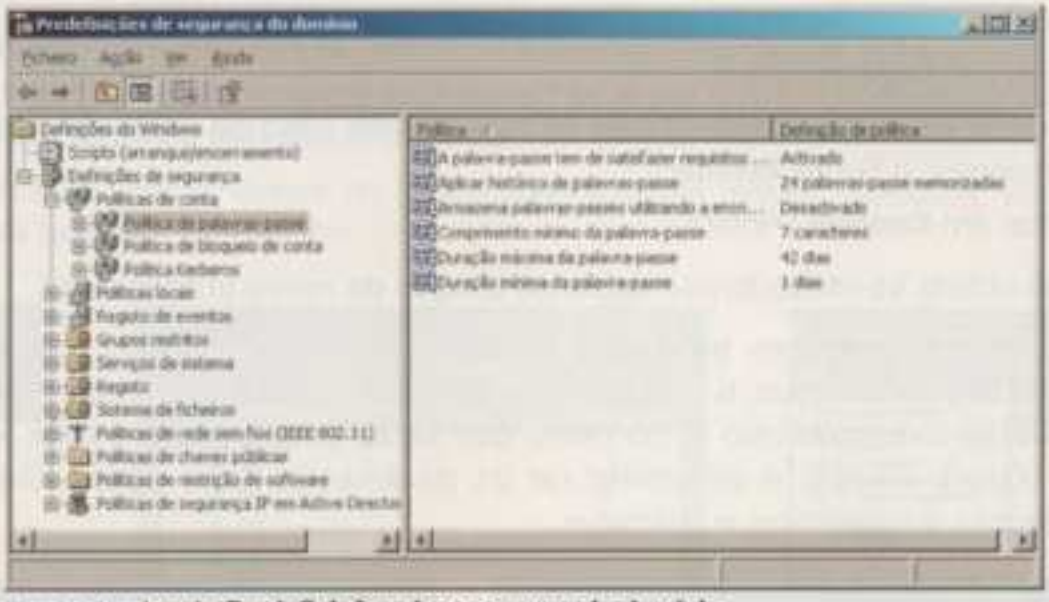

Fig. 3.182 Janela **Predefinições de segurança do domínio**

- Configuramos os parâmetros que nos interessem relativos às palavras-passe dos utilizadores:

  1 – **A palavra-passe tem de satisfazer requisitos de complexidade** (*Password Must Meet Complexity Requirements*) – activar (*enable*) ou desactivar (*disable*) este parâmetro. Vamos optar por desactivar.

  2 – **Aplicar histórico de palavras-passe** (*Enforce Password History*) – permite evitar que os utilizadores repitam as mesmas palavras-passe, se declararmos que pretendemos ter uma lista de palavras-passe. Com esta indicação é-nos possibilitada a designação do número das palavras-passe que queremos que sejam "recordadas", para cada utilizador, pelo sistema. Assim, se escolhermos o número três, então o utilizador terá de usar três palavras-passe diferentes (sempre que lhe for pedido para mudar a palavra-passe) antes de as poder repetir como sendo novas palavras-passe. Caso não haja problemas em que um utilizador repita palavras-passe antigas como sendo novas, basta indicar que não queremos manter uma lista de palavras-passe.

  3 – **Armazena palavras-passe utilizando a encriptação reversível** (*Store Passwords Using Reversible Encryption*) – activar (*enable*) ou desactivar (*disable*) este parâmetro. Vamos optar por desactivar.

  4 – **Comprimento mínimo da palavra-passe** (*Minimum Password Length*) – neste parâmetro é possível indicar um número mínimo de caracteres que se pretenda que cada palavra-passe tenha. Caso não se pretenda atribuir um tamanho mínimo, basta deixar a configuração em branco, ou seja, tamanho 0.

  5 – **Duração máxima da palavra-passe** (*Maximum Password Age*) – permite indicar a quantidade máxima de dias em que uma palavra-passe pode ser utilizada até ter de ser obrigatoriamente substituída. Se não indicarmos quantidade de dias, então o sistema nunca avisará o utilizador de que este terá de modificar a palavra-passe, pois ela será considerada "eterna".

  6 – **Duração mínima da palavra-passe** (*Minimum Password Age*) – ao indicar um período mínimo de vigência da cada palavra-passe, por exemplo 15 dias, garante-se a utilização da mesma palavra-passe, pelo menos, por um período de 15 dias. Assim, se tivermos uma lista de utilização de 3 palavras-passe

diferentes, tendo cada uma de ser usada pelo menos durante 15 dias, então um utilizador só poderá repetir uma palavra passe antiga passados, no mínimo, 45 dias (3 × 15). Caso não seja indicado nenhum número de dias, a palavra-passe poderá ser alterada a qualquer momento.

- O passo seguinte será seleccionar políticas de bloqueamento; para isso temos de seleccionar **Política de bloqueio de conta** (*Account Lockout Policy*).

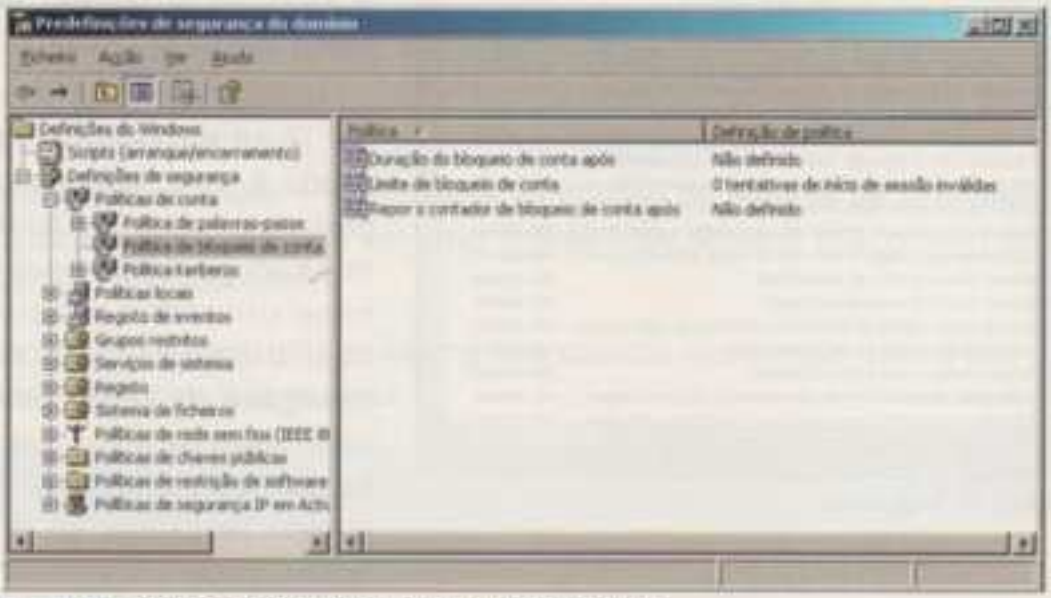

Fig. 3.183 Selecção de **Política de bloqueio de conta**

Neste parâmetro é possível trancar, ou seja, bloquear as contas de acesso. Numa administração de rede simples, talvez não se torne necessário fazer um bloqueamento de contas, e, assim, não há nada a configurar neste parâmetro. Caso se pretenda bloquear contas, torna-se necessário indicar em que situação e durante quanto tempo uma conta permanece bloqueada.

1 – **Duração do bloqueio de conta após** (*Account Lockout Duration*) – nesta situação é possível definir um determinado tempo para que o contador (de "tentativas inválidas de *logon*") regresse ao valor zero, após introdução da palavra-passe (correcta ou inválida). Indicar um valor neste campo poderá questionar a segurança do sistema, pois, neste caso, alguém mal-intencionado apenas teria de esperar até que o período de tempo predefinido fizesse o contador regressar a zero, para voltar a tentar introduzir uma nova palavra-passe, e assim sucessivamente, até acertar com a palavra-passe correcta. Se optarmos por um intervalo de tempo indefinido (*not defined*), então a segurança será restabelecida.

2 – **Limite de bloqueio de conta** (*Account Lockout Threshold*) – neste caso, podemos indicar um número máximo de vezes em que é permitido "falhar" na introdução da palavra-passe. Deste número só contam as tentativas inválidas e consecutivas, tal como acontece nas caixas multibanco, por exemplo. Caso, na primeira tentativa, a palavra-passe tenha sido mal introduzida, mas, na segunda tentativa, a palavra-passe seja validada, o contador de "tentativas inválidas de *logon*" regressará a 0 e só bloqueará após falhar o número máximo de tentativas permitidas.

3 – **Repor o contador de bloqueio de conta após** (*Reset Account Lockout Counter After*) – aqui define-se o tempo de duração do bloqueio da conta após introdução inválida do número de vezes permitido da palavra-passe. Se optarmos por não definir um tempo, a conta ficará bloqueada até que o administrador da rede a desbloqueie. No entanto, ao definir aqui um parâmetro, a conta será automaticamente desbloqueada passado o tempo definido.

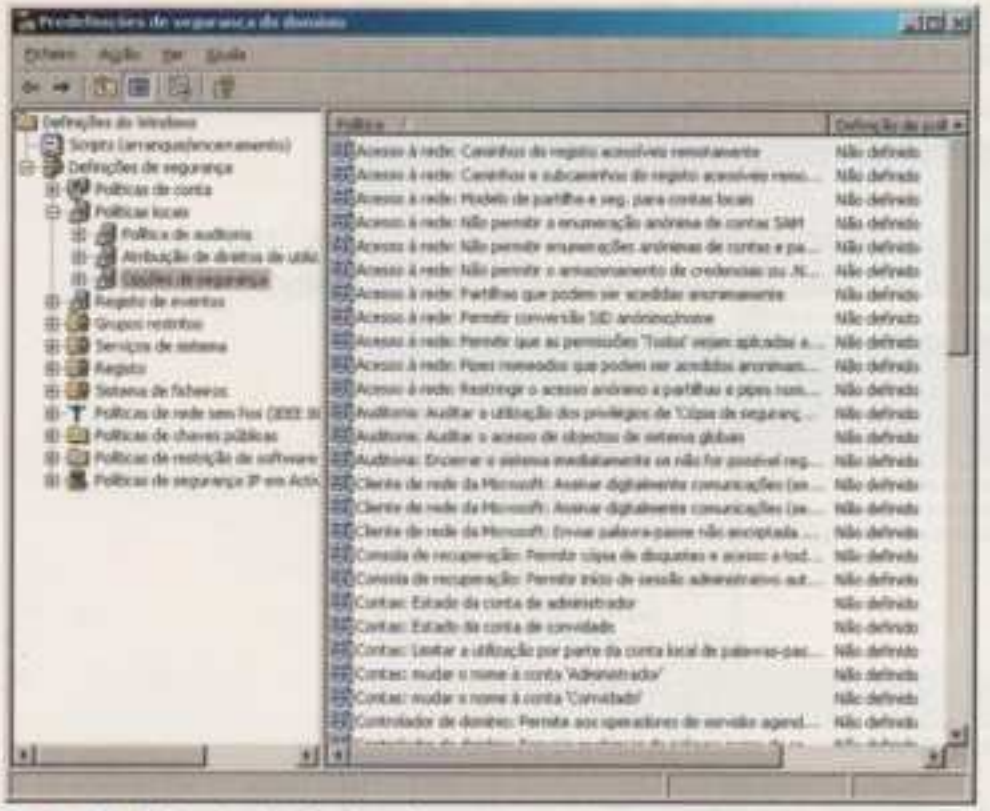

Fig. 3.184 Selecção de **Opções de segurança**

Podemos também querer indicar se os utilizadores são automaticamente desligados da rede num horário em que não deveriam estar a usá-la. Neste caso, teremos de abrir **Políticas locais** (*Local Policies*) e seleccionar **Opções de segurança** (*Security Options*).

Note-se que, se um utilizador já se encontra a trabalhar, ligado à rede, quando chega o período em que já não tem permissão para se ligar a ela, esse utilizador poderá continuar o seu trabalho sem ser desligado da rede. Este parâmetro apenas evita que um utilizador se possa ligar fora do horário permitido; se já estiver ligado, poderá continuar com o seu trabalho.

Se, por outro lado, tivermos a intenção de realmente desligar da rede um determinado utilizador, devemos já ter predefinido um horário para aquele utilizador (configurar este parâmetro na "criação de utilizadores") e, neste caso, devemos activar a opção **Terminar automaticamente a sessão dos utilizadores quando o tempo de início de sessão expira** (*Automatically Logoff Users When Logon Time Expires*).

Política de permissões e direitos do utilizador

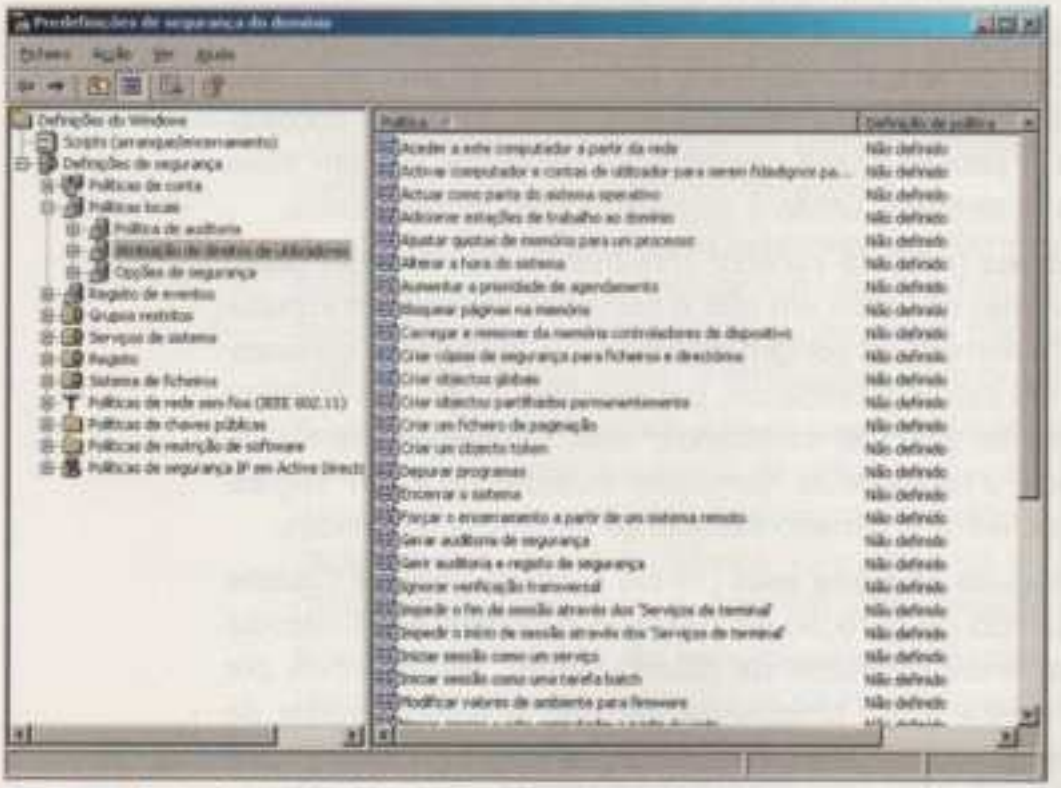

Fig. 3.185 Selecção de **Atribuição de direitos de utilizadores**

Uma das funções de um administrador consiste em fornecer a alguns utilizadores acesso a determinados recursos de rede e manter outros utilizadores afastados desses mesmos recursos. Desde o NT 3.1 que os sistemas operativos da Microsoft deixam controlar o acesso por meio de duas ferramentas: permissões e direitos.

Permissões e direitos... A diferença entre estes dois conceitos é extremamente vaga; talvez se possa definir **permissões** como algo que

autoriza o acesso a diferentes objectos, enquanto que **direitos** dá aos utilizadores a capacidade de fazerem algumas coisas em particular. Basicamente, uma permissão é apenas um cenário que controla o nível de acesso a um objecto na rede e direitos, em geral, tendem a aplicar-se a um sistema particular (por exemplo, o direito de fazer *logon* no sistema, o direito de mudar o seu tempo e o direito de o encerrar).

Para ver ou modificar a atribuição dos direitos locais para um utilizador ou grupo de utilizadores, basta-nos estar na janela em que ficamos no ponto anterior. Assim, ainda dentro da janela **Predefinições de segurança do domínio** (*Default Domain Security Settings*), é possível definir quais os utilizadores que podem realizar determinadas tarefas:

- abrir **Políticas locais** e seleccionar **Atribuição de direitos de utilizadores** (*User Rights Assignment*) para ver uma listagem de direitos que podem ser atribuídos aos utilizadores.

Na tabela 3.8 encontram-se alguns dos direitos mais importantes dos utilizadores locais e respectiva descrição.

Direitos do utilizador	Descrição
Aceder a este computador a partir da rede *(Access this computer from network)*	Permite aos utilizadores acederem ao referido computador através da rede.
Adicionar estações de trabalho ao domínio *(Add workstations to domain)*	Torna as máquinas membros de domínio; permite aos utilizadores alterarem a lista de computadores integrados num determinado domínio. Aos grupos de utilizadores administradores e operadores de contas (*Administrators* e *Account Operators*) é automaticamente dada esta permissão.
Criar cópias de segurança para ficheiros e directórios *(Back up files and directories)*	É normal pensar como é que é possível fazer cópias de segurança de ficheiros, quando, por exemplo, não se tem permissão para sequer os ler; pois é, mas qualquer utilizador a quem é dado este direito pode fazer *backups* de qualquer ficheiro no sistema, incluindo aqueles aos quais lhe foi negado acesso – os direitos sobrepõem-se às permissões!
Alterar a hora do sistema *(Change the system time)*	Altera a hora do sistema do computador local (relógio interno).
Permitir iniciar sessão localmente *(Logon locally)*	Atribui permissão para trabalhar no computador em que esta configuração é feita. Inicia a sessão localmente no próprio computador-servidor.
Restaurar ficheiros e directórios *(Restore files and directories)*	Permite restaurar ficheiros e pastas.
Encerrar o sistema *(Shut down the system)*	Permite encerrar o sistema (Windows Server 2003).
Tomar posse de ficheiros ou outros objectos *(Take ownership of files or other objects)*	Define os utilizadores que podem apoderar-se de ficheiros e directórios. No caso de um utilizador anterior ter saído da turma, por exemplo, a sua conta de utilizador foi apagada, mas um novo utilizador que tenha esta permissão pode ainda aceder aos dados da conta apagada, tornando-se "dono" do directório (*take ownership*) e depois dar acesso a si próprio.
Iniciar sessão como um serviço *(Logon as a service)*	Uma conta pode ser utilizada para fazer *logons* não interactivos. Fornece serviços de segurança (o utilizador que executa uma replicação faz o *logon* como um serviço).

Tabela 3.8 Direitos mais importantes dos utilizadores

Direitos do utilizador	Descrição
Actuar como parte do sistema operativo *(Act as part of the operating system)*	Age como uma parte de confiança do sistema operativo; alguns subsistemas têm este privilégio garantido.
Ignorar verificação transversal *(Bypass traverse checking)*	Atravessa uma árvore directório, mesmo que o utilizador não tenha outros direitos de aceder àquele directório. Por exemplo, não se tem acesso a **C:\Ficheiros**, mas tem-se acesso a **C:\Ficheiros\Sala**, então não se pode aceder a **C:\ Ficheiros\Sala**,a não ser que se tenha permissão de passar por cima da verificação transversal.
Criar um ficheiro de paginação *(Create a pagefile)*	Cria um ficheiro de paginação.
Criar um objecto *token* *(Create a token object)*	Cria *tokens* de acesso. Apenas a autoridade da segurança local deveria ter este privilégio.
Criar objectos partilhados permanentemente *(Create permanent shared objects)*	Cria objectos de partilha permanente.
Depurar programas *(Debug programs)*	Localiza e elimina erros dos programas.
Negar acesso a este computador a partir da rede *(Deny access to this computer from the network)*	Oposto do direito de "aceder a este computador a partir da rede"; revoga especificamente o direito a utilizadores/grupos que normalmente o teriam.
Recusar início de sessão como uma tarefa batch *(Deny logon as a batch job)*	Revoga o direito de fazer o *logon* como serviço batch.
Recusar o início de sessão como um serviço *(Deny logon as a service)*	Revoga o direito de fazer o *logon* como serviço.
Recusar início de sessão local *(Deny logon locally)*	Revoga o direito de fazer o *logon* localmente.
Activar computador e contas de utilizador para serem fidedignos para delegação * *(Enable computer and user accounts to be trusted for delegation)*	Designa contas que podem ser delegadas.
Forçar o encerramento a partir de um sistema remoto *(Force shutdown from a remote system)*	Permite que um computador seja encerrado a partir de um sistema remoto.
Gerar auditoria de segurança *(Generate security audits)*	Gera entradas *(Audit log)*.
Ajustar quotas de memória para um processo *(Increase quotas)*	Aumenta quotas de objectos (cada objecto tem uma quota associado a ele).
Aumentar a prioridade de agendamento *(Increase scheduling priority)*	Acelera a prioridade prevista de um processo.
Carregar e remover da memória controladores de dispositivo *(Load and unload device drivers)*	Adiciona ou remove *drivers* dos periféricos do sistema.
Bloquear páginas na memória *(Lock pages in memory)*	Encerra páginas na memória para evitar que sejam enviadas *(paged out)* para o *backing store* (como PAGEFILE.SYS).
Iniciar sessão como uma tarefa batch *(Log on as a batch job)*	Faz o *logon* ao sistema como uma tarefa batch *(Batch queue facility)*.
Gerir auditoria e registo de segurança *(Manage auditing and security log)*	Especifica que tipos de eventos e acessos de recurso são para ser verificados / auditados. Também permite ver e limpar o log de segurança.

(cont.)

[continuação]

Direitos do utilizador	Descrição
Modificar valores de ambientes para firmware *(Modify firmware environment values)*	Modifica variáveis de ambientes de sistema (e não variáveis de ambientes de utilizador).
Traçar um perfil de um processo único *(Profile single process)*	Usa capacidades de perfis para observar um processo.
Traçar um perfil do desempenho do sistema *(Profile system performance)*	Usa capacidades de perfis para observar o sistema.
Remover computador da estação de ancoragem *(Remove computer from docking station)*	Remove um computador portátil da sua estação de ancoragem.
Substituir um *token* de nível de processo *(Replace a process level token)*	Modifica um *token* de acesso ao processo.
Sincronizar os dados do serviço de directório *(Synchronize directory service data)*	Faz uma actualização da informação do *Active Directory*.

Tabela 3.9 Direitos menos importantes dos utilizadores

Para adicionar ou remover um direito de um utilizador ou grupo, basta clicar duas vezes sobre o **direito**, ou seleccionar o **direito**, clicar com o botão direito do rato sobre o mesmo (no painel de detalhes) e escolher **Propriedades**. Para remover esse direito de um utilizador ou grupo, selecciona-se o nome do utilizador ou do grupo e escolhe-se **Remover** (*Remove*). Para adicionar um utilizador ou um grupo à lista, escolhe-se **Adicionar utilizador ou grupo** (*Add User or Group*) e na caixa de diálogo **Seleccionar utilizadores, computadores ou grupos** (*Select Users, Computers or Groups*) digita-se um nome ou, então, usa-se o botão **Avançado** (*Advanced*) para procurar o nome.

Nota: Para ver ou modificar a atribuição de direitos locais a um utilizador ou grupo de utilizadores num computador que não seja um *Domain Controller*, é necessário abrir a ferramenta de política de segurança local (*Local Security Policy Tool*) do grupo de ferramentas administrativas (*Administrative Tools Group*).

É normal pensar em permissões em termos de ficheiros e directorias, mas há muitas outras coisas na família dos sistemas operativos NT da Microsoft que têm permissões.

Eis um exemplo simples de permissões: clicar com o botão direito sobre num ficheiro chamado **EXEMPLO.TXT**, no disco duro, escolher **Propriedades** e de seguida no separador **Segurança** (*Security*). Para mais detalhes, basta clicar no botão **Avançadas** (*Advanced*).

Não esquecer que a realização deste tipo de permissões só é possível em partições formatadas em NTFS.

3.5. Perfis de utilizador

Introdução

Uma vez que estamos a usar o Windows e suas aplicações, acabamos por querer adaptar às nossas preferências o nosso **Ambiente de trabalho** (*Desktop*) e as aplicações no mesmo. Coisas como a escolha de fontes e de cor do *desktop*, os itens que surgem no menu **Iniciar**, atalhos, tamanhos e exposições das janelas do

Explorador, os ícones existentes no *desktop*, entre outros, fazem todas parte de algo chamado o **Perfil do utilizador** (*User Profile*), que se encontra guardado no disco duro local do computador. Resumindo, um perfil de utilizador é todo o conjunto de parâmetros do ambiente de trabalho de cada utilizador da rede.

Todas estas definições podem ser efectuadas por um utilizador que deseje personalizar o seu *desktop*, mas estas também podem ser configuradas pelo administrador do sistema, responsável por configurar *desktops*, ou até por uma conjugação entre ambos. Por outras palavras, um utilizador poderá criar atalhos (*shortcuts*) e seleccionar um *screensaver*, enquanto que um administrador poderá configurar grupos de programas especiais para o *desktop* do utilizador, por exemplo.

Ao usar perfis de utilizador consegue-se dar ambientes de trabalho diferentes a vários utilizadores que usam a mesma máquina, ou dar o mesmo ambiente de trabalho a um utilizador que use máquinas diferentes, de dia para dia.

Nota: O Windows NT4, o 2000, o XP e o Server 2003 lidam com os perfis de modo idêntico. A única diferença está no nome do directório do perfil. A Microsoft mudou os perfis **\WINNT\PROFILES** do NT4 para ***Documents and Settings*** no Windows 2000 e no XP. Se fizermos esta substituição na nossa mente, somos capazes de aplicar tudo isto em *workstations* NT.

Tipos de perfis

Os perfis de utilizador podem ser implementados de diferentes maneiras, de acordo com as necessidades da organização. Em situações onde não é desejável uma solução baseada em rede, há ainda muitas outras opções a ter em conta:

- **Perfis locais** (*Local Profiles*) – estes são específicos para cada computador. Os utilizadores mantêm apenas perfis locais e são eles que criam e configuram esses perfis. Neste caso, as definições configuradas pelo utilizador, na criação de um perfil local, não o seguem, se este mudar de estação de trabalho. Só é possível voltar a aceder ao perfil quando se voltar a fazer o *logon* na máquina em que o perfil foi colocado.
- **Perfis de utilizador preconfigurados por defeito** (*Preconfigured Default User Profile*) – os utilizadores mantêm apenas perfis locais, mas um administrador pode preconfigurar um *magic*, ou seja, um perfil de utilizador guardado localmente, chamado **perfil de utilizador "por defeito"** (*"default" user profile*). Qualquer utilizador que se liga a este sistema recebe aquele perfil de utilizador "por defeito" como ponto de arranque para a criação do seu perfil de utilizador pessoal.
- **Perfis locais preconfigurados** (*Preconfigured Local Profiles*) – os utilizadores mantêm apenas perfis locais, mas um administrador preconfigura tudo ou uma parte dos perfis do utilizador local.
- **Perfis ambulantes** (*Roaming Profiles*) – estes perfis podem ser acedidos a partir de diferentes pontos da rede. Para os criar é necessário adicionar um caminho (*path*) de perfil à informação da conta do utilizador, para automaticamente criar e manter uma cópia do perfil do utilizador num local de rede (o utilizador pode configurar o seu próprio perfil).

Para definir um destes perfis, teremos de:

- no **controlador de domínio**, criar uma pasta onde serão guardados os perfis dos utilizadores;

- partilhar a pasta criada, por exemplo, com o nome **user_perfil**;
- dentro desta pasta, criar outra com o nome do utilizador (nome utilizado no *logon*);
- na janela **Utilizadores e computadores do Active Directory** (*Active Directory Users and Computers*), clicar com o botão do lado direito sobre o utilizador e seleccionar **Propriedades**;
- seleccionar o separador **Perfil**;
- em **Caminho do perfil**, indicar o caminho da pasta onde serão armazenados os perfis do utilizador **aluno** – **\\Win2003\User_perfil\aluno**;
- no nosso exemplo, o servidor tem o nome **Win2003** e, para cada utilizador, é necessário alterar o nome da pasta do utilizador de **aluno** para o nome do novo utilizador;
- clicar em **Aplicar** e, depois, em **OK**, para validar as configurações efectuadas.

Fig. 3.186 Separador **Perfil** do utilizador **Aluno**

O teste do funcionamento pode ser realizado através de dois computadores com o mesmo sistema operativo, ou por diferentes SO, por exemplo, Windows XP Professional e Windows 2000 Professional

No primeiro computador, executar o *logon* com o utilizador configurado a funcionar como **Perfil ambulante**. Na pasta partilhada, onde se encontram guardados os perfis do utilizador, o computador, inicialmente, utilizará o perfil **Default User Local** como modelo. De seguida, alterar, por exemplo, a cor de fundo do ambiente de trabalho e fazer o *logoff* do utilizador. Verificar se na pasta **\\Win2003\User_perfil\aluno** ficaram armazenados os perfis do utilizador **aluno** (inicialmente, esta pasta estava vazia). Ligar a segunda máquina e fazer o *logon* com o mesmo utilizador. Pode-se constatar que a cor de fundo do ambiente de trabalho ficou igual à do primeiro computador. Caso se esteja a usar o mesmo utilizador em dois ou mais computadores, o perfil guardado é o do computador onde foi realizado o último *logoff*.

- **Perfis ambulantes preconfigurados** (*Preconfigured Roaming Profiles*) – para os criar é necessário adicionar um caminho (*path*) de perfil de utilizador à informação da conta do mesmo e copiar um perfil preconfigurado para o local de rede especificado (o utilizador pode fazer alterações ao seu perfil, mas é o administrador quem cria o estado inicial do perfil). Para copiar perfis, deve usar-se o ícone **Sistema do painel de controlo**.
- **Perfis de utilizador de rede por defeito** (*Network Default User Profiles*) – para os criar é necessário criar um perfil de utilizador por defeito e copiá-lo para a partilha (*share*) **NETLOGON** do *Domain Controller* de autenticação. Isto vai distribuir perfis por defeito a todos os novos utilizadores (os utilizadores podem fazer alterações aos seus perfis). Esta opção pode ser usada em conjunto com perfis ambulatórios ou perfis locais.
- **Perfis obrigatórios** (*Mandatory Profiles*) – estes perfis são muito parecidos com os perfis ambulantes, só que são obrigatórios, ou seja, não podem ser modificados pelos utilizadores. Na prática, um utilizador pode alterar, por exemplo, o ambiente de trabalho, mas as alterações não são gravadas; assim, quando o utilizador fizer novamente o *logon*, a configuração será a mesma da existente antes das modificações efectuadas pelo utilizador.

Para criar este tipo de perfis, é necessário, em primeiro lugar, transformar um perfil em **Perfis ambulantes** (*Roaming Profiles*), como foi analisado anteriormente. Deve-se realizar, pelo menos uma vez, o *logon* e o *logoff*, para que este novo perfil fique armazenado no local especificado no servidor. De seguida, teremos de mudar o nome da pasta que contém o perfil e adicionar **.man** à pasta. Não nos podemos esquecer de alterar o nome deste ficheiro no separador **Perfil** das **Propriedades da conta do utilizador**. Por fim, devemos aceder à raiz da pasta que contém o perfil e modificar o nome do ficheiro **ntuser.dat** para **ntuser.man**.

Após efectuar o primeiro *logon* deste perfil, o servidor onde estão guardados os perfis tem de estar permanentemente disponível, de outro modo o *logon* não é efectuado.

Perfis locais, ambulantes e obrigatórios

No meio de tantos tipos de perfis, qual será o tipo de perfil indicado para a nossa rede? Para poder ajudar a tomar uma decisão, os parágrafos seguintes irão sumariar os **prós** e os **contras** dos diferentes tipos de perfis.

- **Perfis locais** – estes perfis podem ser a melhor escolha num ambiente de clientes diversos (mistos) ou num ambiente onde os utilizadores não necessitam de mudar de máquina.
- **Perfis ambulantes** – este tipo de perfil tem duas grandes vantagens: mobilidade e tolerância a erros. Será talvez o mais indicado para utilizadores que mudem com frequência de postos de trabalho e, visto dar mais flexibilidade, talvez seja mais indicado para utilizadores mais experientes. Os utilizadores não só podem mudar de *desktop* para *desktop* e continuar com as suas definições preferidas, como também contam com um *backup* do seu perfil guardado no servidor, uma vez que os perfis ambulantes não são guardados localmente, mas num ponto da rede. Se houver necessidade de reinstalar a *workstation*, o utilizador não terá, necessariamente, de reconfigurar o ambiente de trabalho. Mais ainda, é possível deixar a *workstation* criar o perfil, desde que não haja nenhuma definição especial a distribuir pelos utilizadores. Esta será, também, a opção a tomar se pretendermos que os perfis sejam localizados e controlados centralmente.

  A parte mais negativa é que os perfis ambulantes poderão estar disponíveis em outras máquinas, mas poderão não trabalhar correctamente após o *download* dos mesmos. Dois dos problemas possíveis com os quais o utilizador se poderá deparar poderão estar relacionados com os atalhos para aplicações que existem apenas na *home workstation* do utilizador e com as diferentes capacidades do monitor e/ou da placa gráfica. Além disso, perfis ambulantes que são "disparados" pela Ethernet, sempre que um utilizador faz o *logon* ou o *logoff*, acabarão por gerar mais tráfego e provocar demora no *logon* e no *logoff* do utilizador.

  Todas as alterações que são feitas no ambiente de trabalho pelo utilizador, enquanto este está a aceder à rede, são registadas no perfil que se encontra no disco local e, assim que for feito o *logoff*, o seu perfil é novamente copiado, mas desta vez do posto de trabalho para o servidor Windows Server 2003, de modo a estar disponível e actualizado da próxima vez.

Finalmente, convém não esquecer que o NT, o 2000 ou o XP guardam uma cópia local do perfil para cada utilizador que faz o *logon* numa determinada máquina. Se os utilizadores estiverem sempre a mudar de máquinas, deixarão cópias atrás de si, ocupando espaço no disco duro e apresentando problemas de segurança (poderão existir alguns itens no *desktop* que não se gostaria de deixar para trás). Para resolver este problema, podem-se configurar as máquinas para que estas apaguem cópias acumuladas de perfis ambulantes.

- **Perfis obrigatórios ou mandatórios** – os perfis obrigatórios, por também serem ambulantes, têm o benefício de terem mobilidade e serem tolerantes a falhas. Podem também estar localizados e ser controlados centralmente, tal como os perfis ambulantes. Além disso, os perfis obrigatórios são a única forma de obrigar um utilizador a carregar um determinado perfil, o que, por sua vez, tira alguma flexibilidade ao utilizador final, protegendo, talvez, alguns utilizadores mais inexperientes. Assim, é possível garantir que os utilizadores com perfis obrigatórios não possam trabalhar, em rede, fora do ambiente para eles predefinido.

  Estes tipos de perfis permitem que o utilizador faça algumas alterações ao seu ambiente de trabalho, enquanto estiver a trabalhar nele; mas, assim que terminar a sessão, tudo regressa ao que estava definido como perfil obrigatório. Nenhuma alteração é guardada – não há actualizações. Como se trata de perfis *read only* (apenas de leitura), os utilizadores podem partilhar um mesmo perfil, em vez de ter um por cada utilizador e, deste modo, há menos perfis guardados no servidor.

  Enquanto que os perfis obrigatórios oferecem mais controlo do que os perfis ambulantes, eles também requerem mais trabalho de configuração. É necessário criar um perfil obrigatório manualmente e só depois colocá-lo num ponto da rede, pois o sistema operativo não consegue criar perfis obrigatórios.

Localização em disco dos perfis de utilizador

Um perfil de utilizador é criado automaticamente pelo sistema assim que um utilizador se liga pela primeira vez a uma máquina NT, Windows 2000 ou XP. Este directório de perfil está localizado em **%SYSTEMROOT%\PROFILES** numa máquina NT4 ou num *upgrade* de um NT4 para Windows 2000. Numa instalação "limpa" do sistema Windows 2000, XP ou Server 2003, os perfis encontram-se guardados num directório chamado **Documents and Settings**, na mesma partição onde está instalado o sistema operativo.

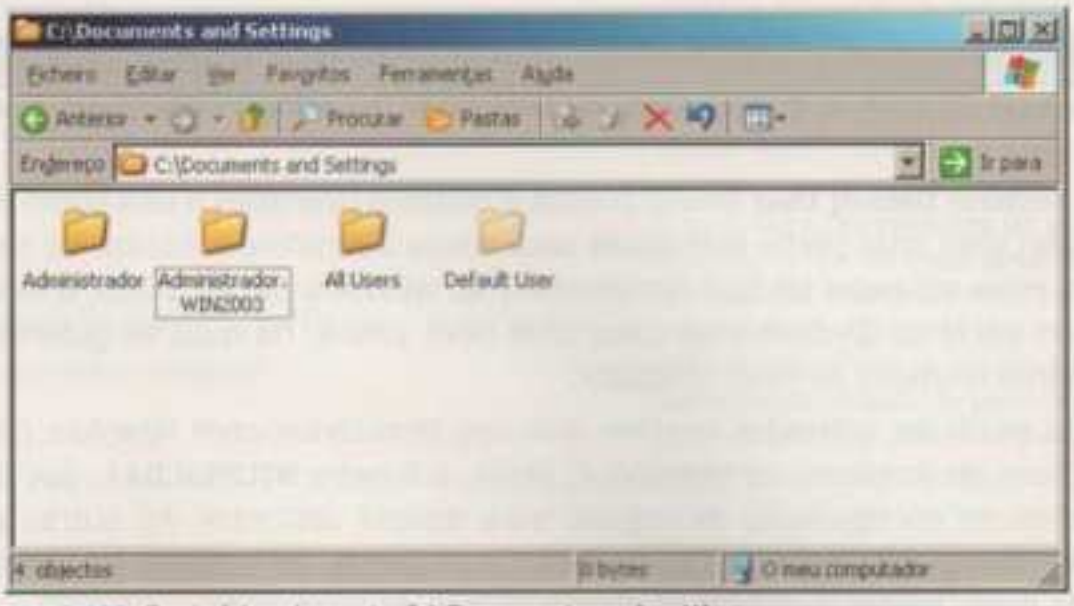

Fig. 3.187 Conteúdos da pasta **C:\Documents and settings**

O directório **Documents and Settings** contém um perfil para cada utilizador que se liga à máquina, bem como os directórios chamados **All Users** e **Default Users**.

Fig. 3.188 Conteúdo de **:\Documents and Settings\Administrador** – perfil do utilizador "administrador"

O directório **All Users** guarda grupos de programas comuns a todos os utilizadores (programas disponíveis para todos os utilizadores numa máquina específica) e atalhos que irão aparecer nos ambientes de trabalho de cada utilizador, naquela máquina. Por exemplo, o grupo de programa **Ferramentas administrativas** está guardado na pasta **All Users** (no menu **Iniciar/Programas**), por isso os programas listados neste grupo ficarão disponíveis para qualquer um que se ligue à máquina.

Fig. 3.189 Conteúdo de **C:\Documents and Settings\All Users\Menu Iniciar\Programas**

O directório **Default User** existe porque o sistema operativo o usa como modelo (*template*) para criar perfis individuais para novos utilizadores. Assim, de cada vez que um novo utilizador se ligar (localmente) ao Windows Server 2003, é feita uma cópia do perfil do *Default User* para uma nova pasta, na qual se guardarão os parâmetros relativos ao novo utilizador.

Cada perfil de utilizador contém diversos directórios com ligações (*links*) a vários itens do ambiente de trabalho e, ainda, o ficheiro **NTUSER.DAT**, que contém definições de configuração de registo para aquele utilizador. As outras pastas guardam informação sobre os conteúdos do ambiente de trabalho do utilizador e itens do menu **Iniciar**, incluindo atalhos e grupos de programas.

Não esquecer que um perfil de utilizador também inclui grupos de programas comuns e atalhos indicados no directório **All Users**.

Fig. 3.190 Ficheiro **NTUSER.DAT** em **C:\Documents and Settings\Administrador**

A **tabela 3.10** descreve os diversos directórios num perfil de utilizador no Windows Server 2003.

Directório	Explicação
Dados de aplicação* (*Application Data*)	Um local para as aplicações guardarem informação específica do utilizador.
Ambiente de trabalho (*Desktop*)	Qualquer ficheiro, directório ou atalho nesta pasta irá aparecer directamente no ambiente de trabalho do utilizador.
Cookies	*Cookies* do Internet Explorer.
Favoritos (*Favorites*)	Aqui podem ser guardados atalhos aos *websites* favoritos e *bookmarks*.
Definições locais* (*Local Settings*)	Uma parte do perfil que não é ambulatório, mesmo que faça o perfil mudar de local. Um lugar para coisas como ficheiros temporários, que podem ocupar muito espaço em disco mas que não têm razão para rede.
*NetHood**	Atalhos que sejam colocados neste sítio irão aparecer na **Vizinhança de rede** (*Network Neighborhood*).
Documentos do proprietário / Os meus documentos (*My Documents or Personal*)	O directório **Documentos do proprietário** aparece em sistemas NT4 e **Os meus documentos** em sistemas posteriores. É o local que a Microsoft recomenda para guardar dados do utilizador, para que estes estejam todos num só sítio. Pode-se mudar a localização de **Os meus documentos** através de políticas, por isso não há razão para alarme se o perfil não tiver a pasta **Os meus documentos**.
*PrintHood**	Atalhos que sejam colocados aqui irão aparecer no directório **Impressoras**.

Directório	Explicação
Os meus documentos recentes* (*Recent*)	Atalhos para ficheiros recentemente usados encontram-se aqui guardados. Há uma ligação a **Documentos** no menu **Iniciar**. O Windows XP chama a este directório **Os meus documentos recentes** (*My Recent Documents*) no menu **Iniciar**.
Enviar para* (*SendTo*)	Este menu é uma lista de opções que surge no contexto do menu de itens no ambiente de trabalho e no **Explorador**. Colocar aqui atalhos para impressoras e pastas, caso se pretenda copiar rapidamente um item para um sítio predefinido, abrir um ficheiro dentro de uma aplicação específica (ex., Notepad) ou até mesmo imprimir um ficheiro.
Menu **Iniciar** (*Start Menu*)	Contém grupos de programas pessoais e atalhos para itens de programas.
Modelos* (*Templates*)	Contém atalhos para modelos criados por aplicações, tais como **PowerPoint** e **Word**.

* Estes directórios estão, por defeito, escondidos no Windows 2000 e no XP. O Windows NT também esconde os directórios **NetHood**, **PrintHood**, **Os meus documentos recentes** e **Modelos**.

Tabela 3.10 Diversos directórios num perfil de utilizador num sistema Windows Server 2003

Além dos directórios, um perfil de utilizador inclui diversos parâmetros definidos pelo utilizador para o **Explorador do Windows** (ver caminho completo na barra de título, por exemplo), a **Barra de tarefas** (mostrar e esconder o relógio, por exemplo), o **Painel de controlo** (preferências de uso do rato ou de ecrã, por exemplo) e os **Acessórios** (calculadora, relógio, livro de endereços, por exemplo). No **Perfil do utilizador**, também se podem guardar impressoras em rede, ligações a discos e favoritos da **Ajuda**. Estes parâmetros, que não estão directamente ligados aos itens do ambiente de trabalho, estão contidos no ficheiro **NTUSER.DAT**, que é a parte do registo de um perfil de utilizador. Corresponde à subárvore **HKEY_ CURRENT_USER** no **Editor de Registo do sistema operativo** (ver **REGEDT32.EXE**).

Modelos ou *templates* de perfis

Como vimos, é bastante fácil atribuir perfis "partilhados" a utilizadores e grupos. No entanto, sempre que dois ou mais utilizadores usem os seus perfis do mesmo directório de perfis, deveriam estar a usar um perfil obrigatório (*read only*). De outro modo serão guardadas, no servidor, todas as alterações feitas, por cada utilizador, ao directório de perfil de grupo.

Caso existam perfis associados a utilizadores com funções específicas ou de departamentos específicos, então será bom manter esses perfis em separado. Assim, sempre que for necessário, é fácil fazer alterações a esses perfis e depois copiá-los sobre os perfis já definidos para esses utilizadores.

Acesso a perfis

Contam-se muitas permissões de utilização associadas aos perfis. Um perfil pode dar acesso a apenas um utilizador ou a um grupo global – embora não seja aconselhável a utilização de perfis ambulantes ou locais para grupos de utilizadores, devido a motivos já explicados anteriormente. Assim, neste caso, sugerem-se perfis obrigatórios.

3.6. Políticas de grupo e de sistema

Políticas de grupo

O termo para um controlo e uma tecnologia de suporte mais alargados é **Política de grupo**. É um termo um pouco confuso por, na realidade, não se referir a grupos. Ao utilizar políticas de grupo, o administrador consegue controlar, de forma centralizada, algumas das definições usadas pelos utilizadores e mesmo definir, até certo ponto, algumas funções e configurações que os utilizadores nem sequer podem fazer. As políticas de grupo podem ser aplicadas tanto sobre o utilizador como sobre o computador, num âmbito local ou mais alargado, a um *site*, domínio ou unidade organizacional.

Há dois tipos de políticas de grupo: o tipo onde existe um controlador de domínio para os apoiar; e o tipo de política de grupo sem controlador de domínio (DC).

Sem controlador de domínio, usa-se a ferramenta **Política de segurança local** (*Local Security Policies*) ou o comando **SECEDIT**, que é executado a partir da linha de comandos.

Com controlador de domínio, usa-se **Políticas de grupo baseadas em domínio** (*Domain-based Group Policies*), onde o *Active Directory* faz muito do trabalho.

Mas, afinal, o que é que se pode realmente fazer com políticas de grupo? Eis uma breve lista:

- publicar ou atribuir pacotes de *software* a utilizadores ou a máquinas;
- atribuir direitos de utilizador (por exemplo, um utilizador *standard* não pode alterar a hora e a data do seu computador);
- definir *scripts* de *start up*, *shut down*, *logon* e *logoff*;
- definir *password*, *lockout* e *audit policy* para o domínio;
- estandardizar muitas outras definições de segurança em computadores remotos, nos quais, anteriormente, as definições eram apenas configuráveis editando o *registry* ou utilizando ferramentas de configuração de segurança externas ao sistema operativo;
- definir e impelir definições (*settings*) no Internet Explorer;
- definir e impelir restrições nos ambientes de trabalho (*desktops*) dos utilizadores. Pode-se, por exemplo, remover a maioria ou todos os itens no botão **Iniciar** de um utilizador, evitar que este adicione impressoras ou nem sequer permitir que ele altere as configurações do ambiente de trabalho;
- restringir as aplicações que um utilizador pode correr, ou seja, pode-se controlar o ambiente de trabalho de um utilizador ao ponto de aquele utilizador poder correr apenas algumas aplicações – talvez o Outlook, o Word e o Internet Explorer, por exemplo;

- redireccionar certos directórios nos perfis dos utilizadores (tais como o menu **Iniciar** e o **Ambiente de trabalho**) para que possam ser guardados numa localização central;
- configurar sistemas de controlo – a forma mais fácil de controlar quotas de espaço em disco é com políticas de grupo;
- configurar e estandardizar definições (*settings*) para características como directórios *offline*, quotas de disco e até mesmo a própria política de grupo.

O ponto-chave, aqui, é que a política de grupo fornece um único ponto de administração, permitindo aos administradores instalarem facilmente *software* e aplicarem definições estandardizadas a múltiplos utilizadores e computadores ao longo de toda uma organização.

Ordem de aplicação das políticas de grupo

Políticas de grupo aplicam-se a *sites*, domínios e unidades organizacionais (OU) – não a grupos (na maioria das vezes).

Políticas de sistemas só se aplicavam aos domínios. Mas, como já se viu, o *Active Directory* tem noção de *sites* e OU. Pode-se criar um objecto de política de grupo (*Group Policy Object* – GPO) – um registo no AD que contém uma ou mais instruções de políticas de grupo – e aplicá-lo a domínios, OU ou *sites*. Por estranho que possa parecer, os GPO (objectos de política de "grupo") não se aplicam a grupos – apenas a *sites*, domínios ou unidades organizacionais (OU).

Em relação às ordens de aplicação de políticas de grupo, podem-se aplicar políticas a diferentes níveis:

- os *sites* podem ter políticas e aquelas políticas aplicam-se independentemente das máquinas e dos utilizadores de domínio que se encontram naquele *site*;
- as unidades organizacionais (OU) podem ter políticas. E as OU podem conter OU, que por sua vez podem conter OU que podem conter OU que contêm OU e por aí fora;
- também existem as políticas locais – não convém esquecê-las.

Sendo assim, quem vence? As políticas são aplicadas pela seguinte ordem: políticas locais, *sites*, domínios, unidades organizacionais (OU), depois OU dentro de OU.

Caso existam contradições entre as configurações de políticas realizadas nas diversas situações, a política que prevalece é a última a ser aplicada e sobrepõe-se às primeiras. Vejamos os seguintes exemplos:

- Se a política de domínio diz: "Tem de estar *logon* antes de poder encerrar a máquina" e a política de OU diz: "Permite o *shut down* antes do *logon*", a política de OU tem precedência, porque é aplicada por último (é a última a ser aplicada).
- Se uma política diz **Encerrar** (*Lock it down*) e a próxima diz **Não configurado** (*Not configured*), a definição mantém-se **Encerrada** (*locked down*). Se uma política diz **Não configurado** (*Not configured*), e a próxima diz **Encerrar** (*Lock it down*), então também está **Encerrada** (*Locked down*) neste caso.
- Se uma política diz **manter ligado** (*Leave it on*) e a próxima diz **desligar** (*Turn it off*), então é desligado.

- Se uma política diz **Desligar** (*Turn it off*) e uma outra, mais próxima, diz **Ligar** (*Turn it on*), e ainda uma terceira diz **Desligar** (*Turn it off*), adivinhe-se? Acaba por ficar desligado. No entanto, para a preservação da nossa sanidade, é desejável evitar estes pequenos desentendimentos entre políticas.

Criação de políticas de grupo locais

O lançamento da ferramenta associada à criação de políticas de grupo locais, a *Group Policy Tool*, é realizado através da execução do comando **GPEDIT.MSC**, na linha de comandos. Esta ferramenta executa automaticamente as políticas relativas à máquina local.

Os administradores podem usar a ferramenta como utilizariam a ferramenta de política de segurança local para configurar definições de conta (como tamanho mínimo da palavra-passe e número de tentativas falhadas de *logon* antes de encerrar a conta) e definir *auditing*. No entanto, o editor de políticas baseado em domínio (*Domain-based Policy Editor*) inclui um conjunto de definições (como instalação de *software* e redireccionamento de pastas) que não estão disponíveis para políticas locais.

Nota: A estrutura da directoria da política de grupo local é equivalente àquela de outros GPO (objectos de política de grupo) e encontra-se em **\Windows\system32\GroupPolicy**.

Para ser possível focar-se uma política local de outro computador, é necessário ter-se direitos de administrador naquela máquina.

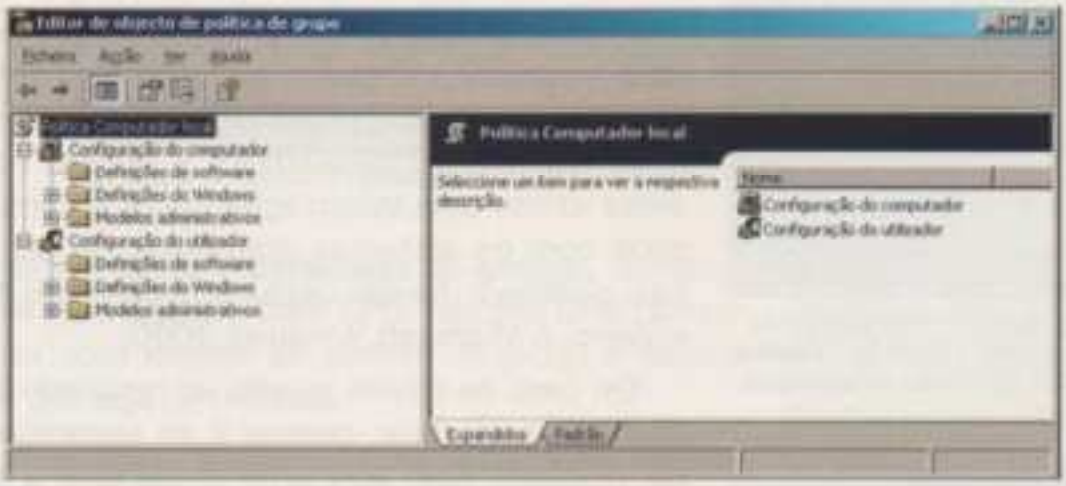

Fig. 3.191 Configuração de políticas de grupo locais

No ecrã que surge é visível uma divisão da árvore em dois grupos, que dizem respeito à configuração do computador (*Computer Configuration*) e à configuração do utilizador (*User Configuration*), que, por sua vez, se dividem em definições de *software* em geral, do Windows e dos modelos (*Templates*) administrativos.

Definições do computador são aplicadas às máquinas durante o iniciar (*startup*) e em certos intervalos de *refresh*.

Definições do utilizador são aplicadas aos ambientes de trabalho do utilizador durante o *logon* e em certos intervalos de *refresh*.

Ao expandir um ramo da árvore, surge, à direita, uma lista de várias opções de configuração.

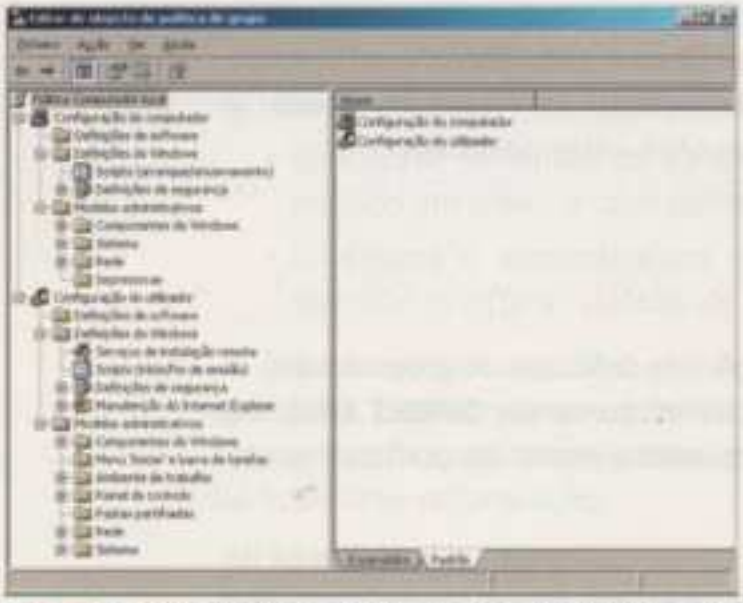

Fig. 3.192 Subdivisão da configuração do computador e do utilizador

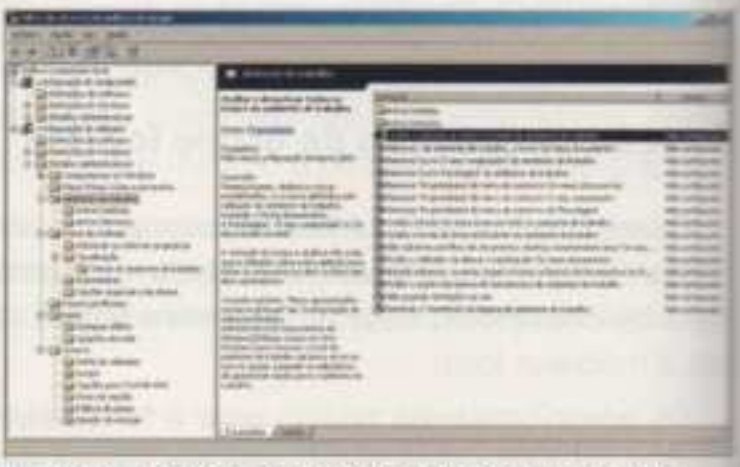

Fig. 3.193 Lista das várias opções de configuração do ambiente de trabalho

Deve seleccionar-se uma e fazer duplo clique sobre o seu nome. No ecrã aparece uma janela **Definição** (*Setting*), onde se deve escolher uma das opções possíveis sobre o item seleccionado.

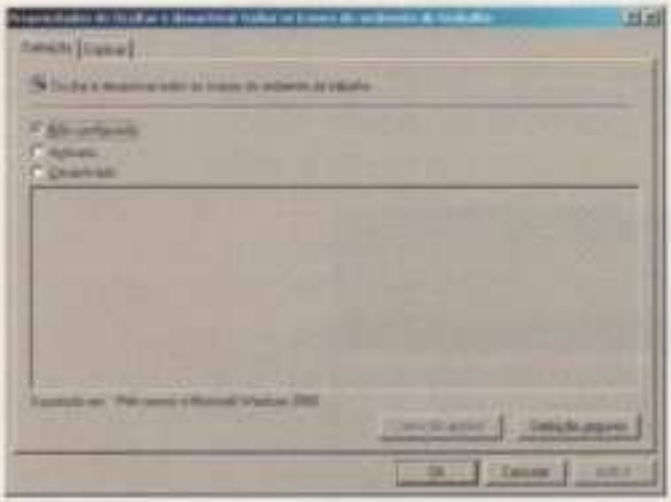

Fig. 3.194 Opção de configuração de uma política de grupo local seleccionada (exemplo: **Ocultar e desactivar todos os ícones do ambiente de trabalho**)

Aqui surgem três opções disponíveis:

- **Não configurado**
- **Activado**
- **Desactivado**

A selecção da primeira opção – **Não configurado** – ignora a mesma, ou seja, mantém-se o comportamento que já estava aplicado. As outras duas activam ou desactivam a opção. Por fim, ainda existe uma informação sobre a compatibilidade com os sistemas operativos de cada uma das políticas. Neste caso, é necessário ter, no mínimo, o Microsoft Windows 2000.

Em caso de dúvida quanto ao resultado da configuração a efectuar, deve-se ir ao separador **Explicar** (*Explain*). Este abre uma janela com a explicação de tudo o que pode acontecer se optarmos por uma determinada configuração.

A sintaxe para abrir o **GPEDIT.MSC** e olhar para a política local numa máquina remota é a seguinte: **gpedit.msc /gpcomputer: *machinename*** (*introduzir o nome do computador*).

Atenção: Convém ter a certeza de que existe um espaço entre **/gpcomputer:** e o nome da máquina.

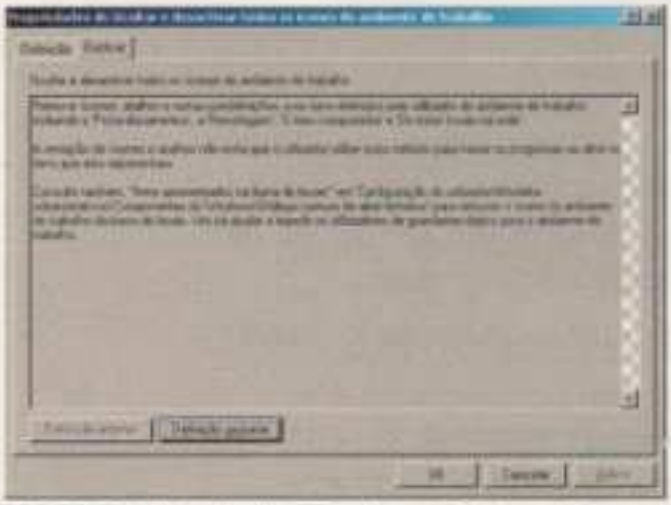

Fig. 3.195 Ajuda/explicação da opção de configuração seleccionada: **Ocultar e desactivar todos os ícones do ambiente de trabalho**

Criação de políticas de grupo

As políticas de grupo são criadas através da ferramenta **Utilizadores e computadores do Active Directory** – *Active Directory Users and Computers*, que tem de se abrir. De seguida, clica-se com o botão direito do rato sobre o nome de domínio ou sobre a OU pretendida.

No nosso exemplo, vamos inserir uma política de grupo na raiz do domínio. Para tal, seleccionamos a raiz do domínio **escola.pt** e, com o botão do lado direito, clicamos em **Propriedades**.

Na janela **Propriedades de escola.pt** vamos ao separador **Política de grupo** (*Group Policy*) para analisar quais os objectos de políticas de grupo (GPO) que estão ligados ao nível do domínio.

No caso de ainda não se ter criado outras políticas, vê-se apenas listada a política de **Domínio por defeito** (*Default Domain Policy*).

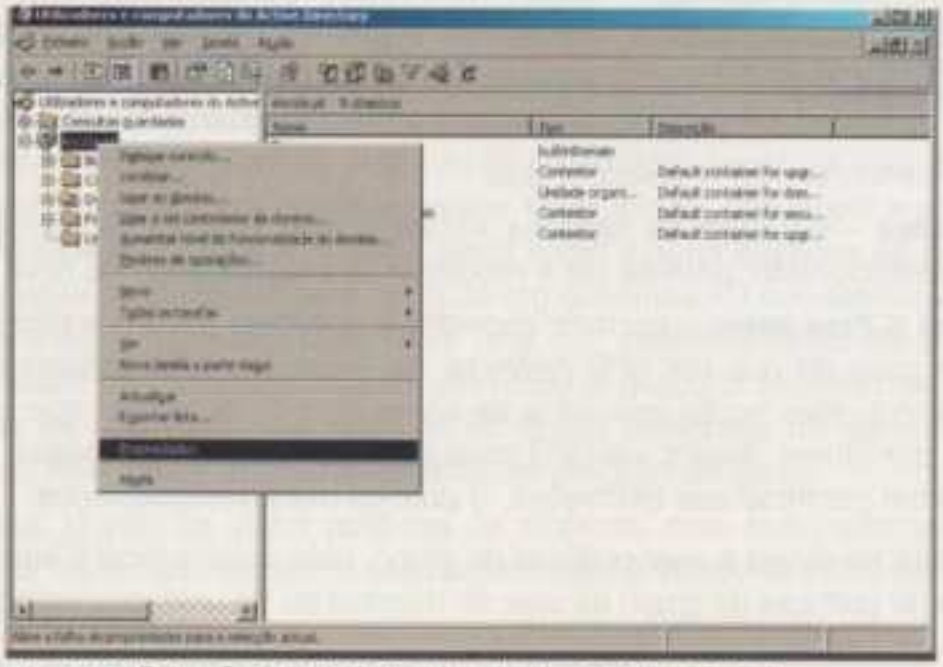

Fig. 3.196 Selecção **Propriedades** da raiz do domínio **escola.pt**

De volta à janela **Propriedades do domínio**, seleccionar **Novo** para criar um novo GPO. Isto cria uma política chamada novo objecto de política de grupo e depois permite que seja renomeado.

Se repararmos, à esquerda, no fundo deste separador, encontra-se a caixa de selecção **Bloquear a herança de políticas** (*Block Policy Inheritance*). Esta selecção previne quaisquer definições de política de grupo de um nível mais elevado cair para este nível. É bom relembrar a ordem pela qual as políticas de grupo são aplicadas: primeiro está o nível do *site*, depois o nível de domínio e por fim as políticas para as unidades organizacionais.

Ainda na mesma janela, encontram-se botões com várias opções:

- **Novo** – permite a criação de um novo GPO (objecto de políticas de grupo).

Fig. 3.197 Separador **Política de grupo** (*Group Policy*) na janela **Propriedades de escola.pt**

- **Editar** – permite editar o GPO seleccionado e também visualizar e modificar a nova política.
- **Adicionar** – permite criar uma ligação (*link*) para um GPO existente; liga um GPO existente ao contentor desejado.
- **Opções** – permite definir duas opções para o novo objecto que estamos a criar:

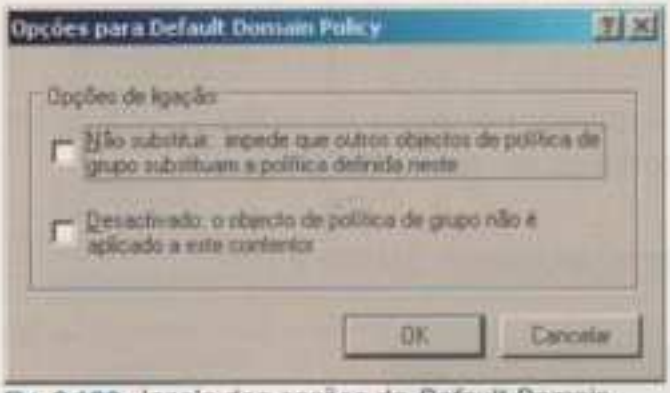

Fig. 3.198 Janela das opções do *Default Domain Policy* – **Domínio por defeito**

  - **Não substituir** (*No Override*), evita que políticas aplicadas posteriormente possam impor opções diferentes (mesmo com a Bloquear a herança de políticas (*Block Policy Inheritance*) activada);
  - **Desactivado** (*Disabled*), desactiva o objecto sem o apagar. Desliga a política, de modo que não seja processada ou aplicada neste nível; ao desactivar a política não se está a desactivar o objecto em si, porque pode voltar a ser activado a qualquer altura, desmarcando esta opção.
- **Eliminar** – elimina o GPO seleccionado.
- **Propriedades** – visualiza as ligações estabelecidas e edita os direitos sobre o objecto seleccionado; permite ver e modificar as propriedades do novo GPO.
- **Para cima** e **Para baixo** – permite especificar a ordem de precedência, no caso de haver mais do que um GPO definido. Se múltiplos GPO estiverem ligados a um contentor, eles serão aplicados de baixo para cima, sendo que o do topo é aplicado por último. Assim, os GPO mais elevados na lista têm maior prioridade. Se existirem conflitos nas definições, a política mais elevada vence.

Nota: Caso se esteja a usar políticas de grupo, uma política local é sempre processada antes de políticas de grupo de *site*, de domínio ou de unidades organizacionais.

Políticas de sistema

Em sistemas NT4, os domínios tornaram-se num lugar para centralizar **políticas de sistema**, um conjunto de instruções que as máquinas usam para construir e controlar ambientes de utilizador. Mas estas políticas de sistema tinham falhas em vários níveis e o AD melhorou-as, através de uma espécie de segunda versão das políticas de sistema, chamada políticas de grupo.

As políticas de grupo existem desde o Windows 2000. Antes disto, apenas uma pequena parte daquilo que as políticas de grupo são capazes – restrições no ambiente de trabalho e algumas poucas definições de segurança – era conseguido usando as políticas de sistema.

Com as políticas de sistema Windows 9x, Me e NT4, podia-se controlar uma grande variedade de coisas – podia dar-se a um utilizador um menu específico de **Iniciar > Programas**, dar-lhe um aspecto específico de ambiente de trabalho ou restringir o utilizador de correr muitos programas, por exemplo. Todas essas restrições seriam reunidas num único ficheiro, chamado **NTCONFIG.POL** (para NT4, 2000, XP ou Server 2003) ou **CONFIG.POL** (para Windows 9x e Me), que depois seria colocado em cada uma das partilhas **NETLOGON** dos controladores de domínio. Quando um sistema Windows 9x, Me, NT4, Windows 2000, XP ou Server 2003 se inicia e faz o *logon* a um domínio NT4 ou AD (*Active Directory*), então aquele sistema faz o

download do **CONFIG.POL** ou do **NTCONFIG.POL** e executa quaisquer instruções que estejam no ficheiro **POL**. As políticas de sistema funcionam porque o sistema operativo do cliente requer os ficheiros de políticas e segue as suas instruções e não porque o DC – que faz o *logon* deles – force os ficheiros e as definições sobre um cliente. Pode ter-se apenas um ficheiro de políticas **NTCONFIG.POL** ou **CONFIG.POL**. Podem usar-se políticas de sistema tipo **NTCONFIG.POL/CONFIG.POL** tanto em domínios baseados em NT4 como em domínio AD.

As políticas de sistema estão, então, contidas num ficheiro, guardado na partilha **NETLOGON** dos *Domain Controllers* num domínio NT4 ou num domínio AD (*Active Directory*) e trabalham porque muitos sistemas operativos da Microsoft sabem como fazer o seu *download* e usá-los. Políticas de sistema tanto podem existir num domínio NT4 como num domínio AD, enquanto que políticas de grupo só podem existir num domínio AD – estas só se aplicam a sistemas Windows 2000, XP e Server 2003.

A pergunta que se coloca é a seguinte: Porque é que ainda se podem usar políticas de sistema em AD, quando os AD têm políticas de grupo mais poderosas à sua disposição? Simplesmente, porque sistemas anteriores ao Windows 2000 são completamente "surdos" face às políticas de grupo. Não podemos esquecer que as políticas funcionam porque o cliente sabe fazer o seu *download* e executá-las. Sistemas Windows 9x, Me e NT4 não sabem como ir obter políticas de grupo e, por isso, as políticas de sistema fazem sentido em domínios AD que tenham esses sistemas mais antigos ligados a eles. Mais uma vez, sistemas Windows 2000 e posteriores também irão procurar fazer o *download* e executar políticas de sistema – mas apenas se não estiverem políticas de grupo presentes no domínio e, claro, domínios tipo NT4 nunca irão conter quaisquer políticas de grupo.

Na prática, já não se usam políticas de sistema, mas sim políticas de grupo, desde que os sistemas operativos utilizados sejam o Windows 2000 ou superior.

Editor de políticas de sistema

No NT4 era possível usar o editor de políticas de sistema para ver e editar aquelas entradas de *Registry* para o computador local (em vez de criar ou editar uma política, optava-se por abrir o *Registry*). Como tal, o editor de política local servia como uma ferramenta de edição de *Registry*, mais agradável ao utilizador, comparado ao **REGEDIT.EXE** ou ao **REGEDT32.EXE**.

O NT4 introduziu a ideia de uma política de sistema. As políticas permitem que se controle o ambiente de trabalho dos utilizadores através dos registos daqueles utilizadores. Num local acessível e central coloca-se um ficheiro chamado **NTConfig.pol**, que contém instruções sobre o que se queria alterado nos *registries* dos utilizadores. *Workstations* NT4 iriam automaticamente ler aquele ficheiro e fazer as alterações nos seus *registries*, de acordo com as ordens do ficheiro. Deste modo era possível controlar os ambientes de trabalho a partir de uma localização central. Infelizmente, não é possível aplicar uma política de sistema a um conjunto de máquinas. Pode-se aplicar uma política de sistema a um grupo de utilizadores, pelo menos teoricamente é possível. Na prática, grupos e políticas não funcionavam assim tão bem.

O *System Policy Editor* – **editor da política de sistema** – (**POLEDIT.EXE**) é uma ferramenta que surgiu no Windows 95 para criar políticas de sistema (e que se

encontra explicada num apêndice no CD, no caso de se ter ambientes de trabalho Windows 9x ou NT4), e é mais amigável e pode ser usada para editar directamente várias definições seleccionadas no *Registry* local. O editor da política de sistema vem com o NT Server e todas as versões do Windows 2000, mas por alguma razão não está instalado, por defeito, com o XP ou o Windows Server. Não é realmente necessário, apenas conveniente.

O editor da política de sistema é um editor de *Registry* "selectivo" e é mais fácil de usar, uma vez que não requer qualquer conhecimento da sintaxe ou da estrutura do *Registry*. Enquanto que esta aplicação oferece várias opções que não estão disponíveis na interface gráfica, seria de muito pouco interesse a utilizadores normais definir os seus próprios perfis, mesmo tendo acesso à aplicação. Embora o editor da política de sistema possa ser usado para editar o *Registry* local da máquina, a maioria das opções dos utilizadores locais focam-se em restringir o ambiente de trabalho do utilizador.

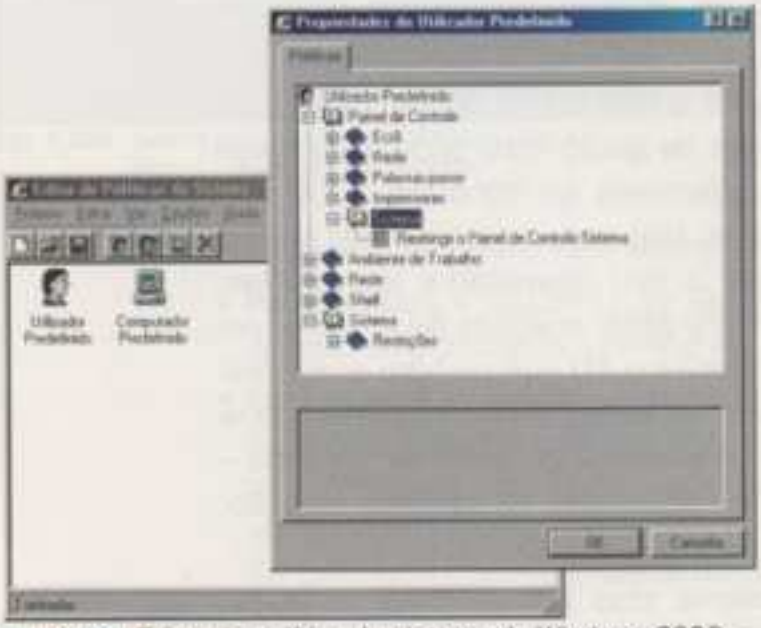

Fig. 3.199 Editor da política de sistema do Windows 2000 – **POLEDIT**

De facto, a melhor maneira de configurar a parte **NTUSER.DAT** do nosso perfil é, simplesmente, configurar o nosso ambiente de trabalho. Ao usar os *applets* na interface gráfica para alterar o esquema de cores, o mapa de *drives* de rede e a ligação a impressoras, estão a fazer-se alterações ao **NTUSER.DAT**. Deve usar-se um editor de *Registry* apenas quando se quer fazer uma alteração que não é oferecida no painel de controlo.

Atenção: Não se deve editar o *Registry* quando se pode fazer as alterações usando o painel de controlo.

Modelos de políticas de sistema

Políticas de sistema só são aplicadas quando se faz o *logon*, enquanto que as políticas de grupo são aplicadas com mais frequência – sempre que se liga o computador, quando se faz o *logon* e, automaticamente, a diferentes horas, dispersas ao longo do dia.

Uma das situações mais críticas das políticas do sistema NT4 é que, uma vez que uma política de sistema é aplicada a uma conta de utilizador ou a uma máquina, a política mantém-se no seu lugar, mesmo que seja removida dos controladores de domínio. Assim, por exemplo, se, por alguma razão, se criar uma política de sistema para definir para todos a cor verde como cor de fundo, então o *Registry* de cada computador que faz o *login* a partir daquele ponto será alterado para definir o verde como cor de fundo. Se alguns utilizadores se queixarem sobre isto e se se decidir remover a política, os seus ecrãs continuarão verdes. Eles poderão, certamente, alterar a cor por eles próprios, mas teria sido bem mais interessante se a política se tivesse desinstalado por si própria, à sua saída. Isso acontece com clientes Windows 2000, XP ou Server 2003: ao removerem a política, os seus efeitos são invertidos, o que pode ser bastante poderoso – por exemplo: se se usou uma política de grupo para abrir (*deploy*) uma aplicação e depois se removeu a política, a aplicação desinstala-se por si própria.

3.7. *Home Folder* / Pasta raiz

Introdução

Uma **Pasta raiz** (*Home Folder* ou *Home Directory*) é uma pasta designada para uso pessoal do utilizador. Esta pasta, depois de devidamente configurada, será o directório de trabalho, por defeito, para o qual se enviam os ficheiros pessoais quando se executa a operação **Guardar**. Assim, de cada vez que, numa aplicação, o utilizador utilizar o menu **Ficheiro > Guardar**, surgirá uma janela com o *Home Folder* como destino. Se o utilizador executar o comando cmd (*command prompt*) no menu **Iniciar > Executar** (*Start > Run*), a sessão é aberta na mesma directoria. Uma vez que todos estes ficheiros se encontram guardados num só local, o processo de *backup* dos mesmos é muito acessível.

Especificar o *Home Folder* de um utilizador

A melhor forma de indicar um *Home Directory* de um utilizador é aceder à janela de **Propriedades** da conta do utilizador e seleccionar a página **Perfil** (*profile*). Aí, na secção **Pasta raiz** (*Home Folder*), deve-se indicar no **Caminho local** a directoria **c:\user_local**, por exemplo, e clicar em **OK**. A pasta **c:\user_local** tem de ser criada previamente no disco do cliente – e não no do servidor! –, e é o que estará seleccionado sempre que se abrir o *command prompt*.

No entanto, também é possível configurar o sistema para que os *Home Folders* dos utilizadores se encontrem no servidor.

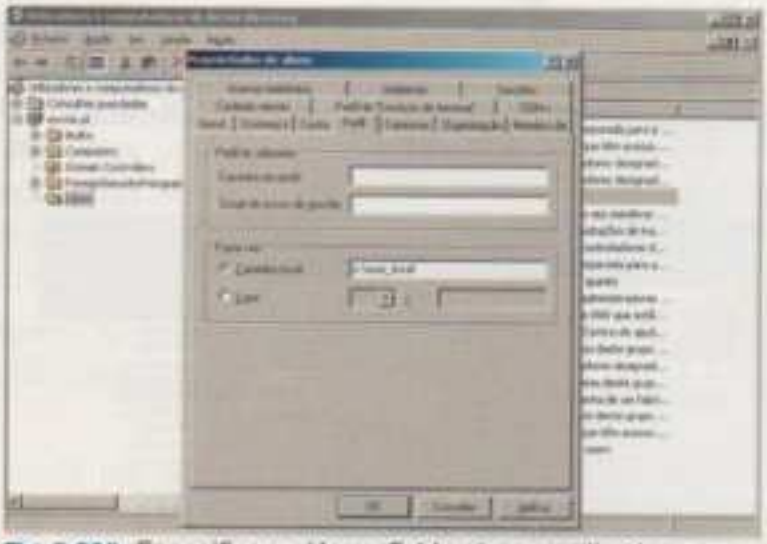

Fig. 3.200 Especificar o *Home Folder* de um utilizador numa pasta do computador-cliente.

Redireccionar o *Home Folder* para um servidor

Para centralizar os *Home Directory* dos utilizadores num servidor devemos, em primeiro lugar, partilhar uma pasta – no nosso exemplo designada **user_doc**. A partir desta pasta irão descender as pastas de cada utilizador (automaticamente criadas, com as devidas permissões e tudo o resto).

Como criar a pasta partilhada user_doc

Na raiz do disco **c:** criar uma pasta chamada **user_doc**.

Clicar com o botão do lado direito sobre a pasta criada e seleccionar **Propriedades** (como na figura 3.201).

Na janela **Propriedades de user_doc**, ir ao separador **Partilhar** e seleccionar **Partilhar esta pasta**. O nome escolhido para o nome da partilha pode ser o atribuído ao nome da pasta. Clicar em **OK** para validar as alterações.

No **Explorador do Windows** pode-se verificar que surgiu uma **mão** sobre a pasta a indicar que esta está partilhada.

De seguida, deve-se aceder à janela de propriedades da conta do utilizador e, tal como no processo anterior, seleccionar a página **Perfil** (*Profile*). Na secção **Pasta raiz** (*Home Folder*) devemos indicar **Ligar** (*Connect*) e atribuir uma letra ao volume que corresponderá ao *Home Folder* – por exemplo, a letra **F:**. No campo **Para** (*To*), indicar um

nome UNC apontando para a partilha (*Share*) do servidor e completar com o nome **%username%**. No nosso exemplo temos **\\win2003\user_doc\%username%**. Efectuados estes passos, clicar em **Aplicar** (*Apply*) para que o sistema possa substituir a variável **%username%** pelo nome usado para efectuar o *logon* no sistema. Para finalizar, clicar em **OK**.

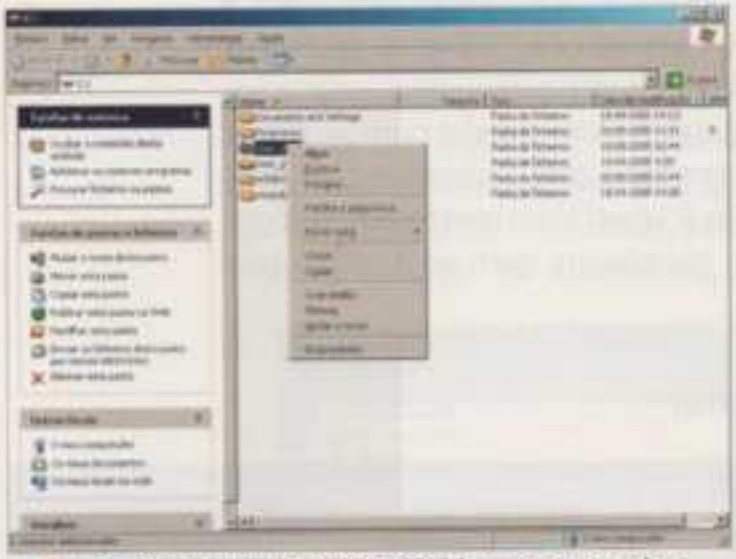

Fig. 3.201 Acesso às **Propriedades** da pasta **user_doc**

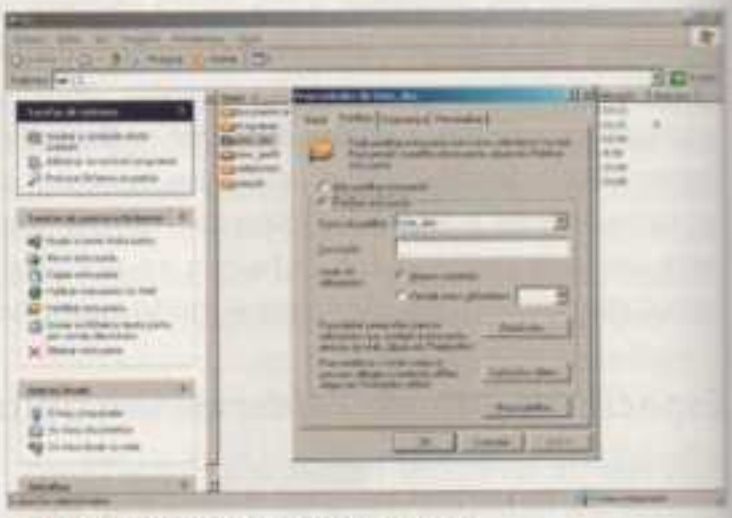

Fig. 3.202 Partilha da pasta **user_doc**

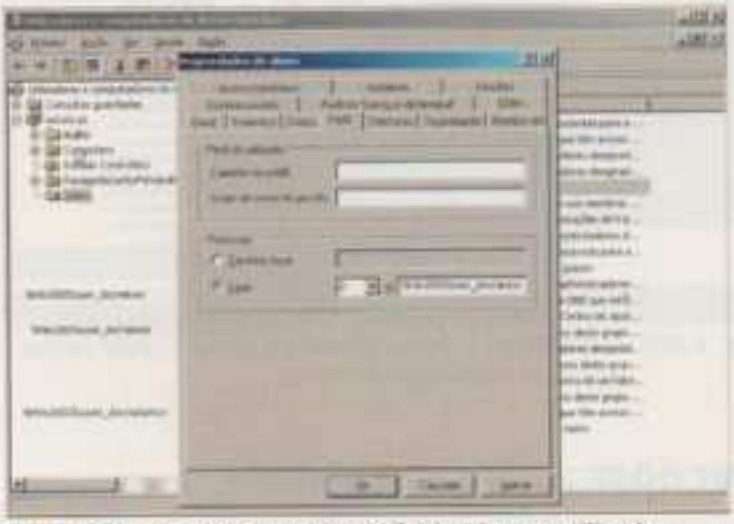

Fig. 3.203 Especificar o *Home Folder* de um utilizador numa pasta do servidor

Assim, sempre que um cliente executar a operação **Guardar** (*Save*) ou aceder ao *command prompt*, o volume **F:** será a pasta activa.

Para efectuar uma ligação ao *Home Folder* através do comando **Net**, pode-se executar somente o comando:

net use f: /home

3.8. *Logon Scripts* – *scripts* de início de sessão

Introdução e construção de *Logon Scripts*

Cada vez que um utilizador se liga a uma rede Windows Server 2003, há uns ficheiros **BAT** (*batch*) que são executados. A esses ficheiros (*batch*) (quase como "ajudas na entrada em rede") dá-se o nome de *Logon Scripts* ou *Login Scripts*. Trata-se de um venerado método antigo para configurar o ambiente de trabalho de um utilizador e os recursos de rede a ele atribuídos. Em tempos remotos, os *Login Scripts* eram escritos na linguagem comum do cliente e corriam do servidor do cliente aquando do *logon*. Estes *scripts* criam mapeamentos de *drives* locais aos servidores, redireccionam portos locais para atribuir impressoras, sincronizam o relógio de sistema com um *timeserver* (servidor de horas), designado central-

mente, e executam ainda outras tarefas relacionadas. Pode-se dizer que os *Login Scripts* atingiram o seu pico na era do NetWare. Na era do NT4, os clientes de rede tornaram-se mais conscientes da rede de trabalho à sua volta e desde o aparecimento do Windows 2000 que temos a capacidade de usar não apenas os *Logon Scripts*, mas também os *Logoff Scripts*, os *Sartup Scripts* (*scripts* de arranque) e os *Shutdown Scripts* (*scripts* de encerramento). O *Logon Script* pode ser usado para tarefas de configuração de acesso à rede, como, por exemplo, para um mapeamento de impressoras e *shares*.

Como vimos, para construir *scripts* é necessário conhecer os comandos permitidos em ficheiros **BAT**. Nos *Logon Scripts* devem ser introduzidos os comandos que se quer que sejam executados, sempre que um posto de cliente entra na rede. Cada vez que se executa a validação de um domínio, corre-se o *Logon Script*, ou seja, este é corrido a partir da máquina (DC ou outra) que valida o utilizador na rede.

Associação de *Logon Scripts* a utilizadores

Através do separador **Perfil** da janela **Propriedades do utilizador**, em **Utilizadores e computadores do Active Directory** (*Active Directory Users and Computers*), é dada a indicação se um determinado utilizador deve correr um *Logon Script*. A configuração do *Logon Script* é feita utilizador a utilizador.

Fig. 3.204 Separador **Perfil** da janela **Propriedades de aluno**

Em **Script de início de sessão** insere-se o nome do ficheiro que contém os *scripts*, que, neste exemplo, designa-se **salas.bat**.

O ficheiro **salas.bat** deve ser guardado na pasta partilhada designada **NETLOGON**.

No Windows 2000 Server e no Windows Server 2003, a pasta partilhada **NETLOGON** encontra-se por defeito na directoria **\Windows\SYSVOL\sysvol\domainname\scripts**.

Nas versões anteriores ao Windows 2000 Server, o nome da pasta partilhada é o mesmo **NETLOGON**, mas a localização é diferente; é necessário procurar onde se encontra esta pasta no sistema.

Além da localização do ficheiro que contém os *scripts*, é necessário ter em atenção a extensão do mesmo. Os clientes Windows NT/9x e Me suportam ficheiros com extensão:

.bat, .cmd, .exe e **.com**

Os clientes Windows 2000 e XP suportam um leque mais alargado de extensões:

.bat, .cmd, .exe, .com, vbe, jse, vbs, js, wsf e **wsh**

Comandos mais usados

Hoje em dia existe uma grande variedade de ambientes e linguagens de *scripting*, incluindo os nativos comandos do Windows Shell, Windows *Scripting Host (WSH), KiXtart, XLNT, Perl, VBScript, JScript* e até mesmo *Python*. Pode usar-se literalmente qualquer linguagem que seja útil e compreendida pela máquina do cliente. Os *Logon Scripts* estão apenas limitados pelo administrador

e pelos clientes. Um administrador que desenvolve *scripts* tem de saber como usar a ferramenta escolhida. Não é boa política tentar escrever um *Logon Script* em **C** se nem sequer se consegue descobrir como fazê-lo dizer **Bom dia**. A maioria de nós não é programador, por isso torna-se necessário usar ferramentas mais simples, como *shell*, *scripts* ou linguagens especiais de *Logon Scripts* como *KiXtart* ou *XLNT*. É fundamental que o cliente também compreenda a linguagem do *script*.

Desde o NT4 que a linguagem de linha de comandos se tornou bastante robusta em comparação com os sistemas operativos Windows mais antigos e existe uma grande compatibilidade na linguagem *shell* no Windows NT, no 2000 e no XP. Mesmo assim, é possível considerar-se o *shell scripting* menos flexível ou intuitivo quando comparado com qualquer uma das várias linguagens *shell* do Unix; talvez por o *software* do Windows (mesmo com Win2K e XP) não ter sido projectado essencialmente para "génios" de linha de comandos mas para pessoas "com ratos".

Já sabemos que os *Login Scripts* podem realizar uma grande variedade de funções. As tarefas mais frequentes são fazer o mapeamento das *drives* para recursos de rede, ligar utilizadores a impressoras, juntar informação de inventários, fazer actualizações de *software* ou de definições de vírus. O *Login Script* também pode ser usado para sincronizar sistemas de clientes com um **servidor de horas** (*timeserver*) na rede.

Vamos especificar alguns destes comandos:

- Mapeamento de portas de impressora para recursos da rede – usando o mesmo comando, **NET USE**, é possível atribuir as filas de impressão que estão partilhadas em rede às portas de impressora dos clientes.

Por exemplo: **NET USE LPT3: \\WIN2003\IMPRESSORA**

Assim, é atribuído à porta **LPT3** no computador-cliente a impressora partilhada com o nome **IMPRESSORA** que se encontra no servidor WIN2003.

Deste modo, os clientes da rede têm as mesmas impressoras de rede atribuídas a uma mesma porta de impressora local.

- Mapeamento de *drivers* para recursos de rede – podem ser atribuídos pontos partilhados na rede a letras das *drives* através do comando **NET USE**.

Por exemplo: **NET USE F: \\WIN2003\JORNALESCOLAR**

No exemplo apresentado é atribuída a letra **F** à pasta partilhada **JORNALESCOLAR** que se encontra no servidor **WIN2003**.

Deste modo, os clientes da rede têm os mesmos *shares* atribuídos a uma mesma unidade de rede.

- Listagem dos recursos de rede mapeados no computador-cliente – para dar ao utilizador uma lista dos mapeamentos de *drives* de recursos de rede, deve usar-se o comando **NET USE**, que exibe uma lista com as unidades mapeadas – qual a letra local usada e qual o recurso de rede a que essa *drive* está ligada.
- Remoção de ficheiros em discos locais – através do comando **DEL** (ou **ERASE**) do **DOS** é possível forçar a remoção de ficheiros (temporários, por exemplo) do disco a partir de um directório (**C:\TEMP**, por exemplo).

Por exemplo: **DEL C:\TEMP*.TMP**

Caso se pretenda apagar todos os ficheiros no directório de ficheiros temporários, deve usar-se o comando **DEL *.*** e depois confirmar o comando dado.

- Cópia de ficheiros para discos locais – útil para a actualização (*update*) de ficheiros nos PC que se ligam ao domínio; é possível colocar comandos (COPY) no *Logon Script* que façam essa cópia (é necessário ter previamente feito o mapeamento da letra da *drive* para um qualquer ponto partilhado na rede).

Por exemplo: **COPY P:\UPDATE\ *.* C:\PROG**

Exemplo de *Logon Scripts*

Os exemplos de *scripts* apresentados ilustram como conseguir executar algumas das tarefas mais comuns num *Logon Script*.

Neste exemplo, será usada a linguagem Windows Shell. O nome do servidor é WIN2003. Convém relembrar que todas as linhas iniciadas por **REM** num *script* são comentários que apenas são vistos ao ler o *script* e todas as linhas iniciadas por **ECHO** são mensagens que surgem no ecrã do utilizador (com excepção da primeira linha **echo off**).

Exemplo da script ***salas.bat.***

```
@echo off
REM salas.bat Versão 1
REM Sair da script se o utilizador fizer logon no servidor WIN2003
IF %COMPUTERNAME%.==WIN2003. GOTO END
REM Apagar o mapeamentos das drives F e G já existentes nos clientes
NET USE F: /DELETE →nul
NET USE G: /DELETE →nul
REM Mapear a letra F com a pasta USERS partilhada no servidor WIN2003
NET USE F: \\WIN2003\USERS /YES →nul
REM Mapear a letra G com a pasta UTILS partilhada no servidor WIN2003
NET USE G: \\WIN2003\UTILS /YES →nul
REM Sincronizar hora do computador cliente com a do servidor
NET TIME \\WIN2003 /SET /YES
END
```

Como se pode ver pelos comentários, o primeiro *script* verifica se o nome do computador onde o utilizador se está a ligar corresponde ao nome do servidor local, e sai, se isto acontecer. Isto é para prevenir mapeamentos desnecessários no caso de um utilizador ter feito localmente um *logon* no próprio servidor.

Após ter apagado quaisquer mapeamentos de *drives* preexistentes, o *script* faz o mapeamento nas letras **F** e **G**, respectivamente, nas pastas partilhadas **USERS** e **UTILS** que se encontram no servidor **WIN2003**.

O comando final diz ao computador-cliente para sincronizar o seu relógio com o do servidor, sem pedir a confirmação ao utilizador.

Este exemplo de *script* funciona bem (para clientes Windows 9x e sistemas XP), se apenas se tiver um servidor, se todos os utilizadores tiverem os mesmos mapeamentos das *drives* e se todos os utilizadores vierem a usar o mesmo *Login Script*.

3.9. Gestão do servidor

Computer Management – Gestão de computadores

Esta ferramenta é útil para gerir computadores em rede; é, por exemplo, possível, através desta ferramenta, saber quem está a aceder à rede e ao que está a aceder.

A ferramenta **Gestão de computador** encontra-se no grupo de programas **Ferramentas administrativas** ou, então, clicando com o botão direito do rato sobre **O meu computador**, no menu **Iniciar**, e seleccionando **Gerir** (*Manage*).

Há três "nós" na árvore da consola da Gestão de computadores: **Ferramentas de sistema**, **Armazenamento** e **Serviços e aplicações**.

Nota: Esta ferramenta gere o computador local, por defeito. Para se ligar a outros computadores na rede, é necessário seleccionar o ícone **Gestão de computadores** na raiz da árvore, clicar com o botão direito do rato e escolher **Ligar a um outro computador** (*Connect to Another Computer*).

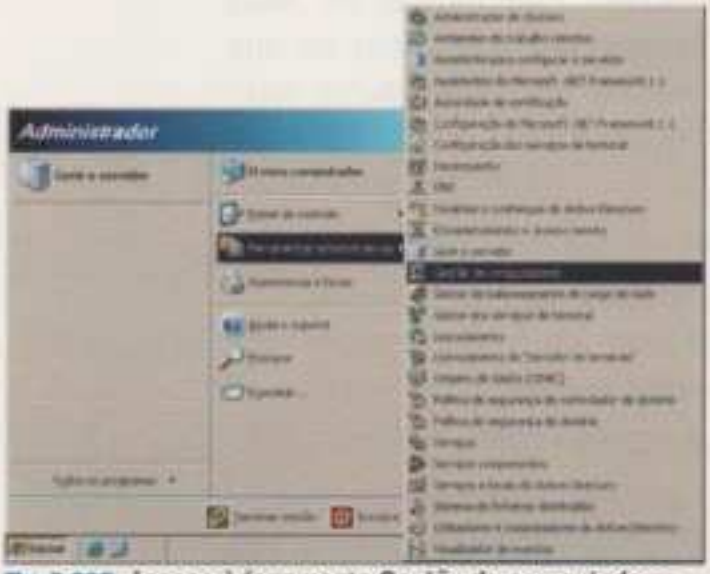

Fig. 3.205 Acesso à ferramenta **Gestão de computadores**

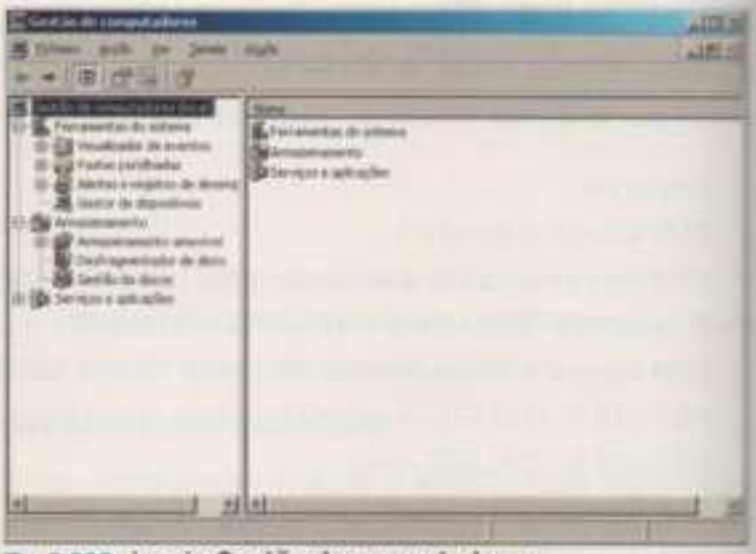

Fig. 3.206 Janela **Gestão de computadores**

Em **Ferramentas do sistema** encontra-se a maioria das funções principais. Neste "nó" é possível executar as seguintes tarefas:

- ver eventos e gerir os *event logs*;
- gerir pastas partilhadas (ver, criar e gerir partilhas; ver sessões e abrir ficheiros; desligar sessões). Para mais informação, consultar o ponto **Pastas partilhadas**;
- criar e gerir utilizadores e grupos locais (no entanto, se o sistema for um controlador de domínio a correr o *Active Directory*, a extensão **Utilizadores e grupos locais** não irá carregar);
- configurar *logs* de performance e alertas;
- **gerir dispositivos** (funciona apenas no modo *read only*, quando está a ver sistemas remotos). Para mais informação, consultar o ponto **Gestão de dispositivos**.

Em **Armazenamento** encontram-se opções para gerir armazenamento removível (por exemplo, CD-ROM e CD Jukeboxes), bem como a ferramenta de desfragmentação de disco e a ferramenta de gestão de disco para gerir discos, partições e volumes.

Em **Serviços e aplicações** encontram-se definições de telefone (*Telephony Settings*), serviços de configuração e uma extensão de indexação (*Indexing Extension*). Quando se instalam novos serviços no sistema, os componentes disponíveis no nó **Serviços e aplicações** sofrerão alterações. Para mais pormenores, consultar o ponto **Serviços**.

Pastas partilhadas – *Shared Folders*

Pode ser bastante útil ao administrador ser capaz de gerir, de forma centralizada, os recursos partilhados pelo servidor numa rede, o que é possível através do ramo **Pastas partilhadas**, em **Ferramentas de sistema** da janela **Gestão de computadores**.

Dentro de **Pastas Partilhadas** existem três itens: **Partilhas**, **Sessões** e **Ficheiros Abertos**.

Seleccionando a primeira opção – **Partilhas** –, surge uma listagem com as várias partilhas existentes no servidor e respectivas características: nome, caminho local (do directório), tipo, número de acesso no momento e descrição.

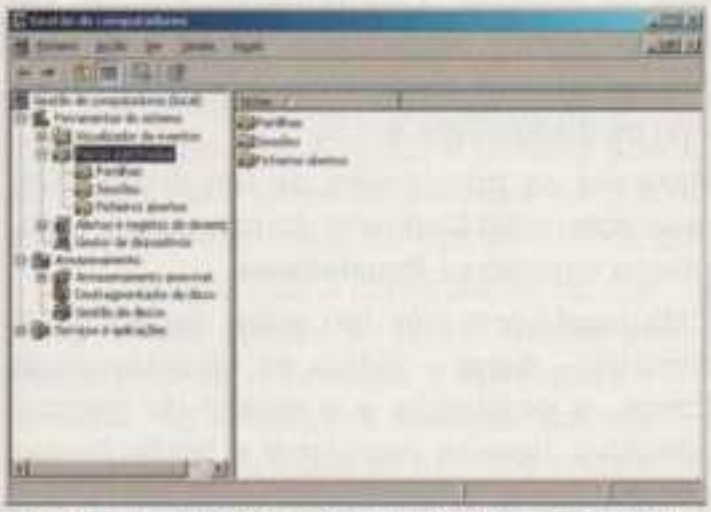

Fig. 3.207 Janela **Gestão de computadores – Ferramentas de sistema – Pastas partilhadas**

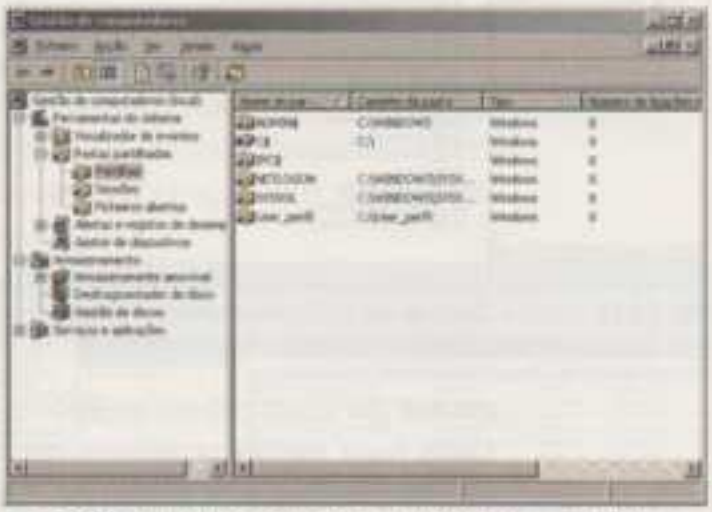

Fig. 3.208 Janela **Gestão de computadores** – Partilhas existentes no servidor

As partilhas com o símbolo **$** estão ocultas e são criadas automaticamente pelo Windows Server 2003 para fins administrativos (não são visíveis pelos clientes da rede).

Fig. 3.209 Janela **Gestão de computadores – Sessões**

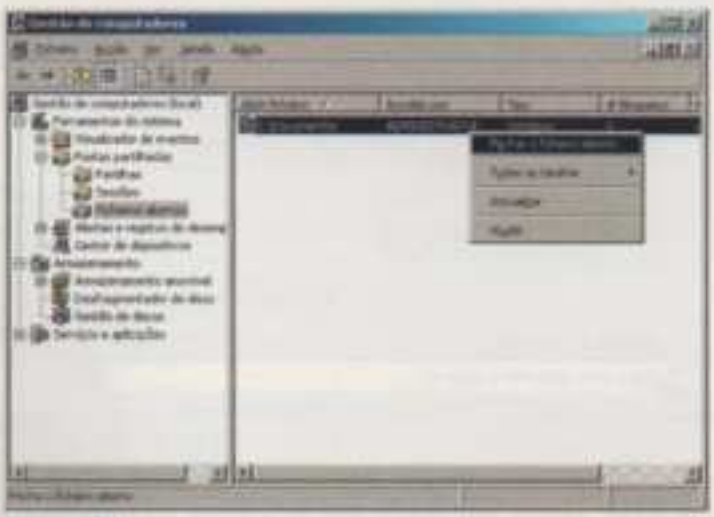

Fig. 3.210 Janela **Gestão de computadores – Ficheiros abertos**

Seleccionando a segunda opção – **Sessões** – surge uma lista dos utilizadores que no momento estão a aceder a algum recurso do servidor. Através desta lista, consegue-se saber que máquina está a ser usada, o tipo, a quantidade de ficheiros abertos, há quanto tempo está ligado (activo ou inactivo) e se o utilizador é ou não um convidado. É até possível desligar a sessão de um utilizador, clicando com o botão direito do rato sobre a sessão e escolher **Fechar sessão**.

A selecção da terceira opção – **Ficheiros abertos** – lista os ficheiros que estão a ser acedidos no momento: o respectivo nome, quem está a aceder, o tipo, a quantidade de bloqueios e o modo de abertura. Aqui também é possível fechar o acesso ao ficheiro, clicando com o botão direito do rato sobre o ficheiro e escolher **Fechar ficheiro aberto**.

Gestão de dispositivos – *Device Manager*

Fig. 3.211 Janela **Gestão de computadores – Ferramentas de sistema – Gestão de dispositivos**

Como sabemos, dentro da **Gestão de computadores** e das **Ferramentas de sistema** existe, além do já explicado ramo **Pastas partilhadas**, o ramo **Gestão de dispositivos**, importante na inspecção e na manutenção dos dispositivos presentes no sistema. Esta ferramenta surge em forma de árvore hierárquica, tendo nos seus ramos os tipos de dispositivos e nos sub-ramos (filhos) os dispositivos em si.

Para ver as prioridades de um dispositivo, clica-se com o botão direito do rato sobre o dispositivo e escolhe-se **Propriedades**.

Esta janela tem três (ou mais) separadores. O primeiro – **Geral** – indica as características gerais do dispositivo: o tipo, o fabricante, a localização e o estado do mesmo. Caso haja algum problema com o dispositivo, deve-se pressionar o botão **Resolução de problemas** e seguir as ajudas dadas.

Fig. 3.212 Janela **Gestão de computadores – Propriedades do dispositivo – Placa de rede** – separador **Geral**

Fig. 3.213 Janela **Gestão de computadores – Propriedades do dispositivo – Placa de rede** – separador **Controlador**

O segundo separador – **Controlador** *(Driver)* – contém informações relativas ao *driver* usado para manter o dispositivo a funcionar correctamente: fornecedor do *driver*, data, versão e signatário. Também se encontram quatro outros botões seguidos da informação geral sobre o *driver*: **Detalhes do controlador** (ficheiros que implementam o *driver* e sua localização), **Actualizar controlador** (*wizard de ajuda para a actualização*), **Recuperar controlador** *(Roll Back Driver)* (possibilita regressar à versão anterior do *driver*, no caso de ter havido problemas com a actualização) e **Desinstalar** (permite desinstalar o *driver*).

O terceiro separador – **Recursos** – apresenta uma listagem dos recursos de memória e IRQ utilizados pelo dispositivo. No caso de se querer gerir estes recursos manualmente (visto a gestão ser feita automaticamente pelo Server 2003), tem de se desmarcar a opção **Utilizar definições automáticas**, seleccionar o tipo de recurso que se pretende alterar e clicar em **Alterar definição**.

No nosso exemplo, temos um quarto separador – **Avançados** –, onde é possível realizar mais operações de configuração sobre o dispositivo.

Serviços

É sempre importante saber trabalhar com os serviços disponibilizados pelo Windows Server 2003 – saber activar e desactivá-los também. Um serviço é uma espécie de programa (sem interface) que corre no servidor com uma determinada tarefa a desempenhar. Normalmente, um serviço é iniciado pelo Windows Server 2003 quando este é ligado e termina apenas aquando do encerramento do servidor. Mas nem todos os serviços se iniciam automaticamente e até é possível parar um determinado serviço sem ter de parar o servidor.

Já sabemos que a configuração de serviços é feita através da janela **Gestão de computadores – Serviços e aplicações – Serviços**. Ao seleccionar **Serviços**, aparece uma listagem de todos os serviços instalados no Windows Server 2003, o que não significa que esteja activo, apenas disponível! Se não estiver activo, pode ser activado manualmente, se assim se desejar. A lista de serviços parece interminável. Como alguns exemplos de serviços temos o **Telnet**, o **Servidor de DNS**, o **Serviço de replicação de ficheiros**, entre outros. Em geral, qualquer programa ou aplicação servidora acaba por fazer a instalação de um ou mais serviços.

Fig. 3.214 Janela **Gestão do computadores – Serviços e aplicações – Serviços** *(standard)*

É importante recordar que, quando algo não está a funcionar como devia, um dos locais para procurar informação e ajuda é precisamente esta janela de configuração de serviços.

A lista do *snap-in* que aparece contém cinco separadores:

- **nome** – identifica o nome do serviço;
- **descrição** – fornece algumas características sobre o serviço;
- **estado** – indica o estado actual do serviço. Se o serviço estiver parado, não há indicação no **estado**; se estiver a funcionar, tem a indicação **iniciado**; se estiver em pausa, indica **"parado"**;

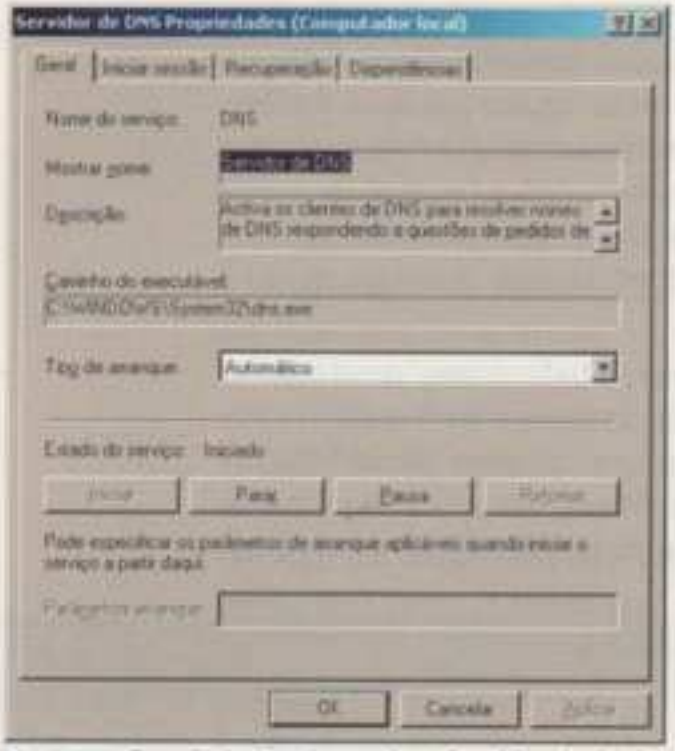

Fig. 3.215 Propriedades do serviço: **Servidor de DNS** – separador **Geral**

Fig. 3.216 Propriedades do serviço: **Servidor de DNS** – separador **Iniciar sessão**

- **tipo de arranque** – indica a configuração de arranque definida para o serviço: automático, manual ou desactivado. Um serviço marcado **automático** inicia automaticamente ao abrir o Server 2003; a indicação **manual** permite iniciar um serviço através da janela de serviços;
- **iniciar sessão como** – indica a conta de utilizador usada para iniciar o serviço.

É possível configurar, para cada serviço, as respectivas opções de tipo de arranque e iniciar sessão, bastando, para tal, clicar com o botão direito do rato sobre o serviço seleccionado e escolher **Propriedades** ou, simplesmente, clicar duas vezes sobre o serviço que se pretende configurar.

Nesta janela constam quatro separadores: **Geral**, **Iniciar sessão**, **Recuperação** e **Dependências**.

O primeiro separador – **Geral** – apresenta:

- **Nome do serviço** – nome real do serviço.
- **Mostrar nome** – nome que identifica o serviço na lista.
- **Descrição** – descreve para que serve o serviço.
- **Tipo de arranque** – automático, manual ou desactivado. Para activar um serviço parado, basta premir o botão **Iniciar**; para parar um serviço, premir **Parar**; e para o parar apenas temporariamente, premir **Pausa**. O botão **Retomar** serve para retomar um serviço que estava em pausa (interrompido).
- **Estado do serviço** – indica o estado do serviço.

No segundo separador – **Iniciar sessão** –, é possível indicar se pretendemos que seja usada uma conta especial de sistema ou uma conta normal de utilizador para validar serviços perante o sistema operativo. Para usar uma conta normal de utilizador, basta indicar o nome do utilizador e a sua palavra-passe.

Para activar ou desactivar um serviço em função do perfil do *hardware* usado no arranque do computador, basta seleccionar os perfis na lista e premir os botões **Activar** ou **Desactivar**.

O terceiro separador – **Recuperação** – permite configurar o comportamento em caso de falhas. Tanto para a primeira como para a segunda e subsequentes falhas é possível ignorar a falha, reiniciar o serviço, correr um programa ou reiniciar o computador.

Para repor o contador de falhas a zero e iniciar uma nova contagem, após um determinado número de dias, introduz-se o número de dias pretendido no espaço **Repor contador de falhas após**.

Se pretendermos reiniciar o serviço, teremos de indicar, em **Reiniciar serviço após**, os minutos ao fim dos quais, após a falha, o serviço é reiniciado.

Caso se tenha optado por correr um programa, convém indicar qual o programa a correr e quais os seus parâmetros (caso existam).

Se a opção for reiniciar o computador, deve-se pressionar o botão **Opções para reiniciar o computador** e indicar quanto tempo após a falha se pretende que o computador seja iniciado. Nesta janela também é possível enviar aos clientes da rede uma mensagem a avisar que o servidor vai reiniciar.

No último separador – **Dependências** – existem duas listagens: a primeira com os serviços de quem o serviço seleccionado é dependente e uma segunda com os que são dependentes do serviço seleccionado.

Fig. 3.217 Propriedades do serviço **Servidor de DNS** – separador **Recuperação**

Fig. 3.218 Propriedades do serviço **Servidor de DNS** – separador **Dependências**

3.10. TCP/IP (*Transmission Control Protocol/Internet Protocol*)

Introdução

O **TCP/IP** é o protocolo mais usado que assegura todas as comunicações na Internet. Por exemplo, para usar o AD e políticas de grupo é obrigatório o uso do TCP/IP. Num sentido mais lato, o TCP/IP é o protocolo mandatário para o Windows Server 2003. Para recordar mais pormenores sobre este protocolo, aconselha-se uma nova leitura da unidade 2, ponto **3.13. Protocolo TCP/IP**, e do ponto **2.1. Planeamento da instalação**, da unidade 3.

Veremos três tecnologias muito básicas e essenciais relacionadas com o TCP/IP que permitem criar uma infra-estrutura para a nossa rede: o **WINS** (*Windows Internet Name Service* – Serviço de Nomes da Internet do Windows), o **DNS** (*Domain Name Service* – Serviço de Nome de Domínio) e o **DHCP** (*Dynamic Host Configuration Protocol* – Protocolo de Configuração Dinâmica de Anfitrião).

Resolução de nomes (*Name Resolution*)

O processo de converter um endereço IP num nome correspondente é conhecido por resolução de nomes. Por exemplo, ao navegar na Internet para obter mais informações sobre o Windows Server 2003, decerto que se vai de imediato ao *site* com o endereço **http://207.46.19.60**, que mais não é do que o *site* **http://www.microsoft.com** (da Microsoft).

Os ficheiros HOSTS e LMHOSTS

Como é que o TCP/IP interliga os nomes dos anfitriões (*host names*) aos endereços IP? Basicamente, fá-lo com o **HOSTS** (*Simple Naming Systems* – Sistemas Simples de Atribuição de Nomes), o **DNS** e, caso se tenha uma rede que ainda não use o *Active Directory*, com o **WINS**.

Quando se configura a sub-rede (*subnet*) não se pretende andar sempre, explicitamente, a usar endereços IP de cada vez que se quer correr um utilitário TCP/IP e ligar-se a outro computador na sub-rede. Em vez disso, cria-se um ficheiro, chamado **HOSTS**, que é parecido com isto:

198.33.56.51 **sjm.escola.pt**
198.33.56.120 **porto.escola.pt**

O **HOSTS** é apenas um simples ficheiro de texto **ASCII**. Cada anfitrião vai para uma linha e a linha inicia com o endereço IP do anfitrião. Cada linha contém um endereço IP, pelo menos um espaço e um nome (de anfitrião).

Isto deve ser feito para cada anfitrião. Até é possível dar múltiplos nomes no ficheiro **HOSTS**:

198.33.56.51 **sjm.escola.pt esccentro**
198.33.56.120 **porto.escola.pt escola norte**

ou até acrescentar comentários, seguidos do símbolo #

198.33.56.51 **sjm.escola.pt esccentro #A máquina principal**
198.33.56.120 **porto.escola.pt escola norte**

O aspecto mais aborrecido é ter de colocar um destes ficheiros **HOSTS** em cada uma das *workstations*. Isto significa que, cada vez que se altera qualquer ficheiro **HOSTS**, tem de se fazer a ronda e alterar todos os ficheiros **HOSTS**. Cada *workstation* tem de ter uma cópia deste ficheiro, que, basicamente, é uma lista telefónica de cada máquina na sub-rede.

Mas, então, porque não colocar um ficheiro **HOSTS** central no servidor e fazer toda a administração com esse ficheiro? – O que se está aqui a pedir é um servidor de nomes (*name server*) e os dois mais usados são o **DNS** e o **WINS**.

O ficheiro **LMHOSTS** trabalha de um modo muito semelhante ao **HOSTS**. É bom compreender o **LMHOSTS**, uma vez que este ficheiro resolve muitos problemas de resolução de nomes com computadores-servidores anteriores ao Windows 2000 e talvez até com computadores-servidores Windows 2000 e Server 2003, numa empresa com domínios baseados em Windows 2000 e NT4.

Se nos recordarmos, o **HOSTS** é um ficheiro **ASCII** que lista endereços IP e nomes de Internet. No entanto, a Microsoft decidiu criar um ficheiro **ASCII** que contivesse nomes **NetBIOS** e o resultado foi o ficheiro **LMHOSTS**. O ficheiro **LMHOSTS** consiste em pares de endereços IP e nomes, tal como **HOSTS**, mas os nomes são nomes NetBIOS de 15 caracteres e não nomes de tipo Internet:

100.100.210.13 **sala10**
211.39.82.15 **biblioteca**

Este ficheiro encontra-se localizado no directório **C:\Windows\system32\drivers\etc\lmhosts**.

WINS (*Windows Internet Name Service* – Serviço de Nomes da Internet do Windows)

Para que o **WINS** trabalhe, tem de se ter configurado um servidor NT4 ou posterior (não trabalha com mais nenhum, nem mesmo com o NT *Workstation*) para agir como servidor **WINS**. O servidor **WINS** age como servidor **NBNS**, mantendo-se informado sobre quem entra e quem está na rede (registo na sua base de dados) e distribuindo informação de resolução de nomes quando necessário; isto é, o **WINS** garante a manutenção e a replicação da base de dados de nomes na rede. No processo de registo de nome com um servidor **WINS**, a *workstation* assegura-se de que se trata de um nome único. Se o servidor **WINS** verificar que existe um outro computador com o mesmo nome, então comunica à *workstation* que este nome não pode ser usado.

A função do **WINS** (serviço de nome **NetBIOS** para Windows) é semelhante ao **LMHOSTS**, mas mais dinâmica. Além disto, outra diferença consiste no facto de a base de dados do **WINS** se construir e manter a si própria, procedendo às suas actualizações sempre que necessário. Deste modo, após a instalação deste serviço, o administrador da rede não tem muito mais com que se preocupar, pois tudo funciona automaticamente.

DNS (*Domain Name Service* – Serviço de Nome de Domínio) e DDNS (*Dynamic DNS*)

O **DNS** é um sistema de resolução de nomes inventado em 1984 para a Internet. Permite navegar na Internet utilizando nomes mais "amigáveis", como, por exemplo, **http://www.unicef.org**, onde o interesse está em descobrir informações sobre a UNICEF e não saber qual o seu endereço IP (que é **57.69.14.59**). O **DNS** torna o uso dos endereços de *e-mail* mais simples, através dos seus registos MX, e também mostrou ser uma maneira facilmente expansível de manter nomes na maior rede do Mundo. O **DNS** é bastante expansível e permite controlar localmente partes da base de dados completa. A sua capacidade para crescer – a sua escalabilidade – é uma mais-valia para o *Active Directory*, uma vez que a Microsoft espera que o AD venha a ser a base de algumas grandes redes. O **DNS** é agora o repositório central de nomes para o *Active Directory*, substituindo o papel do **WINS** no NT4. Durante anos, o **WINS** foi uma "dor de cabeça", por muitas razões, mas foi melhor do que o **DNS** num aspecto muito importante: a sua base de dados era automática e dinâmica. Quase nunca era necessário informar o servidor **WINS** sobre uma máquina na rede; em vez disso, as máquinas comunicavam com o **WINS** e registavam-se automaticamente. Deste modo, o **WINS** mantinha automaticamente uma base de dados das máquinas na rede. O **DNS**, por sua vez, não era automático; tudo era feito manualmente pelo administrador. Tendo esta "falha" em conta, a Microsoft decidiu trabalhar o conceito do **DNS** e criou o DDNS (*Dynamic DNS* – DNS dinâmico), que é parecido com o modelo de gestão de dados de endereços do **WINS**. Os clientes **DNS** – as *workstations* e os servidores que contam com o **DNS** para a resolução de nomes – podem registar-se automaticamente com o **DNS**, por si próprios, dispensando a intervenção do administrador.

Outro ponto que distingue o **DDNS** do **DNS** é que o primeiro suporta o registo de controladores de domínio, isto é, todos os servidores **DNS** registam a informação estruturadas em **zonas**. Uma **zona** corresponde a um domínio ou a uma parte dele, por exemplo, **unicef.org**. Uma zona pode conter:

- **registos do tipo A**, onde ficam registadas as equivalências entre o endereço IP e o nome;
- **registos NS**, que identificam nomes de servidores para determinadas zonas;
- **registos SOA**, que descrevem as características da zona e que indicam quem deve ser contactado, no caso de surgir um problema com a zona;
- **registos CNAME**, que permitem adicionar a um endereço IP um nome reconhecido extra;
- **registos do tipo MX**, onde se guardam o nome do servidor de correio electrónico do domínio.

Aqui surge um novo registo, não existente no **DNS**, designado **SRV**, que arquiva a informação sobre os controladores de domínio. Deste modo, os restantes computadores podem encontrá-los, sejam eles computadores-clientes que estão a aceder ao AD ou controladores de domínio do mesmo ou de outro domínio que necessitam de consultar ou replicar informação.

Utilitários

Cada vez que se instala o TCP/IP num computador, também se instalam alguns utilitários que ajudam a tirar partido das características do TCP/IP. Temos, por exemplo, o:

- **ping** (entre várias funções, testa a ligação entre sistemas que utilizam o protocolo IP);
- **tracert** (rastreia a rota da ligação desde o nosso computador até ao computador remoto);
- **finger** (num sistema que corre o serviço *finger*; mostra informações sobre o utilizador);
- **ftp** (transfere ficheiros entre um cliente e um servidor de **ftp**) ou o **telnet** (utilitário que permite a emulação de terminal de um computador remoto);
- **Arp** (devolve o endereço Mac associado a cada placa de rede e o respectivo endereço IP;
- **Ipconfig** (informa das configurações do endereço IP no nosso sistema operativo).

Para obter mais informação sobre cada comando, deve utilizar a ajuda do Windows: ir ao menu **Iniciar** e seleccionar **Ajuda e suporte** ou, através da linha de comando, escrever o comando seguido de **/?**, por exemplo, **ping /?**.

3.11. DHCP (*Dynamic Host Configuration Protocol* – Protocolo de configuração dinâmica de anfitrião)

Introdução

Quer nos liguemos a uma pequena rede intranet para partilhar uma ligação Internet ou a uma rede Internet mundial, há um grande problema a resolver: cada sistema na rede necessita de um endereço IP único e requer uma configuração – necessita de saber o endereço do seu *router* por defeito, o seu nome de domínio, onde se encontra o servidor DNS mais próximo, etc. Devido ao grande número de equipamentos ligados às redes, houve necessidade de se desenvolver um serviço de atribuição e de configuração dinâmica de endereços IP, e, assim, surge o **DHCP**.

Configuração de um servidor DHCP

Para se configurar um servidor **DHCP**, deve-se atribuir um endereço IP fixo ao servidor. A janela de configuração do TCP/IP encontra-se seguindo os seguintes passos:

Ir ao menu **Iniciar > Painel de controlo** e clicar duas vezes sobre **Ligações de rede**.

Seleccionar **Ligação de área local**, clicar com o botão direito do rato e escolher a opção **Propriedades**.

Fig. 3.219 Abrir a janela **Ligações de rede**

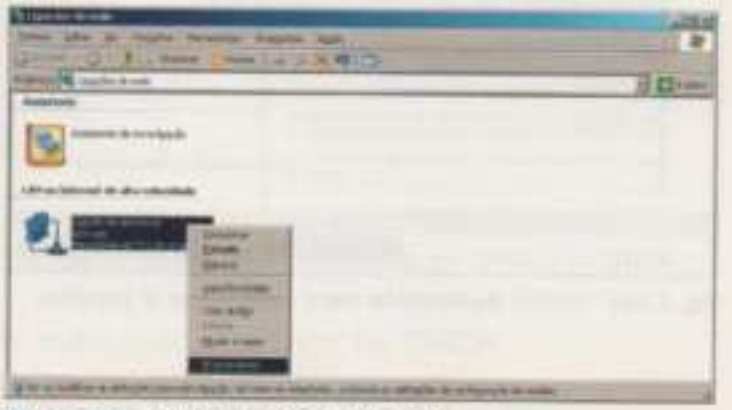

Fig. 3.220 Janela **Ligações de rede**

Para se configurar o TCP/IP deve-se, na janela **Propriedades de Ligação de área local**, seleccionar **TCP/IP** (Protocolo Internet) e clicar em **Propriedades**.

Na janela **Propriedades de TCP/IP** (Protocolo Internet), seleccionar **Utilizar o seguinte endereço IP** e escrever o endereço IP que se pretende atribuir ao servidor e a correspondente máscara de sub-rede. Opcionalmente, ainda é possível especificar os endereços de até dois servidores de **DNS** seleccionando **Usar os seguintes endereços de servidores DNS**. No nosso exemplo, o servidor é um servidor de **DNS**. De seguida, pressionar em **OK** para continuar.

Fig. 3.221 Janela **Propriedades de Ligação de área local**

Fig. 3.222 Janela **Propriedades de TCP/IP** (Protocolo Internet)

Instalação servidor DHCP

Para se instalar o serviço de **DHCP**, deve-se usar o *wizard* (assistente) da ferramenta **Configurar o servidor**, que – como vimos no ponto **3.2. Administração Rápida** – se acede a partir do menu **Iniciar > Programas > Ferramentas administrativas**.

Ir ao menu **Iniciar** (*Start menu*) **> Ferramentas administrativas** (*Administrative tools*) **> Assistente para configura o servidor** (*Configure your server wizard*).

Quando surgir o "ecrã de boas-vindas", deve-se pressionar em **Seguinte** as vezes necessárias até chegar ao ecrã **Assistente para configurar o servidor – Papel do servidor**, que permite seleccionar a opção **Servidor DHCP**. Seleccionar esta opção e pressionar em **Seguinte** para prosseguir com a instalação.

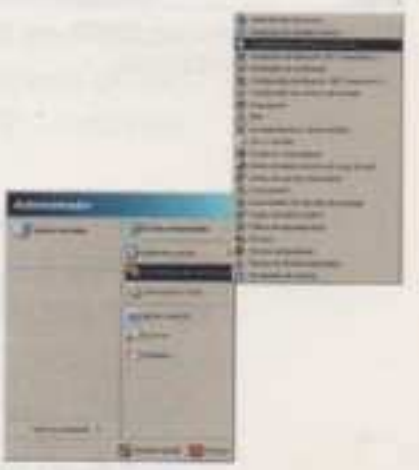

Fig. 3.223 Lançamento do **Assistente para configurar o servidor**

Verificar se as opções seleccionadas estão correctas. Caso isto se verifique, clicar em **Seguinte** para dar início à instalação do serviço de **DHCP**.

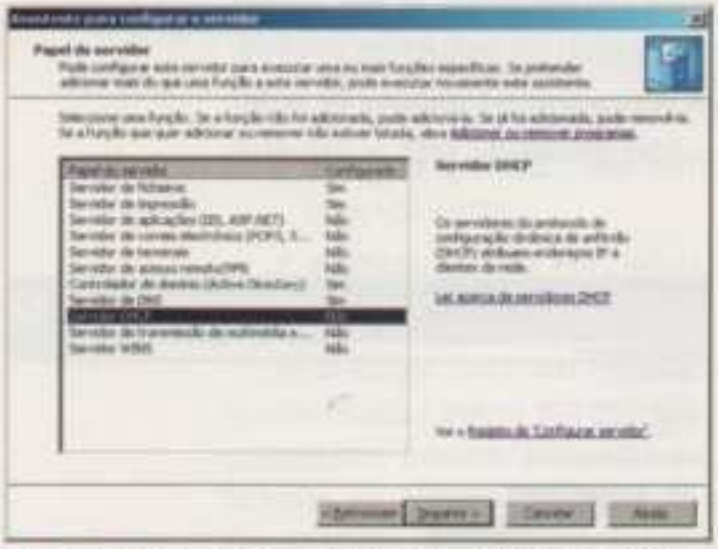

Fig. 3.224 Janela **Assistente para configurar o servidor**

Fig. 3.225 Janela de verificação das opções escolhidas para a instalação do servidor de **DHCP**.

Há que aguardar! O processo de instalação do serviço de **DHCP** está em curso.

No final da instalação do serviço de **DHCP** (figura 3.227), pode-se configurar o serviço e, para isso, deve-se clicar em **Seguinte**. No nosso exemplo, a configuração do serviço de **DHCP** é realizada mais à frente – ver **Criação de um âmbito *scope***. Deste modo, clica-se em **Cancelar** para terminar o processo de instalação.

Ao clicar em **Concluir** (figura 3.228) termina o processo de instalação do serviço de **DHCP**.

No fim cria-se um atalho, no grupo de ferramentas administrativas, para lançar a ferramenta de configuração do serviço de **DHCP**.

Apesar do serviço estar instalado, ainda falta configurá-lo.

Fig. 3.226 Serviço de **DHCP** em fase de instalação

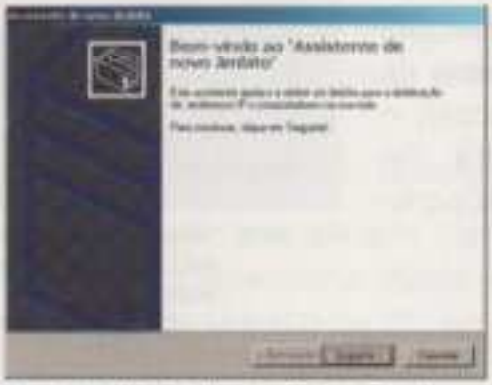

Fig. 3.227 Início de configuração do serviço de **DHCP**

Fig. 3.228 Fim de instalação do serviço de **DHCP**

Criação de um âmbito – *scope*

O endereço IP que um cliente pede ao servidor de **DHCP**, para se validar na rede, encontra-se num grupo de endereços que estão algures entre os limites inferiores e superiores que serão pormenorizados na criação do **âmbito** (*scope*). Resta saber o que fazer para se criar um *scope*:

- Ir ao menu **Iniciar**, a **Ferramentas administrativas** e seleccionar **DHCP**.

Cria-se um *scope* clicando na árvore do serviço de **DHCP** e, no menu **Acção**, deve-se escolher a opção **Novo âmbito**, que lançará um assistente.

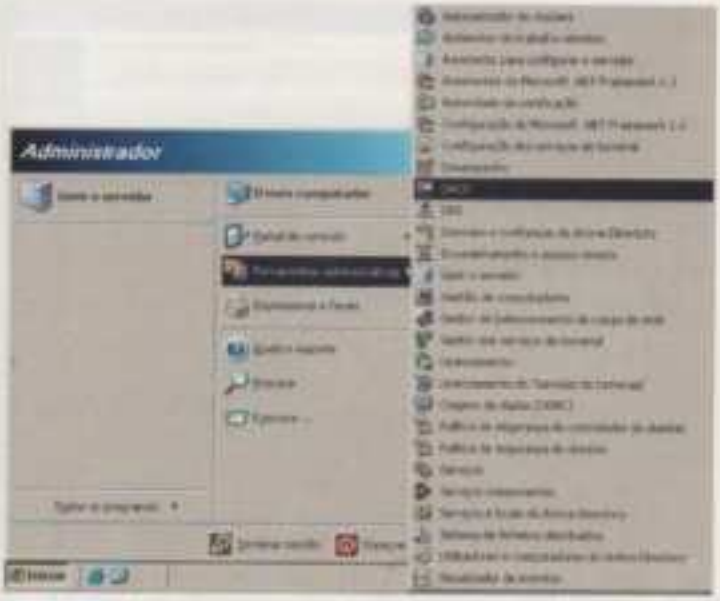

Fig. 3.229 Lançamento de configuração do serviço de **DHCP**

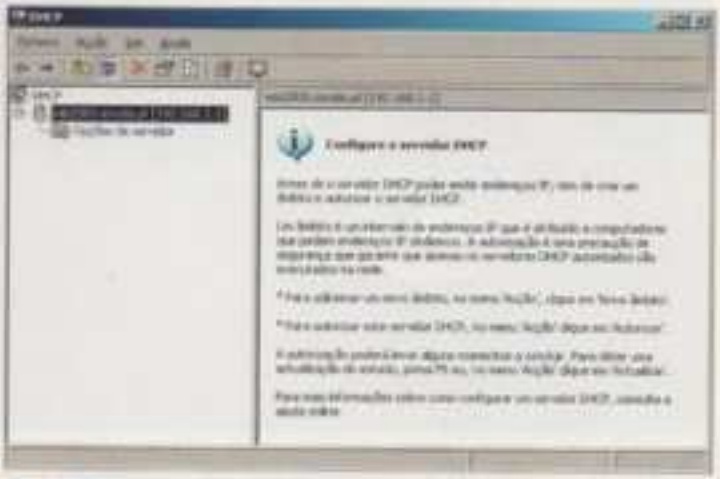

Fig. 3.230 Janela de configuração do serviço de **DHCP**

Surge, então, um assistente que nos ajudará a configurar o serviço de **DHCP**. Para prosseguir com a instalação, clicar em **Seguinte**.

Este assistente (*wizard*) vai pedindo alguns dados (como, por exemplo, a atribuição de um nome ao *scope* e uma breve descrição) e, após introdução dos mesmos, deve-se clicar em **Seguinte**.

Fig. 3.231 Janela **Assistente de novo âmbito**

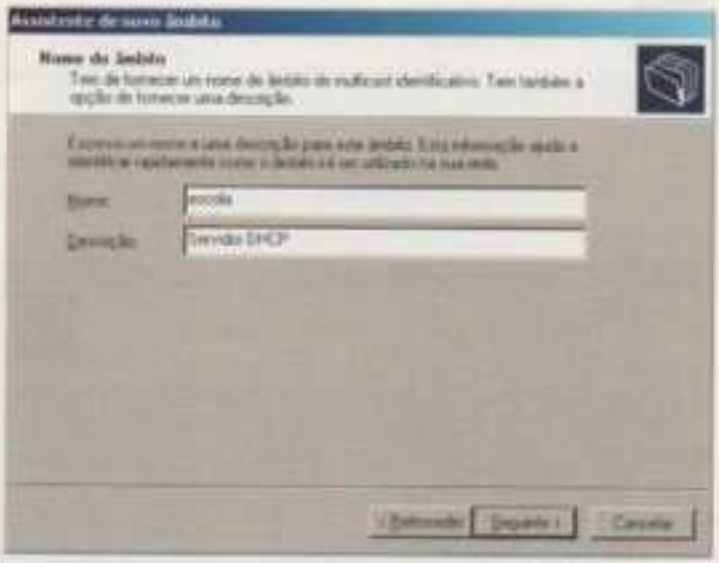

Fig. 3.232 Janela de configuração do nome do âmbito

No ecrã da figura 3.233 devem-se introduzir os limites do **âmbito** (*scope*), indicar os valores superiores e inferiores que cada cliente pode ter e a máscara – *subnet mask* – que identifica a rede. Assim, o endereço da rede, neste exemplo, é dado pelos três primeiros bytes (**192.168.1**) e o endereço de cada *host* tem de ser único e pode variar entre 100 (**192.168.1.100**) e 200 (192.168.1.200), inclusive. Depois clicar em **Seguinte**.

Para excluir elementos do conjunto de endereços definido, para que estes não venham a ser facultados a nenhum cliente, pode-se ir à janela **Adicionar exclusões** (figura 3.284); aí deve introduzir-se o valor do endereço na caixa **Endereço IP inicial**, caso se pretenda excluir um endereço específico, ou, então, caso se pretenda excluir um conjunto de endereços próximos, deve indicar-se o primeiro e o último endereços do conjunto nas caixas **Endereço IP inicial** e **Endereço IP final**, respectivamente, e clicar em **Adicionar**. Repetir esta operação as vezes que forem necessárias. Para remover uma exclusão, deve-se seleccionar a mesma na lista correspondente e clicar em **Remover**.

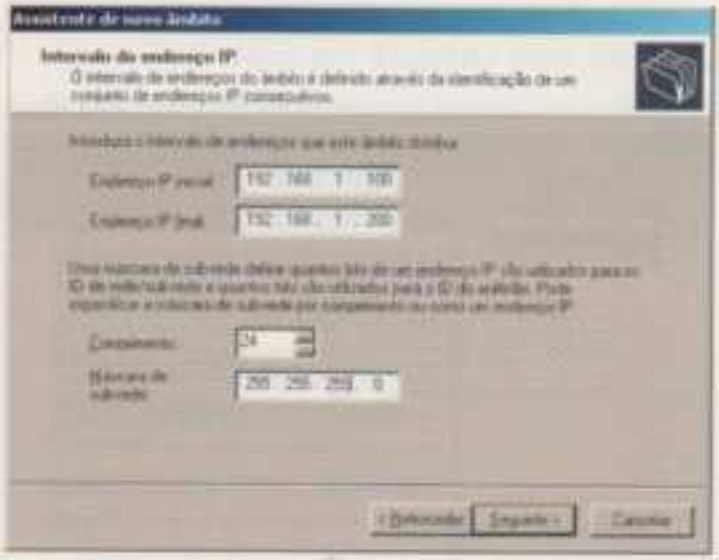

Fig. 3.233 Configuração do **Intervalo de endereço IP**

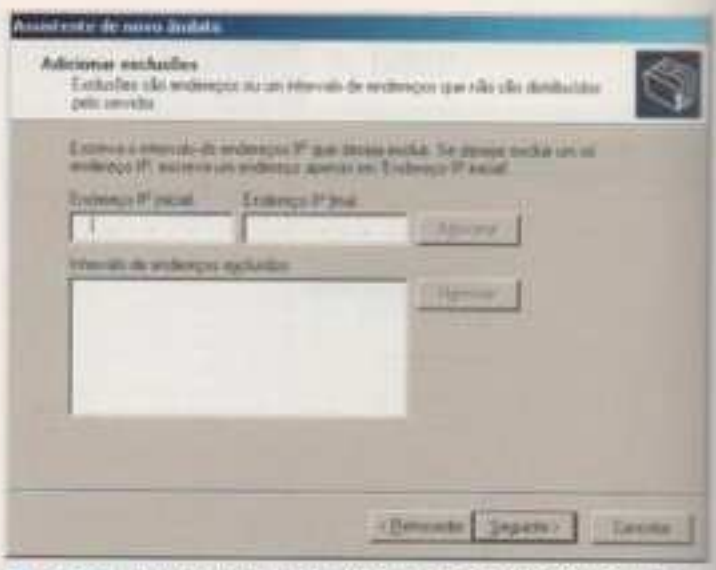

Fig. 3.234 Configuração da exclusão de endereços IP do âmbito

É também possível limitar, a nível de tempo, a concessão do serviço de **DHCP**, no que respeita à atribuição de um endereço IP aos clientes. Assim, ao indicar o tempo de validade do endereço fornecido, consegue-se libertar endereços para que estes possam ser (re)utilizados por outros clientes; isto é, se um determinado cliente sair da rede inadvertidamente, o servidor não sabe que este já não se encontra na rede, mas, ao fim de 10 dias (no nosso exemplo), o servidor atribui um novo endereço.

Este assistente de configuração também permite configurar outros parâmetros, além da criação de um **scope** – tipo endereços IP de *routers* ou servidores de **WINS** e de **DNS**. Para configurar estas opções, vai-se a **Configurar opções do serviço DHCP** e, após a selecção da opção, pressiona-se em **Seguinte**.

Fig. 3.235 Validade do serviço

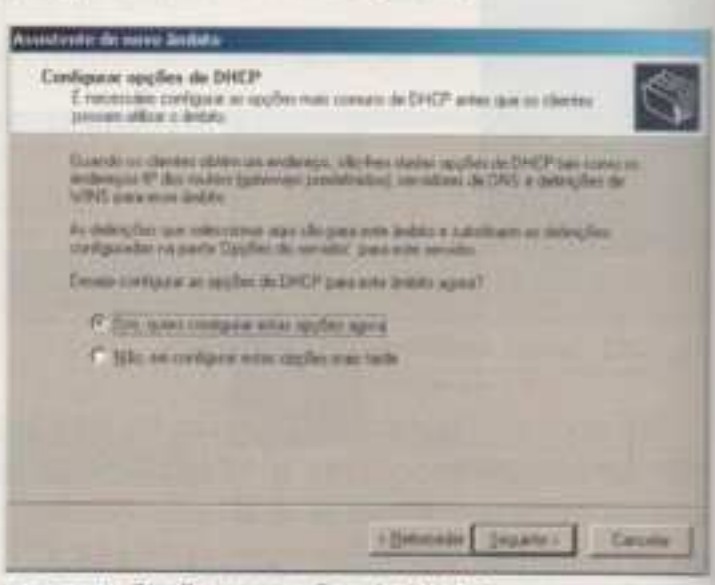

Fig. 3.236 **Configurar opções de DHCP**

Na janela **Router (*gateway* predefinido)** devem indicar-se (pela ordem que considerarmos mais adequada) as portas de ligação usadas pelos clientes da rede. Estas portas correspondem ao endereço IP dos *routers* responsáveis pela interligação entre dois segmentos de uma rede.

Para indicar os servidores de DNS, vai-se à janela **Servidor de DNS e de nomes de domínio**. Aí deve-se indicar os endereços dos servidores de DNS, para a resolução dos nomes dos endereços. Para obter o endereço do nome do servidor, basta clicar em **Resolver**. Aqui também é possível indicar o número de servidores de DNS que se quer.

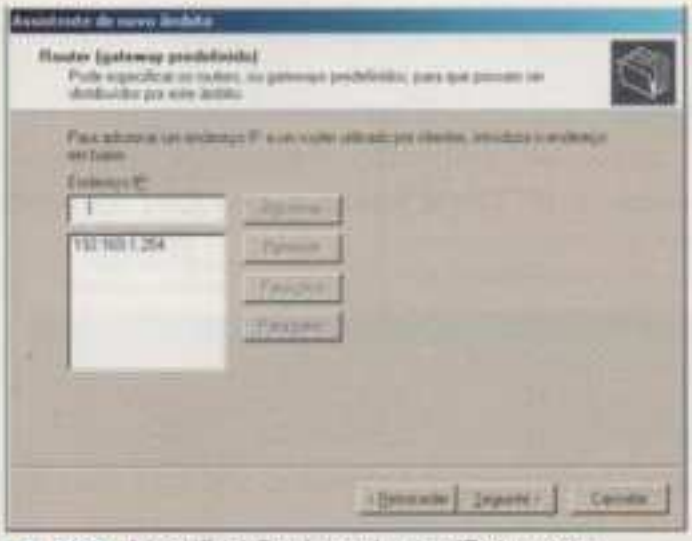

Fig. 3.237 Identificação do endereço IP do *router*

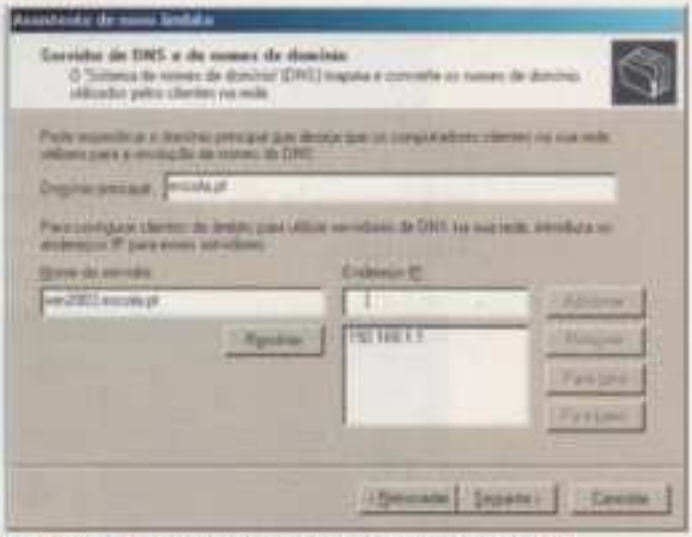

Fig. 3.238 Indicação do(s) servidor(es) de **DNS**

Para identificar os servidores de WINS (usado por clientes Windows NT ou 9x, por exemplo), abre-se a janela **Servidores WINS** e seguem-se os procedimentos indicados para os servidores DNS.

Para finalizar todas as configurações necessárias à criação de um *scope*, só falta activá-lo. Para tal, abre-se a janela **Activar âmbito**, selecciona-se a opção **Sim, quero activar este âmbito agora** e clica-se em **Seguinte**.

Fig. 3.239 Indicação do(s) **Servidores WINS**

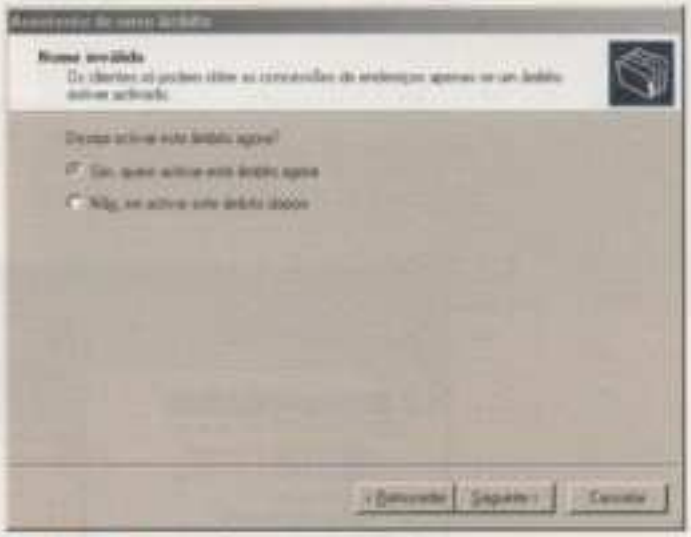

Fig. 3.240 Activação do *scope* (âmbito)

Finalmente, temos o *scope* configurado. Clicar em **Concluir**, para terminar.

Após a configuração do âmbito – *scope*, podemos expandir a árvore do âmbito – *scope* criado, como se pode verificar na figura 3.242.

Fig. 3.241 Conclusão do assistente de criação do *scope*

Fig. 3.242 Aspecto do âmbito – *scope* criado

Autorização de um servidor de DHCP

Após a activação do *scope* criado, ainda é necessário autorizar/credenciar o servidor de DHCP, para que este serviço possa ser fornecido. Para tal é suficiente seleccioná-lo no respectivo ramo da árvore, ir ao menu **Acção** e escolher a opção **Autorizar**.

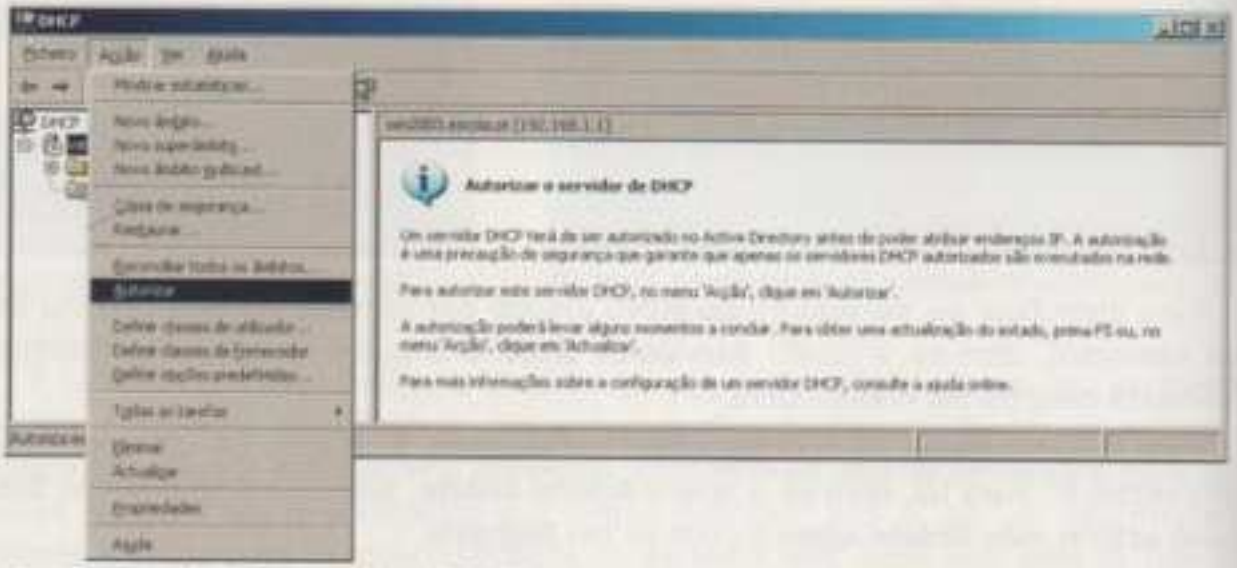

Fig. 3.243 Autorização do servidor de DHCP

Após a autorização do servidor de DHCP, constata-se que, na raiz do nome do serviço de DHCP, surge uma "circunferência verde", que, anteriormente, estava a vermelho.

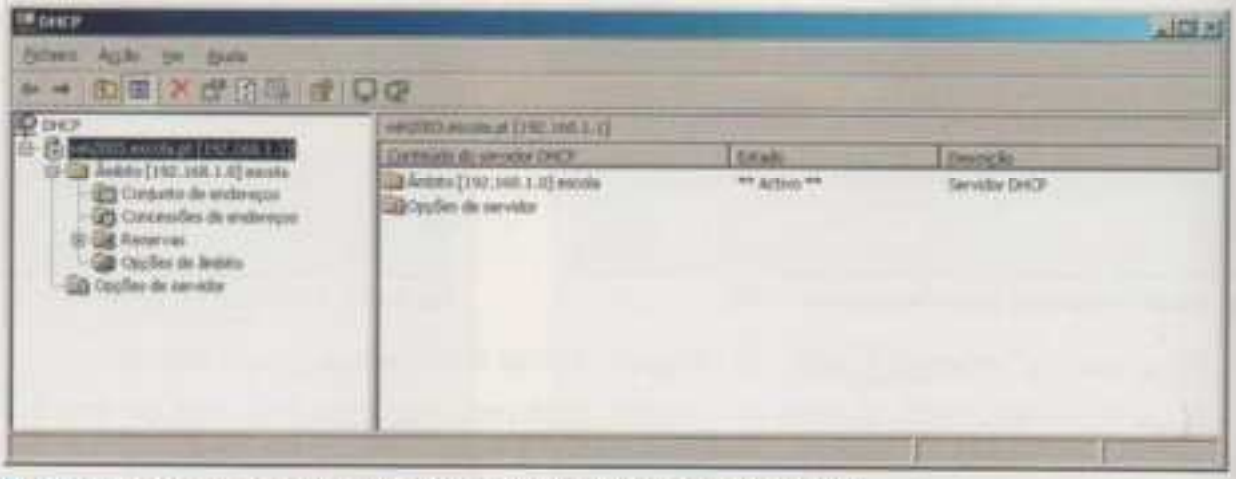

Fig. 3.244 Aspecto do servidor de DHCP após realizada a autorização

Reservas de endereços

É possível um cliente pedir que lhe seja atribuído sempre o mesmo endereço IP do servidor de DHCP e impedir que este seja fornecido a outro cliente. Para que isto se verifique, deve-se instruir neste sentido o servidor de DHCP, ou seja, o servidor de DHCP fornece um certo endereço apenas a um cliente que tenha a placa de rede com o Mac Address especificado, que se compõe por um conjunto de seis grupos de dois dígitos, que identificam a placa e o seu fabricante como únicos. Para proceder à configuração de uma reserva, na árvore, deve seleccionar-se **Reservas**, ir ao menu **Acção** e escolher **Nova reserva**.

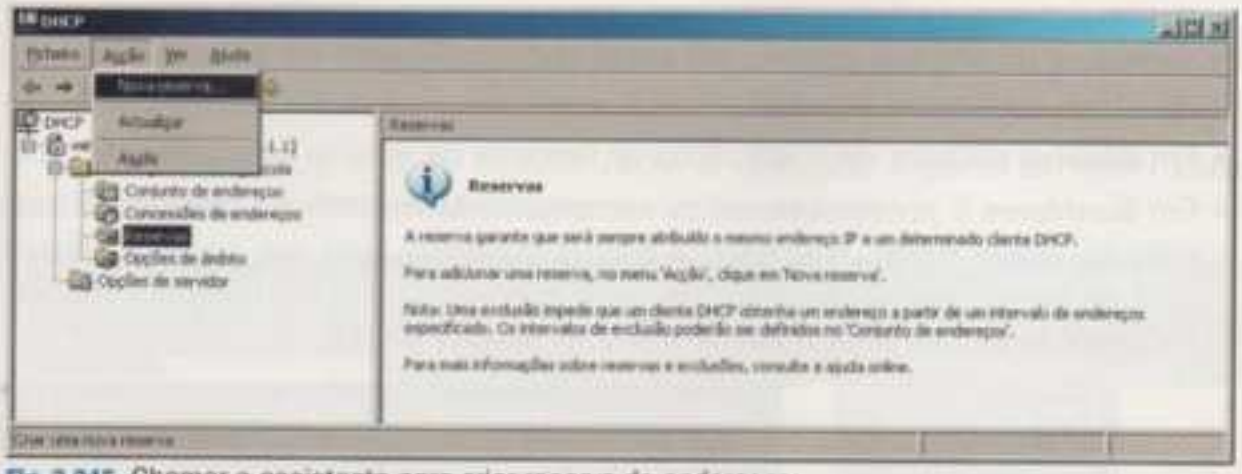

Fig. 3.245 Chamar o assistente para criar reserva de endereços.

Na janela da figura 3.246 deve indicar-se o nome que identifica a reserva, introduzir o endereço IP a ser utilizado e o endereço MAC da placa de rede do computador que se pretende atribuir ao referido endereço IP. O endereço MAC pode ser obtido consultando o manual da placa ou por via informática (digitar, na linha de comandos, o comando **IPCONFIG/ALL** – se se tratar dos Windows NT, 2000 ou XP; caso se trate do Windows 9x, deve usar-se o comando **WINIPCFG**); para finalizar, devem-se indicar os modos suportados: se funciona apenas no modo DHCP, ou apenas no modo BOOTP, ou em ambos. Podem reservar-se diversos endereços e, para isso, deve-se clicar em **Adicionar** e, para terminar, em **Fechar**.

Fig. 3.246 Criar reserva de endereços.

3.12. Gestão de licenças

Licenciamento

Já é sabido que para cada exemplar do Windows Server 2003 é necessário uma licença de servidor e uma licença CAL de cliente de acesso ao *software*. Também já é do nosso conhecimento que com o Windows Server 2003 se pode optar por dois tipos de licenciamento de clientes: *per user* (por utilizador) ou *per server* (por servidor). Para recordar em que consiste a diferença entre estes dois tipos de licenciamento e para relembrar os aspectos do controlo de licenças, aconselha-se uma nova leitura da subunidade **2.1. Tipos de licença** e da subunidade **2.5. Processo de instalação**.

O **licenciamento** (*licensing*) é apenas um programa das ferramentas de administração da rede que permite registar novas licenças e controlar o número de licenças a ser usadas nos servidores de rede. O acesso ao programa de licenciamento é realizado a partir do menu **Iniciar** – **Ferramentas administrativas** e seleccionar **Licenciamento**.

A principal janela do **Licenciamento** conta com quatro páginas referentes a diferentes dados sobre o número de licenças adquiridas e em uso na rede:

- Em **Histórico de aquisições** encontra-se uma listagem das licenças de *software* registadas no **Licenciamento**.

- Em **Visualizar produtos** pode-se encontrar uma listagem de todos os produtos da rede e ler alguma informação sobre o licenciamento de produtos da rede inteira ou apenas do domínio.
- Em **Clientes** pode-se ver a utilização de licenças de acesso por cliente de rede.
- Em **Servidores** é possível visualizar hierarquicamente toda a organização, permitindo, deste modo, o acesso a outros domínios para ver os seus esquemas de licenciamento de produtos, para acrescentar ou até mesmo para retirar licenças por servidor a um ou mais servidores da rede.

Fig. 3.247 Acesso ao programa de licenciamento do Windows Server 2003

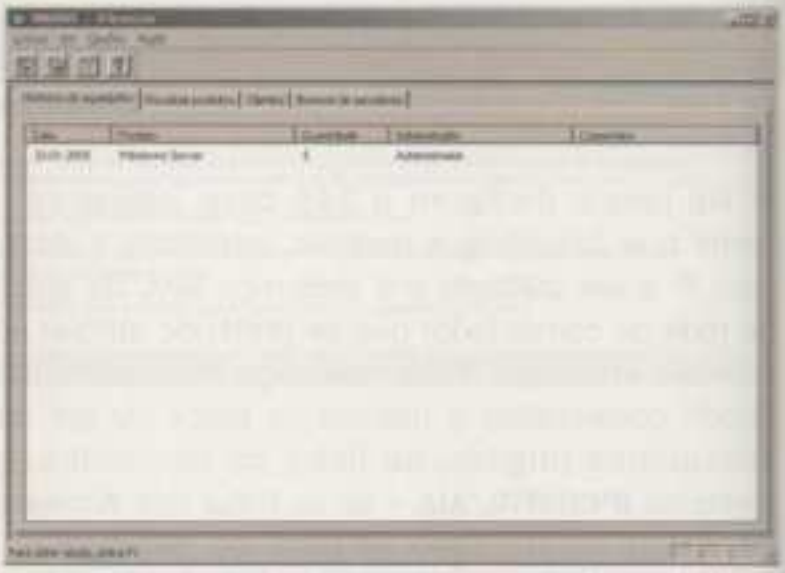

Fig. 3.248 Janela de licenciamento do Windows Server 2003

Registo de novas licenças

Para se registarem novas aquisições de licenças, no licenciamento devem ser seguidos os seguintes passos:

- ir ao menu **Licença** ou pressionar o segundo botão da barra de ferramentas com o desenho de uma licença;
- usar o comando **Nova licença**;
- abrir a janela **Nova licença de acesso de cliente.**

Na janela de registo de novas licenças deve-se seleccionar o produto para o qual se pretende registar a aquisição de mais licenças de cliente. Depois é necessário indicar a quantidade de licenças que se pretende registar, o modo de licenciamento – ou seja, se são licenças por utilizador ou por servidor – e, caso se ache pertinente, ainda é possível acrescentar um pequeno comentário. Terminado o registo das novas licenças, é possível ver quais as que se encontram registadas e quais as que se encontram em uso, através da interface do programa de licenciamento.

3.13. Monitorização e optimização

Monitorização

Existem no Windows Server 2003 as seguintes ferramentas de monitorização:

- O *System Monitor* (monitorizador de sistema), que conta com dois componentes, nomeadamente o **Monitor de sistema** – que mostra estatísticas em tempo real da performance – e os *logs* dos **Alertas e registos de desempenho** – que é

a função de *logging* da monitorização de sistema. Um *log*, como já sabemos, é uma espécie de ficheiro de texto onde é guardada informação variada, como, por exemplo, sobre erros, defeitos, alarmes, alertas, etc.

O acesso ao programa de monitorização é realizado a partir do menu **Iniciar**, em **Ferramentas administrativas** e seleccionar **Desempenho**.

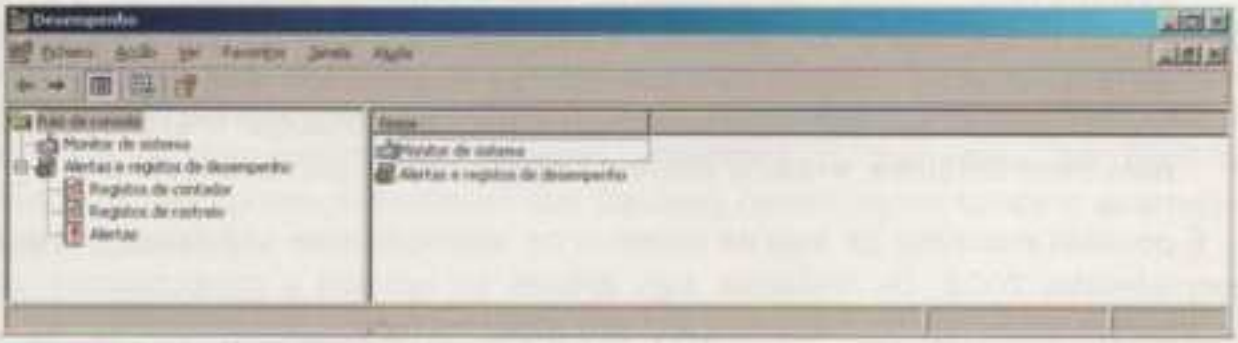

Fig. 3.249 Janela **Desempenho** do Windows Server 2003

O **Monitor de sistema** (*System Monitor*) possibilita, entre outros:

- ver, de forma simples e em tabelas/gráficos ou em relatórios, os sinais vitais do servidor;
- monitorizar como os processos estão a utilizar o tempo do processador, a memória, o espaço em disco e outros recursos do servidor;
- abrir *logs* guardados para rever dados (informações) históricos.

O **Alertas e registos de desempenho** (*Performance Logs and Alerts*) assume as funções de registo de uma monitorização de performance NT4. Usando a função de *logging*, é possível fazer-se o seguinte:

- monitorizar o *stress* e a performance de um sistema por um certo período de tempo, em vez de observar o rendimento (*output*) actual/corrente;
- automaticamente, estar a par dos valores mínimos, máximos, médios e actuais/correntes dos valores críticos do sistema;
- enviar alertas para o *Event log*, notificar alguém ou correr um programa quando os contadores excederem as tolerâncias programadas ou quando ocorrem eventos importantes.

O **Visualizador de eventos** (*Event Viewer*), que se encontra localizado no grupo dos programas das **Ferramentas administrativas**, mantém vários registos de eventos separados no servidor:

- O **Aplicação** (*Application Log*) regista eventos específicos de aplicação que não estão suficientemente próximos para chegarem ao *system log*. O nome deste registo até pode ser um pouco enganador, pois não se trata tanto de aplicações de utilizadores, mas mais de licenciamento, o serviço **BINL**, usado para apoiar os serviços de instalação remota, os *backups*, a aplicação com (ou sem) sucesso de políticas de segurança e afins.

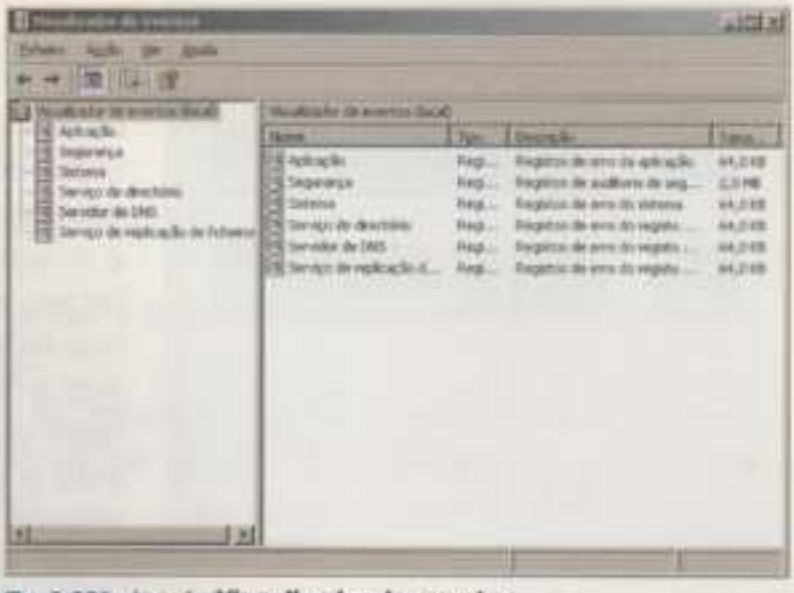

Fig. 3.250 Janela **Visualizador de eventos**

- O **Segurança** (*Security Log*) regista quaisquer eventos de verificação de contas (*audit*) que se relacionam com assuntos de segurança, tal como, por exemplo, utilizadores a aceder a ficheiros ou a alterar a base de dados das contas de segurança.
- O **Sistema** (*System Log*) regista o início e o fim dos serviços e quaisquer eventos relacionados com o sistema. Aqui é possível descobrir que o servidor de DHCP limpou com sucesso a sua base de dados ou que um trabalho de impressão se concluiu com sucesso. Se recebermos uma caixa de mensagem a dizer que algo não funcionou e para se consultar o *Event Monitor* para mais detalhes, então o *System Log* deve ser o primeiro local a ir.

É possível encontrar os *logs* de sistema, de aplicação e de segurança em qualquer servidor 2003. Os restantes *logs* apenas se aplicam a computadores que necessitem deles devido à sua função/ seu papel na rede.

- O **Serviço de directório** (*Directory Service Log*) regista eventos relacionados com controladores de domínio a par com a base de dados de segurança.
- O **Servidor de DNS** (*DNS Server Log*) encontra-se no servidor DNS e grava eventos associados com resolução de nomes de computador ou de endereços IP.
- O **Serviço de replicação de ficheiros** (*File Replication Service Log*) lista eventos relacionados com o serviço de replicação de ficheiros.

Fig. 3.251 Janela de acesso ao **Gestor de tarefas**

- O **Gestor de tarefas** (*Task Manager*) oferece um modo de monitorizar o estado geral do servidor. No Windows Server 2003, o gestor de tarefas pode ser acedido pressionando, em simultâneo, as teclas **Ctrl+Alt+Del** e, de seguida, seleccionando **Gestor de tarefas**.

O **Gestor de tarefas** tem cinco separadores:

- **Aplicações**
- **Processos**
- **Desempenho** (**performance**)
- **Funcionamento em rede**
- **Utilizadores**

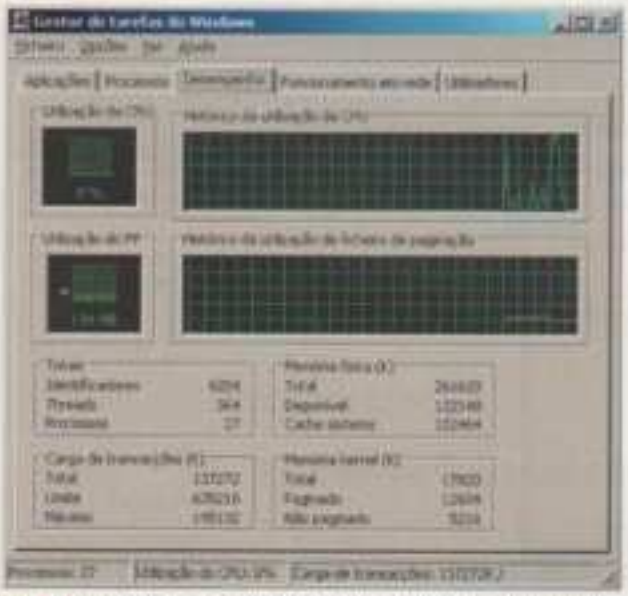
Fig. 3.252 Janela **Gestor de tarefas do Windows**

É possível usar-se o gestor de tarefas não só para reunir informações sobre um servidor, mas também para interagir com ele e resolver alguns problemas. Por exemplo, se o servidor parecer preguiçoso ou lento, pode-se abrir o gestor de tarefas e ir ao separador **Desempenho** para visualizar, em tempo real, a utilização do processador. Se o gráfico indicar que o processador se encontra a trabalhar a "tempo inteiro" (*full-time*), pode ir-se ao separador dos **Processos** para ver qual é o processo que está a tomar todo o tempo do servidor e descobrir, através do separador das **Aplicações**, se uma aplicação parou de responder e necessita de ser encerrada.

Princípios gerais sobre optimização

Para se optimizar um computador é necessário ver onde se encontram os "estrangulamentos" ao seu desempenho e eliminá-los. Um "estrangulamento" existe quando um componente necessita de demasiado tempo para realizar uma certa tarefa. No entanto, mesmo tendo encontrado e eliminado qualquer "estrangulamento", isto não significa que não possam surgir outros e acontece que, cada vez que se elimina um "estrangulamento", se ganha menos do que se ganhou com a remoção do anterior. E mais, ao melhorar as características de um sistema num determinado aspecto, acabamos, muitas vezes, por piorá-las noutros e não podemos esquecer que algumas optimizações também acarretam alguns custos.

Optimização em Windows Server

Ter um servidor optimizado evita atrasos nos utilizadores que a ele acedem. Visto isto, é importante ter uma boa ligação à rede e alta velocidade na mesma e no servidor, sendo, por vezes, necessário investir em ligações e processadores mais rápidos, em discos maiores, em mais memória RAM, etc. Apesar dos cuidados que se devem ter, o Windows Server 2003 já conta com algumas surpresas interessantes no que respeita à sua optimização. Atendendo à situação em que se encontra, este sistema operativo é capaz de ajustar dinamicamente alguns dos seus parâmetros de funcionamento e fornecer recursos a quem mais parece precisar deles. Também conta com a ferramenta **Desempenho**, para monitorizar o sistema, e que permite localizar os estrangulamentos no servidor por meio de uma análise de múltiplos valores e da sua evolução. Ter um servidor optimizado permite não só melhorar o desempenho do mesmo, mantendo a sua configuração, como também melhorar a performance de um determinado processo e a partilha do tempo de processador entre os vários processos; com um processador optimizado também se acaba por ter mais memória livre e mais espaço no disco rígido. Por fim, ter um processador optimizado também é benéfico, no sentido de se poder planear o dimensionamento do servidor no futuro, caso variem as necessidades de acesso.

4. Segurança no Windows Server 2003

4.1. Cópias de segurança

Introdução

Para prevenir acidentes e manter os servidores seguros, convém fazer o seguinte:

- manter múltiplas cópias de dados importantes e dos servidores mais importantes, como os controladores de domínio;
- garantir fisicamente a segurança da rede; por exemplo, manter os servidores fechados atrás de uma porta ou rede, para evitar acidentes "estúpidos" ou provocados por pessoas mal-intencionadas;
- proteger os dados dos utilizadores e do sistema de rede com uma boa estratégia de *backup* (cópia de segurança);

- estar preparado para o pior, com um plano de recuperação de desastre, de modo que uma grande parte do pessoal da organização o possa seguir; não se deve depender apenas de uma única pessoa para recuperar a rede e voltar a pô-la a trabalhar, pois, se essa pessoa falhar, ninguém mais é capaz de restaurar a rede;
- compreender como funciona o servidor, para saber como resolver alguns problemas e talvez até evitar outros no futuro;
- instalar as actualizações (*service packs*) que a Microsoft lança, para resolver algumas das falhas que vêm com os produtos da Microsoft.

A segurança contra intrusos é importante, mas a prevenção de perdas de dados também é importante. Os *backups* (cópias de segurança) são a primeira linha de defesa contra as falhas dos servidores, o último recurso quando tudo o resto falha. Se pensarmos bem, o que realmente importa são os dados que se encontram no servidor. A caixa é substituível e o sistema operativo pode ser reinstalado, se for necessário. O que não pode ser substituído são os dados. E, se perdermos aqueles dados e se não os conseguirmos recuperar, é possível que a vida da empresa fique em risco.

Para ajudar na protecção de dados, o Windows Server 2003 vem com uma versão do Windows *backup* (**Cópia de segurança do Windows**). Ao usar este programa de *backup* (**cópia de segurança**), é possível fazer cópias de segurança para ficheiros ou para *tapes* ou até criar ficheiros para recuperação de sistema.

Sistemas de *tapes* (cassetes)

A aplicação que vem com o Windows Server 2003 permite, como já foi dito, fazer cópias de segurança para qualquer tipo de *media* compatível com o sistema, como, por exemplo, discos rígidos, unidades ópticas e magnéticas, entre outros. Apesar desta grande variedade, as **tapes** continuam a ser o sistema de *backups* mais utilizado, por ser menos dispendioso e possuir grande capacidade. A *Tape Streamer* deve constar da lista de compatibilidade de *hardware* (HCL) do Windows 2003.

Existem várias tecnologias de sistemas de *tapes*, entre as quais se podem destacar:

- **a tecnologia DAT** (*Digital Audio Tape*) – tem grande capacidade de armazenamento de informação, uma elevada velocidade e um custo relativamente baixo, daí ser a mais utilizada;
- a tecnologia DLT (*Digital Linear Tape*) – é uma espécie de dispositivo magnético, que usa fitas com capacidade acima dos 600 GB, a aproximadamente 72 MB por segundo.

Ferramenta de *backup* (cópia de segurança) em modo gráfico

O programa **Cópia de segurança** (*backup*) encontra-se na secção **Ferramentas do sistema** no directório **Acessórios**, que se encontra em **Iniciar > Programas**.

O acesso ao programa **Cópias de segurança** pode ser lançado digitando NTBACKUP na linha de comandos ou acedendo ao menu **Iniciar** e, em **Executar**, escrever o comando **NTBACKUP**.

A janela que surge dá-nos as boas-vindas ao **Assistente de restauro ou de cópia de segurança**. Nesta janela podemos avançar com o assistente, bastando para tal clicar em **Seguinte**. Vamos clicar em **Modo avançado** para aceder à janela da figura 3.255.

Se for retirada a selecção **Iniciar sempre em modo de assistente**, da próxima vez que for lançado o programa de **Cópia de segurança** esta janela não surgirá, aparecendo automaticamente a janela da figura 3.255.

Fig. 3.253 Acesso ao programa **Cópia de segurança**

Fig. 3.254 Janela de **Assistente de restauro ou cópia de segurança**

A janela **Bem-vindo ao 'Modo avançado do utilitário de cópia de segurança'** (figura 3.255) permite-nos escolher entre fazer uma cópia de segurança (Avançado) ou fazer um restauro/recuperação (Avançado) ou até gerir a automatização de *backups* (através da criação de uma disquete de emergência e cópia da partição do sistema).

No separador **Bem-vindo** selecciona-se **Assistente de cópias de segurança (avançado)** para dar início ao assistente (*wizard*) da cópia de segurança (*backup*).

Clicar em **Seguinte**, para prosseguir com a instalação.

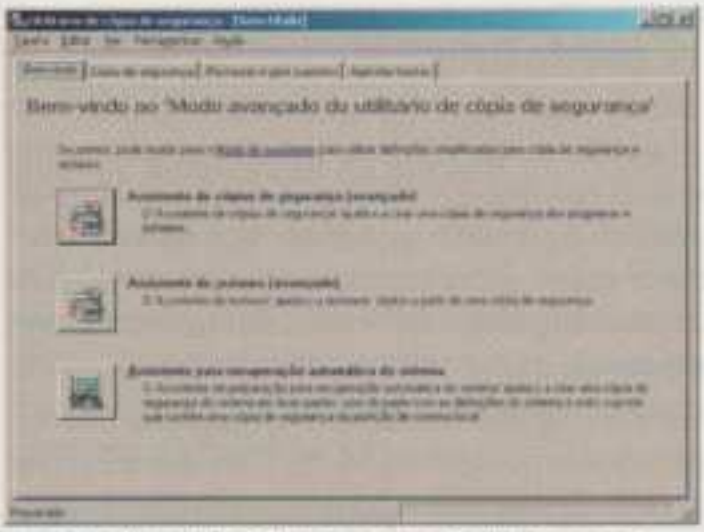

Fig. 3.255 Janela inicial de boas-vindas da ferramenta **Cópia de segurança** (*Backup*)

Fig. 3.256 Janela **Assistente de cópias de segurança**

De seguida há que escolher os dados dos quais se quer fazer *backups*. Como se pode ver na figura 3.257, no Windows Server 2003 são-nos apresentadas duas opções:

- **Fazer cópias de segurança de todos os dados neste computador**
- **Fazer cópias de segurança de ficheiros, unidades ou dados de rede seleccionados**

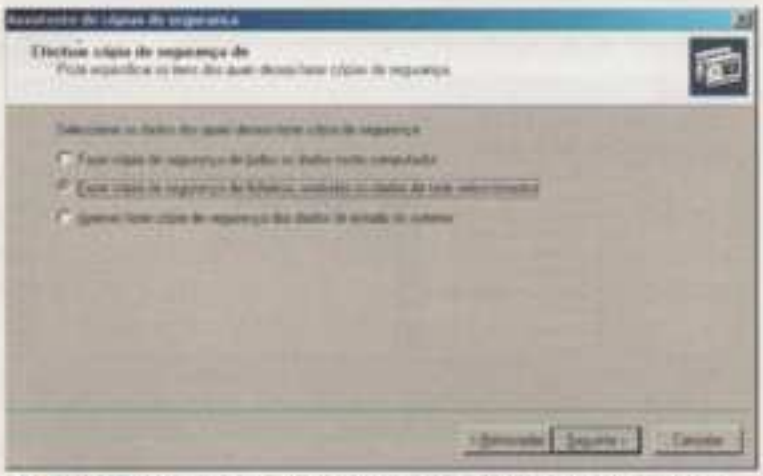

Fig. 3.257 Cópia de segurança de ficheiros seleccionados

Os controladores de Domínio terão uma terceira opção:

- **Apenas fazer cópia de segurança dos dados de estado do sistema**, fazer apenas cópias de segurança dos ficheiros de configuração (*system state data*), como, por exemplo, o *Registry* ou os ficheiros de arranque.

Para já, vamos optar por seleccionar a segunda opção, que nos permite seleccionar os ficheiros.

Selecção de ficheiros e directórios

Pode-se percorrer a janela seguinte para encontrar os ficheiros e os directórios dos quais se queira fazer cópias de segurança, quer se esteja num computador local, na rede ou até em domínios de confiança (*trusted domains*) – ver figura 3.258.

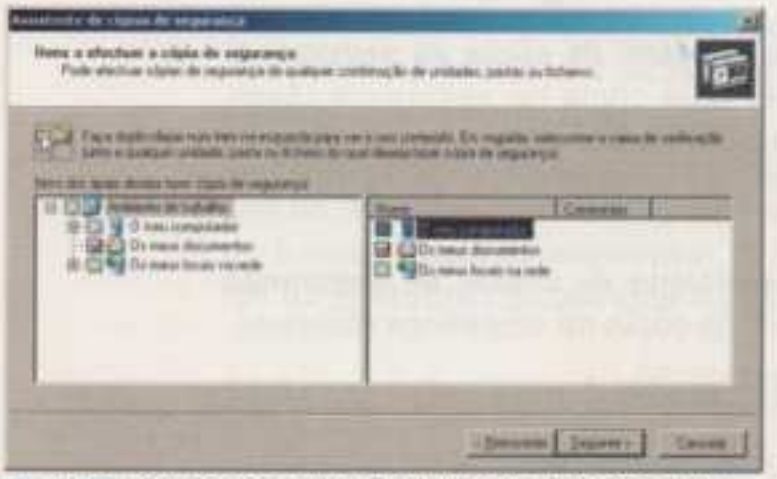

Fig. 3.258 Janela para selecção de discos, ficheiros e/ou directórios para *backups*

Eis uma lista das letras atribuídas às *drives* de todas as partições. As *drives* listadas são *drives* lógicas e não físicas. É possível separar as *drives* disponíveis clicando sobre os cabeçalhos do nome, tamanho total ou espaço livre. Esta lista inclui todas as *drives* no servidor e não apenas as *drives* fixas ou locais. Assim, é possível fazer o *backup* de uma *drive* inteira ou, então, só de alguns dos seus directórios ou até mesmo apenas dos ficheiros seleccionados. Caso se queira ver os directórios de uma *drive* de aplicação, basta fazer duplo clique sobre a *drive* em questão e, ao fazer um duplo clique sobre um dos directórios da *drive*, tem-se acesso aos subdirectórios, e assim sucessivamente até chegar aos ficheiros individuais. É também possível "des-seleccionar" qualquer objecto dentro de um directório (caso se pretenda fazer um *backup* do mesmo, com excepção de alguns ficheiros/objectos) evitando, deste modo, que este objecto faça parte da cópia de segurança.

É possível fazer cópias de segurança de quantos ficheiros e directórios diferentes quisermos e de quantas e diferentes *drives* quisermos. O que, no entanto, não é possível fazer são cópias de segurança de todos os ficheiros de um determinado tipo, independentemente da sua localização. O programa de *Backup* está organizado por localização e não por tipos de ficheiro.

Fig. 3.259 Janela de *drives* seleccionadas para fazer cópias de segurança.

Ao lado das *drives* ou dos directórios existem umas "caixas" (☐), que podem estar ligadas ☑, desligadas ☐ ou apenas parcialmente ligadas ☑, enquanto que as caixas ao lado dos ficheiros apenas podem estar ligadas ☑ ou desligadas ☐. Ligado ☑ significa que é para fazer *backup* de tudo o que lhe corresponde; desligado ☐ significa que não é para ser incluído no *backup*.

Localização para o armazenamento das cópias de segurança

Em seguida deve-se escolher uma localização para a cópia de segurança, usando a caixa de diálogo da figura 3.260.

Se tivermos uma *tape drive*, pode-se fazer a cópia de segurança para lá; de outro modo, é necessário escolher uma localização para o ficheiro de **backup (.BKF)**. Por defeito, o ficheiro de *backup* tem o nome **Backup.bkf** e encontra-se guardado em **Os meus documentos**; também é possível clicar no botão **Procurar** – *browse* para seleccionar uma localização alternativa para o *backup* e, da primeira vez que se corre o programa **Backup**, é mesmo necessário escolher uma localização para o *backup*.

Uma vez que se indicou onde colocar o ficheiro de *backup*, clica-se sobre **Seguinte** para termos acesso ao ecrã final que mostra as nossas opções de *backup* (ver figura 3.261). Ao pressionar em **Concluir**, dá-se início ao *backup*.

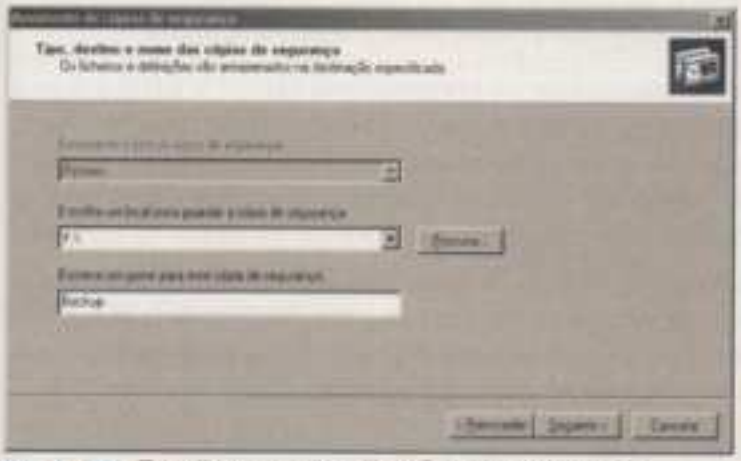

Fig. 3.260 Escolher uma localização para o *backup*.

Fig. 3.261 O ecrã final do assistente que mostra as opções de *backup* configuradas.

Opções avançadas de *backup*

O que foi explicado não passa de um *backup* básico, usando todas as opções que foram surgindo, por defeito. Se pretendermos ter um pouco mais de controlo sobre como o *backup* é feito (ou seja, as opções para o "Como" e o "Quando"), então devemos pressionar o botão **Avançado** antes de clicar sobre **Concluir**, para iniciar a segunda parte do assistente e decidir sobre as opções avançadas, como constam da tabela 3.11.

Opção	Definição por defeito (*default setting*)	O que significa?
Tipo de cópias de segurança que devem ser efectuadas	Normal	Pode-se escolher entre cópias de segurança normal, cópia, incremental, diferencial ou diária. Estes tipos de cópias de segurança serão descritos posteriormente com mais pormenor, no ponto **Tipos de *backups***.
Verificar os dados após a cópia de segurança	Não	Permite verificar a integridade dos dados copiados. Fazer a verificação de uma cópia de segurança faz com que se comparem os dados do *backup* com os de origem, para nos certificarmos que os dados foram copiados correctamente. Verificar o *backup* demora algum tempo, mas é uma boa maneira de obter um registo de que os dados foram copiados como era de esperar.
Utilizar compressão de *hardware*, caso esteja disponível	Não	Se o *hardware* o permitir, é possível comprimir dados para poupar espaço. Esta opção só está disponível se estivermos a fazer cópias de segurança para tapes. Se escolhermos esta opção, a *tape* terá uma capacidade maior do que teria de outro modo.

Opção	Definição por defeito (*default setting*)	O que significa?
Acrescentar ou substituir um *backup* existente na *tape*/no *media*	Acrescentar	Se o dispositivo de *backup* já contiver um *backup*, tem-se a opção de substituir aquele *backup* por um novo ou de acrescentar o *backup* actual ao catálogo (*catalog*). A opção que se toma depende do que é mais importante para nós. Sugere-se a substituição de *backups* completos (embora se deva guardar sempre, pelo menos, um *backup* completo, no caso de algo poder acontecer ao actual e se se necessitar dele para recuperar a totalidade da informação do disco) e um acrescento em caso de *backups* incrementais e diferenciais.
Restrição de acesso	Não	No caso de termos optado por substituir um *backup* existente no *media*, podemos escolher se pretendemos restringir o acesso a esses *backups* apenas aos membros do grupo de administradores e à pessoa que criou esses *backups*.
Definir o nome do *backup* e qual o *media* a usar	Foi criado o tempo e a data do *backup*	Aqui define-se um nome para o *backup*. Se estivermos a usar um novo dispositivo, ou a substituir os dados do dispositivo existente, pode-se escolher um novo nome para o *tape* ou ficheiro.
Quando se deve executar o *backup*	Agora	Esta opção permite definir se pretendemos correr o *backup* agora ou se preferimos escolher um tempo (data/hora) em que este deve ser efectuado. Se estivermos a fazer uma cópia de segurança de um servidor, então, com certeza, iremos querer agendar o *backup* para uma hora em que ninguém esteja a usar os dados do servidor. Também é possível, através da selecção do botão **Definir agendamento**, pedir ao programa de *backup* para este fazer, autonomamente e de forma periódica, uma cópia de segurança de tanto em tanto tempo e a iniciar a uma determinada hora.
Efectuar cópias de segurança de dados armazenados remotamente	Não	Esta opção faz cópias de segurança de ficheiros que raramente são utilizados e que foram automaticamente arquivados num armazém remoto.
Desactivar cópia de *volume shadow* – sombra de volume	Não	*Volume shadow copying* permite que se façam cópias de segurança a ficheiros enquanto estão a ser usados.

Tabela 3.11 Opções de armazenamento

Após termos escolhido as opções, volta-se a ver o ecrã de conclusão, mostrando as opções actuais configuradas.

Fig. 3.262 Selecção de um tipo de *backup*

Tipos de *backups*

Olhando com mais atenção para a primeira página das opções avançadas de *backup*, vamos ver que tipos de *backup* existem e como saber qual o que escolher.

Por defeito, o tipo de *backup* no programa de *backup* do Windows é **Normal**, ou seja, faz *backups* completos, a não ser que tenha indicações contrárias, e, nesse caso, no separador **Tipo de cópia de segurança** da figura 3.262 pode-se escolher uma das opções descritas na tabela 3.12.

Antes de avançarmos com uma descrição sumária de cada tipo de *backup*, convém fazer referência ao chamado atributo de Archive – Arquivo (A), que é definido

para a maioria dos ficheiros, em DOS. O sistema operativo 'liga' esse atributo sempre que se fazem alterações a um ficheiro e 'desliga-o' cada vez que se efectua o *backup* do ficheiro. Deste modo, o programa de *backup* consegue saber quais os ficheiros modificados desde o último *backup* – ou seja, todos aqueles que tenham este atributo definido.

Eis os vários tipos de cópias de segurança disponíveis no Windows Server 2003:

Tipo de *backup*	Descrição
Normal	Copia todos os ficheiros seleccionados (independentemente de o atributo **Archive** estar, ou não, definido) e depois faz o *reset* do atributo de arquivo (**Archive**), ou seja, desliga-o, indicando que os ficheiros foram copiados.
Incremental	Copia todos os ficheiros seleccionados que tenham o atributo de arquivo (**Archive**) definido, e, depois da cópia de segurança, retira o atributo **Archive**.
Diferencial	Copia todos os ficheiros seleccionados que tenham o atributo **Archive** definido e não desliga esse atributo após a cópia de segurança.
Diário	Copia todos os ficheiros seleccionados que foram editados/alterados no dia em que o *backup* foi efectuado. Não altera o atributo **Archive**.
Cópia	Copia todos os ficheiros seleccionados (tal como no modo **Normal**) mas não retira, ou seja, não faz o *reset* do atributo **Archive** após a cópia de segurança dos ficheiros.

Tabela 3.12 Tipos de *backup*

É possível usar estes tipos de *backups* em modo combinado, para fazer uma cópia de segurança de ficheiros de forma mais completa e eficiente. O intervalo mais longo entre cópias de segurança nunca devia exceder um dia. Correr um *backup* normal todos os dias é um processo moroso e que ocupa muito espaço, por isso, talvez seja preferível correr um *backup* normal em intervalos regulares, talvez uma vez por semana; no entanto, convém complementar este *backup* semanal completo com um *backup* diferencial diário ou um *backup* incremental. Correr um *backup* diário diferencial oferece uma cópia diária de todos os ficheiros que tenham sido alterados desde o último *backup* completo; *backups* incrementais copiam todos os ficheiros que tenham o seu atributo **Archive** definido. Tanto um *backup* diferencial, como um *backup* incremental, são um óptimo suplemento ao *backup* normal regular.

Backups diários não são, na realidade, um método de preservar dados, mas uma forma de rapidamente encontrar ficheiros que estão a ser usados e transferi-los para outros *media*.

Copiar ficheiros só é útil se pretendermos fazer uma cópia completa de todos os ficheiros seleccionados sem fazer o *reset* do atributo **Archive**. Uma acção de cópia deste género é uma forma de copiar ficheiros para uma nova localização.

Recuperação de dados

Ter *backups* só se torna funcional se os pudermos voltar a colocar no servidor de onde vieram. Para restaurar/recuperar ficheiros, deve voltar a abrir-se o programa **Cópia de segurança** do Windows. Aí pode-se correr a opção – **Assistente de restauro avançado** ou ir ao separador **Restaurar e gerir suportes**. A janela é parecida com a que permitia seleccionar ficheiros para *backups*, mas aqui estamos a ver o conteúdo da cópia de segurança (em *tape* ou ficheiro) e não de uma *drive* do servidor.

Fig. 3.263 Janela de boas-vindas ao **Assistente de restauro**.

Depois da janela de boas-vindas, surge um ecrã que nos pede para seleccionar o dispositivo de onde se quer fazer a recuperação de dados. As opções disponibilizadas irão depender do tipo de dispositivo para onde se fez a cópia de segurança (figura 3.266).

O *backup* que se encontra no *media* estará organizado em directórios, dispostos de acordo com o seu tamanho, tipo e descrição. Com um duplo clique sobre o mesmo, tem-se acesso aos seus conteúdos. Depois só temos de seleccionar os directórios ou os ficheiros que interessam recuperar. A simbologia usada ☐, ☑ ou ☑ é igual à usada na selecção dos ficheiros para *backup* (figura 3.265).

Fig. 3.264 Selecção do *media*/dispositivo (*tape*) de onde se quer fazer a recuperação de dados.

Fig. 3.265 Selecção dos directórios/ficheiros a partir de um *backup* para recuperação.

Em seguida, clicar em **Seguinte** e o assistente irá dispor um ecrã que lista as opções tomadas em relação à recuperação de directórios/ficheiros (figura 3.266).

Em caso de engano, podemos sempre clicar em **Voltar** (*Back*) e alterar as opções/selecções feitas.

Para especificar uma nova localização (novo destino) para a recuperação de dados ou para alterar as opções de configuração de recuperação de ficheiros, deve pressionar-se o botão **Avançadas** da figura 3.266. A não ser que se dêem indicações diferentes, o programa **Cópia de segurança** do Windows procede ao restauro dos ficheiros para a sua localização original. No caso de se pretender fazer um restauro, ou seja, uma recuperação de dados para uma nova *drive* com uma

Fig. 3.266 Janela das opções tomadas da recuperação de directórios/ficheiros em *backup*.

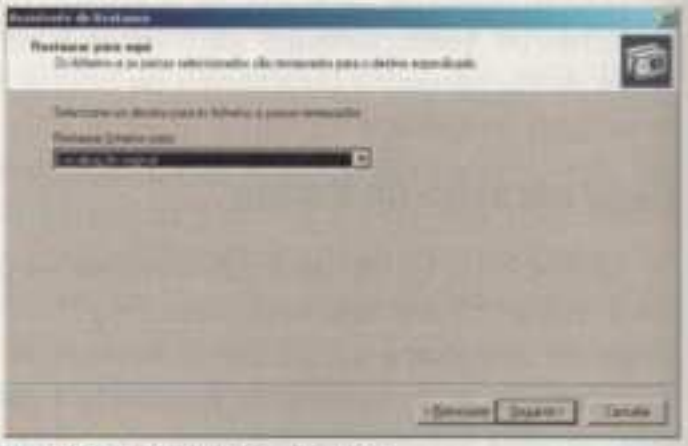

Fig. 3.267 Destino dos ficheiros

letra diferente da original, ou no caso de se querer, por exemplo, colocar os conteúdos de um *backup* diário num disco Zip (*Zip disk*), então teremos de escolher uma das três opções de destino que surgem na janela da figura 3.267:

- para a **localização original**;
- para uma **localização alternativa** – os ficheiros e os directórios serão restaurados, com a estrutura de directórios intacta, para a localização especificada;
- para uma **pasta única**, um directório a designar – os ficheiros serão todos colocados dentro de um único directório para um directório a designar e perde-se a estrutura original de directórios.

Se indicarmos que pretendemos restaurar ficheiros para uma localização alternativa ou para uma pasta, então o assistente irá dispor uma caixa de texto onde teremos de indicar o sítio do restauro. Só se podem restaurar dados para uma localização alternativa; não é possível fazer a recuperação para uma localização alternativa de informação sobre a configuração do sistema, tal como o *Registry*, por exemplo. Quaisquer ficheiros de configuração de sistema terão de regressar às suas localizações originais.

Pressionar em **Seguinte**, na figura 3.267.

O que acontece se um ficheiro com aquele nome já existe na localização para onde estamos a fazer o restauro?

O ecrã da figura 3.268 dá-nos algumas opções de decisão de substituição (do ficheiro no disco):

- **Deixar os ficheiros existentes** – nunca substituir o ficheiro existente no disco (seleccionado por defeito);
- **Substituir os ficheiros existentes se forem mais antigos do que os ficheiros da cópia de segurança**;
- **Substituir os ficheiros existentes** – os ficheiros existentes no disco são substituídos pelos ficheiros equivalentes da cópia de segurança.

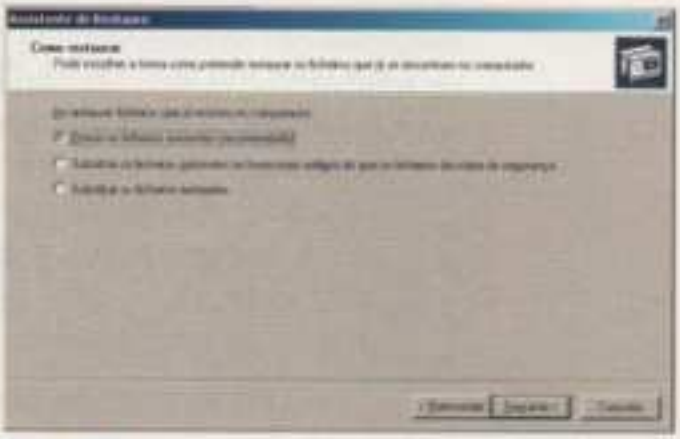

Fig. 3.268 Opções possíveis em caso de ficheiros com o mesmo nome

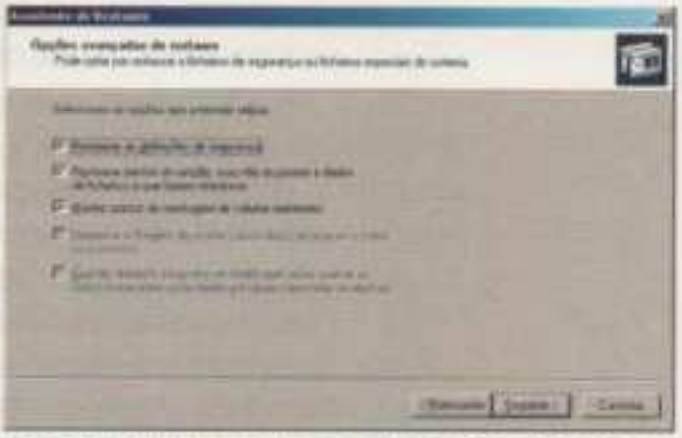

Fig. 3.269 Janela de selecção das opções de restauro das definições de segurança dos ficheiros

O assistente prossegue (figura 3.269), solicitando se pretendemos optar por restaurar as definições de segurança ou ficheiros especiais do sistema; para tal mantemos seleccionadas as três primeiras opções (que surgem por defeito) e clicamos em **Seguinte**, para continuar com o assistente.

Pressionar em **Concluir** para dar início ao restauro dos ficheiros.

Surge uma janela com um resumo das opções de restauro de dados; ao clicar em **Concluir**, procede-se à conclusão da operação de recuperação de dados.

Fig. 3.270 Janela de conclusão do restauro

Criação de um disco automatizado de recuperação de sistema – ASR (*Automated System Recovery Disk*)

Cada vez que se edita com sucesso a configuração do sistema, deve fazer-se uma cópia de segurança da configuração, para nos protegermos de uma altura em que podemos editar as definições sem sucesso. Esse disco de *backup*, que **em tempos foi chamado disco de reparação de emergência** (*emergency repair disk*), é agora chamado de **disco ASR** (*Automated System Recovery*), ou seja, disco automatizado de recuperação de sistema.

É importante que se saiba que o disco ASR, que vem com o Windows Server 2003, é diferente do disco de reparação de emergência que vinha com o NT4. O disco ASR não inclui dados de ***Registry***.

Podem-se substituir partes do *system registry* pela consola de recuperação, se fizermos uma actualização regular da informação do directório ***RegBack***.

Para criar um disco ASR, devem ser seguidos os seguintes passos:

- Ir a **Iniciar > Acessórios > Ferramentas de sistema** e correr o utilitário **Cópia de segurança**. No ecrã inicial do utilitário (figura 3.255) encontram-se botões para três assistentes: assistente de cópia de segurança; assistente de restauro (recuperação) e **assistente para recuperação automática do sistema**, que, como já foi dito, permite gerir a automatização de *backups* através da criação de uma disquete de emergência e cópia da partição do sistema.

  Pressionar o último botão.

  – Escolher a localização da cópia de segurança para um *backup* completo dos ficheiros de configuração (*system state*) do computador. Não se deve escolher uma disquete, pois não tem espaço suficiente! É necessário muito espaço para a colocação dos dados de todos os ficheiros de configuração.

  – Após conclusão do *backup*, deve inserir-se uma disquete limpa na *drive* **A:** e clicar em **OK** quando o assistente nos pedir para copiar ficheiros para o disco. O **Backup** irá copiar para a localização do *backup* os dados dos ficheiros de configuração, informação de serviço e informação de configuração de disco e **asr.sif**, **asrpnp.sif**, e **setup.log** para o disco. Os ficheiros não são ficheiros de arranque. Trata-se de ficheiros de informação do sistema, como os usados para instalar o sistema operativo, basicamente, ficheiros **SIF**.

Existem outras soluções de *backup* para Windows Server 2003 com maiores potencialidades e ainda mais robustas, como, por exemplo, o **TapeWare** – comercializado pela HP para ser utilizado com os seus *tapes* DAT.

Fig. 3.271 Aspecto geral do *software* **TapeWare** para realizar cópias de segurança e restauro.

4.2. Segurança de discos

Disco básico – *Basic Disk* e disco dinâmico – *Dynamic Disk*

O Windows Server 2003 suporta duas variantes na gestão de discos:

- disco básico;
- disco dinâmico.

Um disco básico pode ter o seu espaço livre dividido em várias partições, que podem ser primárias ou estendidas, desde que não ultrapasse um máximo de quatro partições primárias ou uma estendida (no máximo) e três primárias. No caso de se ter uma partição estendida, ela pode ser dividida em várias unidades lógicas. Os sistemas operativos devem ser instalados numa partição primária (e não em unidade lógicas) e, caso existam mais partições, o sistema corre o SO instalado na partição marcada como activa.

Este modelo tem-se mantido desde o DOS até ao lançamento do Windows 2000, em que se introduziu, pela primeira vez, na gestão de discos, o conceito de disco dinâmico com capacidades acrescidas e que não é suportado por quaisquer outros sistemas operativos anteriores a Win2K.

Os discos dinâmicos encontram-se presentes no Windows Server 2003 e, por isso, caso se pretenda usar qualquer tipo de volumes *multidisk* ou tolerantes a falhas (*fault tolerant*), então torna-se necessário usar os discos dinâmicos. Estes trabalham em conjunto no Windows Server 2003, em unidades lógicas chamadas *disk groups* (grupos de discos).

O que é um disco dinâmico? Quando se faz um disco dinâmico, estão a substituir-se os conteúdos da tabela de partições (*partition table*) – ou seja, toda aquela informação crítica do disco sobre o disco e as partições – com uma única entrada, que basicamente significa "vai ler a base de dados do disco dinâmico para obter a minha informação de partição, porque eu sou um disco dinâmico". Ao criar um disco dinâmico está-se a escrever 1 MB de base de dados (*database*) de informação no final daquele volume de disco. Esta base de dados contém toda a informação da partição para cada um dos discos dinâmicos no servidor. Uma das características mais agradáveis dos discos dinâmicos é que a informação contida nesse ficheiro de 1 MB é replicada para todos os outros discos dinâmicos no sistema. Os conteúdos da base de dados em cada disco são idênticos. Esta é uma grande vantagem sobre os discos básicos, que têm um único ponto real de falhas quando se chega a toda aquela informação crítica necessária para manter a integridade do disco. Se algo acontecer ao primeiro sector do disco básico, é difícil recuperá-lo. Caso se faça um *upgrade* ao disco básico com partições para um disco dinâmico, é necessário lidar com a tabela inicial de partições. Os conteúdos dessa tabela são copiados para a base de dados. O resto do disco é então reservado para novos volumes que serão gravados apenas na base de dados e não na tabela de partições. Isto significa que há uma diferença no modo como os volumes são vistos num disco dinâmico, dependendo do facto de terem sido criados antes ou depois da conversão para dinâmico.

O acesso ao gestor dos discos é realizado a partir do menu **Iniciar** e, em **Ferramentas administrativas**, seleccionar **Gestão de computadores**.

Vamos expandir a árvore até se seleccionar **Gestão de computadores**. No lado direito da janela irão surgir os discos instalados neste computador (ver figura 3.273).

Fig. 3.272 Acesso ao **Gestor de computadores**.

Fig. 3.273 Janela **Gestão de discos**

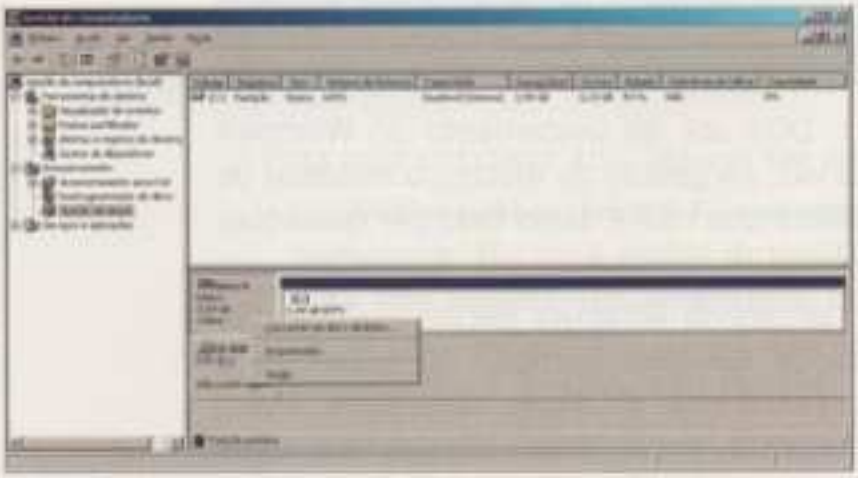

Fig. 3.274 Conversão de disco básico para disco dinâmico

Para fazer um *upgrade* de um disco básico para um dinâmico, basta clicar no quadrado que se encontra à esquerda da representação das partições de um disco e seleccionar, no menu **Acção**, a opção **Todas as tarefas** e, finalmente, escolher **Converter em disco dinâmico**, ou, simplesmente, clicar com o botão do lado direito do rato no quadrado que se encontra à esquerda da representação das partições e escolher **Converter em disco dinâmico**.

No ecrã da figura 3.275 que surge devem escolher-se os discos a converter e pressionar em **OK**.

Na janela da figura 3.276, pressionando o botão **Detalhes** temos acesso a uma listagem das unidades lógicas configuradas em cada um dos discos.

No caso de se ter a certeza da configuração pretendida, basta clicar em **Converter** e, de seguida, em **Sim**, confirmando, deste modo, os discos a converter.

Este processo de conversão não danifica os dados, mas impossibilita versões anteriores ao Win2K de aceder aos discos.

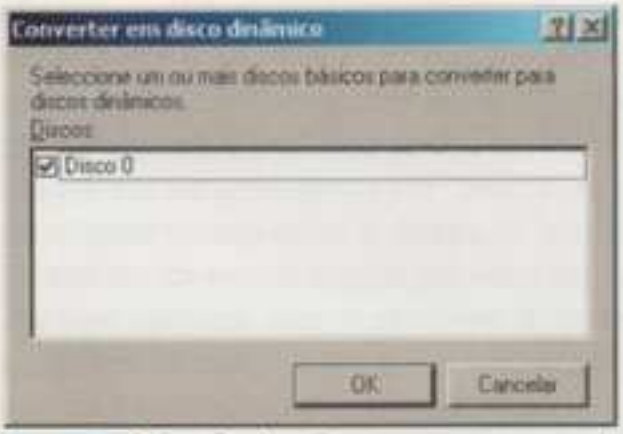

Fig. 3.275 Selecção dos discos a converter para disco dinâmico.

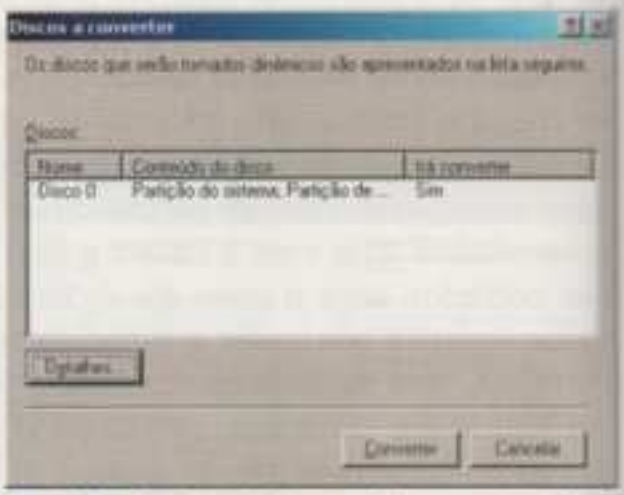

Fig. 3.276 Janela a indicar os discos que serão convertidos em discos dinâmicos.

Após a conversão dos discos, as partes do mesmo deixam de se chamar partições e passam a chamar-se volumes.

Existem vários tipos de volume:

- **Volume simples** – muito parecido com a partição, distinguindo-se dela por poder ser formado por partes não contíguas do disco, ou seja, o volume pode ser repartido por partes espalhadas pelo disco.
- **Volume expandido (*Spanned volume*)** – trata-se de um volume feito por partes (não necessariamente do mesmo tamanho) de vários discos e que pode ser expandido.

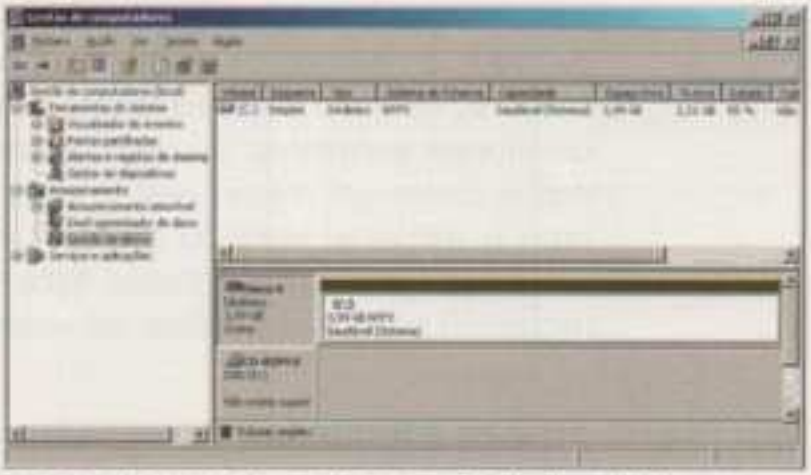

Fig. 3.277 Aspecto geral após conversão do disco básico em dinâmico.

- **Volume *stripe* ou *stripe set* sem paridade (RAID 0)** – é um volume estabelecido por partes iguais de diversos discos e que não pode ser expandido.
- **Volume *mirrored* ou espelhado (RAID 1)** – é um volume formado por dois discos ou duas partes de discos iguais, sendo uma parte (ou um disco) a réplica exacta da outra. Este volume implementa tolerância a falhas.
- **Volume RAID 5 (*stripe set* com paridade)** – muito semelhante ao volume RAID 0, mas distinguindo-se deste por ser tolerante a falhas. Este volume necessita, no mínimo, de três discos físicos (enquanto que o RAID 1 só precisa de dois).

Nota: Os discos dinâmicos não são suportados por alguns portáteis.

Apagar um volume de disco dinâmico

Apagar um volume de disco dinâmico é simples e directo: clicar com o botão direito do rato sob o volume a apagar e escolher **Apagar volume** (*Delete volume*). Após a mensagem de aviso, pressionar **Sim** para continuar a apagar o volume.

Converter um disco dinâmico em disco básico

O processo de conversão de um disco básico para disco dinâmico pode ser revertido. O único contra é que não se podem converter volumes num disco dinâmico para volumes num disco básico, porque eles não existem na tabela de partição do disco, apenas existem na base de dados de um disco dinâmico. Se existirem volumes no disco, então a opção **Converter para disco básico**, no menu de atalho do disco, estará a cinzento. É necessário apagar todos os volumes antes de esta opção ficar disponível. Assumindo que o disco está vazio, o processo é simples para um disco de dados: basta clicar com o botão direito do rato sobre o quadrado que se encontra à esquerda da representação das partições e escolher **Converter para disco básico**. O processo ficará concluído. Não é necessário reiniciar o computador.

Mirrored volume (Volume espelhado)

Para ter um servidor tão seguro quanto possível, convém ter sempre a partição de sistema em *disk mirroring* ou em *disk duplexing*.

Como já foi referido, um volume *mirror* é constituído por dois discos, ou duas partes de discos iguais, cada um contendo uma réplica do conteúdo do outro. Assim, sempre que é feita qualquer operação de escrita ou de leitura num disco, a mesma é feita simultaneamente no segundo disco. A desvantagem deste tipo de volume em relação aos outros encontra-se ao nível de utilização de espaço em

disco, devido à redundância dos ficheiros armazenados (gravação de duas cópias de todos os dados dos volumes). A vantagem reside no facto de ser tolerante a falhas e, no caso de haver problemas num disco, o sistema desactiva o volume defeituoso, permitindo o acesso ao restante. Assim, se um dos discos falhar, os dados continuam disponíveis no outro disco. É possível criar volumes *mirror* sem fazer o *reboot* e, voltando a repetir, não é necessário regenerar dados para os recuperar, caso um dos discos falhe. Os dados continuarão disponíveis; apenas não serão tolerantes a falhas até voltarmos a fazer o *mirror* dos mesmos.

Striped volume (*stripe set* sem paridade)

Um *striped volume* sem paridade é um volume em que a soma dos espaços de cada disco é destinada ao armazenamento de informação. Estes volumes são criados à custa de espaço livre em dois ou mais discos, em que a quantidade armazenada em cada disco é sempre a mesma, ou seja, ao criar um *striped volume* de 600 MB repartido em três discos, cada disco será ocupado com 200 MB. Como já foi referido anteriormente, não se pode criar este tipo de volumes com espaços de diferentes tamanhos em cada disco. Este tipo de volume permite ao administrador criar volumes de tamanho consideravelmente grande e melhorar o desempenho do sistema. Uma vez que um *striped volume* é constituído por porções de vários discos, todas as operações a efectuar serão muito mais rápidas, visto cada uma delas levar muito menos tempo na sua execução. No caso do *striped volume* ser constituído por quatro discos, cada disco será ocupado apenas um quarto do total da informação escrita, havendo, deste modo, uma espécie de separação objectiva da carga colocada pelo sistema em cada um dos discos, permitindo uma maior velocidade de escrita e de leitura. No entanto, e ao contrário do que sucede com os volumes simples e *spanned volumes*, os *striped volumes* não podem sofrer alterações na sua dimensão e nem podem ser objecto de *mirroring*.

Volume RAID 5 (*stripe set* com paridade)

Ao contrário do *stripe set* sem paridade, o volume RAID 5 tem de ser formado por espaços de três ou mais discos que funcionam como se fossem um só. Num volume RAID 5, os dados são escritos do mesmo modo que num volume RAID 0; a diferença é que, num *stripe set* com paridade, a informação de paridade para os dados escritos também se encontra escrita num dos discos, mas sempre num disco separado daqueles onde se encontram os dados correspondentes à informação de paridade. Isto não significa que haja, separadamente, um "disco de paridade", mas significa que cada disco que suporta volume RAID 5 poderá conter alguns dados originais **ou** a informação de paridade necessária para reconstruir esses mesmos dados originais, mas nunca ambos no mesmo disco. Assim, no caso de haver uma falha num dos discos que compõem o volume, a informação de paridade possibilita calcular qual a informação contida no disco que falhou, e os dados daquele disco podem ser reconstruídos a partir da informação de paridade que se encontra num dos outros discos.

Como se pode ver na figura 3.278, nenhum membro isolado do *stripe set* mantém todos os dados originais ou toda a informação de paridade. Em vez disso, os dados e a informação de paridade encontram-se distribuídos pelo *stripe set* e, assim, se um dos discos membros falhar, a informação pode ser reconstruída a partir dos outros membros do *stripe set*.

Esta informação poderá parecer redundante relativamente à que se encontra armazenada nos restantes discos, mas, quando comparado aos *disk mirroring*, que desperdiçam 50% do espaço em disco, os volumes RAID 5 requerem muito menos espaço para informação redundante, principalmente se dispusermos de uma grande quantidade de discos.

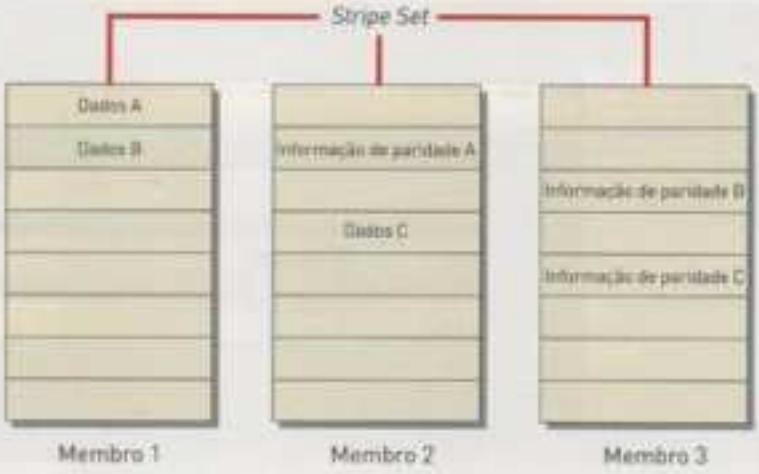

Fig. 3.278 *Striped volume* com paridade

Disk duplexing

Tratando-se do Windows Server 2003, o *disk duplexing* é muito semelhante ao *disk mirroring*, exceptuando o facto de o *disk duplexing* se referir à informação de *mirror* em dois discos separados, ligados à controladora de discos diferentes, de modo que os dados não fiquem vulneráveis a falhas da controladora, pois o Windows Server 2003 não consegue distinguir se existem múltiplas controladoras ou não. O *disk mirroring* tem os dois discos ligados à mesma controladora.

Fig. 3.279 Comparação entre o *disk mirroring* e *disk duplexing*

Quando comparado com o RAID 5, este nível de RAID tem uma performance bastante boa, especialmente ao nível de segurança no servidor, com as duas controladoras, embora não seja muito eficiente em termos de espaço, visto cada conjunto de dados guardados ter um conjunto "gémeo" na outra metade do *mirror set*.

Criação de volumes simples

Um volume simples é um tipo de volume criado num só disco e constituído por uma ou mais partes no mesmo, em que toda a informação é escrita sequencialmente nas várias porções de espaço que formam o volume simples.

Para criar um volume simples é necessário ter um disco que funcione como disco dinâmico (ou seja, um disco que previamente foi convertido para disco dinâmico) com espaço livre suficiente para criar um volume, e o sistema de ficheiros tem de ser NTFS.

Qualquer criação de volumes segue praticamente os mesmos passos e é feita através de um assistente, ao qual se chega clicando com o botão direito do rato sobre a representação do espaço livre do disco (figura 3.280) – com tamanho igual ou superior ao tamanho do volume que se pretende criar (no *snap-in* da **Gestão de discos**).

Depois selecciona-se **Novo volume** e **Seguinte**.

Fig. 3.280 Ordem para criar **Novo volume**

Fig. 3.281 **Assistente de Novo volume**

No ecrã que surge (figura 3.282), deve-se seleccionar o tipo de volume que se pretende criar. Se, previamente, não se tiverem convertido, no mínimo, três discos para formato dinâmico, a opção **Volume RAID 5** não estará disponível. No caso de só se ter convertido um disco, então a opção **Volume Mirror** também não se encontrará disponível, visto, neste caso, a única opção disponível ser a de um **volume simples**. Assim sendo e, neste caso, optamos então por criar um **volume simples**, onde apenas se usa um disco e depois clicarmos em **Seguinte**.

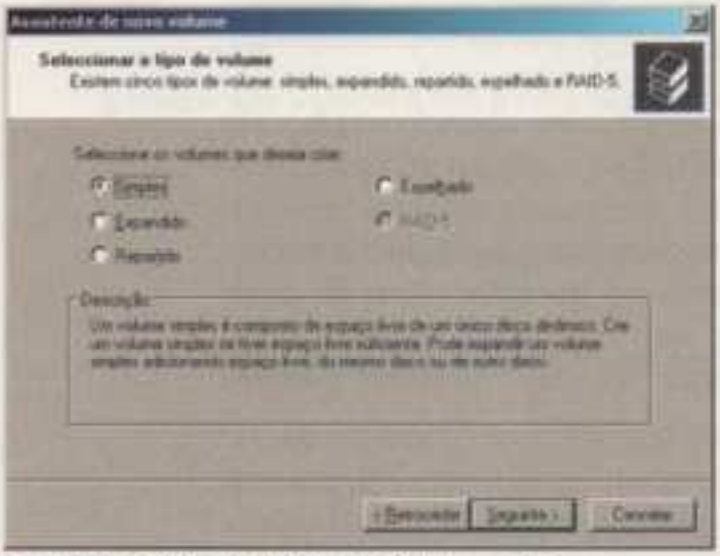

Fig. 3.282 Selecção do tipo de volume a criar

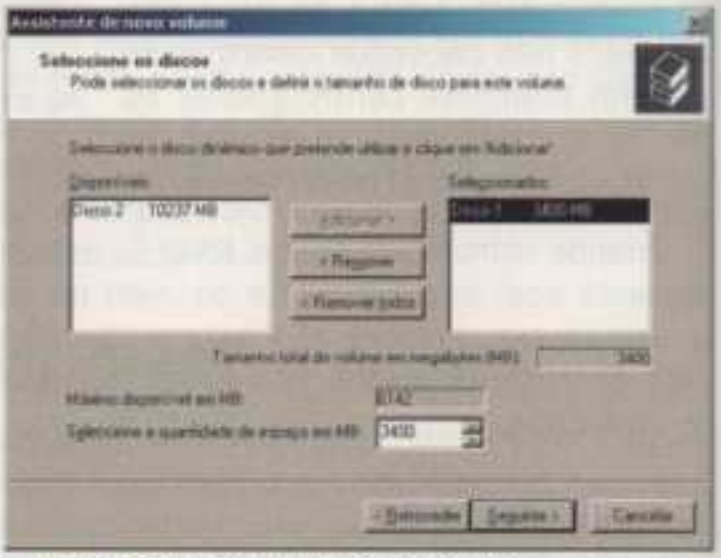

Fig. 3.283 Selecção do disco e do tamanho

No ecrã da figura 3.283, teremos não só de especificar o tamanho do volume a ser criado, como também seleccionar o disco em que o mesmo será criado, usando para tal o botão **Adicionar** (ou **Remover**, em caso de erro). Neste caso, só é possível a selecção de apenas um disco, visto tratar-se de um volume simples. Se fosse um **Volume mirror**, já se teriam de seleccionar dois discos ou, no caso da criação de um RAID 5, no mínimo três. Depois pressiona-se o botão **Seguinte**.

De seguida, teremos de seleccionar/atribuir uma letra ou caminho para acedermos ao volume sempre que o quisermos. Feito isto, clicar em **Seguinte** (figura 3.284).

A janela da figura 3.285 consiste num assistente de ajuda para a operação de formatação do volume. Preenchem-se os campos (sistema de ficheiros a usar, etc.) e clica-se em **Seguinte**.

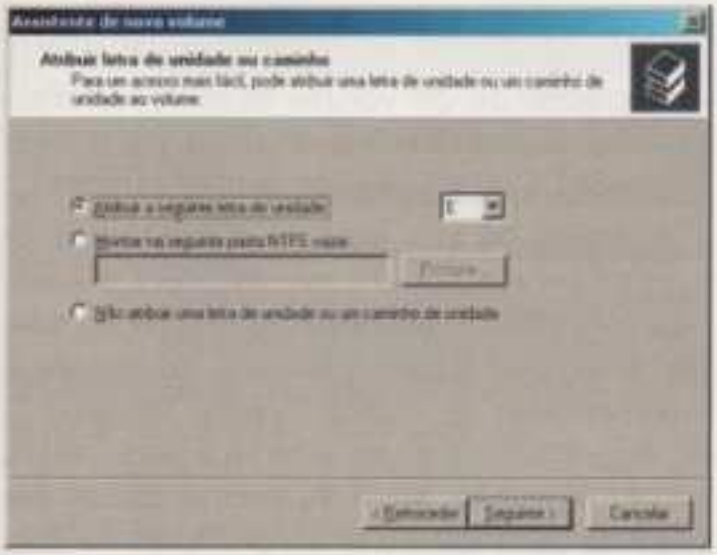

Fig. 3.284 Selecção/atribuição de uma letra/caminho para acesso ao volume

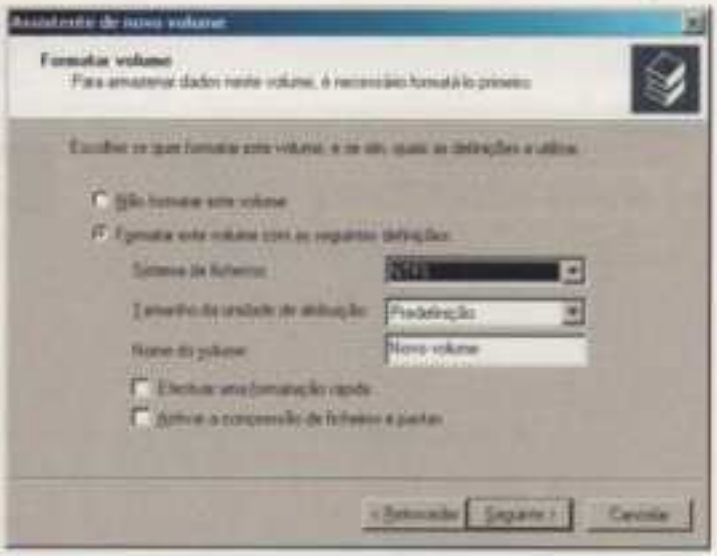

Fig. 3.285 Formatação do volume

Por fim surge o tradicional ecrã com um resumo do que foi feito em relação à criação deste volume. Para se dar início à formatação, clicar em **Concluir**.

Fig. 3.286 Conclusão do assistente para criar um volume simples

Na figura 3.287, pode-se verificar que o volume **E:** foi criado no **disco 1** e se encontra em fase de formatação.

No final da formatação, o volume **E:** está pronto a ser utilizado. Na figura 3.288 pode-se verificar que existe a indicação de **Saudável** no volume **E:**.

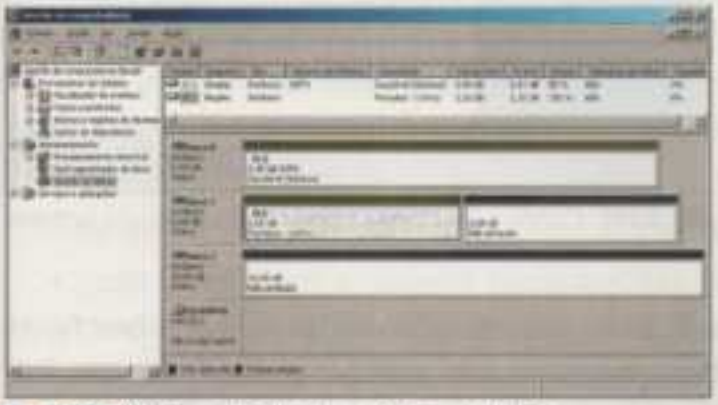

Fig. 3.287 Volume **E:** em fase de formatação.

Fig. 3.288 Volume **E:** pronto a ser utilizado

Criação de um *Mirrored Volume* (Volume espelhado)

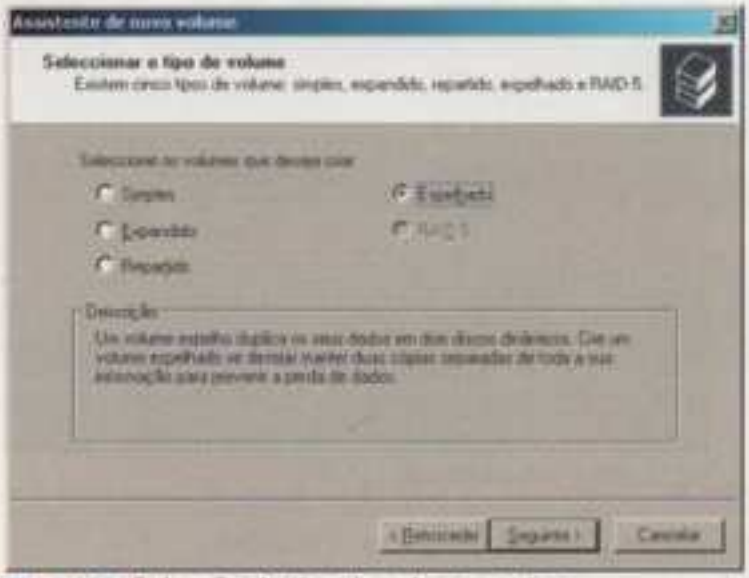

Fig. 3.289 Selecção do tipo de volume a criar

A criação de um volume espelhado/reflectido segue praticamente os mesmos passos referentes à criação de um volume simples.

Primeiro há que verificar a existência de espaço livre em, pelo menos, dois discos. Depois teremos de aceder ao *snap-in* da **Gestão de discos** (botão direito do rato sobre a representação do espaço livre de um disco – ver figura 3.280) e, no ecrã que abre, seleccionar a opção **Novo Volume** e clicar em **Seguinte** para dar início ao processo de criação de um volume (ver figura 3.281). Na janela que abre (figura 3.284), devemos seleccionar o tipo de volume pretendido (**volume espelhado**) e clicar em **Seguinte**, tal como foi feito na criação de um volume simples.

No ecrã da figura 3.290, devemos seleccionar os dois discos que farão parte do volume (usando os botões **Adicionar/Remover**) e o tamanho do volume. Na selecção do tamanho do volume há que ter em atenção o seguinte: visto o volume de armazenamento disponibilizado por cada disco ser igual, o disco com menor espaço será o que limitará o tamanho do volume. Feitas as selecções, pressionar o botão **Seguinte**.

A janela da figura 3.291 é idêntica à da figura 3.284, onde vamos seleccionar/atribuir uma letra (exemplo **F:**) ou um caminho para termos acesso ao volume criado. Feito isto, clicar em **Seguinte**.

Surge um assistente semelhante ao da figura 3.285, para ajudar na formatação do volume, e, após o preenchimento dos passos necessários, clicar novamente em **Seguinte**; de seguida surge o resumo da criação do tipo de volume: **repartido**.

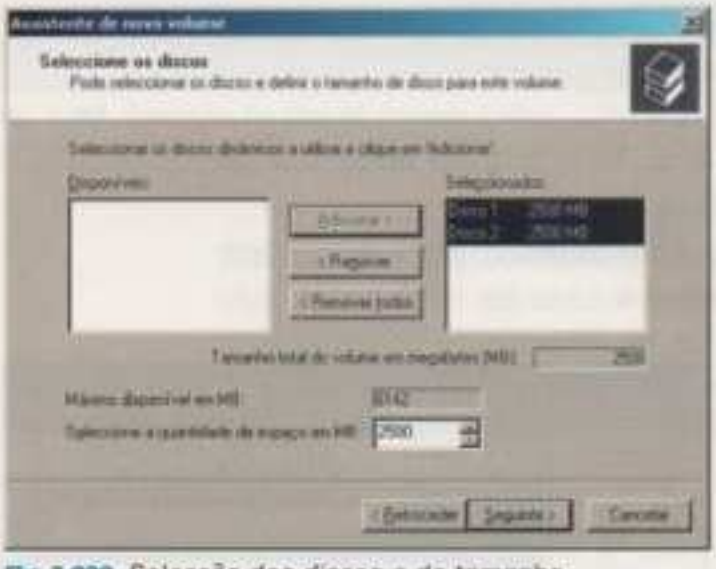

Fig. 3.290 Selecção dos discos e do tamanho

Fig. 3.291 Conclusão do assistente para criar um volume espelhado

Após pressionar em **Concluir** (figura 3.291), os discos serão formatados (ver figura 3.292) e sincronizados (ver figura 3.293); processo que pode levar algum tempo. Surgirá um novo volume **F:** distribuído pelos dois discos seleccionados (discos 1 e 2).

Fig. 3.292 Volume **F:** em fase de formatação

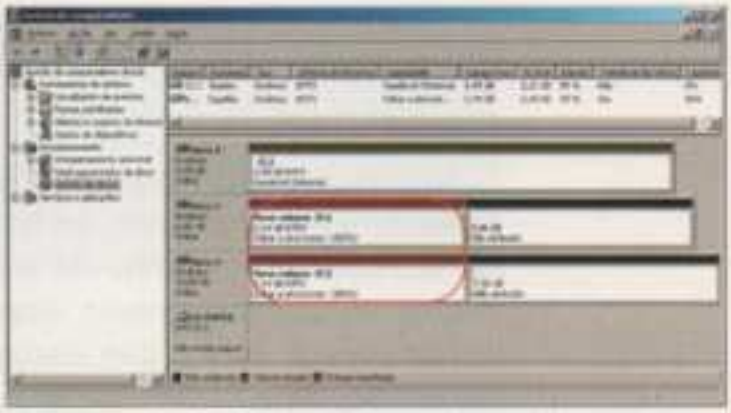

Fig. 3.293 Volume **F:** em fase de sincronização

No final da formatação, o volume **F:** está pronto a ser utilizado. Tal como se pode verificar pela figura 3.294, onde existe a indicação **Saudável** no volume **F:**.

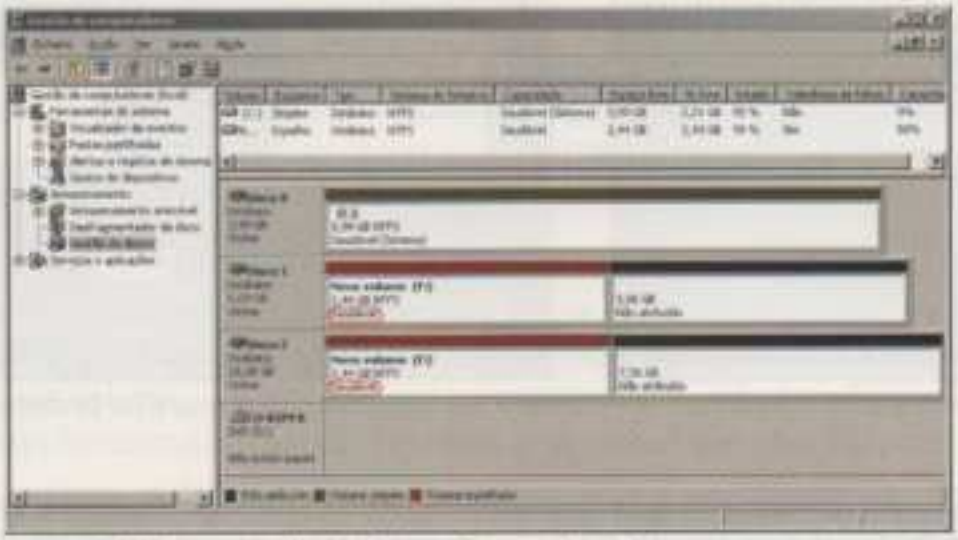

Fig. 3.294 Volume espelhado **F:** pronto a ser utilizado

Era possível realizar o espelho do volume **C:** da figura 3.280; para tal, era necessário clicar sobre o volume **C:** e dar início à criação de um novo volume. Não esquecer que é obrigatório existir um outro disco com espaço livre de igual tamanho ou superior relativamente ao volume **C:**. O segundo disco já tem de estar convertido para disco dinâmico.

Criação de um *striped volume* – RAID 0 (*stripe set* sem paridade)

Criar um *stripe set* sem paridade é como criar qualquer outro volume de disco dinâmico. Precisamos de, pelo menos, dois discos dinâmicos com espaço disponível. Para criar um *striped volume*, vamos voltar ao assistente que usámos para criar um volume simples e um volume espelhado e, basicamente, seguimos os mesmos passos, só que, desta vez, fazendo as selecções tendo em conta que se trata de um tipo **volume repartido** – *striped volume* (ver figura 3.295).

Na criação de um *striped volume* temos de ter em atenção o seguinte:

- os *stripe sets* têm de incluir, pelo menos, dois discos físicos e não mais que 32;
- cada *stripe* terá o mesmo tamanho. Ou seja, se a maior área de espaço livre no disco 0 é de 50 MB, então o maior *stripe set* que se pode criar em três discos é de 150 MB, mesmo que o disco 1 e o disco 2 tenham, cada um, 200 MB de espaço livre;

- os *stripe sets* não incluem qualquer informação de paridade, por isso, o tamanho de volume que o assistente lista é um reflexo real da quantidade de dados que se podem guardar no *striped volume*.

Na fase seguinte (figura 3.296), devemos seleccionar os dois discos que farão parte do volume (usando os botões **Adicionar**/**Remover**) e o tamanho do volume. Na selecção do tamanho do volume, há que ter em atenção o seguinte: visto o volume de armazenamento disponibilizado por cada disco ser igual, o disco com menor espaço será o que limitará o tamanho do volume. Feitas as selecções, clicar em **Seguinte**.

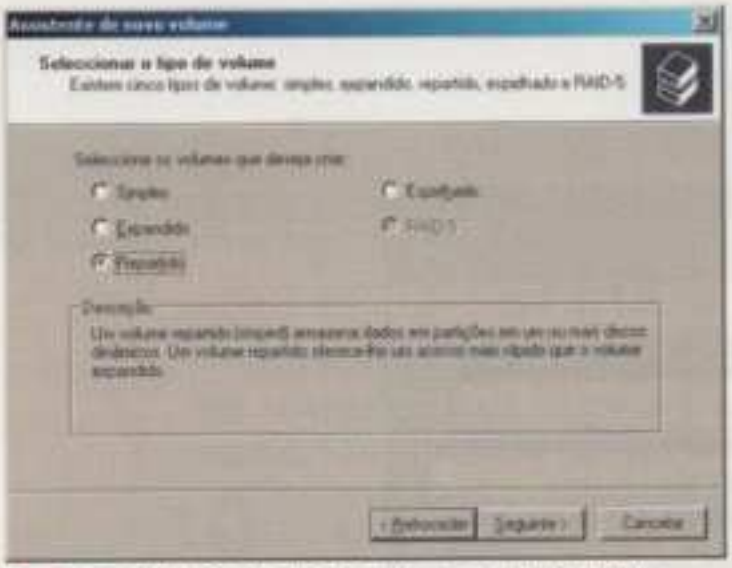

Fig. 3.295 Selecção do tipo de volume a criar **Repartido**

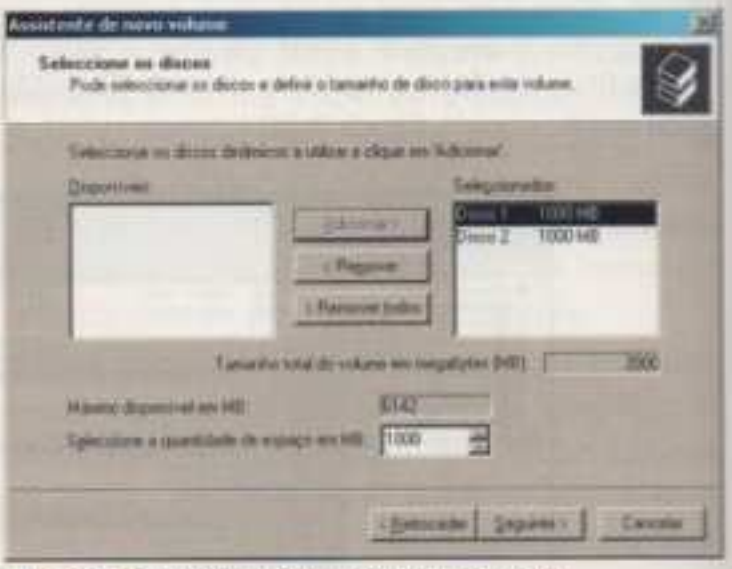

Fig. 3.296 Selecção dos discos e do tamanho

A janela que se segue é idêntica à da figura 3.284, onde vamos seleccionar/atribuir uma letra (por exemplo, **E:**), ou o caminho para termos acesso ao volume criado. Feito isto, clicar em **Seguinte**.

Surge um assistente semelhante ao da figura 3.285 para ajudar na formatação do volume e, após o preenchimento dos passos necessários, clicamos novamente em **Seguinte**; surge, então, o resumo da criação do tipo de volume: **Repartido**.

Após clicar em **Concluir**, o volume será formatado (ver figura 3.297), processo que pode levar algum tempo. Surgirá um novo volume **E:** distribuído pelos dois discos seleccionados (discos 1 e 2).

No final da formatação, o volume **E:** está pronto a ser utilizado.

O aspecto do ecrã da **Gestão de discos**, após a criação de um *striped volume* é como a figura 3.298 apresenta.

Fig. 3.297 Volume **E:** em fase de formatação

Fig. 3.298 Volume **E:** pronto a ser utilizado

No nosso exemplo será adicionado, a cada disco, o espaço de 1000 MB, pelo que o volume final será 2000 MB.

Se algo acontecer a qualquer disco-membro do *stripe set* sem paridade, todos os dados contidos no *set* serão perdidos, embora os outros discos no *stripe set* não sejam afectados.

Criação de um *spanned volume* (Volume expandido)

Um volume expandido é semelhante ao *volume striped*, onde se destacam as seguintes diferenças:

- o volume expandido é formado pela junção das áreas de dois ou mais discos e o tamanho disponibilizado por cada disco para o volume pode ter dimensões diferentes;
- um volume expandido não melhora a performance do sistema, visto a informação ser escrita de forma sequencial ao longo dos discos, ou seja, o sistema utiliza totalmente um disco e só depois começa a usar o seguinte; no *striped volume*, como já vimos, a informação é escrita alternadamente entre vários discos.

No entanto, criar um *spanned volume* é quase como criar um *striped volume* ou qualquer outro tipo de volume. Seguem-se os mesmos passos, excepto na selecção do tipo de volume – que, neste caso, será o **Expandido** (ver figura 3.299) – e na escolha do tamanho reservado em cada disco (ver figura 3.300).

Como o volume é formado pelas áreas de dois ou mais discos, pelo menos dois têm de ter espaço livre disponível, embora os tamanhos disponíveis em cada disco não tenham de ser idênticos, visto o tamanho máximo ser calculado pela soma do espaço disponível nos dois discos.

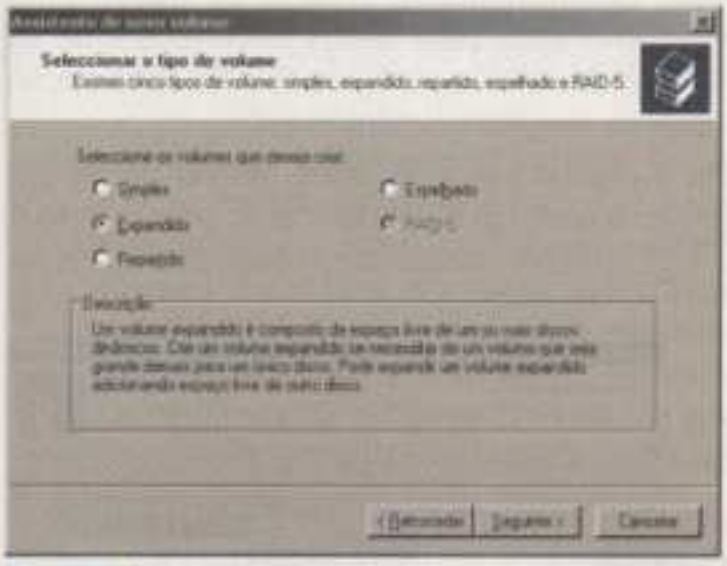

Fig. 3.299 Selecção do tipo de volume a criar **Expandido**

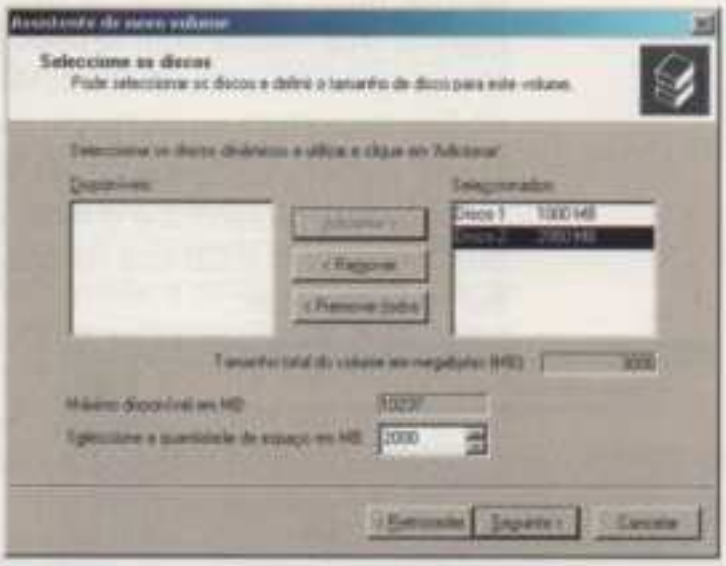

Fig. 3.300 Selecção dos discos e do tamanho

No final, podemos verificar no **Gestor de discos** que foi criado um volume expandido **G:**, que se encontra repartido por 1000 MB no disco 1 e 2000 MB no disco 2. O volume **G:** é visto pelo utilizador de igual modo, como se fosse um volume simples, só que o tamanho final deste volume é dado pelo somatório dos dois discos. Neste exemplo, o volume **G:** tem 3000 MB.

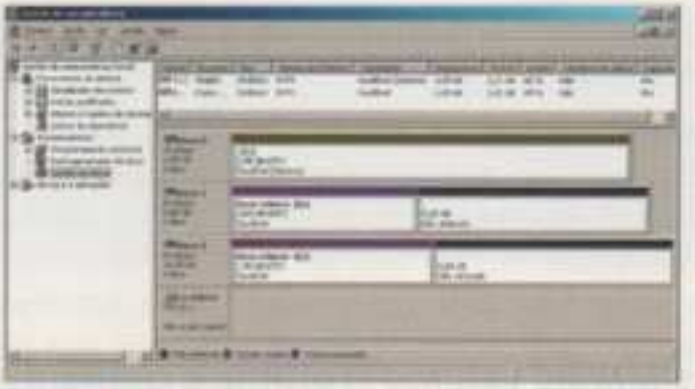

Fig. 3.301 Volume expandido **G:** pronto a ser utilizado

Nota: É possível proceder à expansão de um *simple volume* através da adição de espaço de um segundo disco. Deste modo, o *simple volume* é convertido em *spanned volume*.

Criação de um volume RAID 5 (*stripe set* com paridade)

Fig. 3.302 Aspecto geral dos discos do computador antes de se efectuar a criação do *stripe set* com paridade (RAID 5).

Ao contrário do *stripe set* sem paridade, o volume RAID 5 tem de ser formado por espaços de três ou mais discos livres que funcionam como se fossem um só.

No **Gestor de discos** podemos verificar que temos três discos livres no nosso computador.

Relação de espaço disponível por cada disco:

- Disco 1 – 6 GB
- Disco 2 – 10 GB
- Disco 3 – 12 GB

Convém realçar que os três discos estão configurados como "discos dinâmicos" (ver figura 3.302).

Criar um volume RAID 5 segue os mesmos passos de criação usados nos outros tipos de volume já explicados, exceptuando-se o facto de haver, pelo menos, três discos com espaço livre e convertidos para discos dinâmicos e de se ter de seleccionar o volume RAID 5 no tipo de volume na figura 3.303. Esta opção só fica disponível se existirem as condições descritas anteriormente.

Na escolha do tamanho do volume a ocupar em cada disco, temos de ter em atenção que o disco 1 é o mais pequeno, com 6 GB de capacidade, pelo que só é possível utilizar 6 GB nos discos 2 e 3. O tamanho ocupado em cada disco tem de ser de valor igual.

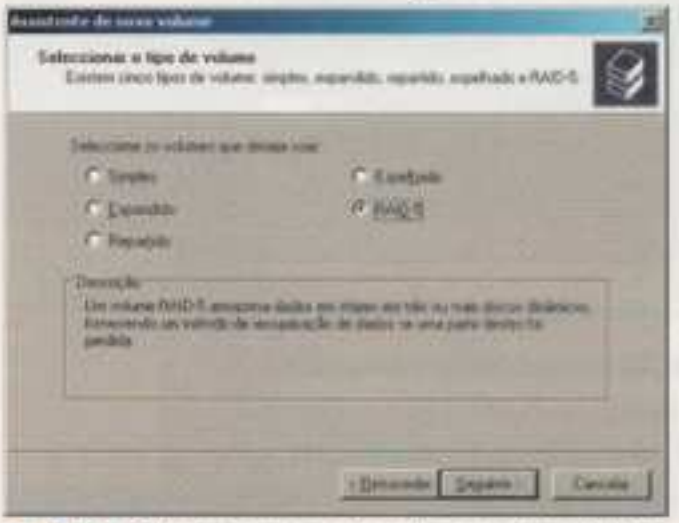

Fig. 3.303 Selecção do tipo de volume a criar: RAID-5

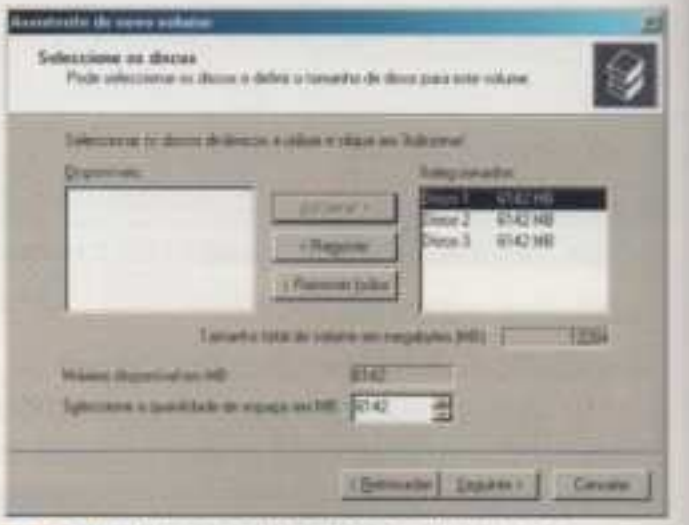

Fig. 3.304 Selecção dos discos e do tamanho

No final, podemos verificar que, no nosso exemplo, o espaço ocupado pelo volume **E:**, em cada disco, é de 6 GB.

Apesar de o espaço ocupado em cada disco ser 6 GB, o que realmente se encontra disponível no volume **E:** é apenas 2/3 do espaço total; isto é, 1/3 do espaço total não pode ser utilizado para guardar dados do utilizador (figura 3.306).

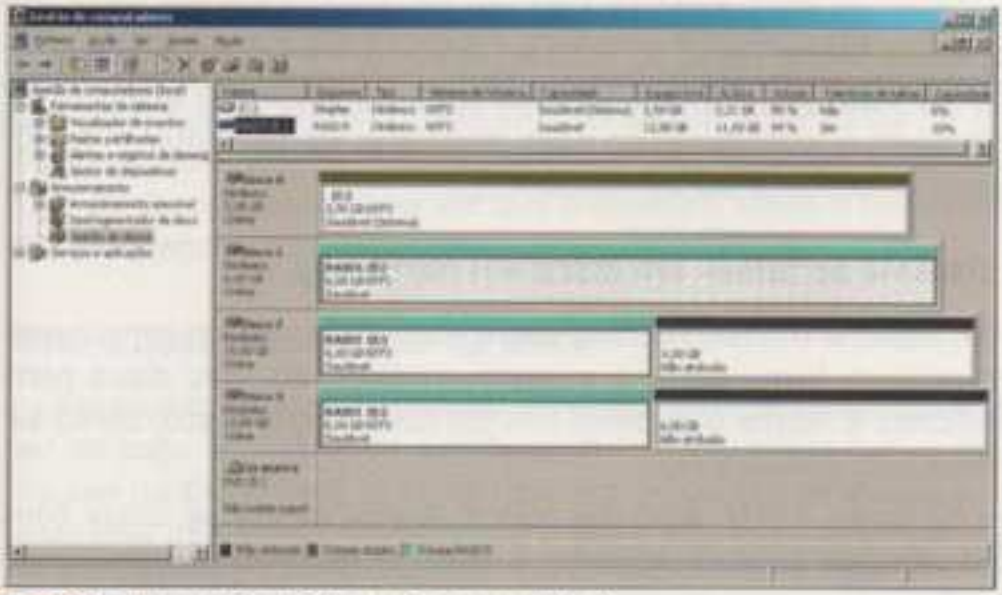

Fig. 3.305 Volume RAID 5 **E:** pronto a ser utilizado

Fig. 3.306 Tamanho disponível no volume RAID 5

Recuperação do sistema

Recuperar de uma simples falha num disco não é assim tão difícil, desde que não se trate do disco com os ficheiros do sistema operativo.

Caso se trate da recuperação de uma falha num disco de dados num volume tolerante a falhas – *fault tolerant*, por exemplo, um **volume espelhado *(mirror set)*** ou **volume RAID 5** –, é possível regenerar os dados em falta e voltar a tornar o volume tolerante a falhas (*fault tolerant*), através dos passos que a seguir se explicam. Mas, mesmo antes de seguir esses passos, os dados continuariam a estar disponíveis. Assim sendo, deve-se:

- clicar com o botão direito sobre o ícone das ferramentas de **Gestão de discos** no painel esquerdo e escolher **Voltar a analisar discos** (*Rescan Disks*). Aparecerá uma caixa de diálogo a informar que a ferramenta da **Gestão de discos** está a fazer a análise aos discos. Terminada a análise, basta clicar com o botão direito sobre o volume que falhou e escolher **Voltar a activar o volume** (*Reactivate volume*). O Windows Server 2003 irá alertar para a necessidade de correr o CHKDSK no volume. Clicar em **OK** e o disco aparecerá como estava antes, e o volume irá de novo ter uma letra da *drive* e estar operacional.

Obs.: No caso de se estar a usar o *disk duplexing* – onde cada disco tem a sua própria controladora –, antes de se proceder à instalação de um novo disco para substituição do disco que falhou num volume espelhado (*mirror set*), deve-se sempre quebrar o espelho (*mirror*) e olhar para dentro dos registos do sistema (*system logs*) para nos certificarmos que o problema está, de facto, no disco. A falha poderá estar na controladora e se a controladora estiver a falhar, instalar um novo disco não vai resolver o problema, pois será necessário substituí-la.

Recuperação do sistema ao falhar um disco com volume RAID 5

Os volumes com paridade, como é o caso deste, são *fault tolerant*, o que significa que, se falhar um disco do volume, é possível recuperá-lo. O sistema detecta a falha de modo automático e o acesso ao volume continua garantido, visto ser possível, a partir da informação de paridade, reconstruir o conteúdo do disco danificado. Assim sendo, deve-se substituir o disco em falha por um novo, não esquecendo que o espaço livre do novo disco terá de ser igual ao usado em cada um dos restantes discos que fazem parte do volume. O disco é adicionado ao clicar com o botão direito do rato sobre a porção danificada do volume e seleccionar **Reparar Volume**, indicando a localização do novo disco que irá substituir o danificado. Este processo pode demorar algum tempo.

Recuperação do sistema ao falhar um disco em *mirroring*

Para recuperar um espelho (*mirror*) no caso de um dos discos que o constituem falhar, deve-se, em primeiro lugar, partir o espelho, instalar um novo disco para substituição do danificado e recriar o espelho (*mirror*) com o novo disco, como se o estivéssemos a fazer pela primeira vez.

Para tal, no ecrã da figura 3.307 devemos abrir a **Gestão de discos**, clicar com o botão direito sobre uma das áreas do espelho e escolher **Remover espelho**.

De seguida (figura 3.308), escolhemos o disco em que pretendemos remover a imagem reflectida. Neste exemplo, vamos escolher o "Disco 1" e clicar em **Remover espelho**.

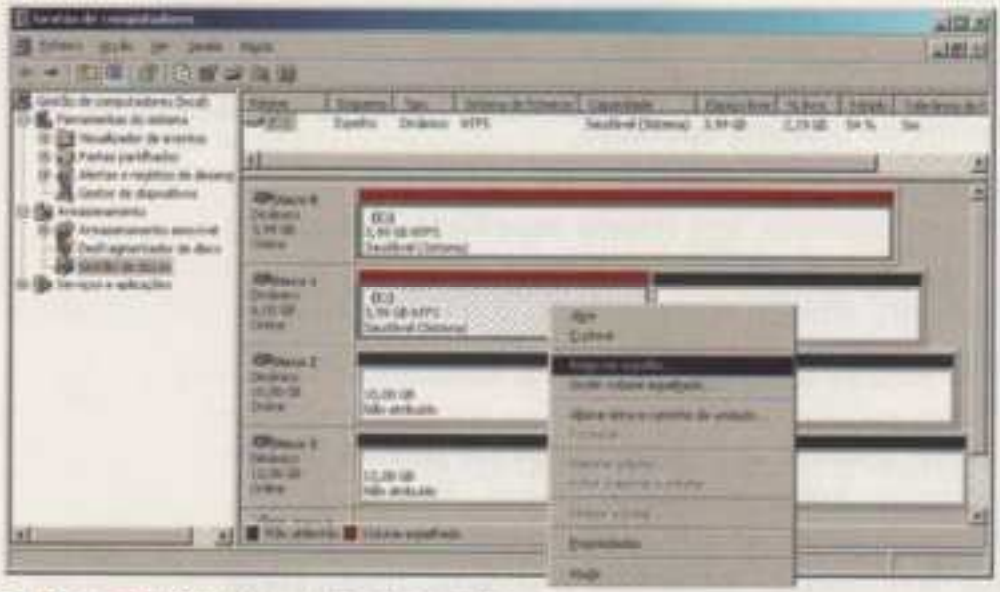

Fig. 3.307 Ordem de remoção do espelho

Fig. 3.308 Escolha do disco de onde será removida a imagem do espelho.

Fig. 3.309 Aspecto final após a remoção do espelho

Após a remoção do espelho obtemos uma imagem do gestor de discos idêntica à da figura 3.309.

Para terminar, é necessário substituir o disco danificado e criar um novo volume espelhado (*mirror*).

Desfragmentação de discos

Uma das formas mais fáceis para melhorar o desempenho do disco é através de uma regular desfragmentação do disco. O Windows Server 2003 vem com uma ferramenta de desfragmentação de discos melhorada, mesmo em termos de velocidade. Até agora não era possível desfragmentar volumes que eram formatados com *clusters* superiores a 4 K. Além disso, o **Desfragmentador de discos** (a nova ferramenta de desfragmentação) consegue desfragmentar o MFT (*master file table* – tabela de ficheiros-mestre). O MFT, que é muito parecido com a tabela de distribuição de ficheiros em partições FAT, consegue saber onde se encontram todos os ficheiros num volume e, se este estiver fragmentado, pode causar sérios problemas de desempenho, uma vez que aumenta o número de leituras (*reads*) necessárias para encontrar um ficheiro.

Usar o Desfragmentador de disco

Para usar o **Desfragmentador de disco**, para desfragmentar um volume ou para ver se este necessita de ser desfragmentado, clicar com o botão direito sobre o volume no **Explorador** ou na ferramenta da **Gestão de discos** e abrir a folha de **Propriedades** do volume. Clicar sobre o separador das **Ferramentas** (que contém todas as ferramentas de manutenção dos discos).

Pressionar o botão **Desfragmentar agora**, para abrir o ecrã da figura 3.311.

Fig. 3.310 Separador **Ferramentas** das propriedades do disco **C:**

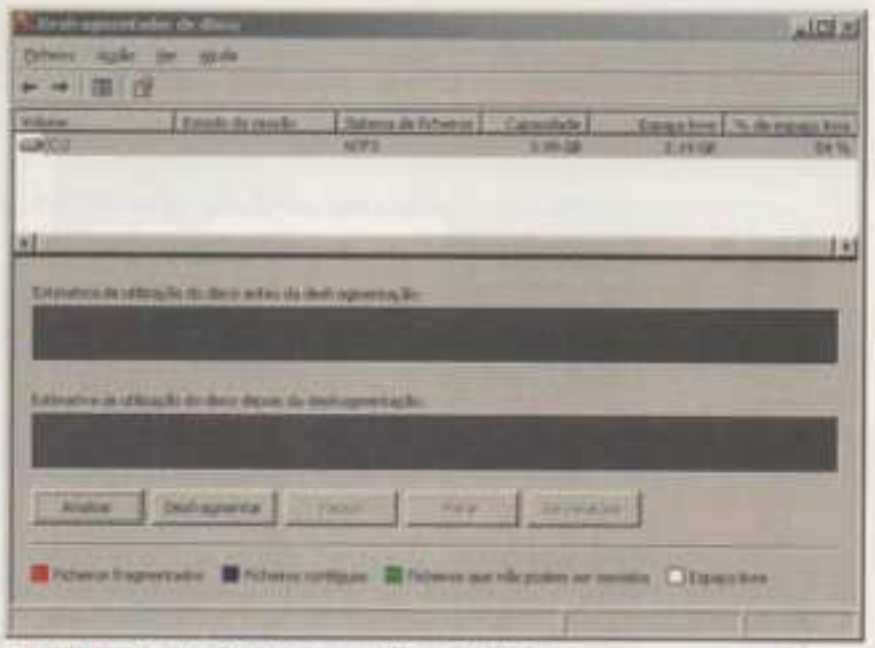

Fig. 3.311 Janela **Desfragmentador de disco**

Se repararmos, apenas se encontram listados os volumes locais. No Windows Server 2003 ainda não é possível desfragmentar volumes através da rede. Em primeiro lugar, há que verificar se o disco realmente necessita de ser desfragmentado. Para tal deve-se seleccionar o volume na lista e pressionar o botão **Analisar**. O processo de análise é bastante rápido e, logo de seguida, é-nos apresentada uma janela com as recomendações, como a figura 3.312.

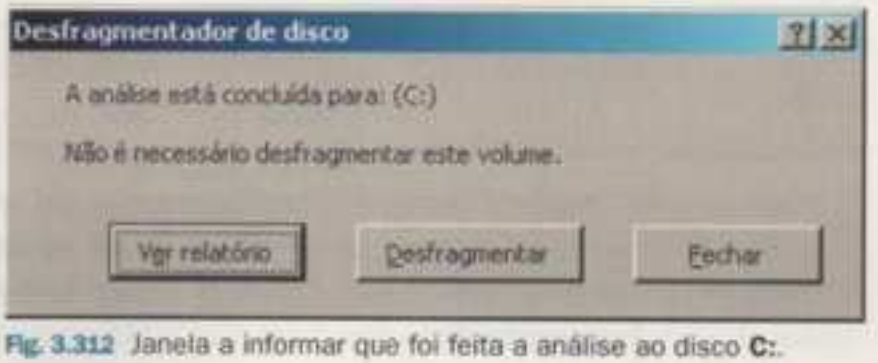

Fig. 3.312 Janela a informar que foi feita a análise ao disco **C:**.

Se a análise referir que o volume está "sujo", o que pode querer indicar alguma corrupção, deve-se correr o CHKDSK para ter acesso ao estado do volume. Também é possível saber se um volume está "sujo" digitando **fsutil dirty query c:** na linha de comandos.

Se pretendermos ter ainda mais informações sobre o estado de fragmentação do disco, basta clicar sobre o botão **Ver relatório** (*View Report*), para abrir uma caixa de diálogo como a que consta da figura 3.313.

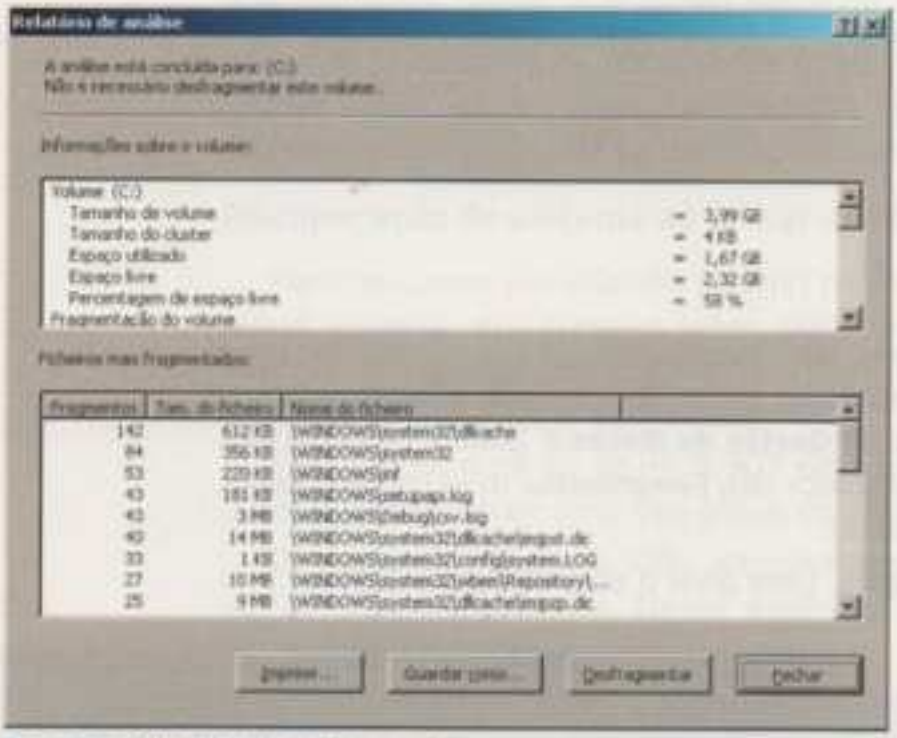

Fig. 3.313 Relatório da análise ao disco

A maioria da informação sobre o volume deve ser bastante simples de interpretar: o tamanho do volume é o tamanho da partição, o tamanho do *cluster* é o tamanho de cada unidade lógica de armazenamento na *drive* (neste caso, 4 kB) e o resto da secção descreve quanto espaço no disco está presentemente a ser utilizado, quanto se encontra livre e qual a percentagem de espaço livre. A secção **Fragmentação do volume** abaixo da secção de **Informação sobre o volume** descreve o estado dos ficheiros. A **Fragmentação total** descreve como está fragmentado todo o disco; a **Fragmentação de ficheiro** diz como estão fragmentadas as partes utilizadas no disco (ou seja, a proporção de ficheiros que está fragmentada), e a **Fragmentação de espaço livre** descreve como está fragmentado o espaço não utilizado no disco. A **Fragmentação de espaço livre** é importante quando se trata de criar novos ficheiros – quanto mais fragmentado está o espaço não utilizado, maior a probabilidade de os novos ficheiros serem fragmentados também. A **Fragmentação de ficheiros** fornece informação de fragmentação a nível de ficheiros. Esta área lista o número total de ficheiros no disco, o tamanho médio de um ficheiro, os fragmentos totais e o número médio de fragmentos por ficheiro. O valor ideal para fragmentos por ficheiro deve estar o mais próximo possível de 1.00, uma vez que este número indica que todos os ficheiros são contíguos (adjacentes). O resto da informação mostra a fragmentação para partes específicas da estrutura do volume do disco. Depois de analisado o estado actual do volume, deve-se fechar todos os ficheiros que estão a utilizar o volume de fragmentação (incluindo os ficheiros de aplicação) e depois pressionar o botão **Desfragmentar**. A ferramenta vai começar por reorganizar os ficheiros no disco para depois os colocar em *clusters* contíguos. Desfragmentar o disco não vai libertar espaço no disco, mas vai agrupar todo o espaço livre, permitindo que seja utilizado mais eficazmente, o que pode melhorar bastante o desempenho do sistema.

Nota: É possível desfragmentar um volume com ficheiros abertos, mas torna mais difícil a desfragmentação do volume do sistema. Demorará muito menos tempo, se todos os ficheiros forem fechados antes do início do processo de desfragmentação.

4.3. Auditoria do servidor

Introdução à auditoria e à monitorização da rede em Windows Server 2003

Uma das funções do administrador de um servidor e de uma rede é proteger a rede e os utilizadores e prevenir possíveis danos, intencionais ou inadvertidos; tarefa nem sempre facilitada, visto ser necessário atribuir aos utilizadores permissões para estes realizarem certas tarefas, que, por sua vez, poderão vir a ser prejudiciais para o sistema. Se, porventura, algo acontecer que possa pôr em risco a segurança da rede ou dos seus dados, o administrador é chamado a esclarecer a situação. Será nesta altura que se verifica a necessidade de auditoria de uma rede, que não só resolve certas situações, como também confirma que nada de irregular se passa.

Configuração dos acontecimentos a monitorizar

Algumas situações que surgem na rede e no servidor são automaticamente monitorizadas pelo sistema, mas outras apenas serão monitorizadas por indicação da nossa parte; para isso, vamos a **Iniciar > Programas > Ferramentas administrativas** e escolhemos **Política de segurança do domínio**.

Dentro da janela das **Predefinições de segurança do domínio** seleccionamos **Política da auditoria**.

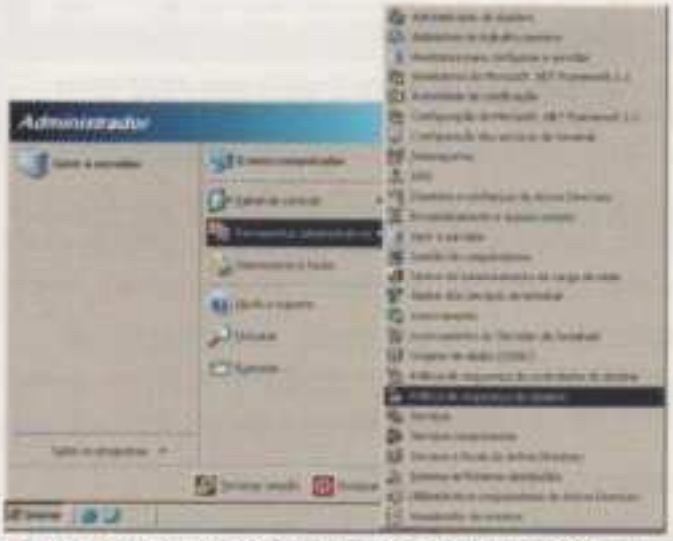

Fig. 3.314 Acesso a **Políticas de segurança do domínio**

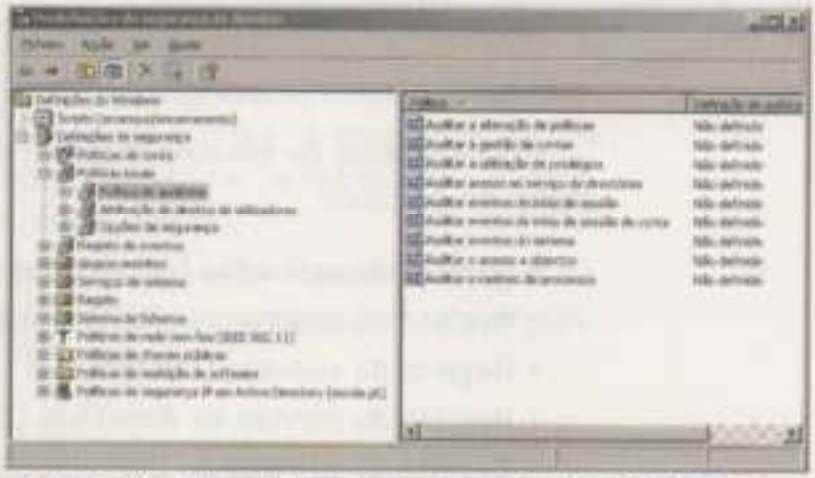

Fig. 3.315 Acontecimentos/eventos a monitorizar: **Política de auditoria**

Para seguir/localizar o acesso ao ficheiro ou ao directório, ou seja, para configurar os elementos a monitorizar, deve-se fazer duplo clique sobre o item que se encontra listado à direita. Surge a janela da figura 3.316.

Neste ecrã é necessário seleccionar a opção **Definir estas definições de política** para monitorizar o acontecimento. Depois de seleccionado, surgem outras duas caixas de opções: **Com êxito** e **Sem êxito**. A caixa **Com êxito** faz um registo de todos os acontecimentos que são levados a cabo, ou seja, de

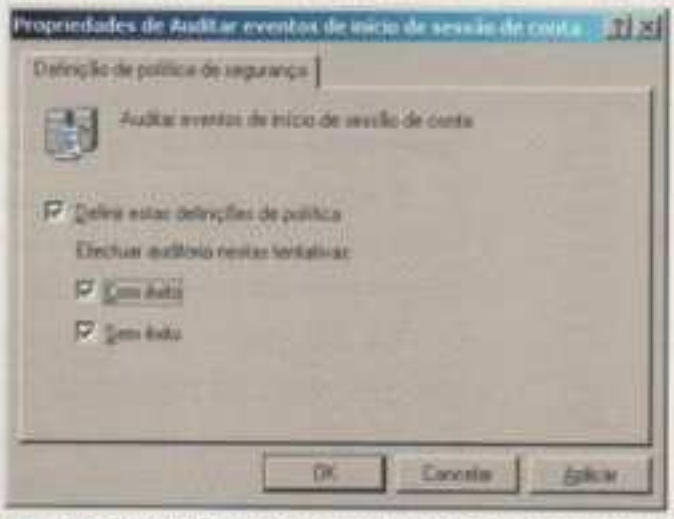

Fig. 3.316 Configuração da uma auditoria a um evento

todos os inícios de sessão de conta conseguidas, e a caixa **Sem êxito** regista as tentativas falhadas, ou seja, todas aquelas tentativas de início de sessão de conta não conseguidas.

Visualizador de eventos – *Event Viewer*

O **Visualizador de eventos** (*Event Viewer*) encontra-se localizado no grupo de programas das ferramentas administrativas, e também pode ser chamado a partir da linha de comandos digitando **EVENTVWR.MSC**. O **Visualizador de eventos** já foi abordado no ponto **3.13 – Monitorização e optimização**.

Esta ferramenta, presente no Windows Server 2003 em modo gráfico, serve para auxiliar na função de auditoria da rede e do servidor.

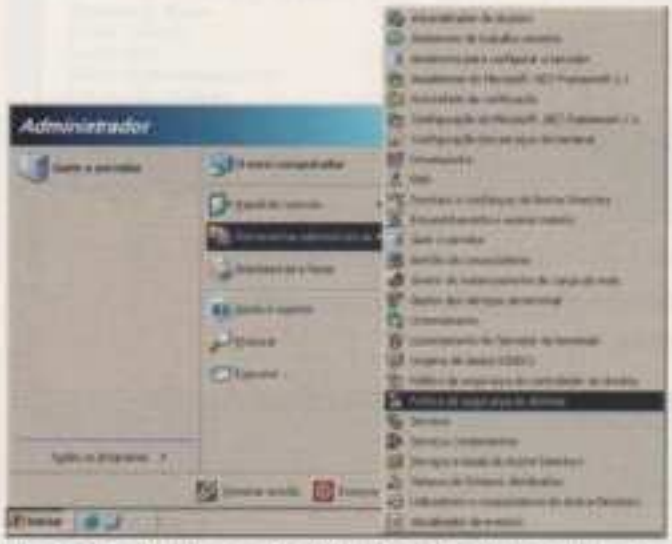

Fig. 3.317 Acesso ao **Visualizador de eventos** (*Event viewer*)

Fig. 3.318 Aspecto genérico da janela **Visualizador de eventos** (*Event Viewer*)

O **Visualizador de eventos** mantém vários registos de eventos (*event logs*) separados no servidor:

- **Registo da aplicação** (*Application log*)
- **Registo de segurança** (*Security log*)
- **Registo do sistema** (*System log*)
- **Registo do serviço de directório** (*Directory Service log*)
- **Registo do servidor de DNS** (*DNS Server log*)
- **Registo do serviço de replicação de ficheiros** (*File Replication Service log*)

Notas:

O *Event Viewer*, para servidores que tenham o papel de *member servers*, apenas apresenta o registo da aplicação, o registo do sistema e o registo de segurança.

Embora o conteúdo da janela **Visualizador de eventos** (*Event Viewer*) possa ser diferente do apresentado na figura 3.318, o tipo de dados armazenados e o modo como são apresentados são idênticos.

Os acontecimentos registados no **Visualizador de eventos** são vistos em função de três registos principais: o da aplicação, o do sistema e o da segurança.

Estes registos (*logs*) podem ser encontrados em qualquer computador com o Windows Server 2003. As outras categorias (os restantes registos) apenas se aplicam a computadores que deles necessitam, devido ao papel que desempenham na rede.

O **registo do serviço de directório** regista eventos relacionados com os controladores de domínio, acompanhando a base de dados de segurança, e o **registo do serviço de replicação de ficheiros** lista eventos relacionados com o serviço de replicação de ficheiros.

O **registo do servidor de DNS** (que se encontra, como esperado, num servidor DNS) regista eventos associados à resolução de nomes de computadores para ou de endereços IP.

Event Viewer: Application – Aplicação

O **registo da aplicação** regista eventos que sejam atribuídos por aplicações e que não sejam suficientemente abrangentes para chegarem ao registo do sistema. Uma aplicação servidora pode, por exemplo, registar falhas de processos ou o início e o fim de processos demorados. O nome deste registo pode enganar, pois não se trata tanto de aplicações de utilizadores, mas mais de licenciamento, de *backups*, de aplicações de políticas de segurança, com ou sem sucesso, etc.

Event Viewer: Security – Segurança

Este *log* regista qualquer evento auditado que se relacione com assuntos de segurança, tal como utilizadores que estejam a aceder a ficheiros ou a alterar a base de dados das contas de segurança. No Windows 2000, era explicitamente necessário ligar o registo de segurança (*security logging*). No Windows Server 2003 encontra-se ligado por defeito.

Event Viewer: System – Sistema

Esta categoria regista o início e o fim de serviços e qualquer outro evento relacionado com o sistema, como, por exemplo, situações em que a impressão de um documento decorreu com sucesso ou com erros, falhas de periféricos ou instalações, com ou sem sucesso, de novos *drivers*, entre outros.

Se surgir uma caixa de diálogo a informar que algo não funcionou e que se deve verificar o monitor de eventos (*Event Monitor*) para mais detalhes, o primeiro lugar a ir é ao **registo do sistema**.

Utilização do *Event Viewer* – Visualizador de eventos

Visualizador de eventos facilita o acesso a informação sobre um determinado período, caso esta informação tenha sido guardada em disco. Para isto basta accionar os comandos **Abrir** e **Guardar Como**, no menu **Acção**.

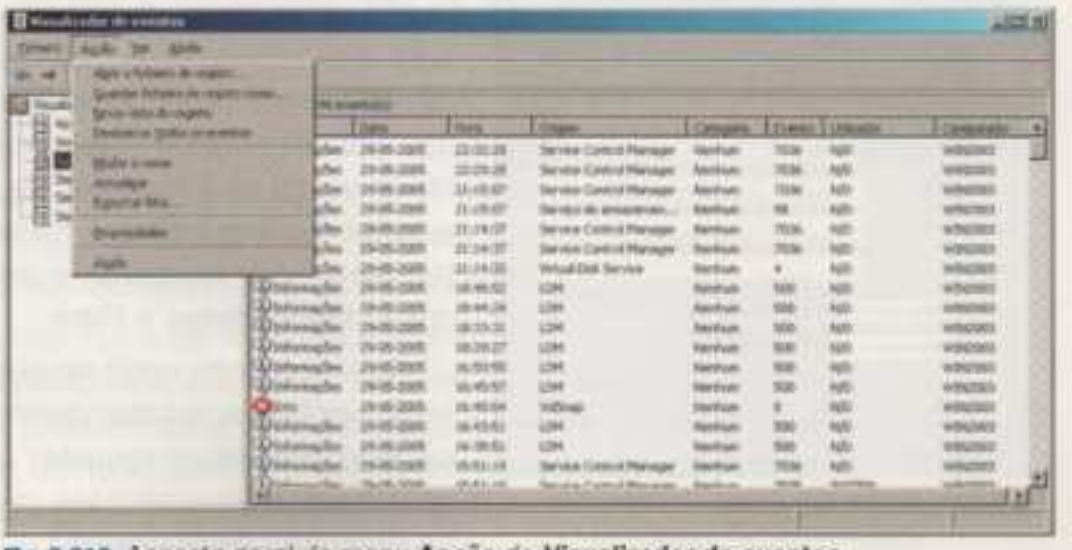

Fig. 3.319 Aspecto geral do menu **Acção** do **Visualizador de eventos**

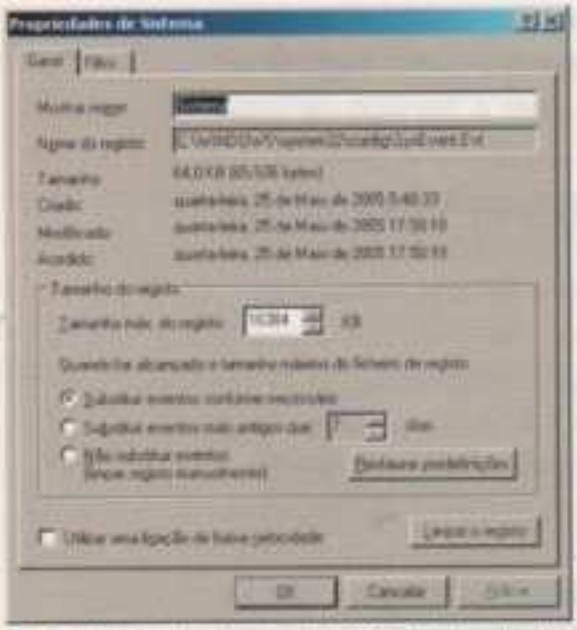

Fig. 3.320 Janela das propriedades do visualizador de sistema

Também é possível, no menu **Acção**, **Limpar todos os eventos** que surgem na lista ou, por meio do comando **Propriedades**, também acessível através do menu **Acção**, configurar os limites que se pretendem designar para o registo de acontecimentos.

No ecrã que surge (figura 3.320) pode-se configurar, para cada um dos eventos registados, o nome que identifica o grupo de eventos na árvore, definir o tamanho máximo que o ficheiro do registo pode atingir e, através da opção **Substituir eventos conforme necessário**, indicar se pretendemos limpar os eventos mais antigos para libertar espaço no ficheiro do registo. Também é possível optar por, automaticamente, eliminar os eventos que aconteceram há mais de X dias (o número de dias é configurável), através da opção **Substituir eventos mais antigos que *X* dias**, ou, caso nunca se pretenda eliminar os eventos do ficheiro do registo, seleccionar a opção **Não substituir eventos (limpar registo manualmente)**.

Gravidade dos acontecimentos

Existem, no **Visualizador de eventos** (*Event Viewer*) três tipos de ícones que indicam o grau de gravidade de um acontecimento, além das normais descrições de erro e da identificação do PC em que este se detectou:

Informações – acontecimento realizado com sucesso; informação de carácter genérico;

Aviso – acontecimentos que poderão futuramente originar situações de erro;

Erro – acontecimento não realizado devido a erro.

Filtragem de acontecimentos

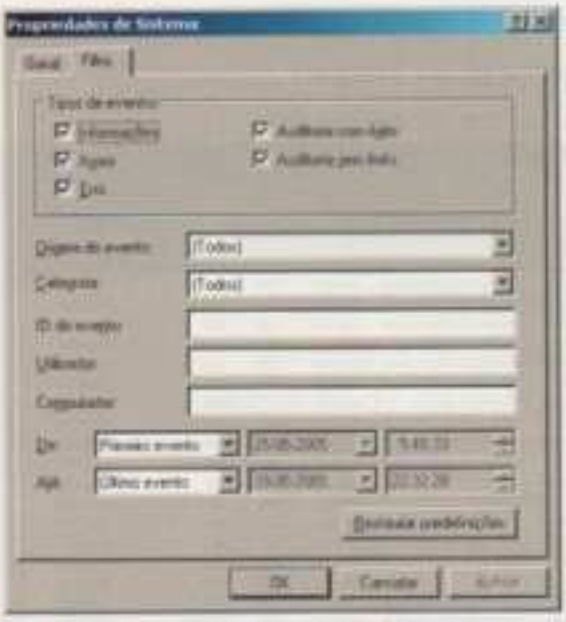

Fig. 3.321 Janela do separador **Filtro** das propriedades do visualizador de sistema

Através do *Event Viewer* podemos aceder a dados para obter informação sobre os mesmos; ao percorrer a lista de acontecimentos, podemos encontrar acontecimentos inesperados, por exemplo, ao descobrir um ou outro símbolo que representa a gravidade do acontecimento. Mas também podemos querer procurar informação sobre apenas um determinado acontecimento e, para realizar esta filtragem de acontecimentos, ou seja, para restringir os acontecimentos exibidos na janela **Visualizador de Eventos**, teremos de ir novamente ao menu **Acção** e escolher a opção **Propriedades > Filtro**.

Aqui podemos optar se queremos, ou não, que na lista sejam incluídos acontecimentos do tipo **Informações**, **Aviso** ou **Erro**. Podemos também optar por incluir na lista as operações bem-sucedidas ou os erros relativos a falhas na execução de operações.

Também é possível reduzir os acontecimentos a visualizar, indicando a origem do evento, a sua categoria ou os códigos específicos dos mesmos. Os últimos parâmetros permitem-nos indicar em que período de tempo (data e hora) queremos monitorizar os acontecimentos ou vê-los todos registados a qualquer hora e a qualquer dia.

Tendo preenchido as opções pretendidas, basta clicar em **OK**.

4.4. Gestão da energia

UPS (FANI)

Convém usar sempre uma **UPS** (***U**ninterruptible **P**ower **S**upply* – fonte de alimentação ininterrupta) ou, em português, **FANI** (**F**onte de **A**limentação **N**ão **I**nterruptível) para proteger os servidores e o *hardware* de rede (tal como as *hubs* e os *routers*) de sobrecargas eléctricas, de correntes eléctricas "irregulares" e/ou de falhas no fornecimento de electricidade, evitando, deste modo, a perda de dados não guardados a tempo.

Além da função de uma UPS fornecer permanentemente um sistema informático quando existe falha de energia na rede eléctrica, existe outra muito importante que se destina a evitar ou, em certas situações, simplesmente, atenuar picos de corrente e de tensão que podem surgir na rede eléctrica. Estes picos, por vezes, podem atingir, durante alguns milissegundos, 5 a 10 vezes o valor nominal da corrente e/ou da tensão. Nestas situações, o gestor da rede pode não se aperceber de um problema na rede eléctrica, mas o equipamento pode sofrer danos graves.

Além deste problema, a má qualidade da "terra" numa instalação eléctrica é também, normalmente, um problema de difícil detecção por parte de um informático, quer devido à sua pouca formação nesta área, quer por falta de equipamentos de medida adequados. Estes problemas podem provocar avarias em que o gestor pode ser levado a "pensar" que são de cariz de *software* e/ou de *hardware*, atrasando e dificultando a detecção e a reparação da fonte do problema.

De um modo simplificado, uma UPS é constituída por um conversor de corrente alternada em corrente contínua, que interliga a rede eléctrica (funciona a corrente alternada de 380/230 V a 50 Hz) aos acumuladores (funcionam a corrente contínua). Os equipamentos funcionam à tensão e à frequência da rede eléctrica (380/230 V a 50 Hz); por esta razão, é necessário que as UPS tenham outro circuito responsável por converter a corrente contínua armazenada nos acumuladores em corrente alternada. Estes dois circuitos, a par dos acumuladores, são os principais componentes de uma UPS.

No mercado existem dois grandes grupos de UPS. As UPS ***Online*** e as ***Offline***. Vamos ver o que distingue estes dois tipos de UPS.

- **UPS *Offline***. Neste tipo de UPS, os acumuladores só fornecem energia às cargas (computadores, *switch*,...) se houver falha no fornecimento de energia eléctrica. Se a rede voltar, os acumuladores deixam de funcionar e são carregados.

  Desvantagens: Caso haja falha de rede, a UPS tem de fornecer energia às cargas através dos acumuladores; para isso, é necessário que haja comutação da alimentação pela rede eléctrica para a alimentação através dos acumuladores. Esta comutação demora, normalmente, entre 4 e poucas dezenas de milissegundo. Assim, situações de picos de corrente/tensão que durem, por exemplo, 1 milissegundo, podem provocar graves danos nos dispositivos.

Este tipo de UPS não resolve este e outros problemas semelhantes.

Vantagens: O preço destas UPS é bastante inferior relativamente às UPS *Online*.

- **UPS *Online***. Neste tipo de UPS, as cargas estão permanentemente a ser alimentadas pelo barramento de corrente contínua (acumuladores), mesmo quando há rede eléctrica.

  Desvantagens: Preço mais elevado relativamente às UPS *Offline* e maior desgaste dos acumuladores, dado que estes estão permanentemente a ser descarregados (alimentar cargas) e carregados.

  Vantagens: Como a alimentação das cargas é feita através do barramento de corrente contínua, mesmo que surjam picos de tensão/corrente de 1, ou menos, milissegundo, quem sofre com esta anomalia é o circuito de entrada da UPS (conversor de corrente alternada em corrente contínua) e os acumuladores. Estes problemas são eliminados e não se propagam para a saída da UPS (alimentação das cargas). Esta é a grande vantagem deste tipo de UPS.

Conclusão:

Desde que haja possibilidades, deve-se optar por instalar UPS *Online*; o problema provocado pelos picos de tensão/corrente são eliminados, enquanto que, na solução de UPS *Offline*, não existe a garantia da eliminação dos mesmos.

Normalmente, uma UPS consegue fornecer energia de 10 minutos a 1 ou 2 horas, consoante a capacidade dos acumuladores. Se houver necessidade de se prolongar o fornecimento de energia de uma UPS ou de um conjunto de UPS, pode-se:

- Aumentar o número de acumuladores, embora provocando um aumento substancial no preço, no tamanho e no peso. Para ter uma noção do tamanho e do peso, basta ver e pegar na bateria de um carro. Mesmo aumentando o número de baterias, existe sempre um limite na duração do fornecimento de energia.
- Para melhorar a autonomia, no caso de falha da rede eléctrica, pode-se adicionar um gerador de energia eléctrica, alimentado, por exemplo, a gasóleo. Nesta situação temos de manter as UPS para que estas protejam a instalação contra picos de tensão/corrente e da falha de rede eléctrica. Desde a detecção da falha de rede até um gerador estar a trabalhar a 100%, normalmente, passam mais de 15 s. Neste intervalo é necessário ter as UPS para se garantir o fornecimento de energia à instalação; só depois de o gerador estar a trabalhar a 100%, é que este pode fornecer alimentação às UPS, aumentando substancialmente a autonomia das mesmas.

Nestas situações, a autonomia de uma instalação, no caso de falha da rede eléctrica, pode ser de alguns dias ou até mesmo de várias semanas, pois a autonomia depende da capacidade do depósito de combustível do gerador.

No caso de falha da rede eléctrica, a autonomia das UPS varia consoante a capacidade dos acumuladores, o número de cargas ligadas, e, nas situações de sistemas com grupo gerador, do depósito de combustível. É inevitável que, mais cedo ou mais tarde, a energia dos acumuladores se esgote, pelo que há necessidade se desligar os equipamentos informáticos antes da falha de energia. Caso o gestor da rede não esteja presente na altura em que a autonomia da UPS chega ao fim, então aí podemos preconfigurar o(s) computador(es) para que este(s) se possa(m) desligar sozinho(s), de modo automático.

Antes da compra de uma UPS convém analisar alguns parâmetros, tais como:

- potência máxima fornecida (em VA). Potência máxima que a UPS consegue fornecer em caso de falha de rede;
- autonomia máxima (em minutos), com a UPS a trabalhar na máxima potência em caso de falha de rede;
- sistema de *bypass*, que possibilita a remoção da UPS, por exemplo, para manutenção, sem haver necessidade de se desligar o circuito das cargas; ou seja, é possível realizar a comutação UPS/rede eléctrica e vice-versa, sem haver necessidade de corte à saída da UPS;
- alimentação da UPS pelo sistema monofásico (230 v) ou trifásico (380 V);
- interligação com um computador via porta série, USB ou Ethernet;
- *drivers* para se interligar com o Windows Server 2003;
- *online* ou *offline*.

Caso exista a possibilidade de interligar a UPS ao computador por porta série, ou USB ou Ethernet, e caso existam *drivers* para comunicar com o Windows Server 2003, é possível configurar o Windows Server 2003 para desligar o servidor antes da energia da UPS falhar por completo.

Para configurar uma UPS basta ir ao menu **Iniciar > Painel de controlo** e escolher a ferramenta **Opções de energia**.

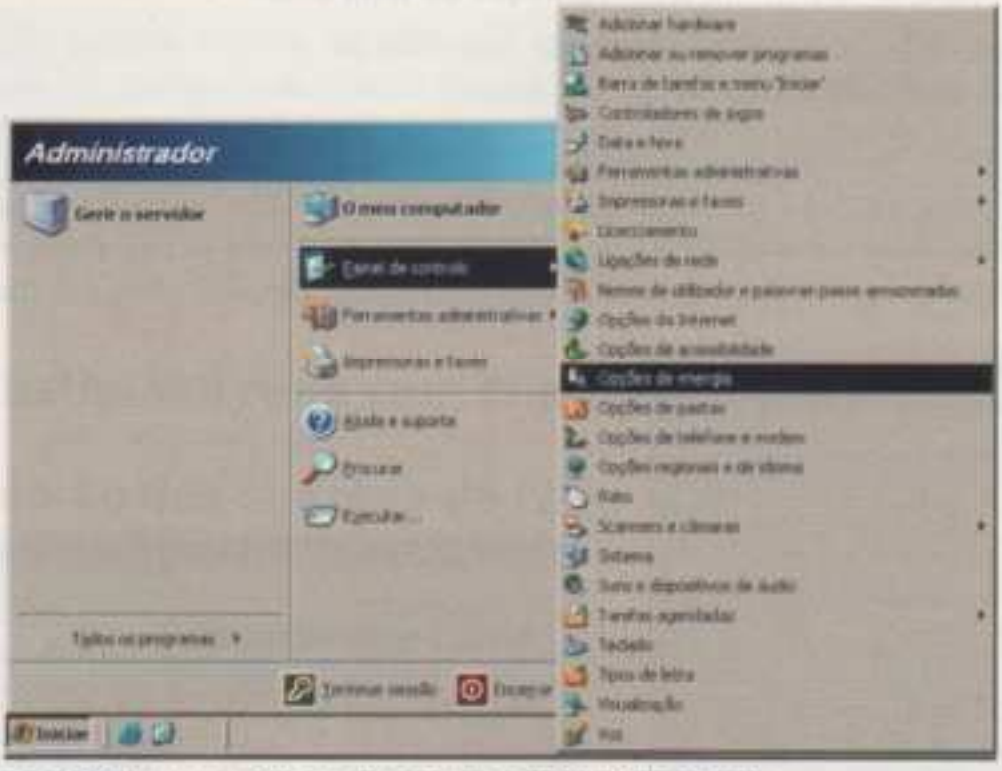

Fig. 3.322 Acesso a **Opções de energia** do **Painel de controlo**

Gestão da energia

A ferramenta **Opções de energia** permite configurar, como o nome indica, algumas opções relacionadas com a gestão de energia. Assim, ao aceder-se a **Opções de energia**, tem-se acesso aos vários separadores (que variam, caso se trate de um portátil).

O primeiro separador **Esquemas de energia** (figura 3.323) serve para configurar a poupança de energia. Feitas as configurações desejadas, clicar em **Guardar como**.

O segundo separador **Avançadas** (figura 3.324) permite optar entre ter ou não ter o ícone das opções de energia na barra de tarefas (junto ao relógio).

No separador **Hibernar** (figura 3.325) é-nos possibilitada a instalação do suporte para hibernação: o conteúdo da memória permanece em disco, mesmo quando o computador é desligado, e, ao iniciar de novo o computador, além de tornar o arranque mais rápido, tudo volta a aparecer como estava antes do encerramento do mesmo.

Fig. 3.323 Separador **Esquemas de energia** da janela **Propriedades de opções de energia**

Fig. 3.324 Separador **Avançadas** da janela **Propriedades de opções de energia**

Fig. 3.325 Separador **Hibernar** da janela **Propriedades de opções de energia**

O separador UPS permite a configuração de uma UPS.

Configuração de uma UPS

Vejamos como configurar uma UPS em Windows Server 2003.

Em primeiro lugar, há que seleccionar o fabricante da UPS e o devido modelo, através do botão **Seleccionar** da figura 3.326, que abre uma nova janela, na qual também se deve indicar a porta série em que a UPS está ligada. Depois, clicar em **Concluir**.

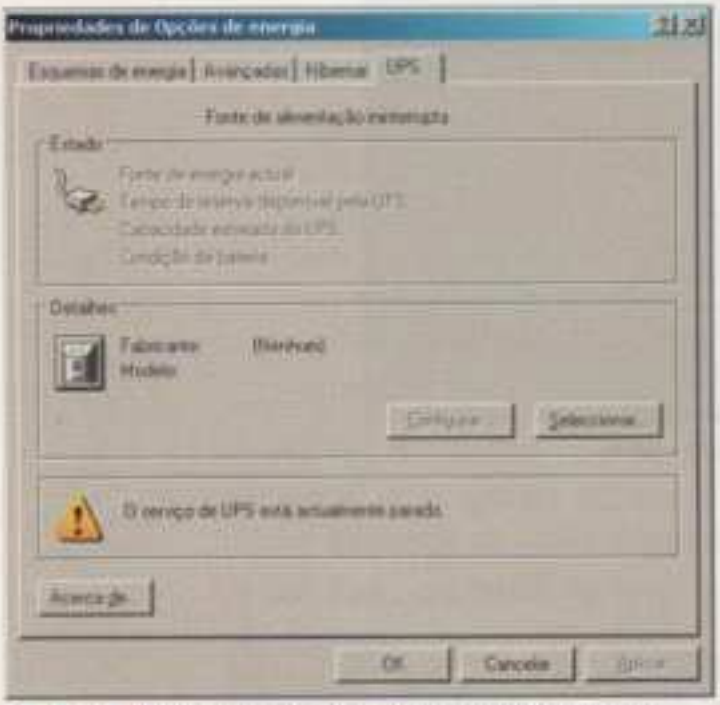

Fig. 3.326 Separador **UPS** da janela **Propriedades de opções de energia**

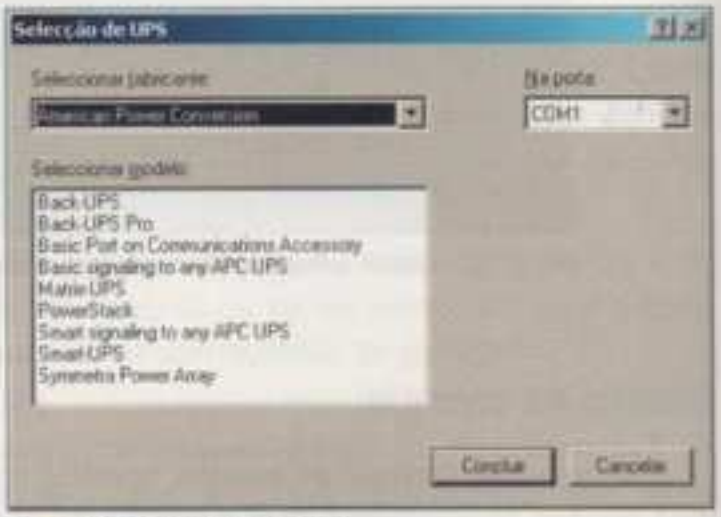

Fig. 3.327 Selecção da **UPS**

Regressamos à janela da figura 3.326, onde vamos configurar a comunicação entre a UPS e o computador-servidor, em caso de falha de corrente eléctrica, clicando em **Configurar**.

Se queremos que os utilizadores da rede sejam notificados das falhas de corrente, de modo que estes tenham tempo de gravar os seus dados, então devemos escolher **Activar todas as notificações** e preencher os campos respeitantes aos segundos entre a falha da corrente e a primeira notificação e aos segundos entre as subsequentes notificações de falha de corrente.

A activação da opção **Minutos em bateria antes de alarme crítico** permite activar um alarme que dispara quando a autonomia da UPS estiver a chegar ao fim. Este campo também permite que possamos identificar a quantos minutos antes do fim da autonomia queremos que o alarme soe.

Caso estejamos interessados em correr um programa antes do encerramento do computador, basta activar a opção **Na ocorrência de alarme, executar este programa.**

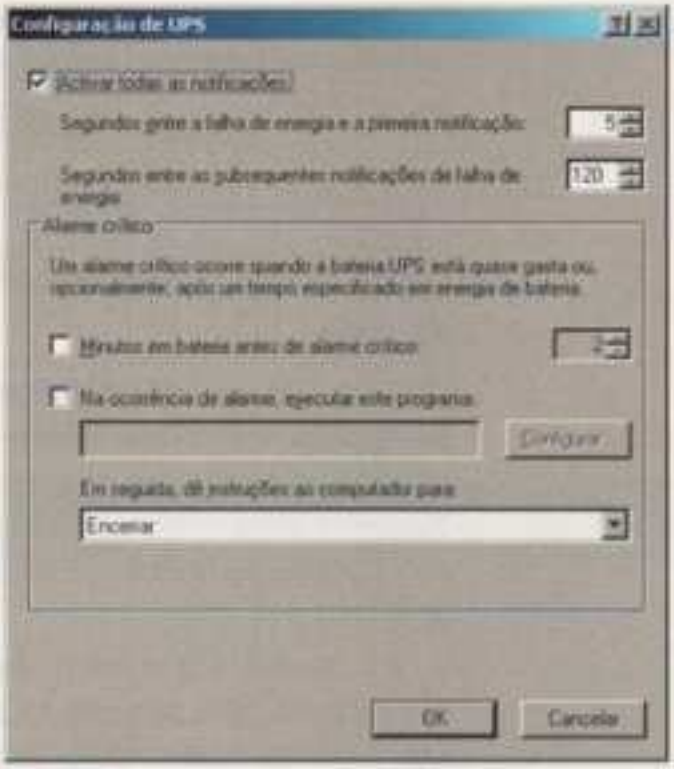

Fig. 3.328 Configuração de uma UPS

Por fim, resta escolher entre desligar o computador-servidor através da opção **Encerrar** ou **Hibernar** e **OK**.

NOTA: Existem marcas de UPS que fornecem *drivers* de comunicação e *software* de gestão específicos para o Windows Server 2003, pelo que poderá haver necessidade de os instalar e configurar. A configuração do *software* de gestão pode variar de marca para marca, mas, no essencial, não varia muito do que vem por defeito no Windows Server 2003 (já analisado).

5. Trabalho em rede com Windows Server

5.1. Gestão dos clientes da rede

Introdução

Já construímos o nosso servidor, criámos utilizadores e partilhámos recursos em rede. Agora necessitamos de configurar os nossos sistemas de clientes para usarem aqueles recursos. É possível existirem diversos clientes numa rede baseada em Windows Server 2003, embora nem todos acedam aos recursos do sistema do mesmo modo.

Nesta unidade vamos aprender como fazer a ligação, como configurar vários sistemas de clientes e como fazer o *logon* à rede.

Partindo do princípio que o servidor se encontra instalado e configurado como domínio, interessa ter postos de trabalho a usarem esse domínio. No caso de existirem utilizadores não identificados perante o domínio, estes poderão aceder aos recursos do mesmo, desde que sejam dadas permissões para tal acontecer, nomeadamente, ter a conta de *guest* (convidado) activa e existirem recursos com acesso dado a **Todos** ou apenas ao **Convidado**. Por questões de segurança, a conta *guest* deve estar desligada.

Ao longo desta subunidade, iremos fazer a ligação sempre ao mesmo servidor, no mesmo domínio e com a mesma conta de utilizador:

- o *username* (nome de utilizador) é: **nomealuno**
- o nome de domínio é: **escola.pt**

O que se deve saber/relembrar antes de proceder à gestão dos clientes da rede

Antes de iniciar qualquer configuração dos clientes, há algumas coisas que se devem relembrar sobre clientes e sobre o ambiente em rede, nomeadamente os conceitos básicos sobre *software* de rede e segurança; protocolos TCP/IP e infra-estruturas; configuração de contas de utilizadores e de contas de computadores (para sistemas que podem participar na segurança ao nível do domínio).

Os domínios oferecem segurança centralizada. Contas de utilizadores de domínio existem para permitir às pessoas usarem um único nome de *login* para fazer o *logon* em qualquer *workstation* e para aceder a recursos em qualquer servidor que pertença ao domínio. No entanto, apenas sistemas baseados em sistemas operativos baseados no NT4, com *service pack* 4 ou superior, Windows 2000 Server e Professional, Windows XP Professional e Windows Server 2003 podem ser membros de domínio.

Se, por exemplo, um sistema Windows 2000 Professional estiver apenas num *workgroup*, os utilizadores de domínio não podem fazer o *logon* à *workstation* com uma conta de domínio. Se pretendermos que os nossos clientes façam o *logon* a um dos sistemas listados e acedam a recursos num domínio, é necessário ligar a *workstation* ao domínio.

Os sistemas operativos baseados no Windows 98 e no Millenium conseguem validar os seus utilizadores num domínio, mas, quanto ao nível das restrições da própria máquina cliente, pouco se pode fazer.

Sistemas baseados em Windows 95, Windows XP Home Edition, Windows para *Workgroups* e clientes DOS não podem ser membros de domínio. Estes sistemas podem apenas participar em *workgroups*. Não existe nenhuma verdadeira base de dados de segurança na *workstation*; os utilizadores podem iniciar a secção (*logon*) sem uma conta de domínio ou mesmo sem uma conta local. No entanto, para permitir aos utilizadores o acesso aos servidores de domínio e aos seus recursos, é possível configurar o *software* de cliente de rede, nestes sistemas, para ligar os utilizadores a um domínio.

O *Active Directory* (AD) acrescenta uma camada de funcionalidades ao *workgroup* e ao modelo de *Primary domain controller* (PDC) existente no Windows NT; o AD é uma base de dados de contas de domínios, de utilizadores e de computadores e, até, de relacionamentos de confiança. O AD utiliza segurança de domínio, mas foi desenvolvido para conseguir gerir redes maiores e mais complexas quando comparadas com aquelas com que os domínios e os *workgroups* conseguem lidar. O que importa recordar aqui é que apenas o Windows 2000 e o XP Professional incluem o *software* de cliente AD completamente funcional. No entanto, pacotes de extensão de cliente AD estão disponíveis para o Windows 9x e o NT4. As extensões de cliente AD para 9x e NT4 incluem suporte para novos métodos de autenticação e pesquisas no *Active Directory*.

Nota:

A extensão de cliente *Active Directory* (também conhecido por Cliente DS) para Windows 95 e Windows 98 está incluída no CD-ROM do Windows 2000 em: **\CLIENTS\WIN9X\DSCLIENT.EXE**

Esta extensão de cliente para o NT4 está disponível para *download* da Microsoft em: http://www.microsoft.com/windows2000/server/evaluation/news/bulletins/adextension.asp

A tabela seguinte sumaria as capacidades de associação em rede dos clientes que se irão configurar nesta unidade:

Sistema operativo de cliente	Membro de *workgroup*	Membro de domínio	Extensões de cliente do *Active Directory*
Windows XP Professional	√	√	√
Windows 2000 Professional	√	√	√
Windows NT4	√	√	adicionar
Windows 98	√		adicionar
Windows 95	√		adicionar
DOS	√		

Tabela 3.13 Capacidade de associação em rede de clientes Windows

Uma palavra final: os sistemas baseados no sistema operativo NT mantêm uma base de dados de segurança local. As alterações de configuração que iremos realizar requerem privilégios administrativos. Ao configurar clientes de Windows NT, Windows 2000 ou Windows XP Professional, é necessário fazer primeiro o *logon* como **administrador** ou utilizar uma conta equivalente.

Agora estamos preparados para começar a ligar sistemas de clientes a um controlador de domínio implementado pelo Windows Server 2003.

Ligação de computadores com Windows XP Professional

O cliente Windows XP Professional é o cliente ideal para o Windows Server 2003. O sistema operativo do cliente e do servidor e a interface do utilizador são os mesmos e o XP suporta todas as grandes características do Server 2003, incluindo administração remota, serviços de instalação remotos e políticas de grupo. O *Plug and Play* universal torna a instalação do *driver* da placa de rede suportada quase automática. Se a placa de rede estiver presente e for detectada quando o sistema operativo é instalado, o XP instala o *driver* automaticamente. Se aceitarmos as configurações típicas de rede durante a instalação do XP, o processo de configuração (*setup*) instala também o protocolo TCP/IP e o *Client for Microsoft Networks*. Se instalarmos o NIC mais tarde, o XP Professional detecta automaticamente o novo *hardware* e carrega o *driver* ou pede ao utilizador a localização do *driver* correcto. Se apenas necessitarmos do protocolo TCP/IP e do *Client for Microsoft Networks*, então o administrador não tem muito que fazer, excepto juntar-se a um domínio ou a um *workgroup* específico.

Verificar a configuração da nossa rede

Em primeiro lugar é preciso fazer o *logon* ao sistema como utilizador com direitos administrativos. Antes de tentar juntar-se ao domínio, deve-se confirmar (no **Painel de controlo – Ligações de rede**) que a placa de rede foi correctamente detectada e que o respectivo *software* foi carregado. Se o *software* foi correctamente carregado, deve-se ver um ícone intitulado **Ligação de área local** (se tivermos mais do que um NIC instalado, ver-se-ão mais ícones de ligação de área local).

Deve-se ver se a ligação está activa e, se seleccionarmos a ligação e expandirmos os detalhes (ver figura 3.330), também se deve poder ver que o endereço IP foi atribuído por DHCP.

Fig. 3.329 Acesso a **Ligações de rede** na janela **Painel de controlo**

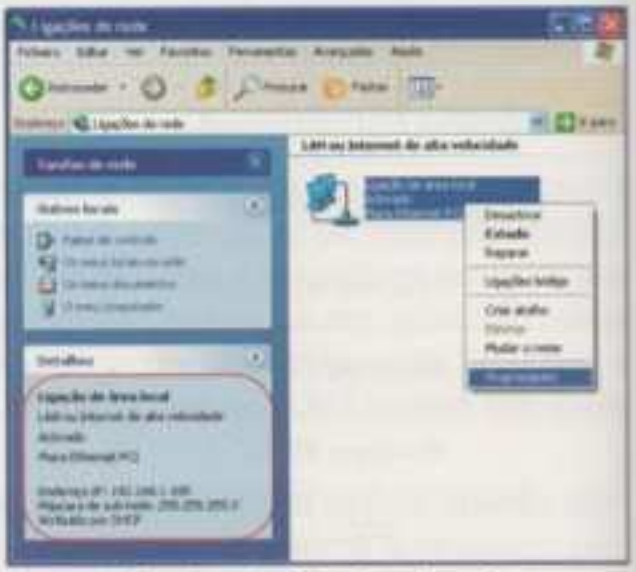

Fig. 3.330 Detalhes de **Ligações de rede**

Se tudo parecer estar em ordem, clicar com o botão direito sobre o ícone da **Ligação de área local** e escolher **Propriedades**, para ver a informação sobre a configuração da rede. Esta página de propriedades, como se pode ver pela figura 3.331, lista todos os componentes instalados: tipo de placa de rede, protocolo e *software* de cliente. Para ter acesso à informação do IP (página de propriedades do **Protocolo de Internet – TCP/IP**), basta seleccionar **TCP/IP** e clicar em **Propriedades**.

Fig. 3.331 Janela **Propriedades de ligação de área local**

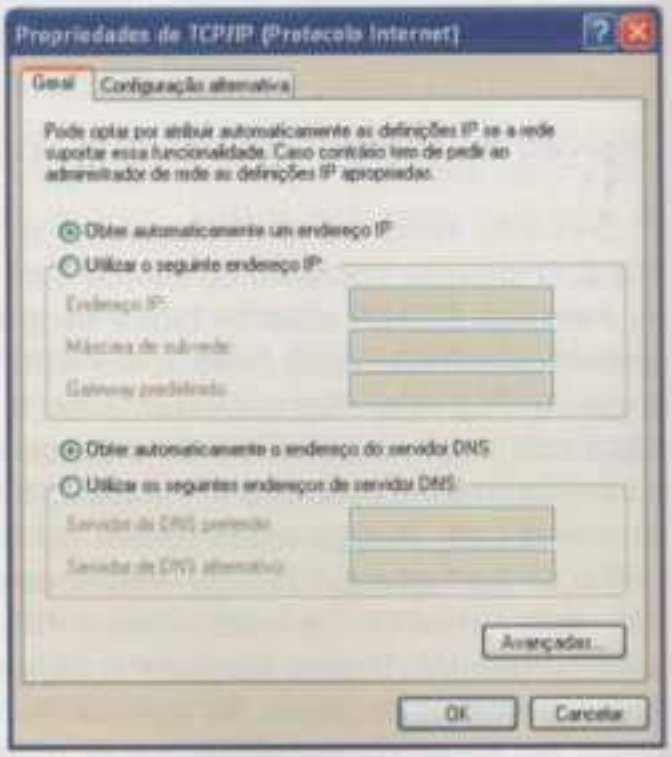

Fig. 3.332 Página de **Propriedades de TCP/IP (Protocolo Internet)**

Na subunidade **3.11 – DHCP** foi instalado o servidor de DHCP e foi criado um âmbito (*scope*), para atribuir endereços aos clientes entre as gamas de endereços **192.168.1.100/24** e **192.168.1.200/24**.

Por defeito, o TCP/IP está configurado para obter automaticamente o endereço IP e, se tudo estiver correctamente ligado, o servidor de DHCP atribui automaticamente um endereço IP ao cliente, dentro do âmbito (*scope*) configurado.

IP FIXO

Caso se opte por atribuir manualmente os endereços IP a cada computador-cliente, é necessário seleccionar **Utilizar o seguinte endereço IP**, introduzir um endereço de rede igual ao do servidor e atribuir um endereço ao computador diferente de todos os *host* da rede, como, por exemplo:

Endereço IP: 192.168.1.10

Máscara de subrede: 255.255.255.0

Gateway predefinido: introduzir, por exemplo, o endereço de um router que dá acesso à Internet ou a outra rede.

Deve-se escolher, ainda, **Utilizar os seguintes endereços de servidor DNS** e introduzir o endereço do nosso servidor de DNS **192.168.1.1**. Não esquecer que o nosso servidor com o Windows Server 2003 é o próprio servidor de DNS.

Fig. 3.333 Página de **Propriedades de TCP/IP (Protocolo Internet)**

Juntar-se a um domínio

Agora que sabemos que a placa de rede está a funcionar correctamente e que já se obteve a informação de configuração do DHCP, está na altura de nos juntarmos ao domínio. Se o cliente Windows XP Professional se vai juntar a um controlador de domínio, necessitamos de lhe **criar uma conta de computador** no domínio-alvo. É aconselhável que isto seja anteriormente feito pelos membros do grupo de administradores no domínio, que, para tal, podem usar a ferramenta **Utilizador e Computador do Active Directory**. No entanto, também é possível criar uma conta de computador a partir da *workstation*, durante o processo de configuração, na parte que diz respeito à rede, ou então, usando o painel de controlo do sistema, no caso de se conhecer o nome do utilizador e a palavra-passe de uma conta com a capacidade de criar contas de computadores no domínio.

Para nos ligarmos a um domínio, começamos por clicar em **Sistema**, que se encontra no **Painel de controlo**, ou, então, clicar com o botão direito **O Meu Computador** e escolher **Propriedades**. Na janela **Propriedades do sistema**, navegar até chegar ao separador **Nome do computador** (figura 3.334). Aí, clicar em **Alterar**, para ligar a um domínio.

Vamos, então, mudar a selecção para **Domínio**, digitar o nome do domínio e depois clicar em **OK** (figura 3.335).

Se ainda não existir uma conta no sistema, o XP Professional pede que se forneça um nome de utilizador com permissões de administrador no controlador de domínio e a respectiva palavra-passe.

Se tudo correr bem, surge uma mensagem a dar as boas-vindas ao domínio.

Fig. 3.334 Separador **Nome do computador** da janela **Propriedades do sistema**

Fig. 3.335 Introdução do nome do domínio

Fig. 3.336 Introdução do nome de um utilizador com permissões de administrador do domínio e da respectiva palavra-passe

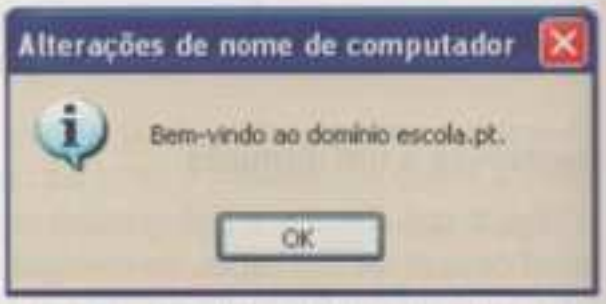

Fig. 3.337 Janela a dar as boas-vindas ao domínio **escola.pt**

Caso não seja possível aceder ao domínio, deve-se verificar se:
- a placa de rede está bem instalada, a funcionar correctamente e activada;
- o computador está ligado à rede do servidor;
- o protocolo TCP/IP está bem configurado e se o servidor de DHCP atribuiu correctamente o endereço ao cliente;
- se o endereço DNS é o do servidor Windows Server 2003 (192.168.1.1).

Se o problema persistir, deve-se, na janela da figura 3.335, em vez de colocar o nome do domínio **escola.pt**, introduzir o nome NetBIOS **escola**.

Convém reiniciar o sistema para que as mudanças sejam reconhecidas.

Quando o sistema reiniciar, dá-nos a opção de *fazer o início* da secção (*logon*) usando uma conta local ou uma conta de utilizador de domínio. De seguida deve-se activar a lista **Iniciar secção em:** e escolher o nome de domínio **escola**.

Quando o XP Professional iniciar a secção, vai validar o utilizador **nomealuno** ao servidor **escola.pt**, dando início à secção e carregando as configurações pessoais do controlador de domínio.

Fig. 3.338 Janela a avisar que o sistema operativo tem de ser reiniciado.

Fig. 3.339 Início de secção do Windows XP Professional no domínio **escola.pt**

Ligação de computadores com Windows 2000 Professional

A junção de um cliente Windows 2000 Professional a um controlador de domínio é em tudo idêntica à realizada no Windows XP Professional. Todas as considerações mencionadas para o Windows XP Professional são válidas aqui.

Antes de se iniciar a instalação deve-se verificar:

- se a placa de rede está bem instalada, configurada e activada;
- se existe ligação ao servidor pela rede;
- se o cliente Microsoft e o protocolo de comunicação TCP/IP estão correctamente instalados e configurados. Caso se opte por obter automaticamente um endereço IP e o endereço do servidor de DNS, deve-se verificar se os endereços IP e de DNS foram correctamente atribuídos pelo servidor de DHCP.

Para se iniciar a integração a um controlador-domínio, é necessário ir a **Painel de controlo**, seleccionar **Ligações de acesso telefónico e de rede** e clicar em **Identificação de rede** (figura 3.340), ou em **Painel de controlo**, seleccionar **Sistema** e na janela **Propriedades do sistema** navegar até ao separador **Identificação da rede** (figura 3.341).

Fig. 3.340 Separador **Nome do computador** da janela **Propriedades do sistema**.

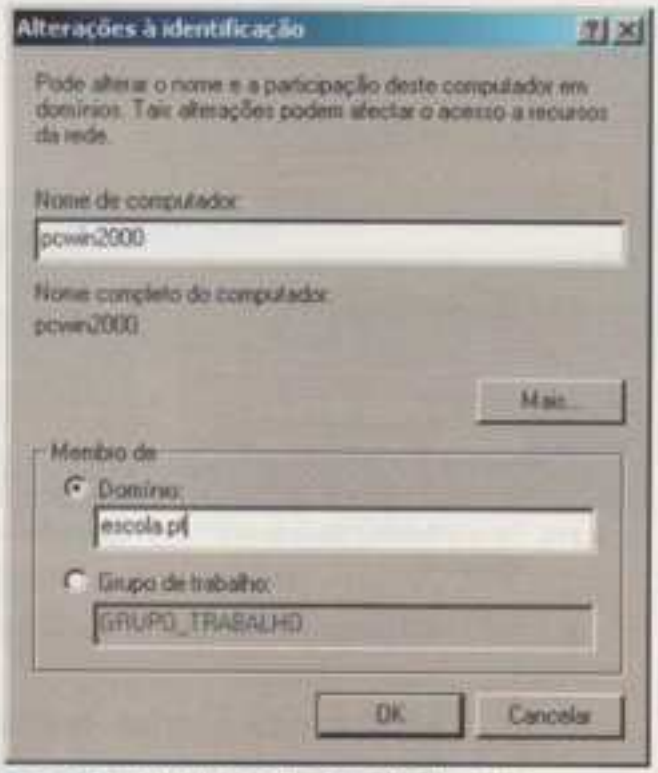

Fig. 3.341 Introdução do nome do domínio

Clicar em **Propriedades**, para ligar a um domínio.

Mudar a selecção para **Domínio** e digitar o nome do domínio, depois de clicar em **OK**.

Deve-se introduzir o nome do utilizador-administrador ou de um utilizador com permissões de administrador no controlador de domínio e colocar, ainda, a respectiva palavra-passe.

Se tudo correr bem, surge uma mensagem a dar as boas-vindas ao domínio.

Convém reiniciar o sistema para que as mudanças sejam reconhecidas.

Fig. 3.342 Introdução do nome de um utilizador com permissões de administrador do domínio e da respectiva palavra-passe

Fig. 3.343 Janela a dar as boas-vindas ao domínio **escola.pt**

Fig. 3.344 Janela a avisar que o sistema operativo tem que ser reiniciado

Quando o sistema reiniciar, na janela **Iniciar sessão no Windows** deve-se clicar em **Opções**, para se expandir a janela (figura 3.345).

Na janela da figura 3.346, por defeito, o início da secção é realizado a partir de uma conta do próprio computador e não pelo controlador de domínio; para tal, no selector que se encontra no lado direito de **Iniciar sessão em:**, dá-nos a opção de iniciar a sessão usando uma conta local ou uma conta de utilizador de domínio.

Após a escolha do início de sessão ser realizada por uma conta do domínio **Escola**, vamos introduzir o nome do utilizador **nomealuno** e a respectiva palavra-passe. Não esquecer que este utilizador tem de estar previamente criado no controlador de domínio.

Fig. 3.345 Janela **Iniciar sessão no Windows**

Fig. 3.346 Selecção de início de sessão por um utilizador existente no computador ou no controlador de domínio

Fig. 3.347 Início de sessão do Windows 2000 Professional no domínio **escola.pt**

O Windows 2000 Professional vai validar o utilizador **nomealuno** ao servidor **escola.pt**, dá início à sessão e carrega as configurações pessoais do controlador de domínio.

Ligação de computadores com Windows NT 4.0 Workstation

A junção de um cliente Windows NT 4.0 Workstation a um controlador de domínio não difere muito relativamente à realizada no Windows 2000 e no XP Professional.

Antes de se iniciar o processo de integração com um domínio no Windows Server 2003, é necessário:

- instalar o *service pack* 4 ou superior;
- verificar se a placa de rede está bem instalada, configurada e activada;
- verificar se está instalado o serviço de *workstation* e se o protocolo de comunicação TCP/IP está correctamente instalado e configurado. Caso se opte por obter automaticamente um endereço IP e o endereço do servidor de DNS, deve-se verificar se os endereços IP e de DNS foram correctamente atribuídos pelo servidor de DHCP;
- verificar se a placa de rede está correctamente ligada à rede.

Para se iniciar a integração a um controlador-domínio, é necessário ir ao **Painel de controlo**, seleccionar **Rede** e navegar até ao separador **Identificação** (figura 3.348). Aí, clicar em **Alterar** (*Change*), para ligar a um domínio (figura 3.349).

Mudar a selecção para **Domínio** e digitar o nome do domínio. Clicar em **Criar uma conta de computador no domínio**, introduzir o nome do utilizador-administrador ou de um utilizador com permissões de administrador no domínio e colocar, ainda, a respectiva palavra-passe. Depois é só clicar sobre **OK**.

Fig. 3.348 Separador **Identificação** da janela **Rede**

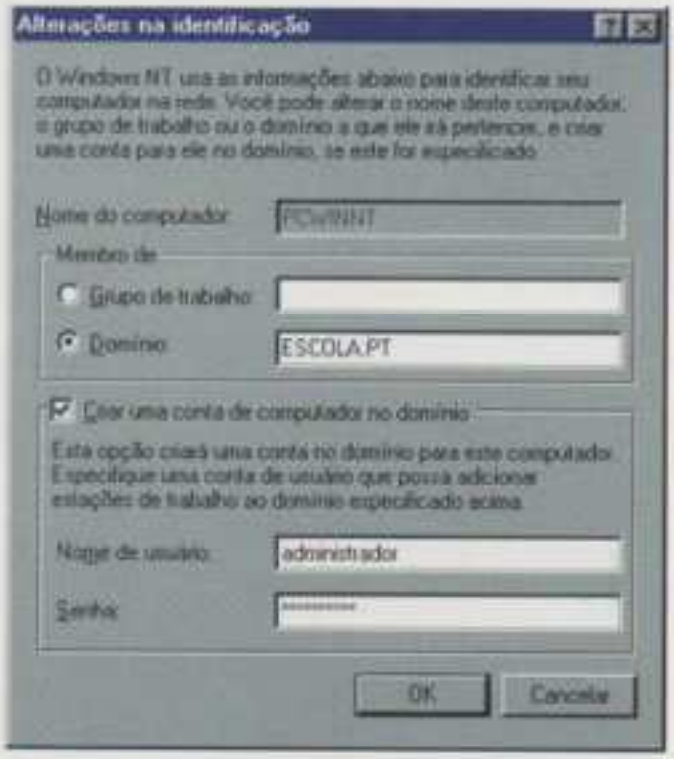

Fig. 3.349 Introdução do nome do domínio e de um utilizador com permissões de administrador do domínio e da respectiva palavra-passe

Se tudo correr bem, surge uma mensagem a dar as boas-vindas ao domínio e tem de se reiniciar o sistema para que as mudanças sejam reconhecidas.

Caso não se consiga aceder ao domínio, deve-se criar uma **conta de computador** no controlador de domínio.

Na janela da figura 3.339 introduz-se o nome NETBIOS e retira-se a opção **Criar uma conta de computador no domínio**. Ao clicar em **OK**, o sistema apresenta uma mensagem a dar as boas-vindas ao domínio.

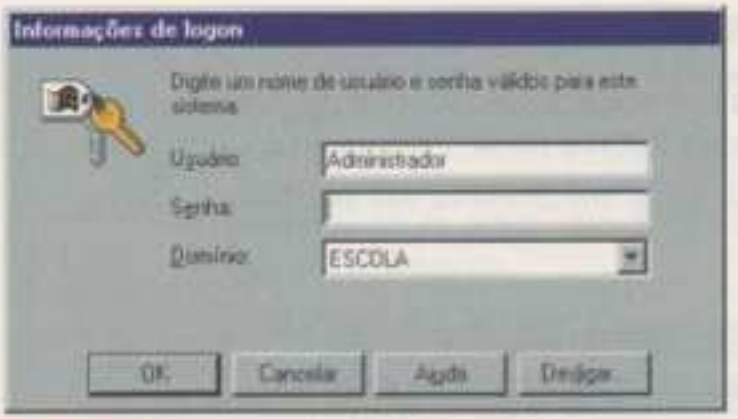

Fig. 3.350 Início de sessão do Windows NT 4.0 no domínio **escola.pt**

Quando o sistema reiniciar, na janela **Iniciar sessão no Windows** deve-se clicar em **Opções**, para se expandir a janela e podermos optar por iniciar a sessão por uma conta existente no controlador de domínio e não por uma conta existente na máquina.

Após a escolha do início de sessão ser realizado por uma conta do domínio **Escola**, vamos introduzir o nome do utilizador **nomealuno** e a respectiva palavra-passe. Não esquecer que este utilizador tem de estar previamente criado no controlador de domínio.

O Windows NT 4.0 Workstation vai validar o utilizador **nomealuno** ao servidor **escola.pt**, inicia a sessão e carrega as configurações pessoais do controlador de domínio.

Ligação de computadores com Windows 9x

A junção de um cliente Windows 9x é quase tão simples como ligar o Windows 2000 e o XP Professional a um controlador de domínio.

Fig. 3.351 Separador **Configuração** das propriedades da rede

Ao contrário do Windows XP, 2000 e NT 40, o Windows 9x não pode juntar-se ao domínio e não requer uma conta de computador. No entanto, continua a ter de se indicar ao cliente, no início de sessão, o utilizador de domínio.

Antes de se iniciar o processo de integração com um domínio no Windows Server 2003, é necessário:

- verificar se a placa de rede está correctamente ligada à rede;
- instalar componentes de rede (cliente para redes Microsoft, placa de rede e protocolo de comunicação);
- verificar se a placa de rede está bem instalada, configurada e activada;
- verificar se o protocolo de comunicação TCP/IP está correctamente instalado e configurado.

Assume-se que o cliente Windows 9x está pronto a ser usado e que já contém os componentes de rede instalados e configurados. As configurações podem ser analisadas no separador **Configurações**, nas propriedades da **Rede**.

Ao contrário de um computador com o Windows NT, Windows 2000 ou XP Professional, uma máquina Windows 9x não pode ser um membro de um domínio. No entanto, o Windows 9x não necessita de pertencer a um domínio específico para que um utilizador faça o *logon* ao domínio.

Antes de se configurar o Windows para fazer o *logon* de utilizadores pertencentes a um domínio, deve-se alterar o nome do grupo de trabalho, para que este seja igual ao nome de domínio. Porquê? Para facilitar a procura dos recursos. Os membros de um domínio também formam um grupo de trabalho (*workgroup*) com o mesmo nome.

Ao colocar-se a máquina com o Windows 9x no mesmo grupo de trabalho em que se encontra o controlador de domínio, os recursos do domínio estarão mais acessíveis. Se o Windows 9x também estiver a correr os componentes de servidor (partilha de ficheiros e impressoras para redes Windows), ele regista-se com os outros servidores no grupo de trabalho.

Para se especificar o grupo de trabalho no Windows 9x, abre-se o separador **Identificação**, nas propriedades da **Rede**, e digita-se o nome do grupo de trabalho no espaço que lá consta. O nome de computador tem que ser único na rede (figura 3.352).

Para se especificar o controlador de domínio de *logon*, volta-se ao separador **Configurações**, nas propriedades da **Rede**, e selecciona-se **Cliente para redes Microsoft** (*Client for Microsoft Networks*) e clica-se em **Propriedades** para abrir a caixa de diálogo da figura 3.353. Neste separador coloca-se um visto na caixa que diz **Iniciar a sessão num domínio do Windows NT** (*Log On to Windows NT Domain*) e digita-se o nome NetBIOS do domínio.

Clicar em **OK** para prosseguir.

Fig. 3.352 Separador **Identificação** das propriedades da rede

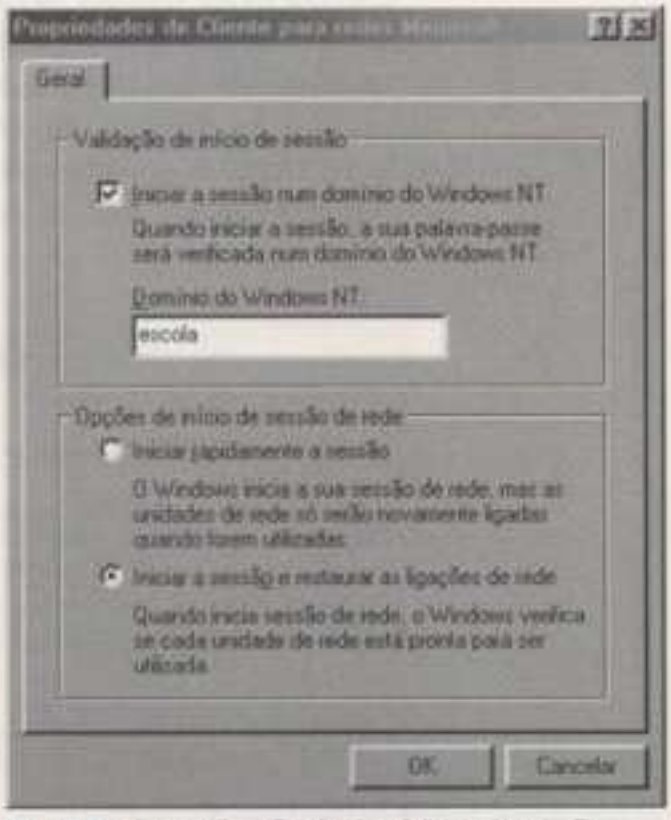

Fig. 3.353 Especificação do domínio na janela **Propriedades de Cliente para redes Microsoft**

O sistema vai solicitar para se reiniciar o computador, para que as mudanças sejam reconhecidas.

Quando o sistema reiniciar, na janela **Introduzir palavra-passe de rede** deve-se introduzir o nome de um utilizador pertencente ao controlador de domínio e a respectiva palavra-passe. Por defeito, na caixa de diálogo-domínio aparece o nome NetBIOS do controlador de domínio introduzido na figura 3.353.

O Windows 9x vai validar o utilizador **nomealuno** no controlador de domínio **escola.pt**. Dá-se início à sessão e são carregadas as políticas do sistema.

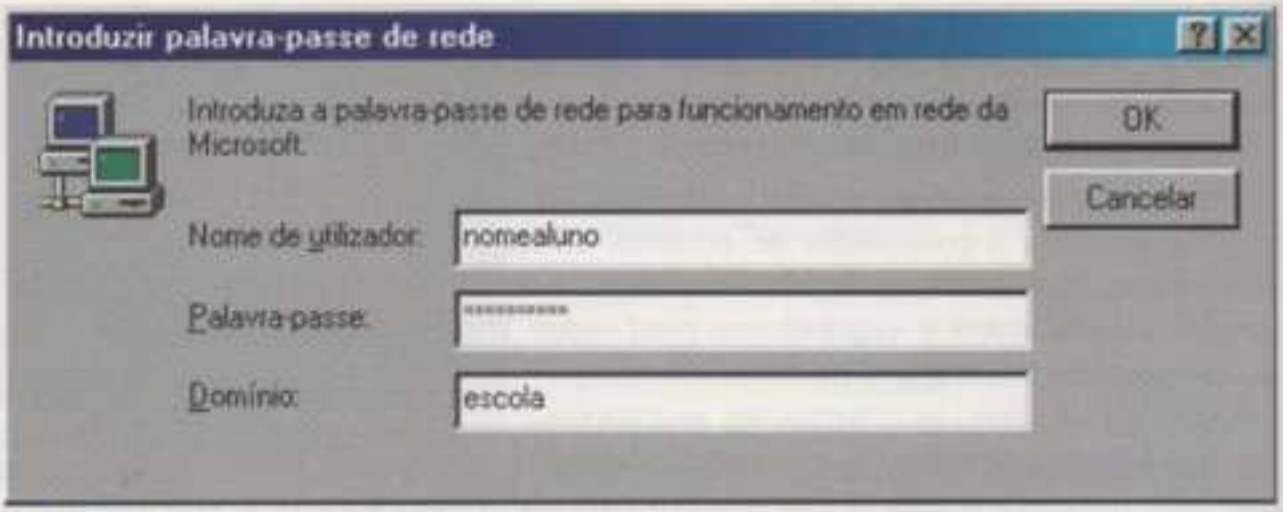

Fig. 3.354 Início de sessão do Windows 98 no domínio **escola**

Ao contrário do que acontece no Windows NT, no 2000 e no XP Professional, o Windows 9x não requer que os utilizadores façam o *logon* no domínio. Pode-se, simplesmente, clicar em **Cancelar**, na janela da figura 3.354, e entra-se localmente e não no controlador de domínio. É bom saber isto, pois, caso haja algum problema com a configuração de acesso ao domínio, pode-se aceder localmente ao computador e, assim, modificarem-se novamente as configurações.

É importante manter sincronizadas a palavra-passe local do Windows e a palavra-passe do domínio. Quando a palavra-passe do Windows e a palavra-passe do domínio são iguais, os utilizadores podem, simultaneamente, fazer o *logon* ao Windows e ao domínio. No entanto, se forem diferentes, os servidores de domínio poderão negar o acesso aos recursos, porque o Windows está a oferecer a palavra-passe errada.

Em caso de dificuldade em realizar o início de sessão (*logon*) ao controlador de domínio a partir do Windows 9x, deve-se verificar os seguintes pontos:

- verificar se estão instalados todos os pacotes de segurança recomendados para o sistema-cliente;
- instalar o cliente DS a partir do CD-ROM do Windows 2000. O DSCLIENT.EXE encontra-se na directoria \CLIENTS\WIN9X. Este ficheiro não se encontra no CD-ROM do Windows Server 2003 e é um ficheiro de CAB de 3 MB de auto-extracção. A instalação é um processo contínuo de "clicar em **Seguinte** para continuar" e de reiniciar.

O DSCLIENT faz a actualização de várias bibliotecas que atingem o início de secção (*logon*) e a autenticação. O cliente DS para Windows 9x requer Internet Explorer 4.01 ou posterior.

- O Windows 95/98 não se regista com o DNS Activo, por isso, deve colocar-se um servidor WINS na rede. Os clientes Windows e os controladores de domínio devem estar configurados para poder usá-lo.
- Os controladores de domínio *Active Directory* usam o DNS para a resolução de nomes. Convém criar entradas estáticas no DNS para os clientes Windows 9x. Isto também significa que os sistemas Windows 9x deverão manter sempre os mesmos endereços. Por isso, deve utilizar-se endereçamento estático ou reservar no servidor de DCHP um endereço fixo para cada cliente Windows 9x.
- Verificar se o nome utilizado para o domínio foi o nome NetBIOS, isto é, se foi colocado o nome **escola** em vez de **escola.pt**.

EXERCÍCIOS PROPOSTOS

1. Indique os nomes das versões disponíveis na família do Windows 2000 Server e do Windows Server 2003. Mencione, ainda, as principais diferenças existentes entre elas.
2. Indique e explique cinco áreas de actuação de servidores com o Windows 2000 Server e com o Windows Server 2003.
3. Que tipo de papel podem assumir os servidores baseados em Windows 2000 e em Server 2003?
4. Indique dois processos para proceder à identificação do papel de um servidor com o Windows Server 2003.
5. Quais são as diferenças entre um servidor, com o Windows Server 2003, configurado como controlador de domínio (*Domain Controllers*), *Member Server* e *Standalone Server*.
6. Indique e explique quais são os processos de licenciamento de servidores com o Windows Server 2003.
7. Qual é a função da **Consola de gestão da Microsoft** (MMC – *Microsoft Management Console*) no Windows Server 2003?
8. Indique e explique qual o tipo de sistema de formatação de ficheiros que deve ser utilizado para a instalação do Windows 2000 Server e do Server 2003.
9. O que é que não pode ser instalado no Windows 2000 Server e no Server 2003, caso não exista um volume NTFS 5?
10. Numa instalação do Windows Server 2003, mencione as diferenças entre uma instalação assistida por computador (não automática) e uma instalação não assistida (instalação automática – *unattended install*).
11. O que é necessário realizar para converter volumes que se encontram formatados em FAT32 para NTFS?
12. Indique os requisitos mínimos e recomendados de *hardware* para se instalar o Windows 2000 Server e o Server 2003.
13. Qual é a função da lista **HCL** fornecida pela Microsoft?
14. Especifique os modos de arranque para iniciar a instalação do Windows Server 2003.
15. Pretende-se iniciar a instalação do Windows Server 2003, que se encontra num CD-ROM, num computador. Explique como configurar o BIOS do computador para que o arranque da instalação seja feito pelo CD-ROM.
16. Explique que cuidados se devem ter na escolha da palavra-passe de um utilizador no Windows Server 2003.

17. Explique se o endereço IP atribuído à placa de rede de um servidor com o Windows Server 2003 deve ser dinâmico.

18. No final da instalação do Windows Server 2003, quais os passos a verificar para ver se os *drivers* estão correctamente instalados?

19. Após a instalação do Windows Server 2003 num servidor, quantos dias temos para proceder à activação do sistema operativo?

20. No final da fase da instalação do Windows 2000 Server / Windows Server 2003, estamos preparados para funcionar como DC? Justifique a resposta.

21. Qual é o nome do executável que se deve utilizar para promover o Windows 2000 Server, o 2003 e o controlador de domínio (DC)?

22. Indique e explique todos os passos na promoção do Windows 2000 Server / Server 2003 a *Domain Controller* (DC) de um domínio. Para tal, considere que o Windows Server já se encontra instalado.

23. Qual é o número máximo de caracteres que o nome NetBIOS suporta?

24. Para despromover o Windows Server 2003 de controlador de domínio (DC) para *Standalone Server*, é necessário reinstalar o sistema operativo?

25. Mencione todos os passos na despromoção do Windows 2000 Server / Server 2003 a funcionar como *Domain Controller* (DC) de um domínio para Standalone Server.

26. Mencione todos os passos necessários para configurar um servidor com o Windows Server 2003 – que se encontra a funcionar como *Standalone Server* – para que passe a operar como *Member Server*.

27. O que pode um administrador de um servidor configurado como *Member Server* disponibilizar na rede?

28. Indique e explique todos os passos na despromoção do Windows Server 2003 de *Member Server* a *Standalone Server*.

29. Indique como configurar um cliente Windows como cliente DNS.

30. Considere que já existe um computador com o Windows Server 2003 na rede a funcionar como DC. Explique como se deve proceder para adicionar um novo servidor Windows Server 2003 que pertença ao controlador de domínio existente. Indique, ainda, quais são as principais vantagens de se proceder à configuração solicitada.

31. Quais são as ferramentas de administração do Windows Server 2003 que estão disponíveis no **Assistente para configurar o servidor** (*Configure Your Server Wizard*)? Este assistente pode ser lançado a partir das **Ferramentas administrativas** (*Administrative tools*)?

32. Mencione dois modos diferentes de partilhar ficheiros e pastas no Windows Server 2003.

33. Especifique como atribuir permissões de leitura ao utilizador "geral" a uma pasta partilhada num servidor Windows Server 2003 designada **Documentos**. Considera que o utilizador "geral" já se encontra criado.

34. Explique como partilhar uma impressora existente num servidor com o Windows Server 2003.

35. Quais são as principais vantagens da implementação e utilização do *Active Directory* (AD)?

36. Como se chama, no Windows Server 2003, a ferramenta que possibilita a gestão de utilizadores e grupos de utilizadores no *Active Directory* (AD)?

37. Indique como criar um grupo designado **turma** e um utilizador designado **alunos** no *Active Directory* (AD). Associe o utilizador criado ao grupo **turma**.

38. Explique como alterar a palavra-passe de um utilizador pertencente a um controlador de domínio, no Windows Server 2003.

39. Mencione as principais diferenças entre grupos do tipo universal, global e local de domínio.

40. O que é que distingue um domínio de um *Workgroup*?

41. Qual é a função das unidades organizacionais num *Active Directory* (AD)? Indique como criar uma unidade organizacional num AD.

42. Indique como implementar uma protecção de modo que num servidor Windows Server 2003 os utilizadores, ao fazerem *login* ao servidor, sejam bloqueados, caso o número de tentativas consecutivas falhadas seja superior a 5. A conta só poderá ser desbloqueada por ordem do administrador do sistema.

43. Explique as diferenças entre perfis obrigatórios ou mandatórios, perfis ambulantes e perfis locais.

44. Indique a localização, no disco rígido, de um servidor Windows Server 2003 dos perfis dos utilizadores.

45. Qual é a vantagem da implementação das políticas de grupo num domínio?

46. Qual a ferramenta de administração para se criar uma política de grupo local?

47. Mencione como implementar uma política de grupo num domínio, para que os utilizadores pertencentes a esta política não tenham acesso ao **Painel de controlo** e aos ícones existentes no ambiente de trabalho do Windows. Indique, ainda, em que sistemas operativos da Microsoft é possível implementar estas políticas de grupo.

48. Qual a função da ferramenta **POLEDIT.EXE**?

49. Explique como associar um *script* a um utilizador pertencente a um *Active Directory*.

50. Comente a funcionalidade de cada uma dos seguintes *scripts*:

a)
```
net use * \\nome_server\fotos /persistent:no
pause
```

b)
```
net use /delete f:
net use /delete g:
net time \\server1 \\SERVER1 /set /y
net use f: \\server1\vol1
net use g: \\server1\cdrom
```

51. Mencione as funcionalidades da consola **Gestão de computadores** existente nas **Ferramentas administrativas** do Windows Server 2003.

52. Explique como proceder à paragem de um serviço no Windows Server 2003.

53. Indique e explique quatro processos de resolução de nomes existentes no Windows Server 2003.

54. Indique duas das diferenças entre o serviço DNS e o DDNS.

55. Indique e explique como instalar o servidor de DHCP num servidor Windows Server 2003. Explique, ainda, como criar um âmbito (*scope*) no servidor de DHCP, para que este atribua endereços aos clientes de DHCP à seguinte gama de endereço:

192.168.0.50 a **192.168.0.150** – máscara de rede **255.255.255.0**.
O âmbito (*scope*) deve ainda excluir a atribuição do endereço **192.168.0.100**!

56. Indique o nome da ferramenta para adicionar novas licenças no Windows Server 2003.

57. Qual é o nome da ferramenta disponibilizada, no Windows Server 2003, para realizar cópias de segurança?

58. Explique como realizar cópias de segurança do volume onde está instalado o Windows Server 2003, para uma pasta partilhada na rede.

59. Que ferramenta(s) existe(m), no Windows Server 2003, para se realizar gestão local e/ou remota dos discos?

60. Quantas partições primárias se podem realizar num disco convertido em *Basic Disk*?

61. Mencione como criar uma nova partição primária de 1 GB no espaço livre do disco. O formato utilizado deve ser NTFS.

62. Indique como se pode alterar uma letra atribuída a um volume.

63. Qual é o espaço mínimo livre que o disco deve ter e em que zona do disco deve existir esse espaço livre, para que se possa converter um disco de *Basic Disk* para *Dynamic Disk*?

64. Indique como converter um disco *Basic Disk* em *Dynamic Disk*.

65. Quais são as vantagem e desvantagens da utilização do *mirror* em discos?

66. Quais são as condições necessárias para que se possa realizar *mirror* de discos no Windows Server 2003?

67. Quais são as melhorias que se obtêm na utilização de um volume *stripe set* sem paridade e na de um *volume striped set* com paridade em discos? Quais são os inconvenientes de cada um deles?

68. Quantos discos são necessários para se criar um volume *stripe set* sem paridade e um *volume stripe set* com paridade?

69. Explique como verificar o estado de um disco e como realizar a respectiva desfragmentação. Explique a função de cada uma das operações efectuadas.

70. Indique o nome de uma ferramenta disponível no Windows Server 2003 para realizar auditoria ao sistema.

71. Mencione as vantagens da utilização de uma UPS na alimentação de um sistema informático e, também, as principais vantagens da utilização de uma UPS do tipo *Online* relativamente às UPS do tipo *Offline*.

72. Indique as operações necessárias para se adicionar uma máquina a um domínio existente num servidor com o Windows Server 2003, nos seguintes sistemas operativos:

a) Windows 9x

b) Windows NT 4.0

c) Windows 2000 Professional

d) Windows XP Professional