Windows Server 2003

# Capítulo 1
# Introdução ao Windows Server 2003

***Bem-vindo à nova família de Servidores da Microsoft!***
***Durante este curso você aprenderá sobre as novas tecnologias 2003 e como aplicá-las.***

As novas características do Windows Server 2003 fazem com que ele seja, até o momento, o sistema operacional mais estável, robusto, escalável e principalmente mais preparado para melhorar o desempenho e os serviços de servidores que executam diferentes funções: Aplicativos, Serviços da Web, Serviços de Diretório, Serviços de Arquivos e Impressão e Serviços de Infra-estrutura. A otimização de todas essas características, sem dúvida, também faz da família Windows Server 2003 a plataforma mais recomendável para as empresas, reduzindo de forma notável aspectos como o TCO (Custo total de propriedade).

## Um pouco de história

Desde o lançamento dos sistemas operacionais de redes, passando pelo Windows NT, os sistemas foram se aperfeiçoando à medida que foram surgindo novas necessidades nas empresas. Desde as conhecidas diferenças introduzidas pelo Windows 2000 ao seu antecessor, o Windows NT 4.0, nós agora conseguimos chegar a um sistema operacional ideal para atender às exigências do mercado de informática, onde já foram implementados grandes aprimoramentos em relação ao seu antecessor, o Windows 2000.

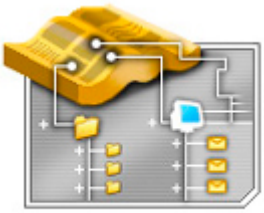
O Windows Server 2003 baseia-se nas experiências do mercado consumidor de informática e, por isso, encontramos nele diversos recursos que procurávamos, sempre nos perguntando: é possível fazer isso? .... e aquilo? Essas perguntas que ficavam sem respostas a partir de agora podem ser atendidas com o Windows Server 2003.

Neste módulo, faremos uma introdução das novas características e funcionalidades da família de servidores Windows Server 2003. Ao finalizar este capítulo, você deverá ter os conhecimentos necessários para identificar funcionalidades, características e requisitos dos diferentes sistemas operacionais dessa família.

## 1. Novas Características

*Armazenamento*

*Active Directory*



*Instalação*

*Serviços Web*

### 1.1. Recuperação Automática do Sistema

Essa nova ferramenta permite recuperar o estado anterior do sistema operacional. Como funciona? Ela utiliza um disquete com informações sobre a configuração e um conjunto de backup. Para iniciar o processo de recuperação, você precisa ter esse disquete, o conjunto de backup da partição do sistema e o CD-ROM de instalação do Windows Server 2003.


© 2003 Microsoft Corporation. Todos os direitos reservados.

Para esse processo, é preciso ter o disquete e a mídia de ASR que contém os arquivos de backup. O sistema operacional será restaurado para o mesmo estado em que estava no momento do Backup da ASR, permitindo a inicialização do seu sistema.

Para criar um conjunto de ASR, visite o seguinte link no TechNet (inglês):

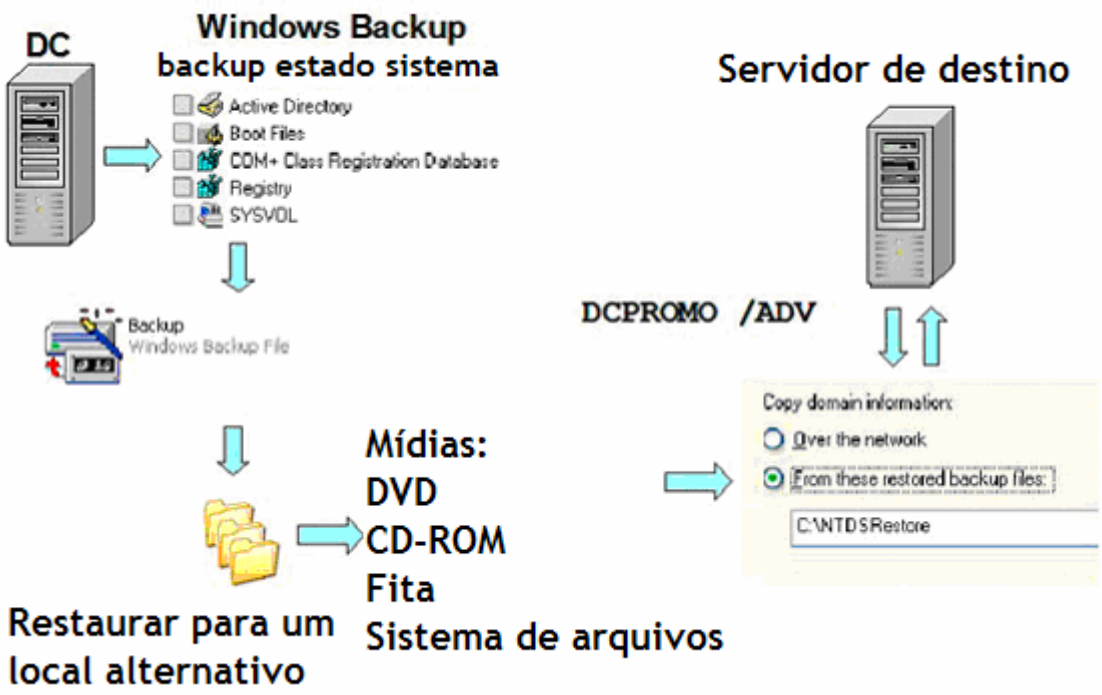
http://www.microsoft.com/resources/documentation/WindowsServ/2003/standard/proddocs/en-us/Default.asp?url=/resources/documentation/WindowsServ/2003/standard/proddocs/en-us/recovery_automatic_sr.asp

**Nota:** Durante o processo de Restauração, a Partição do Sistema será formatada eliminando todos os dados, e o backup será restaurado ao seu local de origem. Todos os arquivos modificados após o momento do backup serão perdidos.

## 1.2. Infra-estrutura Instantânea (Duplicação da Mídia do serviço de diretório)

***Essa nova e incrível característica permite solucionar o seguinte problema:***

Cenário com duas localizações: um Controlador de Domínio na localidade A e a necessidade de instalar um Controlador de Domínio na localidade B. A princípio isso não seria um problema, mas se a rede WAN que une os dois pontos for de 64 Kbps e o diretório inicial contiver 20.000 ou mais objetos, surge uma dificuldade: o tempo necessário para a duplicação inicial, somado ao fato de que, durante esse processo, obviamente não será possível usar a conexão normalmente. Solução: no Windows Server 2003, pode-se instalar o Controlador de Domínio da localidade B a partir de um Backup do Controlador existente na localidade A. Esse processo será descrito detalhadamente no Capítulo 4.



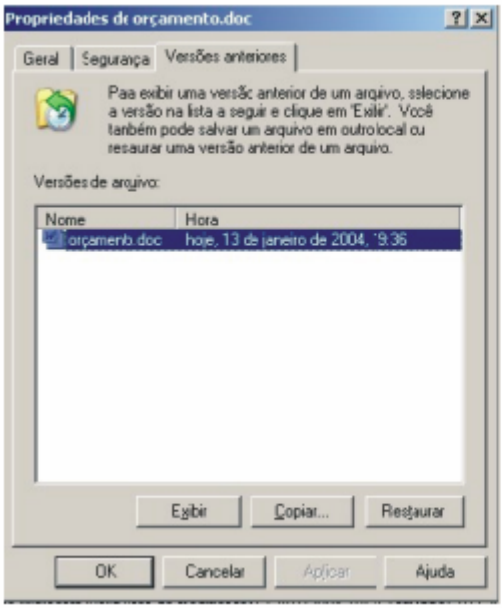


© 2003 Microsoft Corporation. Todos os direitos reservados.

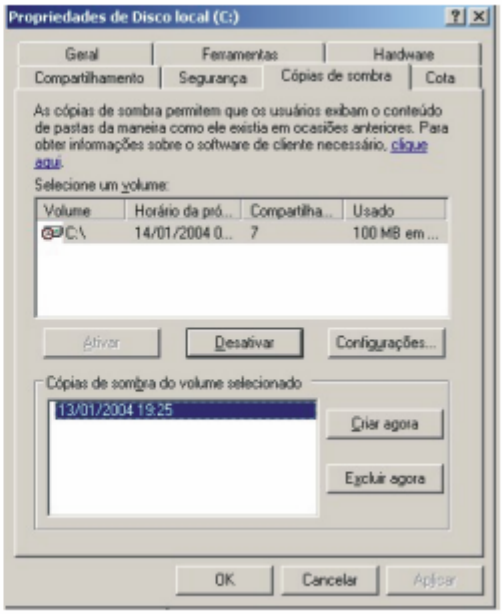
### 1.3. Cópia de Sombra do Volume

Esse novo serviço ajuda a recuperar arquivos excluídos por engano. Para isso, o serviço de Cópia de Sombra salva versões anteriores dos arquivos para recuperação posterior, eliminando a necessidade de recorrer a restauração do backup. Como funciona? Ele utiliza um cache em disco para o armazenamento de versões de arquivos, que podem ser recuperadas quando necessária a partir dessa cópia.

- **Cliente**




- **Servidor**




Se quiser obter mais informações sobre esse assunto, recomendamos que você consulte o seguinte link do TechNet (inglês):

http://www.microsoft.com/resources/documentation/WindowsServ/2003/standard/proddocs/en-us/topnode_snapshot.asp?frame=true

### 1.4. Sistema de Arquivos Criptografados (EFS)

A nova funcionalidade EFS no Windows Server 2003 permite criptografar o sistema de arquivos de forma segura e também possibilita que os outros usuários tenham acesso a esses arquivos. Essa função é muito importante porque, muito embora em diversas ocasiões seja necessário proteger determinados arquivos, também é muito importante poder compartilhá-los entre os usuários. O sistema de criptografia que utiliza o EFS é uma combinação de dois métodos, de criptografia assimétrica e PKI (Public Key Infrastructure), pontos que serão explicados detalhadamente no capítulo 8 "Segurança".

### 1.5. Reversão de Driver

Esse é um novo utilitário para gerenciamento de versões em drivers de dispositivos e permite voltar à versão anterior do driver se o novo causar problemas. Também foram incluídos aprimoramentos na verificação do funcionamento dos drivers com a nova versão do "Driver Verifier V2" e firmware de drivers.

Se quiser obter mais informações sobre esse assunto, recomendamos que você consulte o seguinte link do TechNet (Inglês):


© 2003 Microsoft Corporation. Todos os direitos reservados.

http://www.microsoft.com/resources/documentation/WindowsServ/2003/standard/proddocs/en-us/devmgr_reinstall_old_driver.asp?frame=true

## 1.6. Active Directory

***Vamos analisar as novas funções do Serviço de Diretório oferecido pelo Windows Server 2003.***

### *ADMT versão 2.0*

Agora ficou fácil migrar para o Active Directory utilizando os aprimoramentos da Active Directory Migration Tool (ADMT). A ADMT 2.0 permite migrar senhas do Microsoft Windows NT® 4.0 para o Windows 2000 e o Windows Server 2003, ou do Windows 2000 para domínios do Windows Server 2003.

### *Renomeação de Domínios*

Esse é o suporte para modificar nomes do Domain Name System (DNS) e/ou do NetBIOS de domínios existentes em uma floresta conservando toda a estrutura do Diretório. Em cenários de reestruturação de domínios, ele proporciona uma grande flexibilidade.

### *Esquema*

A flexibilidade do Active Directory agora permite a desativação de atributos e a definição de classes no esquema do Active Directory. Também foi adicionada uma nova funcionalidade que permite excluir o esquema.

### *Diretiva de Grupo*

Junto com o Windows Server 2003, a Microsoft lançou uma ferramenta para administração de GPOs, o Group Policy Management Console (GPMC), que permite administrar múltiplos domínios, ativar e desativar diretivas e arrastar e soltar nas ferramentas. Também inclui a funcionalidade de Backup, Restauração e cópia de diretivas e fornece uma ferramenta de Relatórios para analisar a utilização das diretivas. Você observará aprimoramentos expressivos nas diretivas e muitas novas opções de configuração para administração centralizada.

### *Relações de confiança*

O Windows Server 2003 também traz aprimoramentos significativos no gerenciamento das relações de confiança entre florestas. O recurso **"Autenticação entre Florestas"** permite que um usuário da floresta acesse de forma segura os recursos em outras florestas, utilizando *Kerberos* ou NTLM, sem sacrificar os benefícios do "Single sing-on" e facilitando a administração. Ele também permite selecionar facilmente usuários e grupos para incluí-los em grupos locais de outras florestas, mantendo a segurança e os SID de cada objeto, mesmo em florestas diferentes.

### *Diretivas de Restrição de Software*

Através dessas diretivas, é possível proteger os ambientes de produtos de software não autorizados, especificando quais softwares não estão autorizados. Também é possível estabelecer exceções criando regras específicas.

### *Duplicação de membros nos grupos*

Anteriormente os membros de um grupo eram um atributo desse grupo, portanto, quando durante a replicação o grupo era modificado nos dois Controladores de Domínio diferentes, o resultado era a duplicação da última modificação. Portanto, se fossem acrescentados dois usuários aos grupos, um não era adicionado, mas havia uma limitação em relação à quantidade de usuários por grupo (Limitação de atributo), no máximo 5000. A partir do Windows Server 2003, cada usuário do grupo passou a ser um atributo diferente, o que elimina a limitação de 5000 usuários e soluciona os problemas de duplicação.


© 2003 Microsoft Corporation. Todos os direitos reservados.

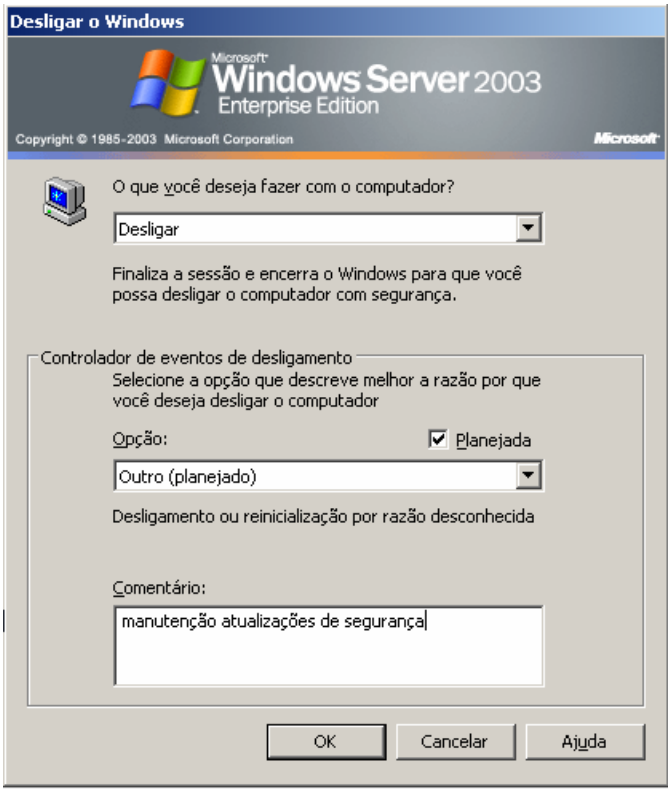
### *Gerenciamento de Sites*

O gerenciamento de sites inclui um novo algoritmo do Gerador de Topologia entre Sites (ISTG), aumentando a limitação do número máximo de sites de 500 para 5000 sites (comprovado em laboratório 3000).

**Nota:** Todas essas características são explicadas em mais detalhes no Capítulo 4 "Active Directory".

## 1.7. Reiniciar “Controlador de eventos” do Reason Collector

O Controlador de Eventos é uma nova ferramenta que permite reunir para análises futuras os motivos pelo qual um Servidor foi reiniciado, parado ou desligado por falta de energia. Neste caso, a ferramenta perguntará, no primeiro login, o motivo das falhas para registrá-lo.




## 1.8. RIS "Serviços de Instalação Remota"

Aprimoramentos no suporte para instalação:

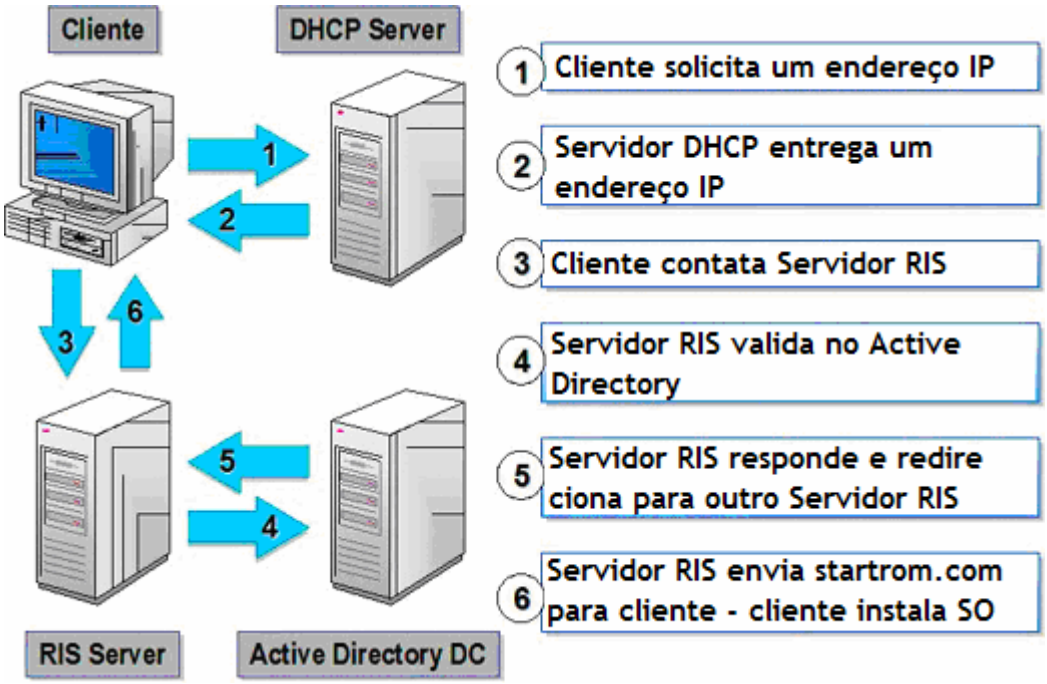
- Todas as versões do Windows 2000 (incluindo Server e Advanced Server)
- Windows XP Professional
- Todas as versões do Windows Server 2003

Todas as versões do Windows XP de 64 bits e Windows Server 2003

Se quiser obter mais informações sobre esse assunto, recomendamos que você consulte o seguinte link do TechNet (inglês):


© 2003 Microsoft Corporation. Todos os direitos reservados.

http://www.microsoft.com/resources/documentation/WindowsServ/2003/standard/proddocs/en-us/sag_RIS_Default_topnode.asp?frame=true




## 1.9. IIS 6.0 - Internet Information Services 6.0

Este componente do sistema operacional sofreu modificações significativas com relação à versão anterior que estão detalhadas a seguir:

### *Arquitetura de Processos Tolerante a Falhas*

O IIS 6.0 isola os sites da Web e aplicativos em unidades chamadas "Classes de Aplicativos". As Classes de Aplicativos fornecem uma forma conveniente de administrar os sites na Web e aplicativos, e aumentam a confiabilidade, já que erros em uma Classe de Aplicativos não provocam erros em outras classes ou falhas no servidor.

### *Health Monitor*

O IIS 6.0 verifica periodicamente o status das Classes de Aplicativos reiniciando-as automaticamente em caso de falhas nos sites da Web ou em aplicativos nessa Classe de Aplicativos, aumentando a disponibilidade. Ele também protege o servidor e outros aplicativos, desabilitando automaticamente sites na Web e aplicativos, se falharem em um curto período de tempo.

### *Novo modo driver kernel, HTTP.sys*

O Windows Server 2003 introduz um novo driver kernel, protocolo HTTP (HTTP.sys), melhorando o desempenho e a escalabilidade. Esse driver foi desenvolvido especificamente para melhorar o tempo de resposta do Servidor da Web.

### *Integração com Aplicativos*

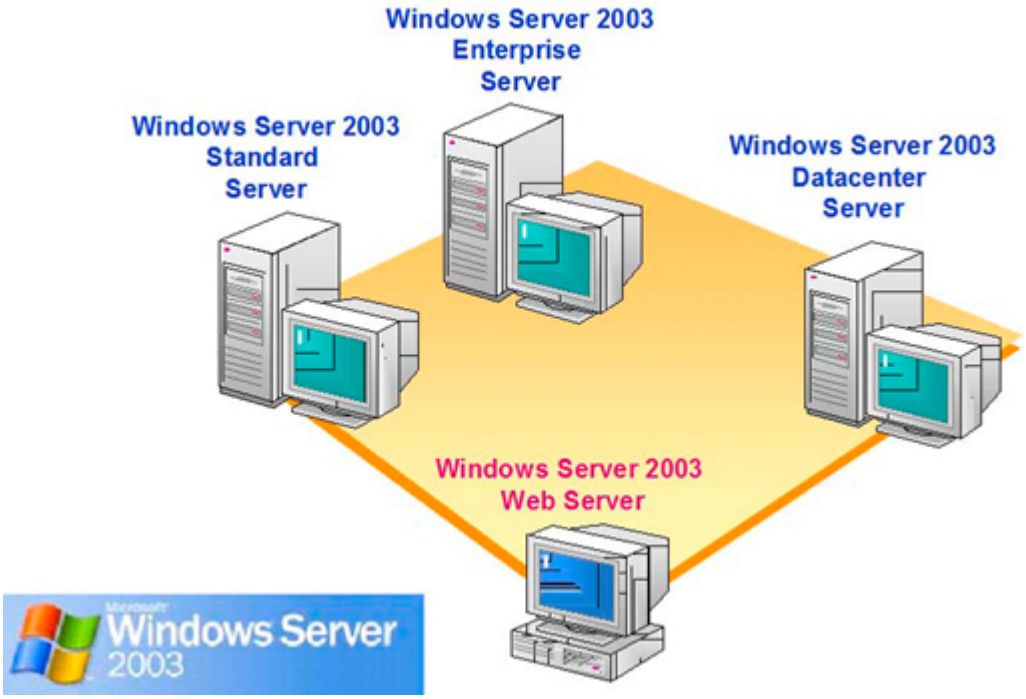

© 2003 Microsoft Corporation. Todos os direitos reservados.

O IIS 6.0 oferece integração com o ASP.NET, o Microsoft .NET Framework e os Serviços da Web em XML, tornando-se a plataforma especialmente projetada para aplicações .Net.

***Segurança***

O IIS 6.0 é **"Locked-down server By default"**, em outras palavras, está protegido na sua instalação, exigindo que o administrador habilite as funções especiais e necessárias para executar o site na Web. Sem isso, ele só pode oferecer conteúdo estático e extensões dinâmicas desabilitadas. Isso faz com que o IIS 6.0 seja o servidor de Web mais seguro.

## 1.10. Versões





© 2003 Microsoft Corporation. Todos os direitos reservados.

O Windows Server 2003 apresenta quatro versões com funcionalidades diferentes que estão descritas no quadro seguinte:

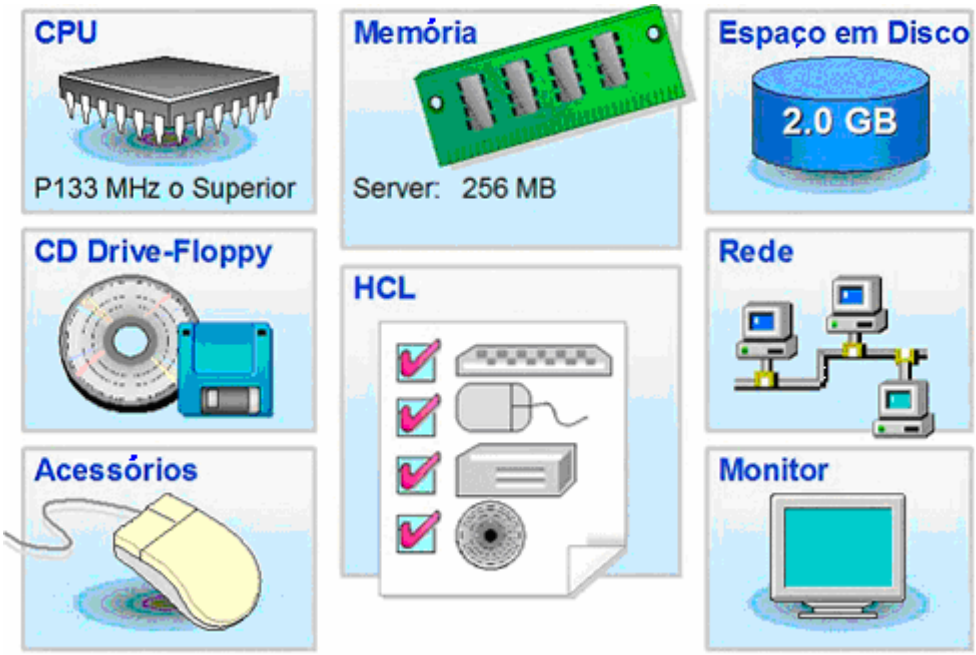
| | |
|---|---|
| Microsoft Windows Server 2003 Web Edition | Para serviços da Web e host, esta versão oferece uma plataforma para desenvolvimento e instalação rápida de serviços e aplicativos da Web. Apenas na versão OEM |
| Microsoft Windows Server 2003 Standard Edition | Para serviços de administração de redes, esta versão do Windows Server 2003 é ideal para servidores de arquivos e impressoras, servidores da Web e grupos de trabalho. Também oferece acesso remoto a redes. |
| Microsoft Windows Server 2003 Enterprise Edition | Contém todas as características do Windows Server 2003 Standard e fornece maior escalabilidade e disponibilidade. Essa versão é ideal para servidores utilizados em grandes redes e para bancos de dados com uso intensivo. |
| Microsoft Windows Server 2003 Datacenter Edition | Possui todas as características do Windows Server 2003 Enterprise Edition, além de suporte para mais memória e mais CPU por computador. Esta versão é ideal para uso de depósitos de dados de grande porte, processamento on-line, transações (OLTP) e projetos de consolidação de servidores. |

O suporte de memória, processadores e funcionalidade varia conforme a versão. É por isso que você deve considerar as suas necessidades ao escolher o sistema operacional.

| - | *Server* | *Web Server* | *Enterprise Server* | *Datacenter* |
|---|---|---|---|---|
| CPU / RAM | 2 CPU<br>4 GB | 2 CPU<br>2GB | 8 CPU<br>32 GB (x86)<br>64 GB (64 bits) | 8-64 CPU<br>64 GB (x86)<br>512 GB (64 bits) |
| Recursos | **Novos Recursos**<br>•NLBS<br>• Firewall Pessoal | **Pode executar:**<br>•IIS 6.0<br>•NLBS<br>•DNS, DHCP, WINS<br><br>**Limitações:**<br>•Sem DC Promo<br>•Sem aplicações<br>•Sem Apl TS<br>•Modo | **Todos os recursos do Standard e também:**<br>•Cluster de 8 nós<br>•Versão de 64 bits | **Todos os recursos do Enterprise e também:**<br>•Programa Datacenter<br>-Datacenter HCL<br>-Manutenção<br>•Suporte a múltiplas instâncias |


© 2003 Microsoft Corporation. Todos os direitos reservados.

## 1.11. Requisitos

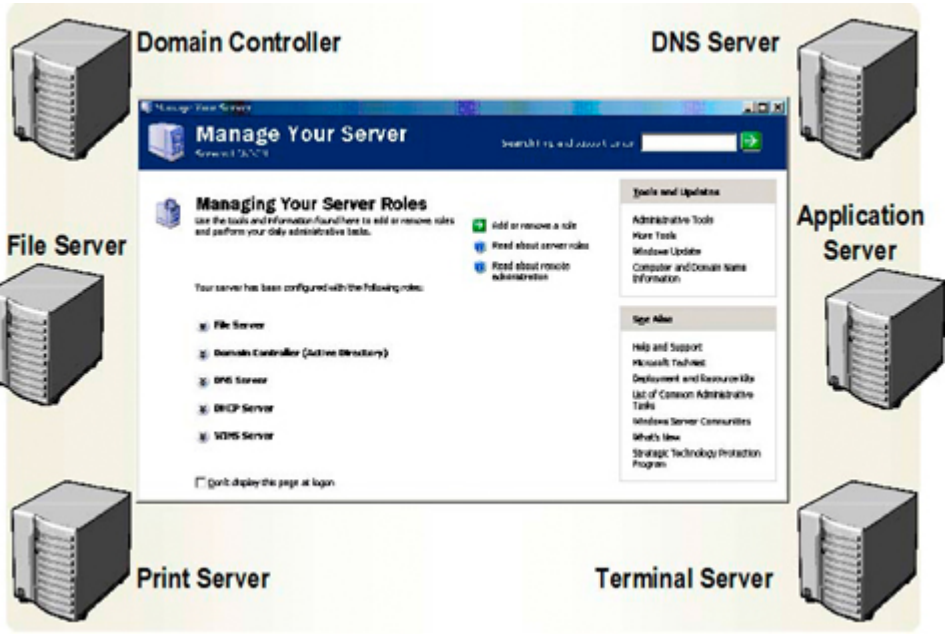



No quadro a seguir, temos os requisitos mínimos e recomendados para cada versão do Windows Server 2003.

| Requisitos de Sistema do Windows Server 2003 | | | | |
|---|---|---|---|---|
| **Requisitos** | **Standard Edition** | **Enterprise Edition** | **Datacenter Edition** | **Web Edition** |
| **Velocidade mínima da CPU** | 133 MHz | 133 MHz para arquitetura x86<br><br>733 MHz para arquitetura Itanium | 400 MHz para arquitetura x86<br><br>733 MHz para arquitetura Itanium | 133 MHz |
| **Velocidade recomendada da CPU** | 550 MHz | 733 MHz | 733 MHz | 550 MHz |
| **Mínimo de RAM** | 128 MB | 128 MB | 512 MB | 128 MB |
| **RAM Recomendável** | 256 MB | 256 MB | 1 GB | 256 MB |
| **Máximo de RAM** | 4 GB | 32 Gb para arquitetura x86<br><br>512 MHz para arquitetura Itanium | 64 MHz para arquitetura x86<br><br>512 MHz para arquitetura Itanium | 2 GB |
| **Suporte de Multiprocessador SMP** | Até 4 | Até 8 | Mínimo de 8 necessários<br><br>Máximo de 64 | Até 2 |
| **Espaço Mínimo no Disco** | 1,5 GB | 1,5 Gb para arquitetura x86<br><br>2,0 Gb para arquitetura Itanium | 1,5 Gb para arquitetura x86<br><br>2,0 Gb para arquitetura Itanium | 1,5 GB |


© 2003 Microsoft Corporation. Todos os direitos reservados.

## 2. Funcionalidades




Os servidores desempenham vários papéis no ambiente cliente/servidor de uma rede. Alguns servidores são configurados para fornecer autenticação e outros para outros usos. Muitos também fornecem serviços de rede que permitem que os usuários se comuniquem ou localizem outros servidores e recursos na rede. Como administrador de sistemas, você deverá conhecer os principais tipos de servidores e que funções que eles realizam na sua rede.

### 2.1. Controlador de Domínio (Active Directory)

Os controladores de domínio armazenam os dados do diretório e gerenciam a comunicação entre os usuários e os domínios, incluindo processos de conexão do usuário, autenticação e pesquisas de diretórios. Quando você instala o Active Directory em um computador que executa o Windows Server 2003, o computador passa a ser um Controlador de domínio.

**Nota:** Em uma rede do Windows Server 2003, todos os servidores no domínio que não sejam Controladores de Domínio são chamados de Servidor Membro. Os servidores não associados a um domínio são chamados de Servidor de Grupo de Trabalho.

### 2.2. Servidor de Arquivos

Um Servidor de Arquivos oferece uma localização central na sua rede onde é possível armazenar e compartilhar os arquivos com usuários através da sua rede. Quando os usuários precisam de um arquivo importante, como um plano de projeto, é possível acessar o arquivo no Servidor de Arquivos, em vez de ter que transferi-lo entre seus vários computadores.

### 2.3. Servidor de Impressão

Um Servidor de Impressão proporciona uma localização central na sua rede, onde os usuários podem imprimir. O Servidor de Impressão oferece aos clientes drivers atualizados de impressora e gerencia a fila de impressão e a segurança.


© 2003 Microsoft Corporation. Todos os direitos reservados.

## 2.4. Servidor de DNS

O Domain Name System (DNS) é um serviço padrão da Internet e de TCP/IP. O serviço de DNS permite que os computadores clientes coloquem em sua rede e solucionem nomes de domínio DNS. Um computador configurado para fornecer serviços de DNS em uma rede é um servidor de DNS, que é necessário para colocar em funcionamento o Active Directory.

## 2.5. Servidor de Aplicativos

Um Servidor de Aplicativos fornece a infra-estrutura e os serviços de aplicativos em um sistema. Os servidores típicos de aplicações incluem os seguintes serviços:

- O grupo de recursos (por exemplo, grupo de conexões de banco de dados e grupo de objetos)
- Administração de transações distribuídas
- Comunicação assíncrona, normalmente fila de mensagens
- Um modelo de objetos de ativação just-in-time
- XML (Extensible Markup Language) Automático e Interfaces de Serviços Web para acessar objetos de negócios
- Serviços de detecção de falha e funcionamento de aplicativos com segurança integrada

O Microsoft Internet Information Services (IIS) fornece as ferramentas e as características necessárias para controlar facilmente um Servidor da Web seguro. Se planejar criar um host de File Transfer Protocol (FTP) da Web e Sites com o IIS, configure o Servidor como Servidor de Aplicativos.

## 2.6. Terminal Server

Um Terminal Server oferece aos computadores remotos, acesso a programas baseados no Windows que funcionam em Windows Server 2003 Standard Edition, Windows Server 2003 Enterprise Edition ou Windows Server 2003 Datacenter Edition. Com um Terminal Server, você instala um aplicativo em um único ponto e em um único servidor. Os múltiplos usuários poderão, então, ter acesso ao aplicativo sem precisar instalá-lo em seus computadores. Os usuários podem executar programas, exceto arquivos, e utilizar os recursos da rede de um local remoto, como se eles estivessem instalados em seu próprio computador. Nós veremos esse assunto em mais detalhes no capítulo 6.

## 2.7. A ferramenta *Gerenciar o Servidor*

Quando o Windows Server 2003 é instalado e um usuário faz o logon pela primeira vez, a ferramenta *Gerenciar o Servidor* é executada automaticamente. Você utiliza essa ferramenta para adicionar ou remover Funções dos Servidores. Quando adiciona uma função de servidor a um computador, a ferramenta *Gerenciar o Servidor* adiciona essa função à lista de funções disponíveis. Depois que a função de servidor é adicionada à lista, você poderá utilizar vários assistentes que o ajudarão a administrar funções específicas de servidor. A ferramenta *Gerenciar o Servidor* também fornece arquivos de ajuda específicos sobre as funções de servidores, listas de verificações e recomendações para solução de problemas.


© 2003 Microsoft Corporation. Todos os direitos reservados.

# Capítulo 2
# Instalação e Migração

## 1. Introdução

Durante este capítulo, você conhecerá os métodos de instalação do Windows Server 2003 e também os métodos de migração a partir de outras versões.

Para executar os exercícios contidos nesta unidade, você deverá ter uma cópia de avaliação do Windows Server 2003 que pode ser encontrada em:

http://www.microsoft.com/windowsserver2003/evaluation/trial/default.mspx

Também será necessário ter o hardware apropriado, que deve estar de acordo com os requisitos para instalação do Windows Server 2003 descritos no Capítulo 1. Se não tiver o hardware apropriado à sua disposição, nós sugerimos que você utilize o software de emulação de Computadores Virtuais, que pode ser obtido em:

http://www.microsoft.com/windowsxp/virtualpc/previous/default.asp

Este software permite criar Computadores Virtuais dentro do seu sistema e atribuí-los recursos de disco e memória, ou seja, um outro computador dentro do seu computador.

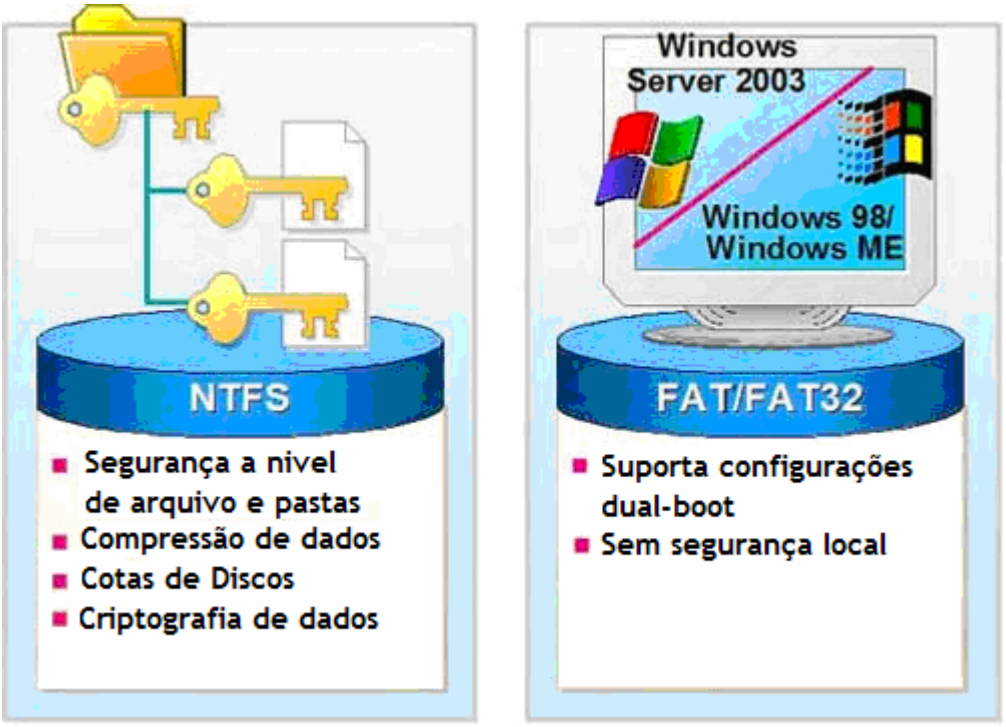
Lembre-se de que esta unidade também possui exercícios de migração do Windows NT Server 4.0. Para esta versão e o Windows 2000 Server, será necessário ter um CD de avaliação desses produtos.

Ao finalizar este capítulo, você poderá:

- Preparar-se para uma instalação do Windows Server 2003
- Instalar o Windows Server 2003 de um CD
- Instalar o Windows Server 2003 da rede
- Solucionar problemas de instalação
- Examinar a ativação do Windows Server 2003
- Descrever como automatizar instalações do Windows Server 2003


© 2003 Microsoft Corporation. Todos os direitos reservados.

## 2. Instalação




### 2.1. Introdução à instalação do Windows Server 2003

A instalação e a configuração do Windows Server 2003 são semelhantes ao processo de instalação do Windows 2000 Server, portanto os especialistas em gerenciamento de sistema poderão utilizar seus conhecimentos para executá-las. No entanto, foram incluídos diversos aprimoramentos:

- ***Novo Assistente para Instalação:*** o novo Assistente para instalação do Windows Server 2003 conserva grande parte do design do Assistente para instalação do Windows 2000 Server. Entretanto, o seu design foi aprimorado para que seja mais fácil localizar informações e tarefas relacionadas com a instalação. O novo Assistente reflete o design baseado em tarefas do Windows Server 2003, através de agrupamento das tarefas comuns com documentação e informações necessárias para ajudar os administradores a realizá-las.

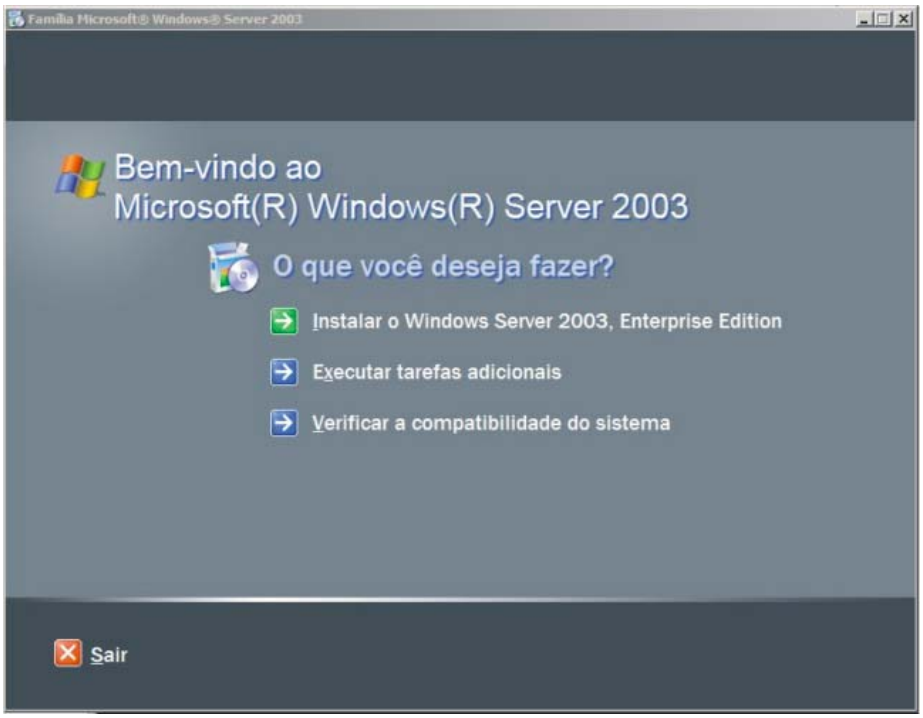
- ***Atualização dinâmica:*** agora o Assistente oferece aos usuários a opção de fazer o download de arquivos de instalação e controladores atualizados da Microsoft. Esta opção também pode incluir uma seqüência de comandos para uma instalação sem operadores.

- ***Comprovação de compatibilidade:*** o Assistente permite que os usuários realizem testes de compatibilidade detalhados em seus PCs. Como parte do processo de comprovação da compatibilidade, você pode visitar o site da Web da Microsoft em busca de atualizações dinâmicas. Também existe uma ferramenta adicional que pode ser utilizada para testar a compatibilidade de aplicativos. O “Kit de Ferramentas de Compatibilidade de Aplicativos" pode ser obtido em:

http://www.microsoft.com/windowsserver2003/compatible/appcompat.mspx


© 2003 Microsoft Corporation. Todos os direitos reservados.

*Assistente para instalação do Windows Server 2003*




Para obter informações sobre compatibilidade de hardware:

http://www.microsoft.com /whdc/hcl/default.mspx

## 2.2. Selecionar Sistema de Arquivos

Depois que você tiver criado a partição onde planeja instalar o Windows Server 2003, a instalação lhe permite selecionar um sistema de arquivos. Como no Windows NT 4.0, no Windows 2000 e no Windows XP Professional, o Windows Server 2003 oferece suporte ao sistema de arquivos NTFS e FAT16/FAT32.

### *NTFS*

Utilizando o NTFS para as partições, seu sistema terá:

- ***Segurança a nível de arquivos e pastas*** O NTFS permite controlar o acesso aos arquivos e às pastas.
- ***Compactação de disco*** O NTFS permite compactar arquivos para criar mais espaço disponível.
- ***Cotas de disco*** O NTFS permite controlar o uso do disco por usuário.
- ***Criptografia de arquivos*****.** O NTFS permite exibir de forma transparente criptografias, arquivos e pastas.

A versão do NTFS no Windows Server 2003 oferece suporte a armazenamento remoto e montagem de volumes em pastas. O Microsoft Windows 2000, o Windows XP Professional, o Windows Server 2003 e o Windows NT são os únicos sistemas operacionais que podem acessar dados em um disco rígido local com o formato NTFS.

Para compatibilidade com o NTFS e o Windows NT 4.0 em configurações de inicialização dupla, o Windows NT 4.0 exige o Service Pack 4, no mínimo. Para obtê-la, recomenda-se usar o Service Pack 6.

http://www.microsoft.com/ntserver/nts/downloads/recommended/SP6/x86Lang.asp


© 2003 Microsoft Corporation. Todos os direitos reservados.

### *FAT e FAT32*

Normalmente, você não utilizaria FAT ou FAT32 para formatar a partição do sistema, a menos que precisasse de uma inicialização dupla com o Windows Server 2003 e outro sistema operacional mais antigo. FAT e FAT32 não oferecem os mesmos recursos de segurança que o NTFS. Se você precisar dos recursos do NTFS, particularmente de segurança para arquivos e pastas, é recomendável usar o sistema NTFS.

**Nota:** Se optar por formatar a partição usando o FAT, a instalação formata automaticamente as partições superiores a 2 GB em FAT32.

## 2.3. Selecionar o Modo de Licenciamento

### 2.3.1. Modelo de licenciamento para o Windows Server 2003: O que não foi modificado

Embora tenham ocorrido modificações no modelo de licenciamento do Windows Server 2003, os seguintes elementos não foram modificados:

- Cada cópia instalada do software de servidor exige a compra de uma licença de servidor do Windows.
- É preciso ter uma Licença Acesso Cliente do Windows (CAL do Windows) para ter acesso ao software do servidor.
- Não é preciso uma CAL se o acesso ao servidor for feito através da Internet e ele não for "autenticado" - por exemplo, o acesso a um site na Web para obter informações gerais onde não seja necessário fornecer credenciais de identificação.
- Uma CAL do Windows (por servidor) também pode ser designada para uso com apenas um servidor, autorizando acesso por meio de qualquer dispositivo ou usuário, quando o tipo de licença de software para o servidor for definido como "por servidor". Nessa modalidade, o número de CALs do Windows é igual ao número máximo de conexões atuais.
- Uma CAL do Windows (por dispositivo ou por usuário) pode ser designada para uso com qualquer quantidade de servidores, autorizando o acesso através de um dispositivo específico ou de um usuário, quando a modalidade da licença do software do servidor estiver definida como "Por dispositivo ou Por usuário" (antes chamada de modo "Per Seat").
- É preciso ter um licença de Acesso de Cliente para o Terminal Server (CAL TS) para utilizar um Terminal Server ou oferecer uma sessão de interface de usuário gráfica remota (GUI), exceto para uma sessão do console. No Windows 2000, havia uma exceção para esse requisito de licença e isso foi modificado.

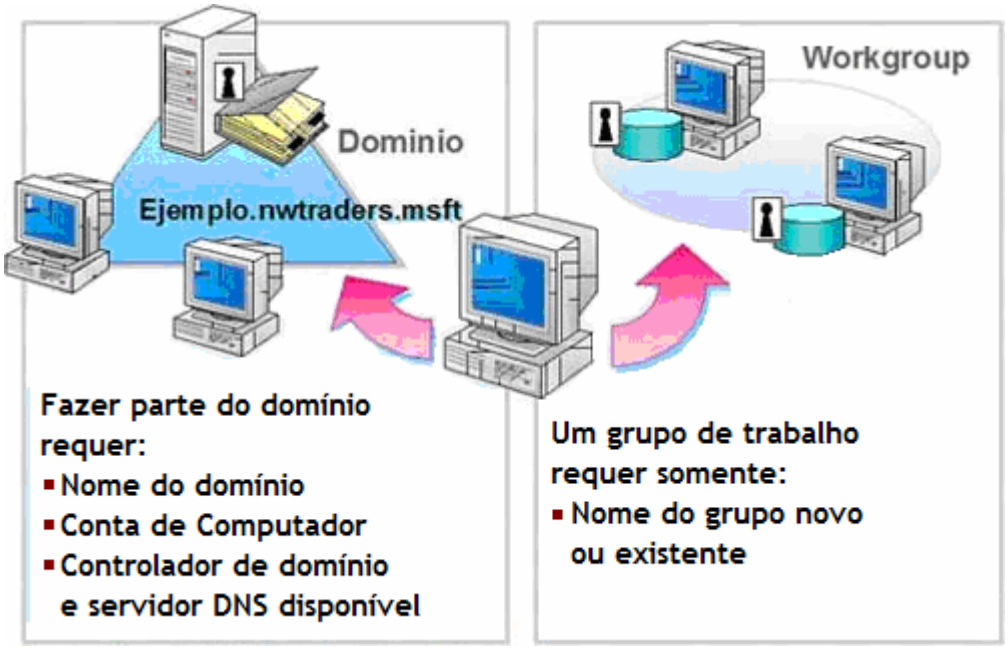
### 2.3.2. Modificações no Licenciamento do Windows Server 2003

- ***CAL baseada em novo usuário.*** A Microsoft introduziu um novo tipo de CAL. Além da CAL existente, baseada em dispositivo (CAL por Dispositivo), uma nova CAL baseada em usuário (CAL por usuário) estará disponível. Você pode optar entre uma CAL por Dispositivo para o Windows, para cada dispositivo que tenha acesso a seus servidores, ou uma CAL por Usuário do Windows, para cada nome de usuário que acesse seus servidores. Com os dois tipos de CALs, você pode optar pelo modelo mais adequado à sua empresa. Por exemplo, uma CAL para Usuário do Windows pode ser mais apropriada se a sua empresa tiver funcionários que tenham acesso remoto utilizando múltiplos dispositivos. As CAL de Dispositivo do Windows podem ser mais aconselháveis a empresas onde vários funcionários compartilham os mesmos dispositivos. Da mesma forma, os Terminal Servers (TS) também oferecerão CALs baseadas em Dispositivo e em Usuário: CAL Per Device TS (CAL de TS por dispositivo ) e CAL Per User TS (CAL de TS por Usuário).

Para obter mais informações: http://www.microsoft.com/windowsserver2003/howtobuy/


© 2003 Microsoft Corporation. Todos os direitos reservados.

## 2.4. Definir grupos de trabalho ou domínios




Durante a instalação, você deve escolher um domínio ou um grupo de trabalho como grupo de segurança para o computador.

### 2.4.1. Domínio

**Nota:** Para obter detalhes teóricos referentes ao Active Directoy, consulte o módulo 4 deste curso.

Durante a instalação, você poderá adicionar o computador a um domínio existente como servidor membro. Para isso, é preciso:

- Um nome de domínio. Um exemplo de um nome de domínio DNS válido seria microsoft.com.
- Uma conta de computador. Para unir um computador a um domínio, é preciso ter uma conta para esse computador no domínio. Você pode criar a conta antes da instalação ou, se tiver privilégios administrativos no domínio, pode criar essa conta durante a instalação. Se a conta do computador for criada durante a instalação, o programa de instalação lhe pedirá para inserir ID de usuário e senha com autorização para adicionar contas de computadores ao domínio.
- Um controlador de domínio disponível e um servidor que executa o serviço do Servidor DNS. Pelo menos um controlador de domínio e um servidor DNS devem estar on-line no momento em que o computador é adicionado ao domínio.

### 2.4.2. Grupo de Trabalho

Como no Windows NT 4.0, você só adiciona o computador a um grupo de trabalho se estiver em uma rede pequena sem um domínio ou se estiver preparando-o para adicionar um domínio posteriormente. Você pode especificar o nome de um grupo de trabalho já existente ou de um novo grupo de trabalho que será criado durante a instalação.

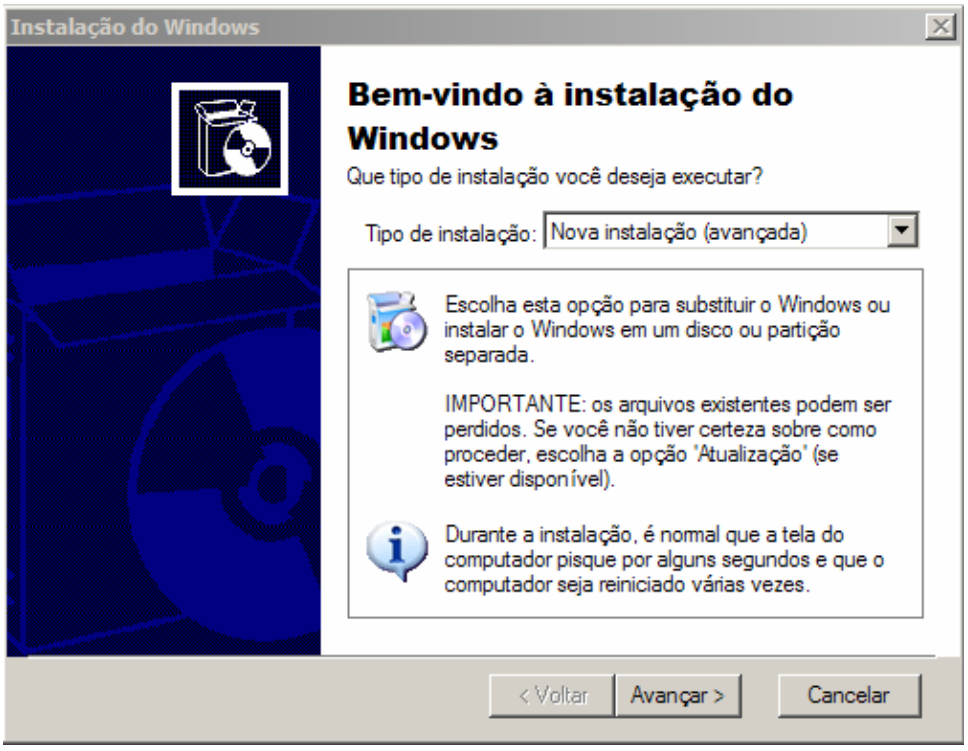

© 2003 Microsoft Corporation. Todos os direitos reservados.

## 2.5. Lista de Verificação

Antes de instalar o Windows Server 2003, complete as tarefas a seguir:

- Verifique se todos os dispositivos de hardware estão na lista HCL.
- Verifique se os componentes atendem aos requisitos mínimos de hardware.
- Selecione a partição do sistema de arquivos, onde instalará o Windows Server 2003, a menos que você necessite de uma configuração de inicialização dupla usando o NTFS.
- Determine se você usa Por Dispositivo ou Por Usuário como modo de licenciamento.
- Determine o nome do domínio ao qual você quer adicionar ou o grupo de trabalho que será criado. Se for usar um domínio, o nome estará no formato DNS: servidor.domínio (onde servidor é o nome do seu computador e domínio é o nome do domínio ao qual o seu computador pertence). Se for adicionar a um grupo de trabalho, o nome estará no formato NetBIOS.
- Crie uma conta de computador no domínio, usando o nome do computador que você está instalando. Embora um administrador de domínio possa criar a conta do computador antes da instalação, você também pode criar uma conta de computador durante a instalação se tiver privilégios administrativos no domínio. Por padrão, os usuários podem criar até 10 contas de computadores neste domínio.
- Determine a senha para a conta de Administrador local.

## 2.6. Instalar a partir de CDs





© 2003 Microsoft Corporation. Todos os direitos reservados.

Para instalar o Windows Server 2003 a partir do CD, inicie o computador com o CD ou os disquetes e siga as instruções dos diversos Assistentes. Embora o processo de instalação não seja notavelmente diferente do Windows NT 4.0 ou do Windows 2000, ter experiência com o processo de instalação do Windows Server 2003 o ajudará a executar esse processo com maior eficácia.

### 2.6.1. Funcionamento do Programa de Instalação

O modo de texto da instalação do Windows Server 2003 não é diferente da parte de instalação no modo texto do Windows NT 4.0 e do Windows 2000. Para instalar, siga os passos abaixo:

- Para começar a instalação, desligue o computador, insira o CD-ROM na unidade e depois ligue o computador. Como alternativa, também é possível executar o Winnt.exe. Uma versão mínima do Windows Server 2003 é copiada na memória e a instalação em modo texto é iniciada. DICA: Se estiver usando um disquete do MS-DOS com o driver para a unidade de CD-ROM, certifique-se de que o driver SmartDrive seja carregado. Caso contrário, a instalação deve demorar mais do que o normal.

- Selecione a partição em que o Windows Server 2003 será instalado.

- Selecione um sistema de arquivos para a nova partição. Também é possível escolher o formato da nova partição.

A instalação copia arquivos no disco e grava parâmetros de configuração. Em poucos instantes, o computador é reiniciado e o Assistente para instalação do Windows Server 2003 é iniciado. Por padrão, a localização dos arquivos da instalação dos sistemas operacionais do Windows Server 2003 é a pasta do Windows.


© 2003 Microsoft Corporation. Todos os direitos reservados.

### 2.6.2. Iniciar o Assistente de instalação do Windows Server 2003

Depois de instalar os recursos de segurança e configurar os dispositivos, o Assistente solicitará as seguintes informações:

- Configuração Regional
- Nome e organização
- Chave de produto (de 25 caracteres)
- Modo de Licenciamento
- Nome do computador e senha da conta do Administrador local.
- Componentes opcionais do Windows Server 2003.

A tabela a seguir descreve algumas das opções disponíveis no Assistente.

***Serviços de Certificados*.** Permite criar e solicitar certificados digitais para a autenticação X.509. Os certificados proporcionam meios comprováveis de identificar usuários em redes não seguras, como a Internet.
***Serviços de Fax*.** Permite enviar e receber faxes a partir do seu computador.
***Serviços de Indexação.*** Permite fazer pesquisas dinâmicas com texto completo nos dados armazenados no computador ou na rede.
***Filas de Mensagem*** Oferece suporte para aplicativos que enviam mensagens para as filas.Também permite a comunicação de aplicativos através de redes heterogêneas e com computadores que podem estar temporariamente fora da linha.
***Serviços de Instalação Remota*.** Permite a instalação remota do Windows XP Professional, do Windows 2000 e do Windows Server 2003 através de uma conexão de rede.
***Armazenamento Remoto.*** Permite que o usuário utilize bibliotecas de fitas, como extensões de volumes NTFS, movimentando dados automaticamente e através de fitas.
***Terminal Server.***Configura o computador para permitir que múltiplos usuários utilizem um ou mais aplicativos remotamente. Também está disponível durante a instalação, por exemplo, RIS e Servidor de Aplicativos.
***Licenciamento do Terminal Server*.**Configura o servidor como Servidor de Licenças do Terminal Services e fornece licenças de cliente.
***Atualizar Certificados Raiz*** Faz automaticamente o download da lista mais atual de certificados raiz do Windows Update, se necessário.
***Windows Media Services*** Permite fazer streaming de conteúdo multimídia para usuários.

Depois que os componentes opcionais forem selecionados, o Assistente do Windows Server 2003 pedirá que você ajuste a data e a hora, o que é essencial para as operações de replicação dos bancos de dados do Windows Server 2003.

### 2.6.3. Instalação de Componentes de Rede

Depois de recompilar as informações sobre o seu computador, o Assistente o orientará através da instalação dos componentes de rede. Esse segmento do processo de instalação começa com a identificação das placas de rede. Depois de configurar os adaptadores de rede, a instalação localizará o servidor que está executando o Servidor de DHCP na rede. Para prosseguir no Assistente, é necessário executar os passos abaixo:

Em primeiro lugar, é preciso instalar os componentes de rede com uma configuração típica ou personalizada. A instalação típica inclui:

- Cliente para Redes Microsoft
- Compartilhar arquivos e impressoras para Redes Microsoft
- Internet Protocol (TCP/IP) em uma instalação típica, configurado para endereço IP dinâmico. Para configurar o TCP/IP, é preciso escolher uma instalação personalizada.
- Adicionar um grupo de trabalho ou um domínio.


© 2003 Microsoft Corporation. Todos os direitos reservados.

### 2.6.4. Fim da instalação

Depois de instalar os componentes de rede, o programa de instalação termina da seguinte forma:

- Copia os arquivos restantes; por exemplo, os acessórios e os BITMAPS
- Aplica a configuração que você especificou anteriormente
- Salva a configuração no disco rígido local
- Fecha os arquivos temporários e reinicia o computador

Para mais informações sobre a nova instalação:

http://support.microsoft.com/default.aspx?scid=kb;en-us;326218

### 2.6.5. Exercício 1

#### 2.6.5.1. Objetivos

Depois de terminar esse exercício, você será capaz de instalar o Windows Server 2003 como servidor membro de um grupo de trabalho.

#### 2.6.5.2. Pré-requisitos

Antes de iniciar esse exercício, você deverá ter um computador que atenda aos requisitos mínimos de hardware para instalar o Windows Server 2003 ou o software Connectix Virtual PC para Windows.

Para terminar esse exercício, será preciso:

- O CD do Windows Server 2003 Evaluation Edition.
- O disquete do MS-DOS para inicialização (opcional). Se o seu computador estiver configurado para inicializar a partir de CD-ROM, você pode inicializar o Windows Server 2003 sem usar o disquete.
- Informações para instalação nos sistemas sem opção de inicialização a partir do CD-ROM: http://support.microsoft.com/default.aspx?scid=kb;en-us;810562 (inglês)
- Um nome de computador e um endereço IP


© 2003 Microsoft Corporation. Todos os direitos reservados.

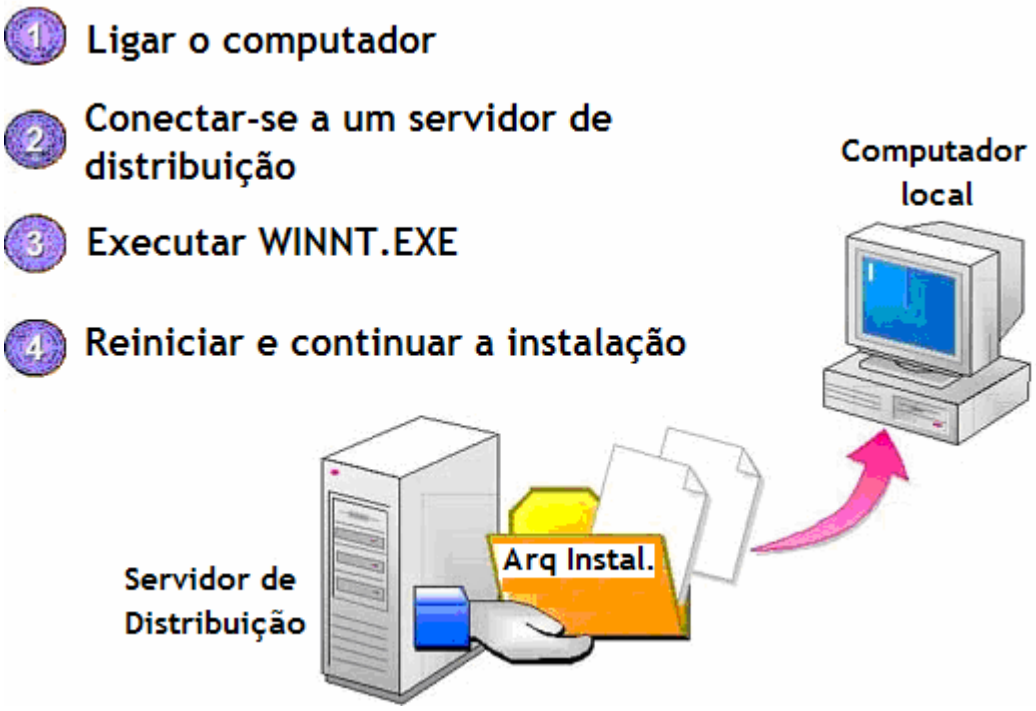
## Exercício 1

### Instalação do Windows Server 2003

1. Ligue o computador com o CD-ROM do Windows Server 2003.
2. Pressione ENTER quando for exibida a notificação de Instalação na tela.
3. Pressione ENTER quando for exibida a mensagem ***Bem-vindo à instalação*** na tela. Leia o ***Contrato de Licença do Windows*** e pressione F8 para aceitar os termos de licenciamento.
4. Pressione C na lista de partições existentes para criar uma partição no disco 0.
5. Quando for solicitado a selecionar o tamanho da partição na caixa ***Criar partição de tamanho (em MB)***, exclua o valor existente, adicione um valor entre ***2000*** e ***4000*** e pressione ENTER.
6. Pressione ENTER na lista de partições exibida para selecionar a partição ***C: Nova (Sem formato) XXXX MB***.
7. Pressione ENTER para selecionar ***Formatar a partição utilizando o sistema de arquivos NTFS***.
8. Retire o disquete da unidade se a instalação tiver sido iniciada.
9. Deixe o CD do Windows Server 2003 na unidade de CD-ROM.
10. ***O computador será reiniciado automaticamente.***
10. Espere a finalização do processo de detecção de dispositivos.
11. Clique em ***Avançar*** na página ***Opções Regionais***.
12. Insira seu nome e organização. Clique em Avançar.
13. Insira a chave de produto na página ***Chave do Produto***. Ela pode ser obtida no site de onde você fez o download do produto.
14. Escolha Por ***dispositivo ou por usuário*** no modo de licenciamento.
15. Use a senha ***Pass@w0rd*** (onde 0 é zero) para a conta do Administrador local.
16. Não instale componentes adicionais.
17. Ajuste a data e a hora na página ***Configurações de Data e Hora*** e clique em ***Avançar***.
18. Clique em ***Configurações personalizadas*** na caixa de diálogo ***Configurações de Rede*** e pressione ***Avançar***.
19. Clique nas propriedades de TCP/IP e insira os parâmetros a seguir: Endereço IP: 192.168.1.200 máscara de sub-rede: 255.255.255.0
20. Clique em ***Avançar*** na página ***Componentes de Rede***.
21. Adicione um grupo de trabalho chamado "Grupo de Trabalho".
22. Deixe o CD-ROM do Windows Server 2003 na unidade durante o resto do processo.
23. Depois de completado o processo de instalação, o computador é automaticamente reiniciado.


© 2003 Microsoft Corporation. Todos os direitos reservados.

## 2.7. Instalar a partir da rede




As instalações a partir da rede funcionam da mesma forma que no Windows NT4.0 e no Windows 2000. No entanto, há 3 requisitos para começar uma instalação a partir da rede:

- Um Servidor de Distribuição que contenha arquivos da instalação i386. (Os computadores Itanium usam a pasta ia64. Essas pastas estão no CD-ROM do Windows Server 2003).
- Uma partição disponível de 2Gb no computador.
- Um cliente de rede para conexão ao Servidor de Distribuição.

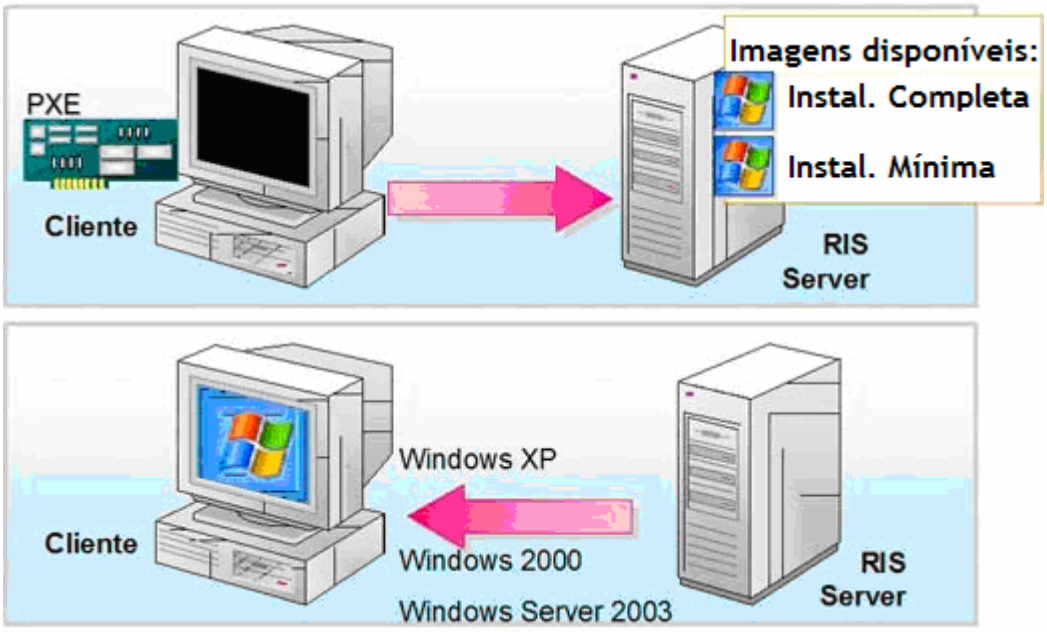
**Nota:** O Microsoft Windows Preinstallation Environment (WinPE) permitirá que um cliente conecte-se ao Servidor de Distribuição. Obtenha informações em:

http://www.microsoft.com/licensing/programs/sa/default.mspx

Os passos para a instalação são semelhantes aos do Windows NT 4.0 e do Windows 2000; a única diferença é que é preciso se conectar ao Servidor de Distribuição e executar o Winnt.exe. Durante o processo inicial, os arquivos necessários são copiados no disco local e, em seguida, o computador é reiniciado. A partir desse momento, o processo de instalação é normal.


© 2003 Microsoft Corporation. Todos os direitos reservados.

## 2.8. Usar Serviços de Instalação Remota (RIS)




Os Serviços de Instalação Remota (RIS) permitem que computadores clientes conectem-se com um servidor durante a fase inicial da inicialização e instalem remotamente o Windows 2000 (em todas as suas versões), o Windows XP (32 e 64 bits) ou o Windows Server 2003 (em todas as suas versões). A instalação a partir da rede é um processo totalmente diferente porque é realizada executando-se o Winnt.exe. Uma instalação remota não exige que os usuários saibam onde estão localizados os arquivos de instalação ou as informações a fornecer ao programa de instalação.

O RIS permite configurar as opções da instalação. Por exemplo, você poderia oferecer aos usuários uma instalação mínima sem opções e outra instalação com opções adicionais. Por padrão, todas as imagens estão disponíveis para todos os usuários. No entanto, você pode restringir as imagens que estão disponíveis para os usuários utilizando permissões NTFS  no arquivo de resposta. Os passos seguintes permitem determinar que imagens um usuário pode selecionar e fazer download.

1. Instale o RIS.
2. Configure os componentes opcionais que você planeja instalar no computador do cliente.
3. As imagens que são armazenadas no servidor RIS.
4. O cliente conecta-se usando o Pre-Boot Execution Environment (PXE) no adaptador da rede ou usando o "Network Boot Disk" criado pelo RIS.
5. O sistema operacional é instalado no cliente a partir do servidor RIS com pouca ou nenhuma intervenção de usuário.

Você pode controlar as informações exigidas pelo usuário, criando e usando scripts. Também é possível criar scripts manualmente ou utilizando o Setup Manager Wizard.

Obtenha informações sobre o Setup Manager:

http://support.microsoft.com/default.aspx?scid=kb;en-us;323438


© 2003 Microsoft Corporation. Todos os direitos reservados.

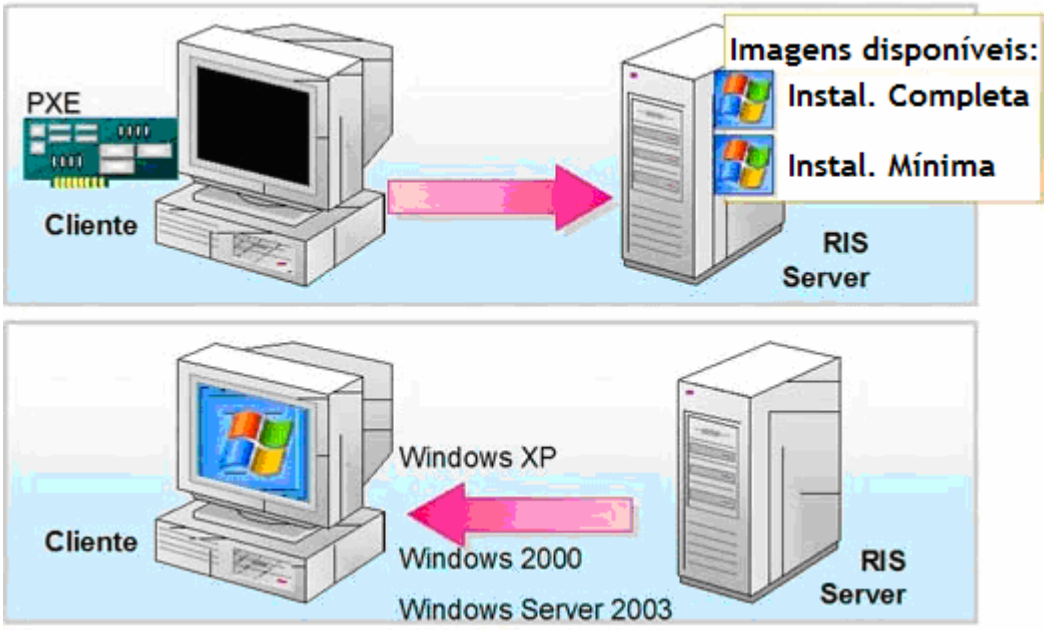
### 2.8.1. Requisitos para o Servidor RIS

- Active Directory
- Servidor DHCP
- Servidor DNS

Obtenha informações sobre o Servidor RIS:

http://support.microsoft.com/default.aspx?scid=kb;en-us;325862

## 2.9. Usar a System Preparation Tool (sysprep)




Se você quiser instalar o Windows 2000, o Windows XP ou o Windows Server 2003 em vários computadores que possuam hardware idêntico, um dos métodos possíveis é utilizar a duplicação do disco. Criando uma imagem de disco de uma instalação do Windows 2000, do Windows XP ou do Windows Server 2003 e copiando essa imagem em diversos computadores de destino, você economiza tempo na implementação do Windows 2000, do Windows XP ou do Windows Server 2003.

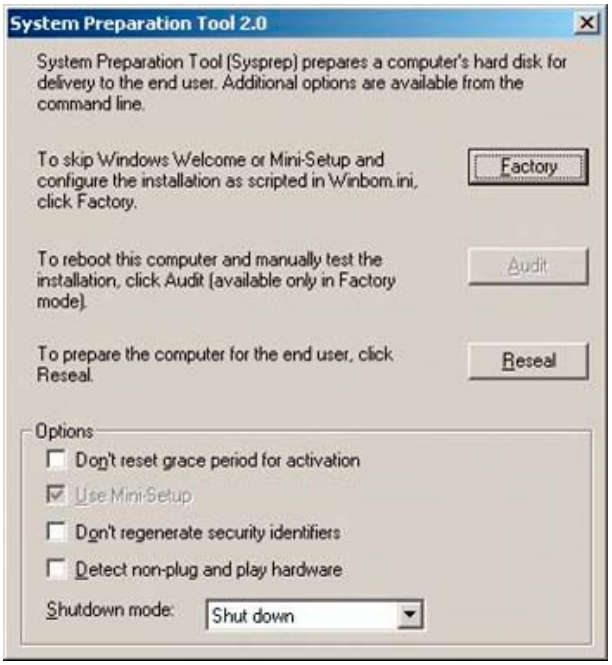
Para instalar o Windows 2000, o Windows XP ou o Windows Server 2003 usando duplicação de disco, configure um computador de referência e duplique uma imagem do seu disco no servidor usando o Sysprep para preparar o computador a ser duplicado. O processo de duplicação de disco consiste nos seguintes passos:

- Instalar e configurar o sistema operacional no computador de referência.
- Instalar e configurar os aplicativos no computador de referência.
- Executar sysprep.exe no computador de referência.

Também é possível executar o Setup Manager Wizard para criar o arquivo Sysprep.inf. O Sysprep.inf fornece respostas, como, por exemplo, o nome do computador ao Mini-Setup que é executado nos computadores de destino. Além disso, esse arquivo pode ser utilizado para especificar drivers especiais. O Setup Manager Wizard cria uma pasta Sysprep na raiz do disco e coloca o arquivo Sysprep.inf nessa pasta. O Mini-Setup verifica a pasta Sysprep à procura desse arquivo para realizar a instalação do sistema operacional.


© 2003 Microsoft Corporation. Todos os direitos reservados.

- Em seguida, desligue o computador de referência e execute o software de duplicação do disco.
- Coloque o disco duplicado no computador de destino.
- Ligue o computador de destino. Um Mini-Setup será executando imediatamente solicitando: Nome do computador, senha do administrador local e chave de produto.




Obtenha informações sobre o Sysprep Versão 2.0 em:

http://support.microsoft.com/default.aspx?scid=kb;en-us;323438


© 2003 Microsoft Corporation. Todos os direitos reservados.

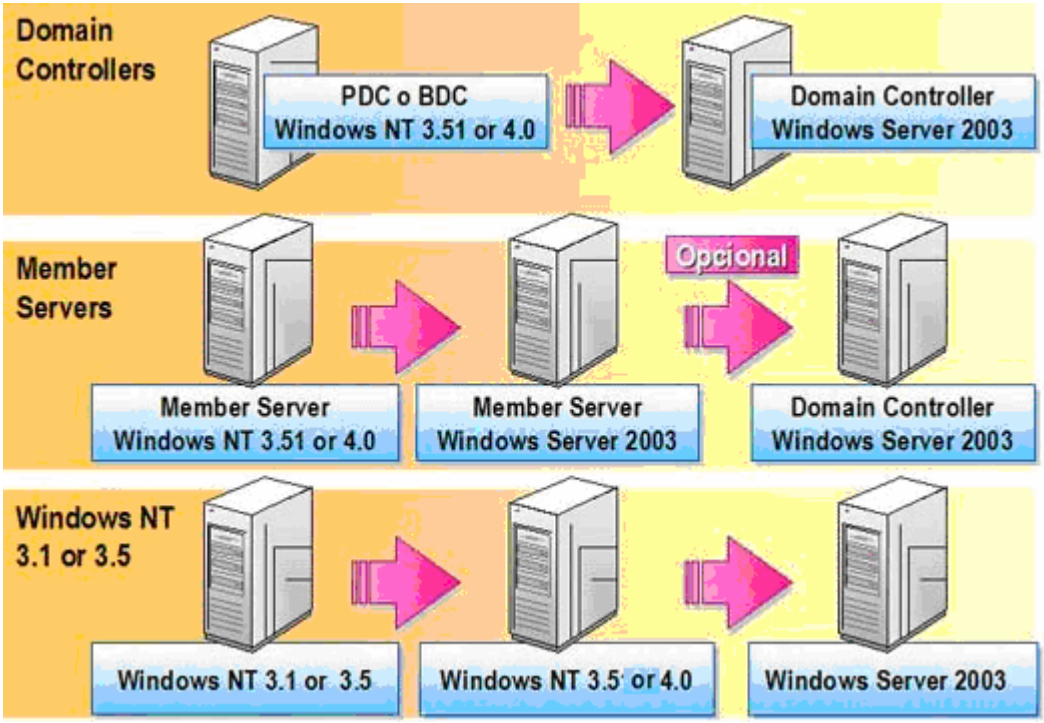
### 2.10. Ativar a Cópia do Windows Server 2003

Devido à pirataria e a outras formas de uso não autorizado, os consumidores nem sempre podem ter certeza de que possuem uma cópia genuína do Windows Server 2003. É por isso que a Microsoft desenvolveu para o Windows Server 2003 a ferramenta "Ativação de Produto" que garante que todas as instalações do seu produto Windows Server 2003 tenham uma licença válida.

**Importante:** Clientes que compram Contrato de Licenciamento por Volume não precisam ativar seus produtos. Se não tiver um contrato de Licenciamento por Volume, você tem 60 dias para ativar a instalação do seu produto. Se esse período expirar e você não tiver concluído a ativação, todos os recursos deixarão de funcionar, com exceção da função de ativação do produto. Depois de instalar o Windows Server 2003, o assistente de ativação e registro será executado. Você pode cancelar o assistente e ativar o Windows Server 2003 posteriormente. Para ativar o Windows Server 2003 usando o Assistente de Ativação do Produto siga o procedimento a seguir:

- Clique em ***Iniciar*** e em ***Ativar Windows***.
- Insira a identificação "chave do produto".
- O assistente tentará se conectar à Microsoft pela Internet.
- Se você não tiver uma conexão à Internet, mas tiver um modem conectado a uma linha de telefone, o assistente detectará o modem e tentará estabelecer uma conexão direta com a Microsoft.
- Se a conexão não puder ser estabelecida, você pode ativar sua cópia do Windows Server 2003 chamando um representante de clientes da Microsoft.

## 3. Migração do Windows NT 4.0





© 2003 Microsoft Corporation. Todos os direitos reservados.

Em seguida, detalharemos a migração de Controladores de Domínio e Servidores Membro do Windows NT 4.0 para o Windows Server 2003, nos sistemas operacionais de servidor.

| De | Resultado |
|---|---|
| Windows NT 3.51 ou 4.0 PDC ou BDC | Controlador de Domínio do Windows Server 2003 |
| Servidor Membro do Windows NT 3.51 ou 4.0 | Servidor Membro do Windows Server 2003 |
| Windows NT 3.1 ou 3.5 | Deve-se primeiro migrar para o Windows NT 3.51 ou 4.0 |

Lembre-se dos requisitos de hardware necessários para a migração do Windows NT 3.1/3.5/3.51 para o Windows Server 2003.

Obtenha mais informações em:

http://www.microsoft.com/windowsserver2003/upgrading/nt4/default.mspx

### 3.1. Migração dos Servidores Membros

Antes de migrar para o Windows Server 2003, é importante fazer backup dos arquivos críticos para garantir que seus dados sejam preservados se houver falha no processo. Para preservar seus arquivos e configurações essenciais, as seguintes tarefas devem ser realizadas:

- Resolver os erros listados no Visualizador de Eventos
- Fazer backup completo de todos os discos
- Fazer backup do registro
- Atualizar o disco de reparo de emergência (Rdisk)
- Remover o software de proteção antivírus

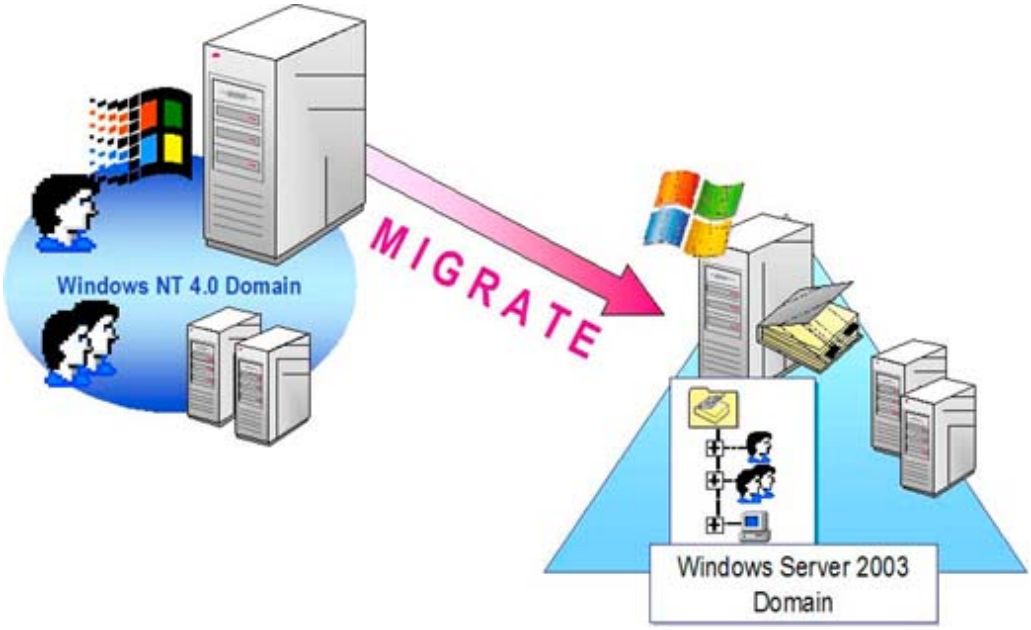
Depois de completar essas tarefas, insira o CD-ROM do Windows Server 2003 e inicie o processo de instalação. Esse processo é semelhante a uma instalação nova. Se ele for realizado a partir de uma rede, execute o Winnt32.exe.

**Nota:** É possível que a partição do sistema não tenha espaço para esse processo de migração. No entanto, no mesmo disco, você pode liberar espaço adicional excluindo dados desnecessários ou utilizando ferramentas de terceiros para expandir a partição.

Quando finalizar o processo, seu servidor passará a ser um servidor membro do Windows Server 2003.


© 2003 Microsoft Corporation. Todos os direitos reservados.

### 3.2. Migração de Domínios




Para compreender o processo de migração, nós o dividiremos em dois processos possíveis: Migração Direta ( In-Place) ou reestruturação.


© 2003 Microsoft Corporation. Todos os direitos reservados.

### 3.2.1. Terminologias

Na tabela a seguir, estão diversos termos e significados relacionados ao processo de migração:

- ***Migração de Domínio.*** É o processo de mover o usuário, as contas de grupo e as contas de computadores de um domínio do Windows NT 4.0 para um domínio do Windows Server 2003. A migração do domínio pode ser realizada através de uma atualização do domínio do Windows NT 4.0 para o Windows Server 2003, ou criando uma nova floresta do Windows Server 2003 e copiando o usuário, o grupo e as contas do computador do domínio do Windows NT 4.0 na nova floresta. Também é possível alcançar a migração do domínio usando uma combinação desses métodos.
- ***Domínio de Origem.*** É o domínio do qual os Objetos de Segurança devem ser migrados.
- ***Domínio de Destino.*** É o domínio do qual serão migrados os Objetos de Segurança. Um Domínio de Destino pode estar na mesma floresta do Windows Server 2003 ou em uma floresta diferente do Domínio de Origem.
- ***Domínio de Conta.*** Contém as contas de usuários e grupos no modelo *Multiple Master Domain* do Windows NT 4.0.
- ***Domínio de Recursos.*** É um domínio do Windows NT 4.0 utilizado para arquivos, servidor de impressão e outros serviços de aplicações. Além disso, ele contém as contas principais dos computadores.
- ***Consolidar Domínios.*** Serve para reestruturar um grande número de domínios em um número pequeno.
- ***Níveis do domínio e funcionalidade de floresta*** É uma característica do Windows Server 2003 que proporciona compatibilidade retroativa a diversos sistemas operacionais do Windows que utilizam o Active Directory. O Windows Server 2003 utiliza níveis de domínio e a funcionalidade da floresta para identificar a funcionalidade que pode ser introduzida no domínio e nos níveis da floresta. A implementação da funcionalidade de domínio ou floresta possibilita a introdução de novas características do Windows Server 2003, que não podem ser ativadas até que todos os Controladores de Domínio sejam migrados na organização. Desse modo, os níveis oferecem Compatibilidade Retroativa. Os níveis de domínio e a funcionalidade da floresta substituem a característica do modo de domínio do Windows 2000.
- ***Clone.*** Serve para criar novas contas no Domínio de Destino. É uma cópia das contas no domínio de origem, mas também mantém o identificador primário de segurança (SID) da conta no seu atributo *SID-History*. O único momento em que é possível clonar contas é durante a migração das contas entre florestas.
- ***SID-History.*** É um atributo de Objetos de Segurança do Active Directory que é usado para armazenar SIDs de objetos transferidos como contas de usuários e grupos de segurança.

### 3.2.2. Migração no Local

Este processo determina as ações necessárias para conservar a estrutura anterior. Portanto, se você tinha 4 domínios no Windows NT 4.0; ao terminar, terá os mesmos 4 domínios com a mesma estrutura no Windows Server 2003.

***O processo a ser finalizado é o seguinte:***

- Migre o PDC do Windows NT 4.0. Dica: Instale um novo BDC, retire-o da rede, promova-o a PDC e instale o Windows Server 2003 nesse computador.
- Em seguida, reinsira esse computador na rede e rebaixe o PDC em produção à BDC.
- Migre depois todos os BDC do domínio.

A estrutura completa é preservada na nova estrutura do Windows Server 2003.


© 2003 Microsoft Corporation. Todos os direitos reservados.

### 3.2.3. Reestruturação do Domínio

Esse processo determina as ações necessárias para mudar a estrutura anterior (consolidação de domínios). Portanto, se você tinha 4 domínios do Windows NT 4.0; ao finalizar, terá 1 domínio do Windows Server 2003 que conterá todas as contas.

***O processo a ser finalizado é o seguinte:***

- Migre primeiro a partir de um PDC do Windows NT 4.0 ou instale de uma floresta nova.
- Utilize a ferramenta Active Directory Migration Tool (ADMT v2) para copiar objetos. Esta ferramenta permite preservar o SID-History dos objetos e esta nova versão permite a migração de senhas.

**Nota:** O ADMT está disponível no CD-ROM do Windows Server 2003.

Obtenha mais informações sobre o ADMT:

http://support.microsoft.com/default.aspx?scid=kb;en-us;325851

## 4. Migração do Windows 2000

O primeiro passo é escolher o melhor sistema operacional equivalente ao que você está utilizando atualmente. A seguinte tabela mostra as equivalências:

| Windows Server 2003 | Windows 2000 Server |
|---|---|
| Standard Edition | Windows 2000 Server |
| Enterprise Edition | Windows 2000 Advanced Server |
| Datacenter Edition | Windows 2000 Datacenter Server |
| Web Edition | Nenhum equivalente |

### 4.1. Migração dos Servidores Membros do Windows 2000

Antes que você migre para o Windows Server 2003, é importante fazer backup dos arquivos críticos para garantir que seus dados sejam preservados se houver falha no processo. As tarefas a seguir servem para preservar seus arquivos e configurações críticos:

- Resolver os erros listados no Visualizador de Eventos
- Fazer backup completo de todos os discos
- Fazer backup do registro
- Atualizar o disco de reparo de emergência (Rdisk)
- Remover o software de proteção antivírus

Depois de completar essas tarefas, insira o CD-ROM do Windows Server 2003 e comece o processo de instalação. Esse processo é semelhante a uma nova instalação. Se for realizá-lo através de uma rede, execute o Winnt32.exe.

**Nota:** Em alguns casos, a partição do sistema não tem espaço para o processo de migração; no entanto, no mesmo disco, você pode obter espaço adicional excluindo arquivos desnecessários ou utilizando ferramentas de terceiros, que extendem a partição.

Ao finalizar o processo, seu servidor passará a ser um servidor membro do Windows Server 2003.


© 2003 Microsoft Corporation. Todos os direitos reservados.

## 4.2. Migração de Domínios

A atualização do Active Directory pode ser gradual e realizada sem interrupção das operações. Se você seguir as recomendações de atualização de domínio, não será necessário colocar o domínio offline para migrar os controladores de domínio, os servidores membro ou as estações de trabalho.

No Active Directory, um domínio é uma coleção de computadores, usuários e grupos definidos pelo administrador. Esses objetos compartilham um banco de dados em comum de diretório, Diretivas de Segurança e Relações de Segurança com outros domínios. Uma floresta é uma coleção de um ou mais domínios do Active Directory que compartilham classes e atributos (esquema), informações de sites e duplicação (configuração) e capacidades de pesquisa em toda a floresta (catálogo global). Os domínios na mesma floresta contêm relações de confiança bilaterais.

Para se preparar para atualizar os domínios que contêm os Controladores de Domínio do Windows 2000, é recomendável aplicar o Service Pack 2 ou posterior a todos os Controladores de Domínio do Windows 2000.

Antes de migrar um Controlador de Domínio do Windows 2000 para o Windows Server 2003 ou instalar o Active Directory no primeiro Controlador de Domínio do Windows Server 2003, certifique-se de que o domínio esteja preparado.

Essas duas ferramentas de linha de comando ajudarão na migração do Controlador de Domínio:

**Winnt32.** Use o Winnt32 para comprovar a compatibilidade de atualização do servidor.
**Adprep.** Use o Adprep no Mestre de Operações de Esquema para preparar a floresta.

O Adprep está contido no CD-ROM do Windows Server 2003 na pasta I386 ou IA64. Lembre-se de que essa ferramenta modifica o Esquema segundo o qual a quantidade de objetos que contêm o Active Directory define o tempo necessário para concluir as operações. Por outro lado, é aconselhável executar essa ferramenta somente no Mestre de Esquema, considerando que, em caso de queda na comunicação da rede, não haverá o risco de que a operação seja interrompida na metade do processo.

### O processo a ser finalizado inclui:

- Executar o adprep.exe / forestprep para preparar a floresta
- Executar o adprep.exe / domainprep para preparar o domínio
- Migrar os Controladores de Domínio gradualmente ou instalar uma cópia nova do Windows Server 2003, promovendo essa instalação a Controlador de Domínio.

Ao concluir essas tarefas, você terá atualizado a versão existente do Active Directory.

Obtenha mais informações sobre a migração do Windows 2000

http://www.microsoft.com/ windowsserver2003/evaluation/whyupgrade/win2k/w2ktows03-2.mspx


© 2003 Microsoft Corporation. Todos os direitos reservados.

### 4.2.1. Exercício 2

Durante este exercício, você realizará um processo de migração do servidor membro do Windows NT 4.0 para o Windows Server 2003 e um processo de migração do servidor membro do Windows 2000 para o Windows Server 2003.

***Próximos passos.***

- Primeiro instale um Windows NT Server 4.0, na instalação do servidor membro.
- Siga os passos descritos no exercício 1, iniciando a instalação do sistema operacional, ou seja, execute o Winnt32.exe ou faça a instalação inserindo o CD-ROM.

***Resultado:*** Processo de migração do Windows NT 4.0 para o Windows Server 2003

- Instale agora o Windows 2000 Server como Servidor Membro.
- Siga os passos descritos na prática 1, iniciando a instalação do sistema operacional, ou seja, execute o Winnt32.exe ou faça a instalação inserindo o CD-ROM.

**Resultado:** Processo de migração do Windows 2000 para o Windows Server 2003

**Nota:** Lembre-se de que para fazer esses exercícios você pode utilizar o software Connectix Virtual PC.

**Opcional:** Se tiver tempo, você pode realizar o mesmo exercício, do PDC do Windows NT 4.0 e do Controlador de Domínio do Windows 2000, executando o processo de atualização.


© 2003 Microsoft Corporation. Todos os direitos reservados.

# Capítulo 3
# Instalação e Configuração de Serviços DHCP, DNS e WINS

## 1. Introdução

Durante este capítulo, você assimilará conhecimentos sobre serviços de rede como DHCP (Dynamic Host Configuration Protocol), WINS (Windows Internet Name System) e DNS (Domain Name System). Este último, em particular, lhe será muito útil durante o capítulo 4.

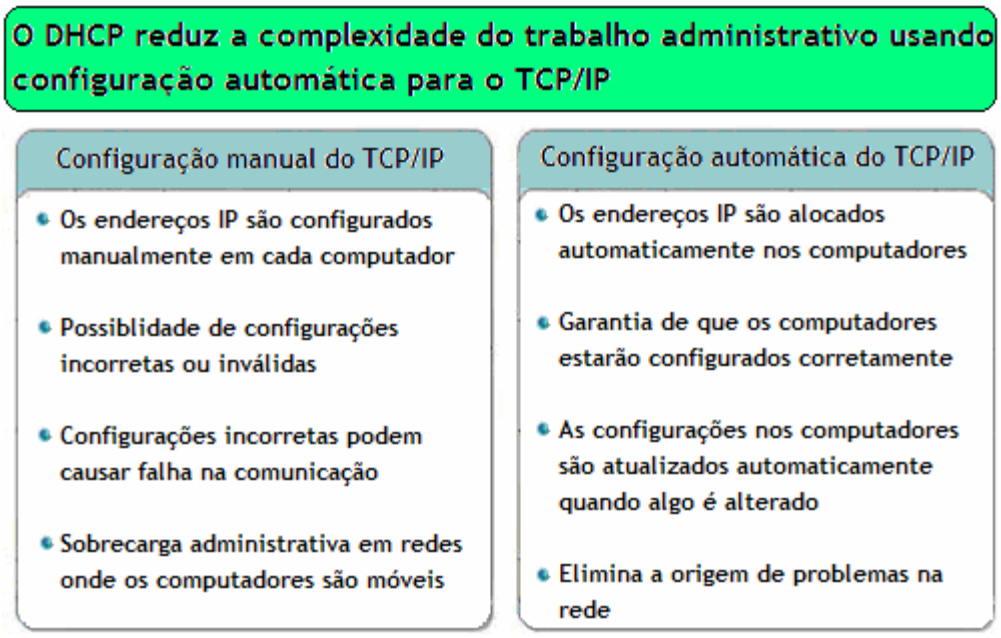
Para a realização dos exercícios contidos neste módulo, será preciso usar a instalação do Windows Server 2003 executada no exercício 1 do capítulo 2 e uma instalação adicional.

***Ao finalizar este capítulo, você poderá:***

- Identificar as características dos serviços DHCP, DNS e WINS
- Instalar e configurar serviços de rede
- Solucionar problemas de serviços de rede

## 2. DHCP - Dynamic Host Configuration Protocol

### 2.1. Por que utilizar o DHCP?





© 2003 Microsoft Corporation. Todos os direitos reservados.

### 2.1.1. Definição

***Dynamic Host Configuration Protocol (DHCP)*** é um padrão IP para simplificar a administração da configuração IP do cliente. O padrão DHCP permite que você utilize os servidores DHCP para controlar a alocação dinâmica dos endereços e a configuração de outros parâmetros de IP para clientes DHCP na sua rede.

### 2.1.2. Por que utilizar o DHCP?

Nas redes TCP/IP, o DHCP reduz a complexidade do trabalho administrativo de reconfigurar os computadores cliente.

Para entender por que o DHCP é útil para configurar clientes TCP/IP, é importante comparar a configuração manual do TCP/IP com a configuração automática que utiliza o DHCP.

### 2.1.3. Configuração manual do TCP/IP

Quando você realiza a configuração IP de cada cliente inserindo manualmente informações como endereço IP, máscara de sub-rede ou gateway padrão, podem ocorrer erros de digitação, que provavelmente gerarão problemas de comunicação ou problemas associados à IP duplicado. Por outro lado, ocorre uma sobrecarga administrativa nas redes quando os computadores são movidos com freqüência de uma sub-rede para outra. Além disso, quando é preciso trocar um valor IP para vários clientes, é preciso atualizar a configuração IP de cada cliente.

### 2.1.4. Configuração automática do TCP/IP

Quando você configura um servidor DHCP para oferecer suporte a clientes DHCP, ele automaticamente fornece informações de configuração aos clientes DHCP e também garante que os clientes da rede utilizem a configuração correta. Além disso, se você precisar realizar uma modificação na configuração IP de vários clientes, poderá realizá-la uma única vez no servidor DHCP, para que o DCHP atualize automaticamente a configuração do cliente para refletir essa mudança.

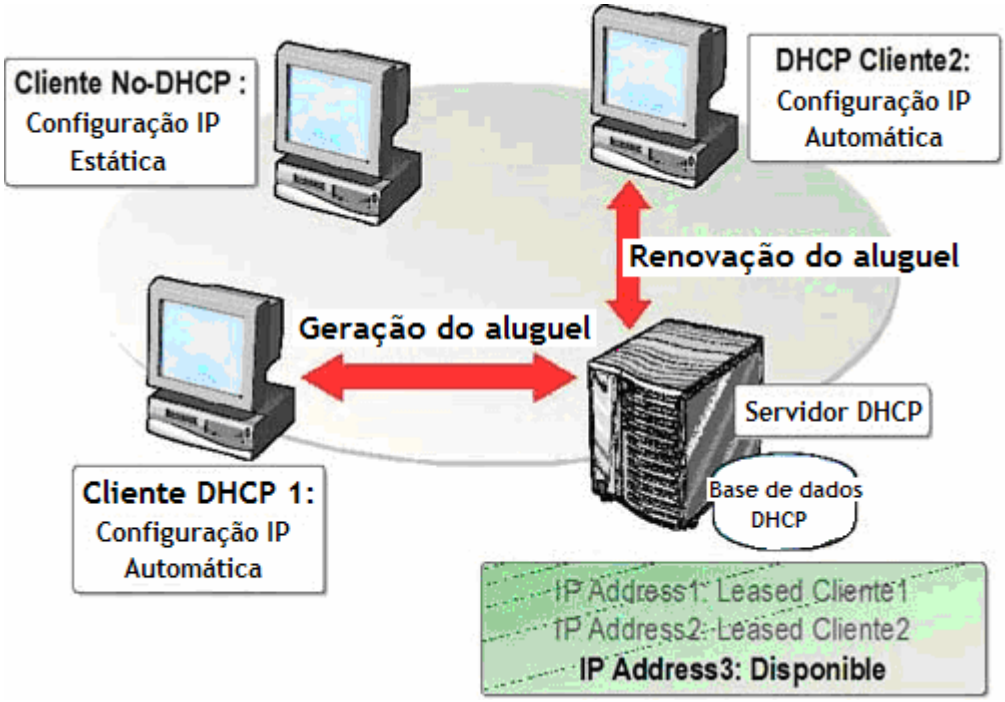
***Exemplo***

Você precisa configurar 100 computadores com a configuração IP, mas sem DHCP. Não lhe resta alternativa além de configurar manualmente cada um dos computadores individualmente. Além disso, também é preciso documentar a configuração IP de cada cliente e realizar uma modificação na configuração IP dos clientes e ainda reconfigurar manualmente cada um deles.

Mas o DHCP oferece uma solução para esse problema. Com o DHCP, você só precisa adicionar a configuração ao servidor DHCP, que atualizará os 100 clientes da rede. Além disso, quando precisar realizar uma modificação na configuração IP, ela será realizada uma única vez no Servidor DHCP, exigindo simplesmente que cada cliente TCP/IP atualize a sua configuração.


© 2003 Microsoft Corporation. Todos os direitos reservados.

## 2.2 Como o DHCP atribui endereços IP?




### 2.2.2.1 Introdução

O DHCP permite controlar a atribuição de IP de um local central; portanto, você pode configurar o servidor DHCP para atribuir endereços IP a uma única sub-rede ou a várias sub-redes. Da mesma forma, o Servidor DHCP pode atribuir a configuração IP aos clientes de forma automática.

### 2.2.2.2 Definições

A ***concessão*** é o tempo no qual um cliente DHCP pode utilizar uma configuração dinamicamente atribuída de IP. Antes da expiração do tempo de concessão, o cliente deve renová-lo ou obter uma nova concessão do DHCP.

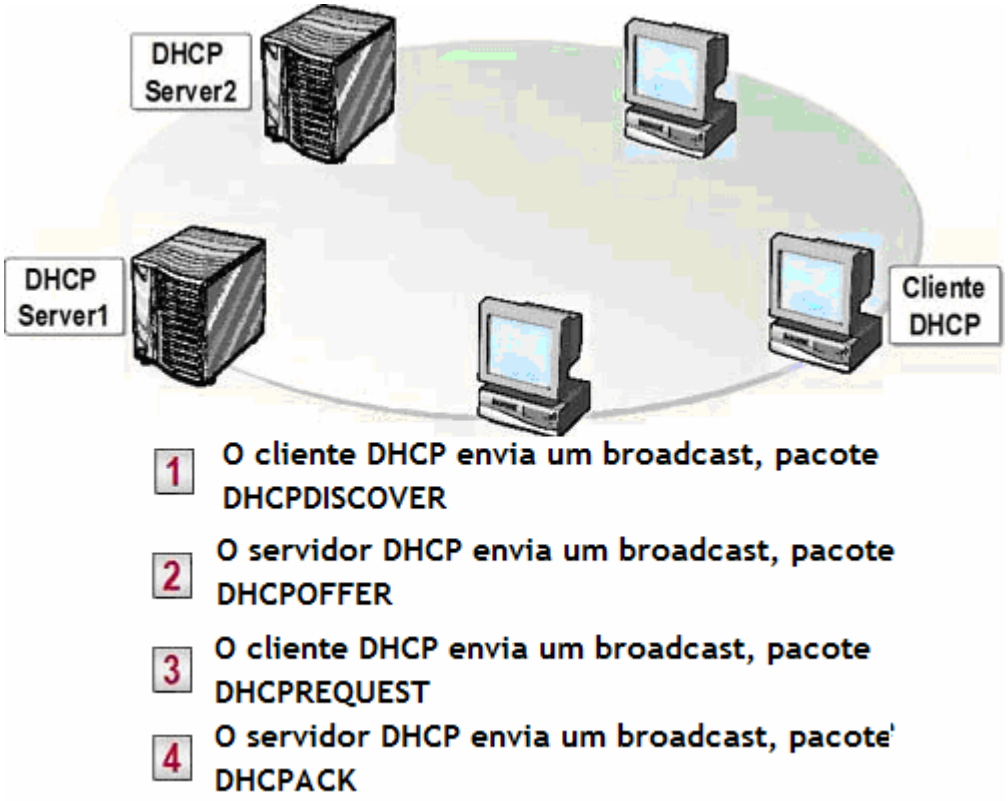
### 2.2.2.3 Atribuição de endereços IP

O DHCP administra a atribuição e a liberação da configuração IP, concedendo a configuração IP ao cliente. O estado de concessão do DHCP depende do tempo que o cliente pode utilizar os dados da configuração IP antes de liberá-la e depois de atualizar os dados. O processo de atribuir a configuração IP é conhecido como ***Processo de Geração de Concessão DHCP***, e o processo de renovar os dados da configuração IP é conhecido como ***Processo de Renovação de Concessão de DHCP***.

Na primeira vez em que um cliente DHCP é adicionado à rede, ele deve solicitar a configuração IP ao Servidor DHCP para que, quando for recebida a solicitação, o servidor selecione um endereço IP do intervalo de endereços que o administrador definiu no escopo. O Servidor DHCP fornece a configuração IP ao cliente do DHCP. Se o cliente aceitar a oferta, o Servidor DHCP atribuirá o endereço IP ao cliente por um período de tempo especificado. Dessa forma, o cliente utilizará o endereço IP para ter acesso à rede.


© 2003 Microsoft Corporation. Todos os direitos reservados.

## 2.3. Como funciona o Processo de Geração de Concessão do DHCP?




***O cliente DHCP envia o pacote DHCPDISCOVER para localizar o Servidor DHCP.*** Esse pacote DHCPDISCOVER é a mensagem que os clientes DHCP enviam na primeira vez que se conectam à rede e solicitam informações de IP de um servidor DHCP. Existem duas formas de iniciar o processo de Geração de Concessão de DHCP. A primeira ocorre quando um computador cliente é iniciado ou o TCP/IP é iniciado pela primeira vez, e a segunda quando um cliente tenta renovar sua concessão e não consegue. (Por exemplo, um cliente pode não conseguir executar uma renovação quando você o move para outra sub-rede.)

***O Servidor DHCP envia um pacote DHCPOFFER ao cliente.*** O pacote DHCPOFFER é uma mensagem que o Servidor DHCP utiliza para oferecer a concessão de um endereço IP ao cliente, quando ele se conecta à rede. Cada Servidor DHCP que responde, reserva o endereço IP oferecido para que ele não seja novamente oferecido a outro cliente DHCP, antes da aceitação do cliente inicial. Se o cliente não receber uma oferta depois de quatro solicitações, ele utiliza um IP do intervalo reservado de 169.254.0.1 a 169.254.255.254. O uso de um desses endereços auto-configurados garante que os clientes situados em uma sub-rede de Servidor DHCP inacessível possam se comunicar com outros clientes. Enquanto isso, o cliente DHCP continua buscando um Servidor DHCP disponível a cada cinco minutos. Quando um Servidor DHCP estiver disponível, os clientes receberão endereços IP válidos, permitindo que esses clientes se comuniquem com clientes na sua sub-rede e em outras.

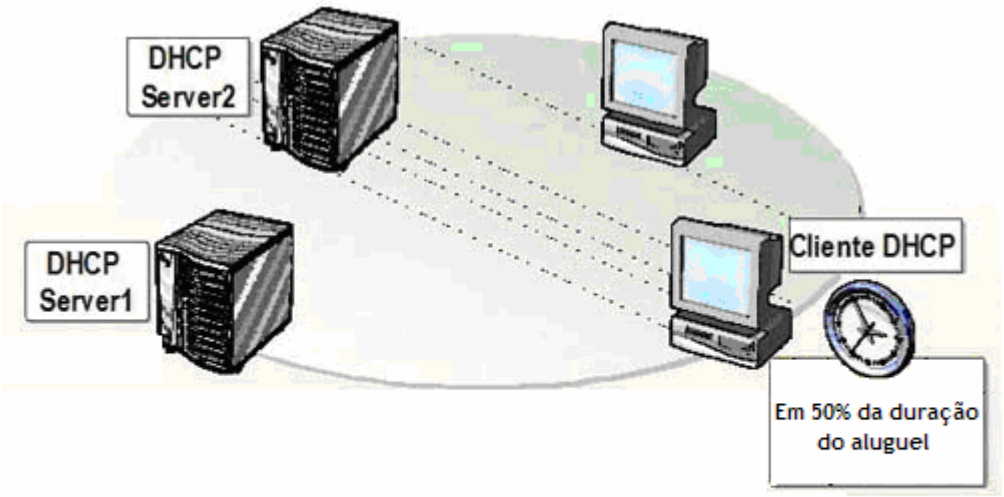
***O cliente DHCP envia um pacote DHCPREQUEST ao Servidor DHCP.*** O pacote DHCPREQUEST é a mensagem que um cliente envia ao Servidor DHCP para solicitar ou renovar sua concessão de IP. O cliente DHCP responde ao primeiro pacote DHCPOFFER que recebe com uma transmissão de DHCPREQUEST para aceitar a oferta. O pacote DHCPREQUEST inclui a identificação do servidor que o ofereceu e o cliente que o aceitou. Todos os outros servidores DHCP posteriores eliminam suas ofertas e mantêm seus endereços de IP para outras concessões.


© 2003 Microsoft Corporation. Todos os direitos reservados.

***O Servidor DHCP envia um pacote DHCPACK ao cliente DHCP.*** O pacote DHCPACK é uma mensagem que o Servidor DHCP envia a um cliente como confirmação de recebimento e finalização do processo de concessão. Essa mensagem contém uma concessão válida para endereço IP e outros dados de configuração IP. Quando o cliente DHCP recebe a confirmação de recebimento, ele inicia o TCP/IP usando a configuração IP prevista pelo Servidor DHCP.

**Nota:** Você pode ver todo o processo de concessão capturando os pacotes com o Monitor de Rede. Lembre-se de que o cliente e o servidor utilizam as portas 67 e 68 UDP. Para realizar o processo em ambientes seguros, será necessário permitir a comunicação dessas portas entre o cliente e o servidor.

## 2.4 Como funciona o processo de Renovação de Concessão do DHCP?




1. O cliente DHCP envia um broadcast, pacote DHCPREQUEST
2. O servidor DHCP envia um broadcast, pacote DHCPACK

### 2.4.1. Definições

***Processo de Renovação de Concessão de DHCP*** é o processo pelo qual um cliente DHCP renova ou atualiza seus dados de configuração IP com o Servidor DHCP.

O cliente DHCP renova a configuração IP antes da expiração do tempo de concessão. Se o período de concessão expirar e o cliente de DHCP ainda não tiver renovado sua configuração IP, ele perderá todos os dados da configuração IP e o processo de Geração de Concessão de DHCP será reiniciado.

### 2.4.2. Período de Concessão

O processo de Renovação de Concessão é o resultado do valor de tempo da concessão. O valor do período de concessão garante que o DHCP mantenha as informações de IP e que os clientes atualizem ou renovem regularmente seus dados de configuração IP. Com o DHCP, é possível manter essas informações e administrar o endereçamento IP do Servidor DHCP. O cliente deve renovar sua configuração IP antes da expiração do período de concessão. Em intervalos específicos, um cliente DHCP tenta renovar sua concessão para garantir que a sua configuração mantenha-se atualizada. Em qualquer momento durante o período de concessão, o cliente DHCP pode enviar um pacote de DHCPRELEASE ao servidor DHCP para liberar a configuração IP e cancelar o restante da concessão.


© 2003 Microsoft Corporation. Todos os direitos reservados.

### 2.4.3. Processo automático "Renovação de Concessão"

Um cliente DHCP tenta renovar automaticamente sua concessão em 50% do tempo de expiração. O cliente de DHCP também tenta renovar sua concessão cada vez que o computador é iniciado e, para isso, envia o pacote de DHCPREQUEST ao Servidor DHCP diretamente do qual se obteve a concessão. Se o Servidor DHCP estiver disponível, ele renova a concessão e envia ao cliente um pacote de DHCPACK com a nova duração da concessão e qualquer parâmetro de configuração atualizado. O cliente atualiza sua configuração quando recebe a confirmação. Se o Servidor DHCP não estiver disponível, o cliente continuará utilizando seus parâmetros atuais de configuração. Se o cliente DHCP não conseguir renovar sua concessão na primeira vez, ele enviará uma transmissão DHCPDISCOVER para atualizar sua concessão de endereço quando 87,5 % da duração da concessão tiver expirado. Nessa etapa, o cliente DHCP aceita a concessão que qualquer Servidor DHCP lhe ofereça.

Se o cliente DHCP reiniciar seu computador e o Servidor DHCP não responder ao pacote DHCPREQUEST, o cliente DHCP tentará se conectar ao Gateway Padrão. Se essa tentativa falhar, o cliente deixará de usar o endereço IP. Se o Servidor DHCP responder a um pacote DHCPOFFER para atualizar a concessão do cliente, ele pode renovar sua concessão de acordo com a oferta da mensagem do servidor e continuar a sua operação. Mas se a concessão tiver expirado, o cliente deverá suspender imediatamente o uso do endereço IP atual. O cliente DHCP começará o novo processo de Descoberta da Concessão DHCP, tentando obter uma nova concessão de um novo IP. Se o cliente DHCP não receber o IP, ele obterá um endereço usando a atribuição automática de IP no intervalo 169.254.0.0.

### 2.4.4. Processo manual de Renovação de Concessão

Se precisar atualizar a configuração DHCP imediatamente, você pode renovar manualmente a concessão de IP. (Por exemplo, se quiser que os clientes DHCP obtenham rapidamente o endereço do Servidor DHCP de um novo roteador instalado na rede, renove a concessão do cliente para atualizar a configuração.)

***Comando:*** **ipconfig /renew**

## 2.5. Exercício 1: Como adicionar o serviço de Servidor DHCP?

Para adicionar um servidor DHCP, você deverá instalar o Serviço de DHCP em um computador executando o Microsoft® Windows® Server 2003.

***Antes de adicionar o serviço de Servidor DHCP:***

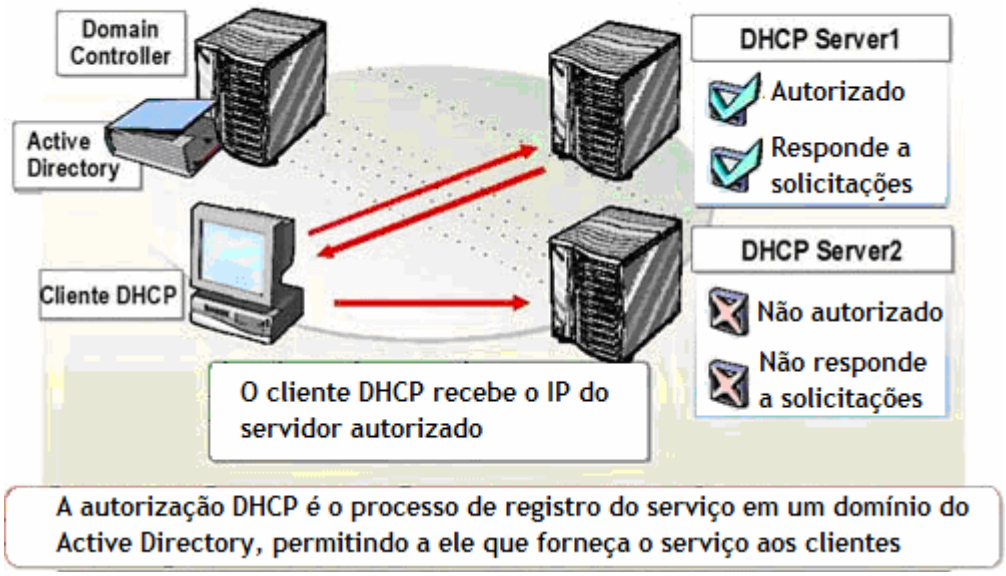
- Verifique se a configuração IP no servidor está correta.
- Verifique se a configuração IP do servidor contém um endereço IP estático e uma máscara sub-rede em ambientes roteados de um gateway padrão.
- Verifique se a conta do usuário tem as permissões corretas.


© 2003 Microsoft Corporation. Todos os direitos reservados.

***Para adicionar o serviço de Servidor DHCP:***

1. Inicie a sessão usando uma conta não administrativa.
2. Clique em ***Iniciar*** e depois em ***Painel de Controle***.
3. Abra as ***Ferramentas Administrativas*** no Painel de Controle e clique direto em ***Gerenciar o Servidor***, selecionando ***Executar como...*** (mantenha pressionada a tecla Shift e clique com o botão direito do mouse sobre o ícone, selecionando a opção *Executar como...*)
4. Selecione ***O seguinte usuário*** na caixa ***Executar como*** e insira uma conta de usuário e senha que tenham permissões apropriadas para realizar a tarefa, clicando em ***OK***.
5. Clique em ***Adicionar ou remover uma função*** na janela do *Gerenciar o Servidor*.
6. Clique em ***Avançar*** na página ***Etapas preliminares***.
7. Selecione ***Servidor DHCP*** no assistente e em ***Avançar***.
8. Clique em ***Avançar*** na página ***Resumo das Seleções.***
9. Clique em ***Cancelar*** no assistente de novo escopo para não criar o escopo nesse momento.
10. Clique em ***Concluir*** no assistente.

## 2.6. Como autorizar o serviço do Servidor DHCP?




### 2.6.1. Definições

***A autorização do DHCP*** é o processo de registrar o serviço de Servidor DHCP em um domínio do Serviço Active Directory®, com o propósito de oferecer suporte aos clientes DHCP. A autorização de DHCP é somente para Servidores DHCP que executam o Windows Server 2003 e o Windows 2000 no Active Directory.

### 2.6.2. Por que autorizar o Servidor DHCP?

Autorizar o Servidor DHCP permite controlar o acréscimo dos servidores DHCP ao domínio. A autorização deve ocorrer antes de o servidor DHCP poder entregar essas concessões a clientes DHCP. Solicitar a autorização de Servidores DHCP evita que os servidores DHCP desautorizados ofereçam endereços IP inválido aos clientes.

Se você estiver configurando um servidor DHCP, a autorização deve ser parte do domínio Active Directory. Se você não autorizar o Servidor DHCP no Active Directory, o serviço de DHCP não poderá


© 2003 Microsoft Corporation. Todos os direitos reservados.

ser iniciado corretamente e, portanto, o servidor DHCP não poderá responder aos pedidos dos clientes. O Servidor DHCP controla o endereçamento IP enviado aos clientes DHCP na rede. Se o Servidor DHCP for configurado de forma incorreta, os clientes receberão uma configuração incorreta do endereçamento IP.

### 2.6.3. Por que um Servidor DHCP autorizado exige o Active Directory?

O Active Directory é necessário para autorizar um Servidor DHCP. Com o Active Directory, os Servidores DHCP não autorizados não podem responder aos pedidos dos clientes. O serviço do Servidor DHCP, em um servidor membro do Active Directory, verifica o seu registro em um controlador de domínio do Active Directory. Se o Servidor DHCP não estiver registrado, o serviço não se iniciará e conseqüentemente o Servidor DHCP não designará endereços aos clientes.

### 2.6.4. Servidor DHCP Autônomo

Em determinadas situações, um Servidor DHCP executando o Windows 2000 ou o Windows Server 2003 é iniciado se não estiver autorizado. Se o Servidor DHCP executando o Windows Server 2003 ou o Windows 2000 estiver instalado como autônomo, ele não é membro do Active Directory. E se estiver situado em uma sub-rede onde o DHCPINFORM não será transmitido a outros servidores DHCP, o serviço do Servidor DHCP inicializará e fornecerá concessões a clientes na sub-rede.

Um servidor autônomo executando o Windows 2000 ou o Windows Server 2003 envia um pacote de transmissão DHCPINFORM. Se não houver resposta ao pacote DHCPINFORM, o serviço do Servidor DHCP será iniciado e começará a atender os clientes. Se um servidor DHCP autorizado receber um pacote DHCPINFORM, ele responde com um pacote DHCPACK e o serviço de Servidor DHCP pára. Um servidor DCHP autônomo continua funcionando se você receber um DHCPACK de outro Servidor DHCP que não seja membro do Active Directory.

## 2.7. Exercício 2: Como autorizar o serviço de Servidor DHCP?

**IMPORTANTE:** Só faça esse exercício depois de ter concluído a teoria e o exercício do Capítulo 4.

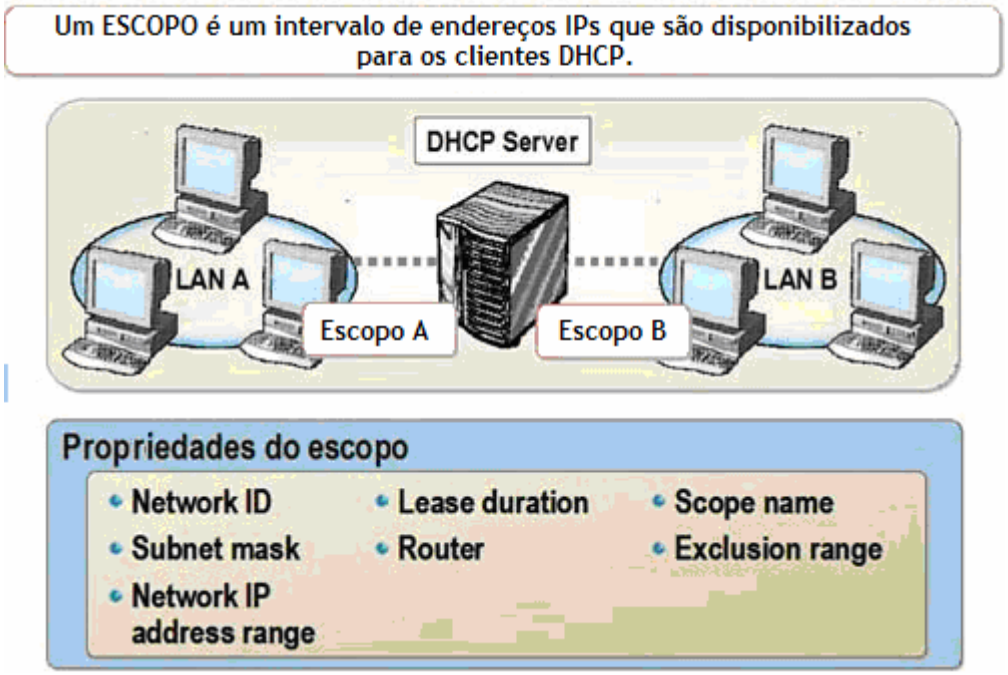
Para autorizar o serviço de Servidor DHCP, um membro do grupo Administradores Corporativos o adiciona a uma lista de Servidores DHCP, que podem fornecer serviços a clientes DHCP no domínio. O processo de autorização funciona somente com servidores executando o Windows Server 2003 e o Windows 2000 em um domínio. A autorização não é possível se os Servidores DHCP executarem versões anteriores como o Microsoft Windows NT® ou outros softwares de Servidor DHCP.

***Para autorizar o serviço do Servidor DHCP:***

1. Abra o console DHCP.
2. Selecione o servidor no console
3. Clique em ***Autorizar*** no menu ***Ação***.
4. Para se certificar de que o servidor DHCP esteja autorizado: no console, pressione F5 para atualizar a tela e verificar se agora o Servidor DHCP pode ser visualizado com uma seta verde para cima.


© 2003 Microsoft Corporation. Todos os direitos reservados.

## 2.8. O que são os escopos do DHCP?




### 2.8.1. Definição

Um ***escopo*** é um intervalo de endereços IP válidos disponíveis para atribuir aos computadores cliente em uma sub-rede em particular. Você pode configurar um escopo no servidor DHCP para determinar o grupo de endereços IP que esse servidor atribuirá aos clientes.

Os escopos determinam os endereços IP atribuídos aos clientes. Você deve definir e ativar um escopo antes que os clientes possam usar o Servidor DHCP para uma configuração dinâmica de TCP/IP. Da mesma forma, pode-se configurar tantos escopos quanto forem necessários no servidor DHCP para seu ambiente de rede.

### 2.8.2. Propriedades do escopo

***Um escopo tem as seguintes características:***

- ***ID de Rede:*** A ID de Rede para o intervalo de endereços IP
- ***Máscara de sub-rede:*** A máscara de sub-rede para a ID de Rede
- ***Intervalo de endereço de IP de rede:*** O intervalo de endereços IP disponíveis para os clientes
- ***Duração de concessão:*** O período de tempo que o Servidor DHCP atribui ao endereço do cliente
- ***Roteador:*** O endereço do Gateway padrão
- ***Nome do escopo:*** Identificador para fins administrativos
- ***Intervalo de exclusão:*** O intervalo de endereços IP excluídos para a atribuição.

Cada sub-rede pode ter um escopo de DHCP que contenha um intervalo único e contínuo de endereços IP. Endereços específicos ou grupos de endereços podem ser excluídos do intervalo do escopo de DHCP. Em geral, somente um escopo pode ser atribuído a uma sub-rede. Se mais de um escopo for necessário em uma sub-rede, eles deverão ser criados primeiro e depois combinados em um superescopo.


© 2003 Microsoft Corporation. Todos os direitos reservados.

## 2.9. Prática 3: Como configurar um Escopo de DHCP?

***Para configurar um Escopo de DHCP:***

1. Abra o console DHCP.
2. Clique no Servidor DHCP do console.
3. Clique em ***Novo escopo*** no menu ***Ação***,
4. Clique em ***Avançar*** no ***Assistente para novos escopos***.
5. Configure o ***Nome*** e a ***Descrição*** na página ***Nome do Escopo***.
6. Configure, na página ***Intervalo de endereço IP***, o endereço IP inicial 192.168.1.1, o endereço IP final 192.168.1.254 e a máscara de sub-rede 255.255.255.0.
7. Configure, na página ***Adicionar exclusões***, o endereço IP inicial 192.168.1.20 e endereço IP final 192.168.1.30 , se aplicável.
8. Configure, na página ***Duração da Concessão***, os ***Dias***, ***Horas*** e ***Minutos***. (O padrão é de 8 dias).
9. Configure ***Opções DHCP*** e selecione ***Não, eu irei configurar estas opções mais tarde***.
10. Clique em ***Concluir*** na página ***Concluindo o Assistente de Novo Escopo***.

***Para ativar um Escopo de DHCP:***

Clique com o botão direito do mouse sobre o escopo do console e em Ativar.

## 2.10 O que é uma reserva de DHCP?

***Uma reserva*** é um endereço IP permanente atribuído a um cliente específico. Você pode reservar um endereço IP permanente a um dispositivo da rede. A reserva é feita no endereço MAC do dispositivo.

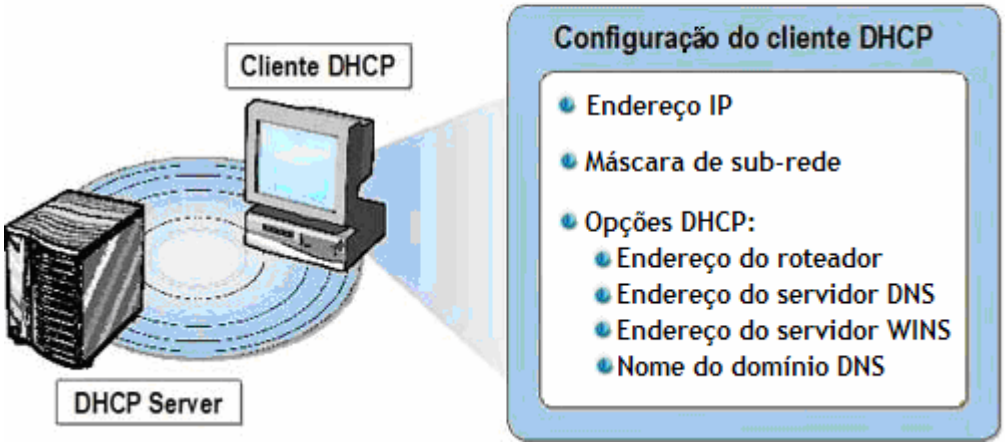
### 2.10.1 Exercícios 4: Atividades para configurar uma reserva de DHCP:

1. Abra o console DHCP.
2. Clique em ***Reservas*** do console.
3. Clique em ***Nova Reserva*** no menu ***Ação.***
4. Insira, na caixa ***Nova Reserva***, os valores a seguir:
   a. Nome da reserva
   b. Endereço IP
   c. Endereço MAC (sem hífen)
   d. Descrição
5. Selecione, em ***Tipos suportados***, uma das opções a seguir:
   a. Both
   b. DHCP only
   c. BOOTP only
6. Clique em ***Adicionar*** na caixa ***Novas Reservas*** e depois em ***Fechar***.


© 2003 Microsoft Corporation. Todos os direitos reservados.

## 2.11. Quais são as opções do DHCP?

As OPÇÕES DHCP são os parâmetros da configuração que será entregue aos clientes através do serviço DHCP.




***As opções do DHCP*** são os parâmetros de configuração que um serviço do DHCP atribui aos clientes quando lhes atribui o endereço IP.

### 2.11.1. Opções comuns de DHCP

- ***Roteador (Gateway padrão):*** É o endereço de qualquer gateway padrão ou roteador. O roteador é normalmente chamado de Gateway Padrão.
- ***Nome do Domínio:*** Um nome de domínio DNS define o domínio ao qual um computador cliente pertence. O computador cliente pode utilizar essas informações para atualizar o Servidor DNS para que outros computadores possam localizar o cliente.
- ***Servidores DNS e WINS:*** São os endereços dos Servidores DNS e WINS para os clientes utilizarem na comunicação da rede.

## 2.12. Exercício 5: Como configurar opções de DHCP?

***Para configurar uma opção de Servidor DHCP:***

1. Abra o console DHCP.
2. Clique em ***Opções do servidor*** do console, sob o nome do servidor
3. Clique em ***Configurar Opções*** no menu ***Ação***.
4. Selecione a opção que você deseja configurar na caixa ***Opções do servidor*** da lista ***Opções disponíveis***.
5. Preencha, em ***Entrada de dados***, as informações necessárias para configurar essa opção.
6. Clique em ***OK*** na caixa ***Opções do servidor***.

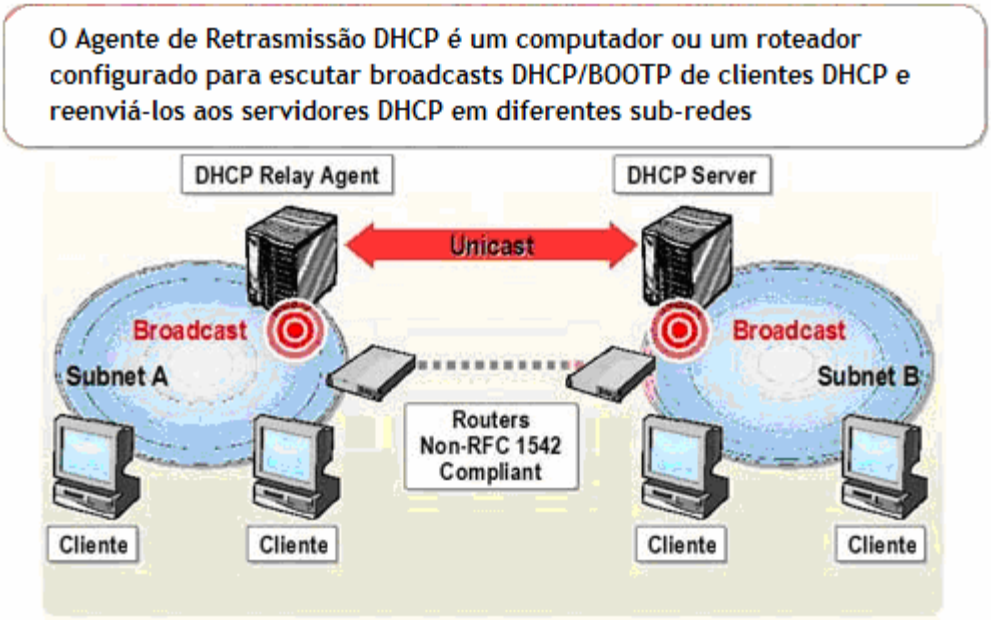
***Para configurar um Escopo de DHCP:***

1. Abra o console DHCP e sob o escopo apropriado, clique em ***Opções do escopo***.
2. Clique em ***Configurar Opções*** no menu ***Ação***.
3. Selecione, na caixa ***Opções do Escopo***, a opção que você deseja configurar na lista ***Opções Disponíveis***
4. Preencha, em ***Entrada de dados***, as informações necessárias para configurar essa opção.


© 2003 Microsoft Corporation. Todos os direitos reservados.

5. Clique em ***OK*** na caixa ***Opções do escopo***.

## 2.13. O que é o Agente de Retransmissão DHCP?




### 2.13.1. Definição

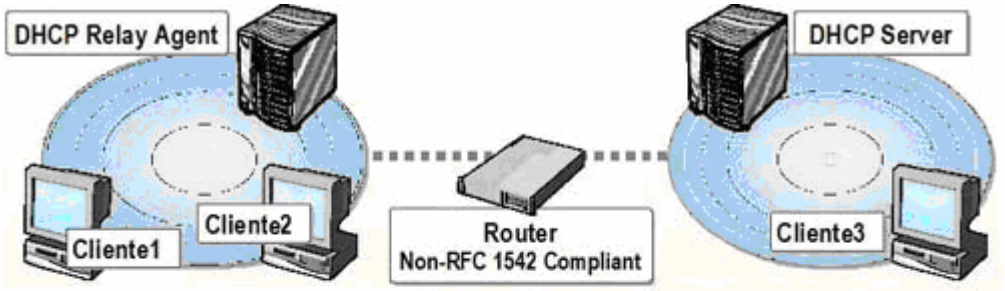
O ***DHCP Relay Agent*** é um computador ou roteador configurado para escutar a transmissão DHCP/BOOTP de clientes DHCP e reenviar essas mensagens aos Servidores DCHP em sub-redes diferentes. Os Agentes de Retransmissão DHCP/BOOTP são parte dos padrões DHCP e BOOTP e funcionam segundo os documentos padrão ***Request for Comments*** (RFCs) que descrevem o design do protocolo e o comportamento relacionado.

Um ***Roteador Compatível RFC 1542*** é um roteador que suporta o reenvio de tráfego de transmissão DHCP.

Os clientes DHCP utilizam broadcasts para obter a concessão do Servidor DHCP. Os roteadores normalmente não deixam estes broadcasts passarem, exceto quando estão configurados especificamente para deixá-las passar. No entanto, sem configuração adicional, os Servidores DHCP só fornecem endereços IP a clientes na sub-rede local. Para que você possa atribuir endereços a clientes em outros segmentos, é preciso configurar a rede para que os broadcasts DHCP possam chegar do cliente ao Servidor DCHP. Isso pode ser feito de duas formas: configurando os roteadores que conectam as sub-redes para deixar passar os broadcasts DHCP ou configurando o Agente de Retransmissão do DCHP. O Windows Server 2003 aceita o serviço de Roteamento e Acesso Remoto configurado para funcionar como Agente de Retransmissão do DHCP.


© 2003 Microsoft Corporation. Todos os direitos reservados.

## 2.14. Como funciona o Agente de Retransmissão de DHCP?




1. Cliente1 envia um pacote DHCPDISCOVER
2. O Agente de Retransmissão reenvia o DHCPDISCOVER para o servidor DHCP
3. O servidor envia o pacote DHCPOFFER para o Agente de Retransmissão
4. O Agente de Retransmissão envia o pacote DHCPOFFER ao Cliente1
5. O Cliente1 envia um pacote DHCPREQUEST
6. O Agente de Retransmissão reenvia o DHCPREQUEST para o servidor DHCP
7. O servidor envia o pacote DHCPACK para o Agente de Retransmissão
8. O Agente de Retransmissão envia o pacote DHCPACK ao Cliente1

O Agente de Retransmissão de DHCP oferece suporte à Geração de Concessão entre o cliente de DHCP e o Servidor DHCP, quando são separados por um roteador. Ele permite que o cliente DHCP receba um endereço IP de Servidor DHCP.

***Os passos a seguir descrevem o funcionamento do Agente de Retransmissão de DHCP:***

1. O cliente DHCP envia um broadcast de pacote DHCPDISCOVER.
2. O Agente de Retransmissão de DHCP, a partir da sub-rede do cliente, reenvia a mensagem DHCPDISCOVER ao Servidor DHCP usando unicast.
3. O Servidor DHCP usa unicast para enviar a mensagem DHCPOFFER ao Agente de Retransmissão de DHCP.
4. O Agente de Retransmissão de DHCP envia um pacote broadcast DHCPOFFER ao cliente DHCP na sua sub-rede.
5. O cliente DHCP envia um pacote broadcast DHCPREREQUEST.
6. O Agente de Retransmissão de DHCP, a partir da sub-rede do cliente, reenvia a mensagem DHCPREQUEST ao Servidor DHCP usando unicast.
7. O Servidor DHCP usa unicast para enviar a mensagem DHCPACK ao Agente de Retransmissão de DHCP.
8. O Agente de Retransmissão de DHCP envia um pacote broadcast DHCPACK ao cliente DHCP na sua sub-rede.


© 2003 Microsoft Corporation. Todos os direitos reservados.

### 2.14.1 Exercício 6: Como configurar o Agente de Retransmissão de DHCP?

***Para adicionar um Agente de Retransmissão de DHCP:***

1. Abra o console de Roteamento e Acesso Remoto.
2. Clique com o botão direito do mouse no servidor e depois em ***Configurar e ativar o Roteamento e Acesso Remoto***.
3. Clique em Avançar na janela do assistente ***Bem-vindo ao Assistente para Configuração do Servidor de Roteamento e Acesso Remoto***.
4. Selecione ***Configuração personalizada*** na página ***Configurações*** e clique em ***Avançar***.
5. Selecione ***Roteamento da LAN*** na página ***Configuração personalizada*** e clique em ***Avançar***.
6. Clique em ***Concluir*** na página ***Concluindo o Assistente de Configuração do Roteamento e Acesso Remoto***.
7. Clique em ***Sim*** na caixa de aviso ***Roteamento e Acesso Remoto***, para iniciar o serviço.
8. Expanda o servidor e o ***Roteamento IP*** no console e selecione ***Geral***.
9. Clique com o botão direito do mouse em ***Geral*** e depois em ***Novo Protocolo de Roteamento...***.
10. Clique em ***DHCP Relay Agent*** na caixa ***Novo Protocolo de Roteamento*** e depois em ***OK***.

***Para configurar o endereço IP do Servidor DHCP no Agente de Retransmissão de DHCP:***

11. Abra o console de Roteamento e Acesso Remoto.
12. Selecione ***Agente de Retransmissão DHCP*** no console.
13. Clique com o botão direito do mouse em ***Agente de Retransmissão DHCP*** e depois em ***Propriedades***.
14. Insira o endereço IP do Servidor DHCP que receberá os pedidos DHCP em ***Geral*** no campo ***Endereço do servidor***.
15. Clique em ***Adicionar*** e depois em ***OK***.

***Para habilitar o Agente de Retransmissão de DHCP em uma interface de roteador:***

16. Selecione ***Agente de Retransmissão DHCP*** no console.
17. Clique com o botão direito do mouse em ***Agente de Retransmissão DHCP*** e depois em ***Nova Interface***.
18. Selecione a interface que quiser ativar o Agente de Retransmissão de DHCP e depois clique em ***OK***.
19. Verifique se está selecionada a caixa ***Retransmitir pacotes DHCP*** em ***Geral***, da caixa ***Propriedades de Retransmissão DHCP***, em ***Geral***. Clique em ***OK.***

Para obter mais informações sobre o DHCP:

http://support.microsoft.com/default.aspx?scid=kb;en-us;323416

http://support.microsoft.com/default.aspx?scid=kb;en-us;325473

http://support.microsoft.com/default.aspx?scid=kb;en-us;323416

http://support.microsoft.com/default.aspx?scid=kb;en-us;323360

http://support.microsoft.com/default.aspx?scid=kb;en-us;323355


© 2003 Microsoft Corporation. Todos os direitos reservados.

## 3. Descrição de Sistema de Nomes de Domínio

O DNS é um serviço de resolução de nomes que resolve endereços amigáveis (como www.microsoft.com) em endereços IP (como 192.168.0.1).

***Sistema de Nomes do Domínio (DNS)*** é um banco de dados hierárquico distribuído que mapeia nomes de hosts DNS a endereços IP. O DNS permite a localização de computadores e serviços usando nomes alfanuméricos mais fáceis de lembrar. O DNS também permite a localização de serviços de rede, como Servidores de E-mail e Controladores de Domínio no Active Directory®.

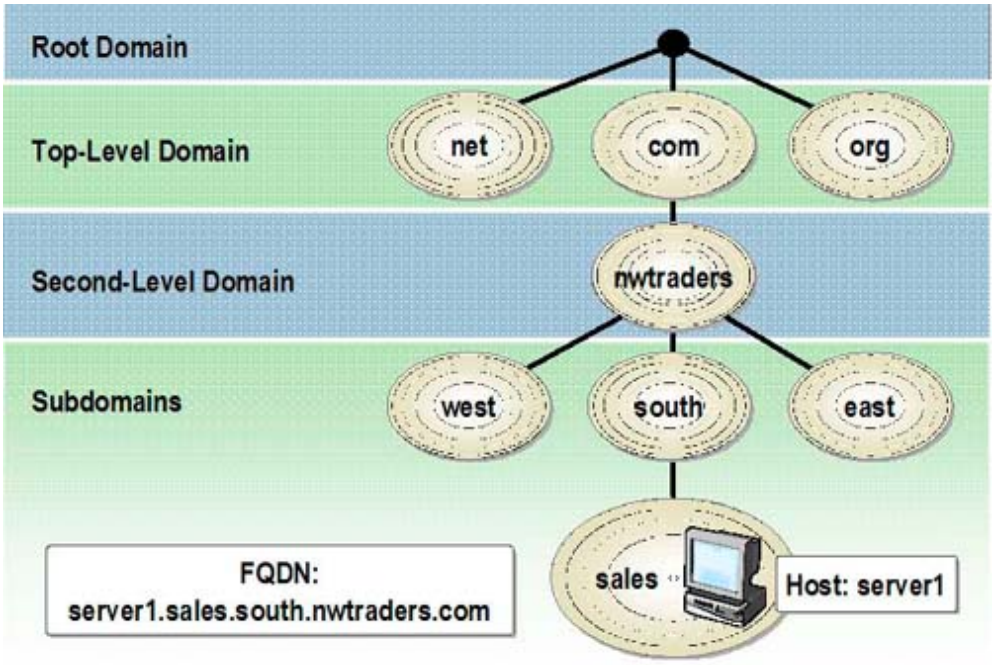
No DNS, os nomes de host residem em um banco de dados distribuído em múltiplos servidores, reduzindo a carga em um servidor e a capacidade para administrar esses sistemas de nomes. Além disso, como o banco de dados DNS é distribuído, o seu tamanho é ilimitado e o funcionamento não sofre prejuízos quando servidores adicionais são adicionados.

O InterNIC é responsável por delegar responsabilidade administrativa de partes do espaço de nome do domínio e também por registrar nomes de domínio. Estes últimos são administrados através do uso do banco de dados distribuído e armazenados em Servidores de Nomes, localizados em toda a rede. Cada Servidor de Nomes contém arquivos de bancos de dados que possuem informações para uma região, domínio, etc, criando assim uma hierarquia.

Para obter mais informações sobre o InterNic:

http://www.internic.net

### 3.1 O Que é Espaço do Nome do Domínio?




O ***Espaço de Nome de Domínio*** é uma árvore de nomes hierárquica que utiliza o DNS para identificar e localizar um host em um determinado domínio, em relação à raiz da árvore. Os nomes no banco de dados DNS estabelecem uma estrutura lógica chamada Espaço de Nome de Domínio que identifica a posição de um domínio na árvore e em seu domínio superior. A conversão principal é simplesmente: para cada nível de


© 2003 Microsoft Corporation. Todos os direitos reservados.

domínio, um ponto (.) é utilizado para separar cada descendente do subdomínio e do seu domínio de nível superior.

O ***Fully Qualified Domain Name (FQDN)*** é o nome do domínio de DNS que indica com certeza a localização do host a que ele se refere e a sua localização no Espaço de Nome do Domínio.

### 3.1.1 Exercício 7: Como instalar o serviço de Servidor DNS?

Para adicionar um servidor DNS, você deverá instalar o serviço de DNS em um computador executando o Microsoft® Windows® Server 2003.

***Antes de adicionar o serviço de Servidor DNS:***

- Verifique se a configuração IP no servidor está correta.
- Verifique se a configuração IP do servidor possui um endereço IP estático, uma máscara de sub-rede e um gateway padrão em ambiente roteado.
- Verifique se a conta do usuário tem as permissões corretas.

***Para adicionar o serviço de Servidor DNS:***

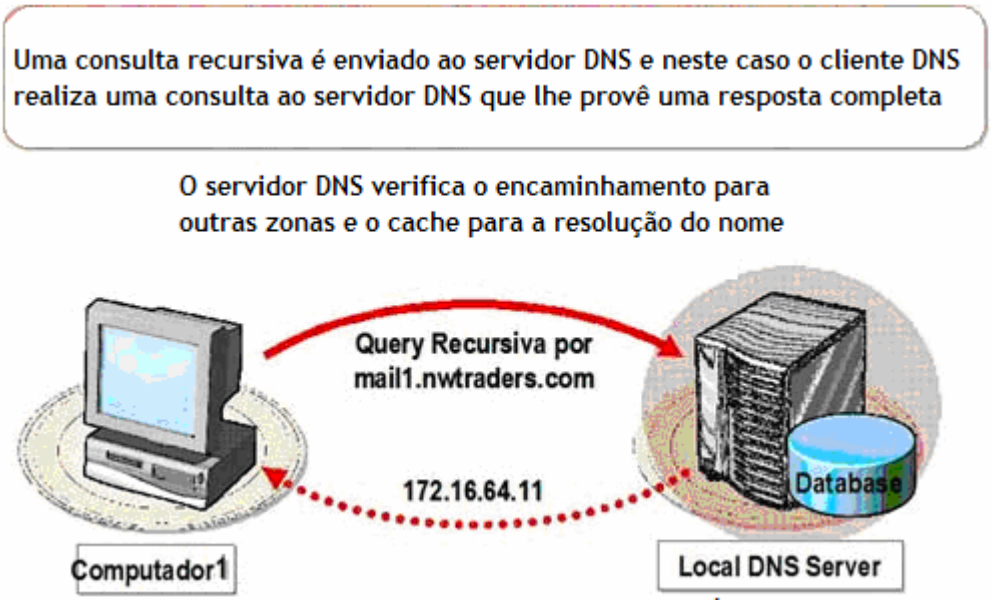
1. Inicie a sessão usando uma conta não administrativa.
2. Clique em ***Iniciar*** e depois em ***Painel de Controle***.
3. Abra as ***Ferramentas Administrativas*** no Painel de Controle e clique com o botão direto do mouse em ***Gerenciar o Servidor***, selecionando ***Executar como...***.
4. Selecione ***O seguinte usuário*** na caixa ***Executar como***, insira uma conta de usuário e senha que tenha permissões apropriadas para realizar a tarefa e clique em ***OK***.
5. Clique em ***Adicionar ou remover uma função*** na janela Gerenciar o Servidor.
6. Clique em ***Avançar*** na página ***Etapas Preliminares***.
7. Selecione ***Servidor DNS*** no assistente e clique em ***Avançar***.
8. Clique em ***Avançar*** na página ***Resumo das Seleções.***
9. Insira o CD do Microsoft Windows Server 2003, se for solicitado.
10. Clique em ***Cancelar*** na página ***Bem-vindo ao Assistente de Configuração do Servidor DNS***.
11. Clique em ***Concluir*** na página ***Configurar o Servidor***.

## 3.2 O que é uma consulta de DNS?

Uma ***Consulta*** é uma solicitação de resolução do nome enviado a um servidor DNS. Existem dois tipos de consulta: Recursiva e Iterativa.

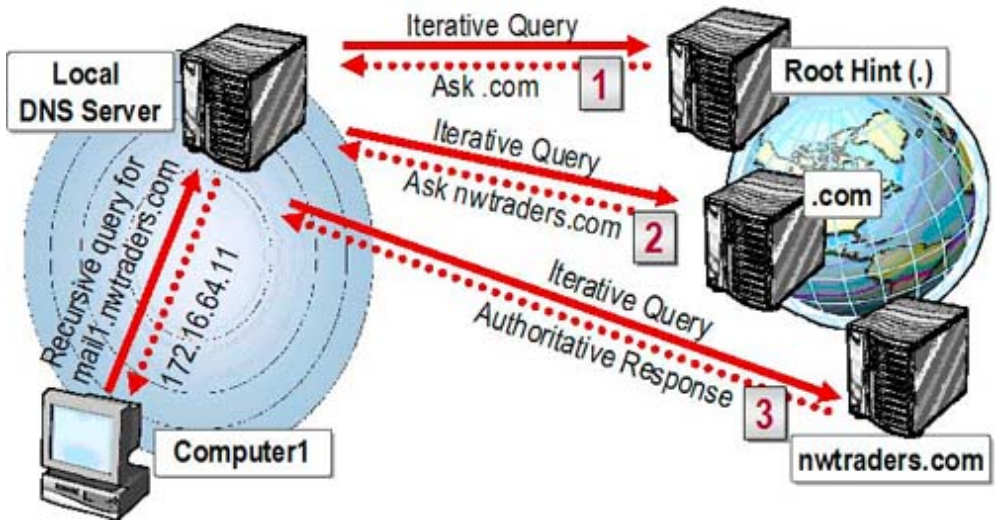

© 2003 Microsoft Corporation. Todos os direitos reservados.

### 3.2.1 Como funciona uma Consulta Recursiva?




Uma ***Consulta Recursiva*** é uma solicitação de resolução ao Servidor DNS, no caso do cliente realizar a consulta diretamente no Servidor DNS. A única resposta aceitável para uma Consulta Recursiva é a resposta completa ou a resposta onde o nome pode ser solucionado. Uma Consulta Recursiva nunca é redirecionada a outro servidor DNS. Se o DNS consultado não obtiver uma resposta do seu próprio banco de dados ou do cache, a resposta é um erro, indicando que não é possível solucionar o nome.

### 3.2.1 Como funciona uma Consulta Iterativa?

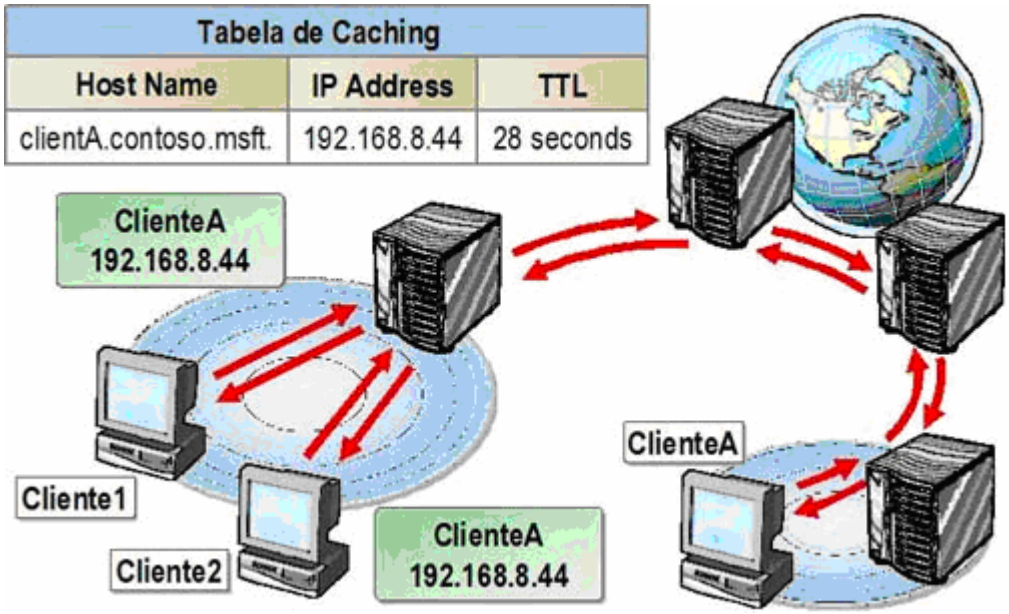



Diferente das Consultas Recursivas, em que um cliente faz um pedido de resolução e o Servidor DNS não obtém a resposta da sua própria base ou do cache, a Consulta Iterativa consulta outros Servidores DNS em nome do cliente para devolver a resposta. Exemplo: quando você precisa acessar um site na Internet, normalmente consulta o DNS de seu ISP, e ele se encarrega de entrar em contato com outros Servidores DNS até obter uma resposta. Mas analise o seguinte: é


© 2003 Microsoft Corporation. Todos os direitos reservados.

impossível na Internet que o DNS do seu ISP contenha todas as soluções possíveis em toda a Internet; por isso, os bancos de DNS distribuem e resolvem nomes de forma Iterativa uns para os outros.

### 3.2.3 Como funciona o cache de Servidores DNS?




***Caching*** é o processo temporário de armazenar informações recentes que resulta em um subsistema especial da memória para um acesso mais rápido.

Quando um servidor está processando uma Consulta Recursiva, é possível que seja necessário o envio de várias consultas para se encontrar resposta definitiva. Na pior das hipóteses, para solucionar um nome, o servidor local inicia na Raiz do DNS e começa a trabalhar para baixo até encontrar seus dados solicitados.

O servidor guarda as informações da resolução em seu cache por um tempo determinado. Este período de tempo é denominado TTL (Tempo de Vida) e é especificado em segundos. O administrador do servidor que contém a primeira zona onde estão os dados decide o valor do TTL. Quanto menor for o valor de TTL, mais fácil será manter dados consistentes em caso de modificações. No entanto, ele também gera mais carga de trabalho para o Servidor de Nomes.

Depois que o Servidor DNS salva no cache os dados, o TTL começa a diminuir até chegar a 0 (zero) e, nesse ponto, o registro é eliminado do cache do Servidor DNS. Enquanto o valor de TTL está ativo, o Servidor DNS soluciona os pedidos utilizando o registro de cache.


© 2003 Microsoft Corporation. Todos os direitos reservados.

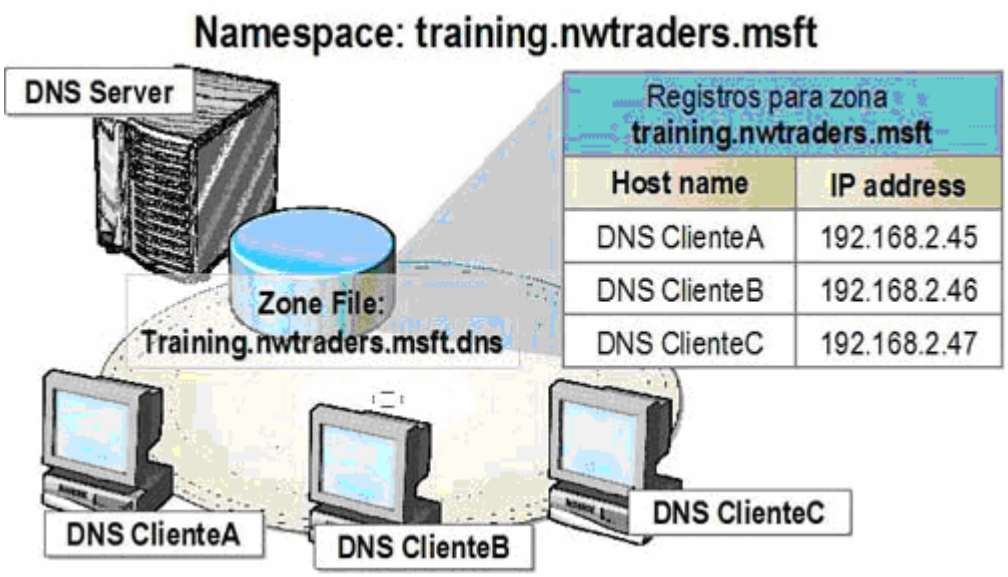
### 3.3. Exercício 8: Como configurar as propriedade do serviço de Servidor DNS?

Para configurar propriedades do serviço de Servidor DNS, você precisa atualizar as Dicas da Raiz do Servidor DNS. As Dicas de Raiz determinam se o seu servidor consulta a raiz da Internet ou se a raiz é um servidor interno.

***Para atualizar as Dicas de Raiz no Servidor DNS:***

1. Abra o console de DNS.
2. Selecione o servidor apropriado no console de DNS.
3. Clique em ***Propriedades*** do menu ***Ação***.
4. Em ***Root Hints***, você pode clicar em:
   - ***Adicionar***, para adicionar um Servidor de Nomes. Adicione o IP do seu servidor.
   - ***Editar***, para editar um Servidor de Nomes.
   - ***Remover***, para sair de um Servidor de Nomes.
   - ***Copiar do Servidor***, para copiar a lista de Servidores de Nome de outros Servidor DNS.
5. Clique em ***OK*** para fechar a caixa ***Propriedades***.
6. Feche o console de DNS.

### 3.4 Como os dados de DNS são armazenados e mantidos?




Uma ***zona*** é uma parte contígua do espaço dos nomes de domínio no qual um servidor DNS tem autoridade para solucionar consultas de DNS. O espaço de nomes de DNS pode se dividir em zonas diferentes, que armazenam informações de nomes sobre um ou vários domínios de DNS, ou parte deles. Para cada nome de domínio de DNS incluído em uma zona, ele se converte em origem autorizada das informações sobre este domínio.

***Antes de criar zonas, é preciso compreender os conceitos a seguir:***

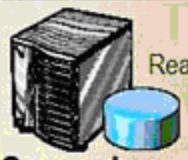
- ***Tipos de zonas.*** Os servidores DNS podem alojar vários tipos de zona. Para limitar o número de servidores DNS na rede, é possível configurar apenas um que permita ou aloje várias zonas. Também é possível configurar vários servidores para armazenar uma ou mais zonas com o objetivo de oferecer tolerância a falhas e distribuir a carga de trabalho administrativa e de resolução de nomes.


© 2003 Microsoft Corporation. Todos os direitos reservados.

- ***Arquivo de zona.*** Os registros de recursos que são armazenados em um arquivo de zona servem para sua própria definição. O arquivo de zona armazena informações utilizadas para converter nomes de hosts em endereços IP e vice-versa.

**Importante:** Para criar zonas e administrar um servidor DNS que não é executado em um controlador de domínio, é preciso ser membro do grupo de administradores dessa máquina. Para configurar um servidor DNS que é executado em um controlador de domínio, é preciso ser membro dos grupos de administradores de DNS, administradores de domínio ou administradores da empresa (Enterprise).

### 3.4.1. Identificação de tipos de zonas

| Zonas | Descrição |
|---|---|
| Primary | Cópia Read/write de uma base de dados DNS |
|   Secondary | Cópia Read-only de uma base de dados DNS |
| Stub | Cópia de uma zona contendo recursos limitados |

Na tabela seguinte, estão descritos os quatro tipos de zonas que podem ser configurados e os arquivos de zona associados a elas.

**Primária Padrão:** Contém uma versão de leitura e gravação do arquivo da zona que é armazenado em um arquivo de texto padrão. As modificações realizadas na zona são registradas nesse arquivo.

**Secundária Padrão:** Contém uma versão de leitura somente do arquivo da zona que é armazenado em um arquivo de texto padrão. As modificações realizadas na zona são registradas no arquivo da zona primária e replicadas no arquivo da zona secundária. Crie uma zona secundária padrão para criar uma cópia de uma zona existente e do seu arquivo de zona. Dessa forma, pode-se distribuir a carga de trabalho da resolução de nomes entre vários servidores DNS.

**Integrada ao Active Directory:** Em vez de armazenar as informações de zona em um arquivo de texto, elas são armazenadas no Active Directory. As atualizações da zona são automaticamente realizadas durante a replicação do Active Directory. Crie uma zona integrada do Active Directory para simplificar o planejamento e a configuração de um espaço de nomes de DNS. Não é necessário configurar servidores DNS para especificar como e quando serão feitas as atualizações, já que o Active Directory mantém as informações da zona.


© 2003 Microsoft Corporation. Todos os direitos reservados.

**Zona Stub:** A zona Stub são cópias de uma zona que contêm somente os registros necessários para identificação no servidor DNS de autorização dessa zona. Uma zona stub contém um subconjunto de dados da zona que consiste em registros SOA, NS e A. As zonas Stub podem ser utilizadas quando um servidor interno DNS representa a raiz no lugar dos Servidores de Raiz da Internet.

### 3.4.1.1 Zona Primária Padrão

O servidor principal de uma zona atua como ponto de atualização da zona. As zonas recém-criadas são sempre desse tipo. Com o Windows Server 2003, as zonas primárias podem ser utilizadas de uma das duas formas: como zonas padrão primárias ou como zonas primárias integradas com o Active Directory. Na zona primária padrão, apenas um servidor pode armazenar e carregar a cópia mestre da zona. Se você criar uma zona e a mantiver como zona primária padrão, nenhum servidor principal adicional terá permissão para acessar a zona. Apenas um servidor pode aceitar atualizações dinâmicas e processar as modificações da zona.

O modelo primário padrão define um ponto de concentração de falhas. Por exemplo, se, por qualquer motivo, o servidor primário de uma zona não estiver disponível para a rede, não é possível realizar nenhuma atualização dinâmica da zona. Lembre-se de que as consultas de nomes nas zonas não são afetadas e podem prosseguir sem interrupção sempre que os servidores secundários da zona estejam disponíveis para respondê-las.

O acréscimo da nova zona primária a um servidor existente pode ser concluído sempre que é preciso ter domínios ou subdomínios adicionais no espaço de nomes de domínio de DNS. Por exemplo, era possível ter uma zona para um domínio de segundo nível como mcrosoft.com e adicionar uma zona principal ao novo subdomínio como nwtraders.msft. Nesse exemplo, é possível criar a zona nova para o subdomínio com o assistente para configuração da nova zona do complemento de DNS. Depois de finalizar, é preciso criar uma delegação na zona primária do novo domínio (como a zona microsoft.com) para completar o acréscimo do novo subdomínio e a sua zona primária.

Nas zonas primárias padrão, pode ser necessário trocar o servidor primário designado para uma zona. Por exemplo, suponhamos que o servidor primário atual de uma zona primária padrão seja o Servidor A e o novo servidor primário da zona seja o Servidor B. Para influir na mudança do estado do Servidor A para o Servidor B, faça as seguintes modificações de zona:

1. Adicione um novo registro de recursos (RR) de host (A) para o Servidor B.
2. Atualize o registro de recursos de servidor de nomes (NS) da zona para sair do Servidor A e incluir o Servidor B como servidor autorizado e configurado, que aponta para o novo registro de recursos RR A adicionado ao passo 1.
3. Revise o nome do campo do proprietário de registro de recursos de início de autoridade (SOA) para a zona do Servidor A ao Servidor B.
4. Remova o registro de recursos A antigo do Servidor A.
5. Teste a zona principal para garantir que os registros de delegação (registros de recursos NS ou A) utilizados se atualizem para fazer referência ao Servidor B.

### 3.4.1.2 Zonas Padrão Secundárias

As especificações de design do DNS recomendam o uso de, pelo menos, dois servidores DNS para armazenar cada zona. Para as zonas de tipo padrão primárias, é preciso ter um servidor secundário para adicionar e configurar a zona que aparece antes dos servidores DNS da rede. Os servidores secundários podem proporcionar um meio para reduzir o tráfego de consultas de DNS nas áreas da rede em que uma zona seja muito consultada e utilizada. Além disso, se um servidor primário parar de funcionar, o servidor secundário pode realizar parte da resolução de nomes na zona até que o servidor primário esteja disponível.


© 2003 Microsoft Corporation. Todos os direitos reservados.

Ao instalar um servidor secundário, tente colocá-lo o mais próximo possível dos clientes que precisam de mais nomes na zona. Além disso, também é recomendável colocar os servidores secundários através de um roteador, seja em outras sub-redes (se for utilizada uma rede LAN) ou em links de WAN. Deste modo, utiliza-se de forma eficaz um servidor secundário como cópia de segurança local nos casos em que um link de rede intermediário é convertido em um ponto de concentração de falhas entre servidores e clientes de DNS que utilizam a zona.

Como o servidor primário sempre mantém a cópia mestre das atualizações e mudanças efetuadas na zona, o servidor secundário depende de mecanismos de transferências de zonas de DNS para obter suas informações e mantê-las atualizadas. Algumas questões como os métodos de transferência de zona, sejam mediante transferências de zona completas ou adicionais, são simplificadas quando são utilizados servidores secundários. Ao considerar o impacto dos servidores secundários nas transferências de zona, considere sua vantagem como origem da cópia de segurança de informações e compare-a com o custo agregado estimado da infra-estrutura de rede.

Uma regra simples é que para cada servidor secundário adicionado aumenta o uso da rede (devido ao tráfego adicional gerado na replicação de zona) e o tempo necessário para sincronizar a zona em todos os servidores secundários.

### 3.4.1.3 Zonas Integradas ao Active Directory

No Windows Server 2003, é possível adicionar mais servidores principais a uma zona devido às características integradas de armazenamento e replicação de diretórios do serviço de DNS. Para isso, é necessário trocar uma zona e integrá-la ao Active Directory.

Para integrar uma zona existente ao Active Directory, modifique o tipo de uma zona no servidor principal de origem onde ela foi criada pela primeira vez. Quando o tipo de zona for trocado de padrão principal para Integrada ao Active Directory, é possível adicionar a zona a outros servidores DNS. Para isso, é preciso configurá-las para iniciar a partir dos serviços de diretório quando o serviço de DNS for reiniciado.

Quando essa opção é selecionada, outros servidores DNS que funcionam como controladores de domínio para o domínio do Active Directory podem consultar o diretório e carregar automaticamente todas as zonas integradas a ele armazenadas no banco de dados de diretórios. Não é preciso executar nenhum outro passo. Qualquer servidor DNS que funcione como parte do Active Directory é também, de forma predeterminada, servidor principal das zonas integradas ao diretório.

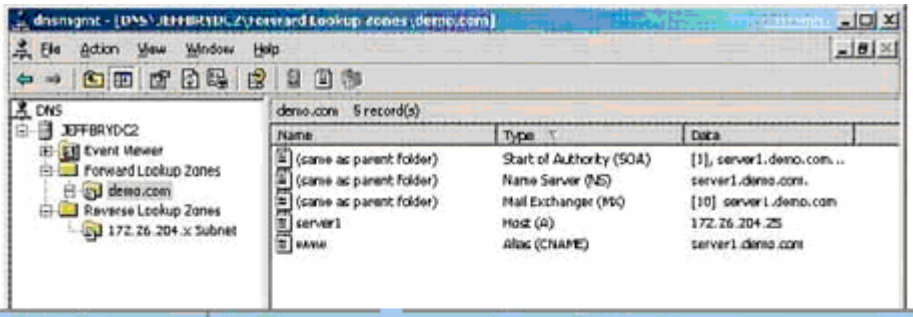
Nas zonas principais integradas ao diretório, os servidores secundários são admitidos, mas não são necessários para oferecer tolerância a erros. Por exemplo, os servidores DNS que funcionam como controladores de domínio do Windows Server 2003 podem ser servidores principais redundantes de uma zona e oferecer as mesmas vantagens que um servidor secundário, além de outras adicionais.

Como o arquivo de zona se mantém no contexto de nomes de domínio do Active Directory, os controladores de domínio devem estar no mesmo domínio para atuar como servidores principais redundantes em uma zona. Quando for necessário compartilhar essas informações de zona entre domínios, deverá ser criada uma zona secundária padrão.

**Nota:** Esse tipo de zona será visto com mais clareza no capítulo 4 "Active Directory".


© 2003 Microsoft Corporation. Todos os direitos reservados.

## 3.5 O que são os Registros de Recursos e Tipos de Recursos?




| Record type | Descricão |
|---|---|
| A | Resolve nomes de host a endereço IP |
| PTR | Resolve endereço IP a nomes de host |
| SOA | O primeiro registro de um arquivo de zona |
| SRV | Resolve nomes de servidores e seus serviços |
| NS | Identifica o servidor DNS para cada zona |
| MX | O servidor de correio eletrônico |
| CNAME | Resolve nomes de host a nomes de host |

Os arquivos de zona contêm informações sobre as quais um servidor DNS faz referência para realizar duas tarefas distintas: converter nomes de host em endereços IP e converter endereços IP em nomes de host. Essas informações são armazenadas como registros de recursos que preenchem o arquivo de zona. Um arquivo de zona contém os dados de resolução de nomes de uma zona, incluindo registros de recursos com informações para responder a consultas DNS. Os registros de recursos são entradas do banco de dados que incluem vários atributos de uma máquina, como o nome do host ou o nome do domínio completo, o endereço IP e o alias.

***Os servidores DNS podem conter os seguintes tipos de registros de recursos:***

**A (host):** Contém informações de atribuições de nome a endereços IP utilizados para atribuir um nome de domínio de DNS a um endereço IP de host na rede. Os registros de recursos A também são conhecidos como registros de host.

**NS (servidor de nomes):** Designa os nomes de domínio de DNS dos servidores com autorização para uma determinada zona ou uma zona que contenha o arquivo de zona desse domínio.

**CNAME (nome canônico):** Permite fornecer nomes adicionais a um servidor que já tem um nome em um registro de recursos A. Por exemplo, se o servidor chamado webserver1.nwtraders.msft armazenar o site da Web de nwtraders.msft, o seu nome comum deve ser www.nwtraders.msft. Os registros de recursos CNAME também são conhecidos como registros de alias.

**MX (mail exchanger):** Especifica o servidor que aplicativos de correio eletrônico podem entregar correspondência. Por exemplo, se você tiver um servidor de correio em execução em um equipamento chamado mail1.nwtraders.msft e quiser que todo a correspondência de NomedeUsuário@nwtraders.msft seja entregue nesse servidor, é necessário que o registro de recursos MX exista na zona de nwtraders.msft e aponte ao servidor de correio desse domínio.

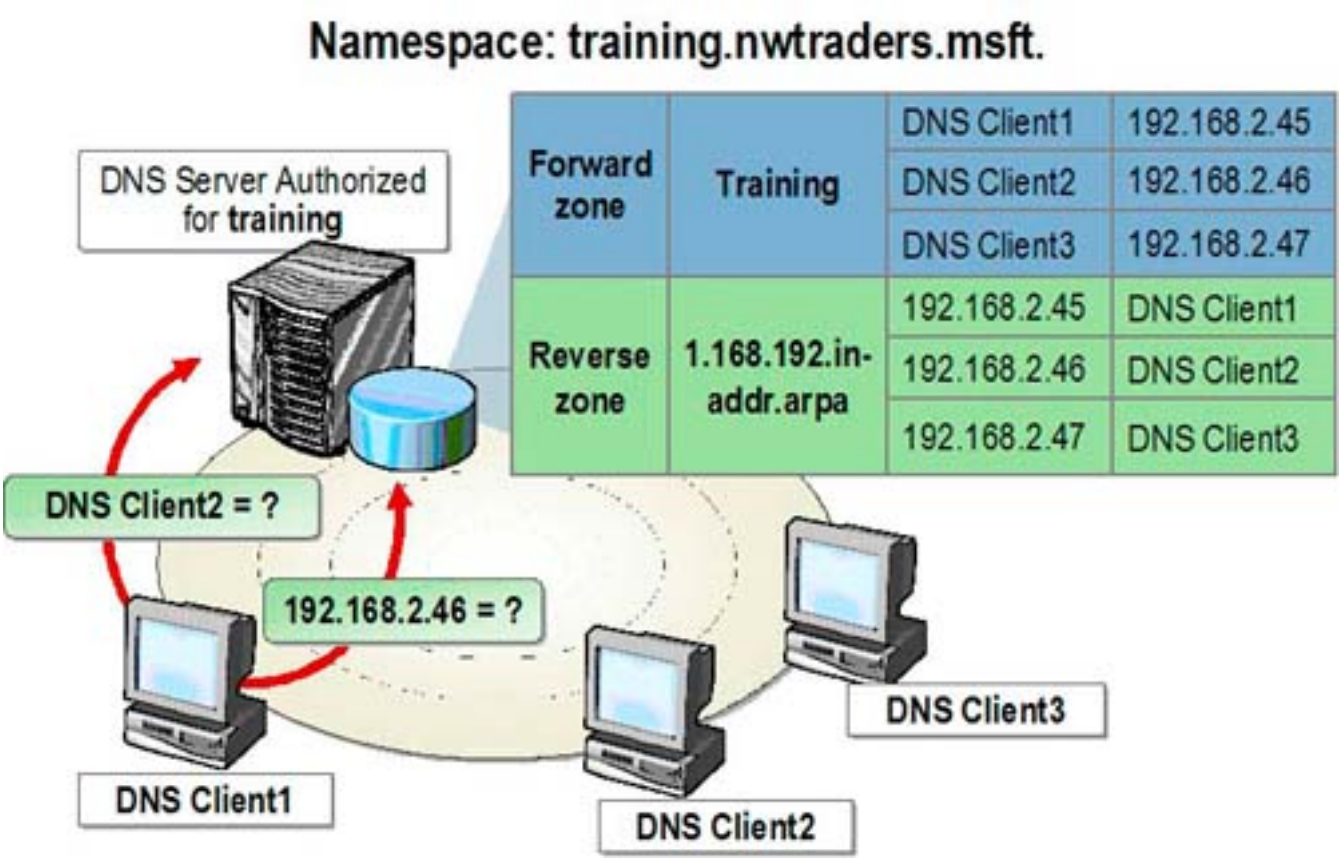

© 2003 Microsoft Corporation. Todos os direitos reservados.

**SOA (Start Of Authority):** Indica o ponto de partida ou o ponto de origem da autoridade para as informações armazenadas em uma zona. O registro de recursos SOA é o primeiro que é criado quando uma nova zona é adicionada. Ele também possui vários parâmetros que outros equipamentos que usam DNS utilizam para determinar por quanto tempo a informação da zona será utilizada e com que freqüência as atualizações devem ser realizadas.

**PTR (ponteiro):** Se você utilizar uma zona de pesquisa inversa criada no domínio in-addr.arpa para designar uma atribuição inversa de um endereço IP de host a um nome de domínio DNS de host.

**SRV (serviço):** É onde são registrados os serviços para os quais os clientes podem encontrar um serviço mediante DNS. Os registros SRV são utilizados para identificar serviços no Active Directory e também são conhecidos como registros de localização de serviço.

## 3.6 Criação de zonas de pesquisa padrão




Na maioria das pesquisas de DNS, os clientes costumam realizar uma busca direta, que é uma solicitação para designar um nome de equipamento a um endereço IP. O DNS também fornece um processo de pesquisa inversa que permite que os clientes solicitem um nome do equipamento conforme o endereço IP do equipamento.

### 3.6.1. Criação de uma zona de pesquisa direta

Para criar uma zona de pesquisa direta, clique em ***Nova zona...*** em ***Zona de pesquisa direta*** para iniciar o Assistente de nova zona. O assistente o guiará pelo processo de atribuição de nomes à zona


© 2003 Microsoft Corporation. Todos os direitos reservados.

e ao arquivo de zona, e também criará automaticamente a zona, o arquivo de zona e os registros de recursos necessários para o servidor DNS onde foi criada a zona.

### 3.6.2. Criação de uma zona de pesquisa inversa

Para criar uma zona de pesquisa inversa, clique em ***Nova zona...*** em ***Zona de pesquisa inversa*** para iniciar o Assistente de nova zona. O assistente indica como especificar a identificação da rede ou o nome da zona e como comprovar o nome do arquivo de zona segundo as informações de identificação da rede. Também são automaticamente criados a zona, o arquivo de zona e o registro de recursos necessários para o servidor DNS onde a zona foi criada.

O domínio in-addr.arpa é um domínio DNS especial de nível superior que está reservado para a atribuição inversa de endereços IP nos nomes do host de DNS. Para criar o espaço de nomes inverso, são formados subdomínios no domínio in-addr.arpa com a ordem inversa dos números em notação decimal com pontos dos endereços IP.

Para cumprir os padrões RFC, o nome da zona de pesquisa inversa exige o sufixo do domínio in-addr.arpa. Para criar uma zona de pesquisa inversa, este sufixo é automaticamente adicionado ao final da identificação da rede. Por exemplo, se a rede utiliza o identificador de rede de classe B 172.16.0.0, o nome da zona de pesquisa inversa é convertido em 16.172.in-addr.arpa.

## 3.7. Configuração de zonas padrão

Para cada zona, o servidor que mantém os arquivos de zona primária padrão é chamado de ***servidor primário***, e os servidores que armazenam os arquivos de zona secundária padrão são chamados ***servidores secundários***. Um servidor DNS pode armazenar o arquivo de zona primária padrão (como servidor primário) de uma zona e o arquivo de zona secundária padrão (como servidor secundário) de outra zona.

***Para configurar um ou vários servidores DNS para armazenar:***

- Uma ou várias zonas primárias padrão.
- Uma ou várias zonas secundárias padrão.
- Uma combinação de zonas primárias padrão e zonas secundárias padrão.

**Nota:** Para criar uma zona secundária padrão, é preciso criar primeiro uma zona primária padrão.

### 3.7.1 Especificação de um Servidor DNS Mestre para uma zona secundária

Ao adicionar uma zona secundária padrão, é preciso designar um ou vários servidores DNS de onde obter informações de zona. O servidor ou os servidores designados são conhecidos como Servidores DNS Mestres. Um ***Servidor DNS Mestre*** transfere informações da zona ao servidor DNS secundário. Você pode designar um servidor primário ou outro servidor secundário como Servidor DNS Mestre para una zona secundária padrão.

Para especificar um Servidor DNS Mestre na página Servidores Mestres no Assistente de nova zona, insira o endereço IP do Servidor Mestre na caixa de Endereço IP e clique em Adicionar.

## 3.8 Exercício 9: Configurar as zonas DNS

Configurar uma zona de pesquisa do tipo primário

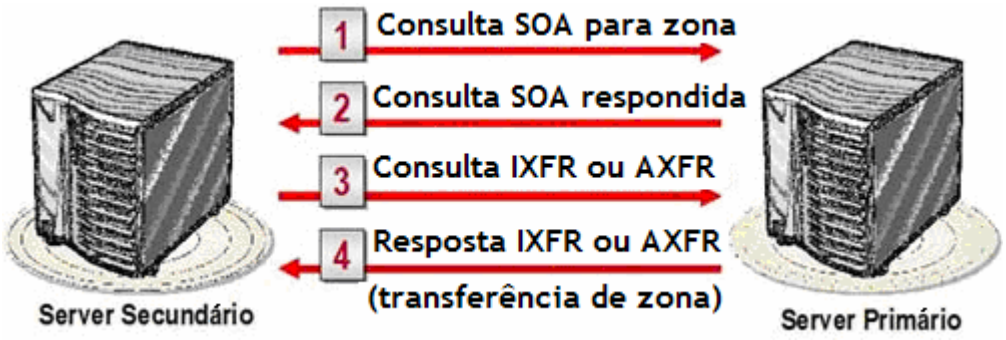
**Nome de zona**: ***nwtraders.msft***


© 2003 Microsoft Corporation. Todos os direitos reservados.

Depois de concluir essa tarefa, você obterá uma zona primária configurada.

1. Abra o console DNS.
2. Clique com o botão direito do mouse no Servidor DNS do console de DNS e depois em ***Nova zona...***
3. Clique em ***Avançar*** na página ***Bem-vindo ao Assistente de nova zona***,
4. Selecione ***Zona primária*** na página ***Tipo de Zona*** e clique em ***Avançar***.
5. Selecione ***Zona de pesquisa direta*** na página ***Zona de Pesquisa direta ou inversa***, e depois clique em ***Avançar***.
6. Insira o nome de DNS da zona na página ***Nome da Zona***, e clique em ***Avançar***.
7. Clique em ***Avançar*** na página ***Arquivo de Zona*** para aceitar os padrões.
8. Clique em ***Não permitir atualizações dinâmicas*** e clique em ***Avançar***.
9. Clique em ***Concluir*** na página ***Concluindo o Assistente de nova zona***.
10. Feche o console de DNS.

## 3.9. Processo de transferência de zona




Para proporcionar disponibilidade e tolerância a falhas na resolução de nomes, os dados da zona devem estar disponíveis a partir de mais de um servidor DNS de uma rede. Por exemplo, se você utilizar um único servidor DNS e ele não responder, as consultas de nomes falharão. Quando você configura mais de um servidor para armazenar uma zona, é preciso realizar transferências de zonas para replicar e sincronizar os dados da zona entre os servidores que estão configurados para armazená-las.

### 3.9.1. Transferência de zona

A ***transferência de zona*** é o processo no qual um arquivo de zona se replica em outro servidor DNS. As transferências da zona são realizadas quando as atribuições de nomes e endereços IP são modificadas no domínio. Quando isso ocorre, os arquivos de zona modificados são copiados do Servidor Mestre para seus servidores secundários.

### 3.9.2. Transferência de zona adicional

No Windows Server 2003, as informações de uma zona são atualizadas através de ***transferências de zona adicionais (IXFR)***, que só replicam as trocas realizadas no arquivo de zona, em vez de replicar todo o arquivo. Os servidores DNS que não aceitam IXFR solicitam o conteúdo inteiro de um arquivo de zona quando iniciam uma transferência de zona. Isso é conhecido como AXFR ou ***transferência de zona completa***.

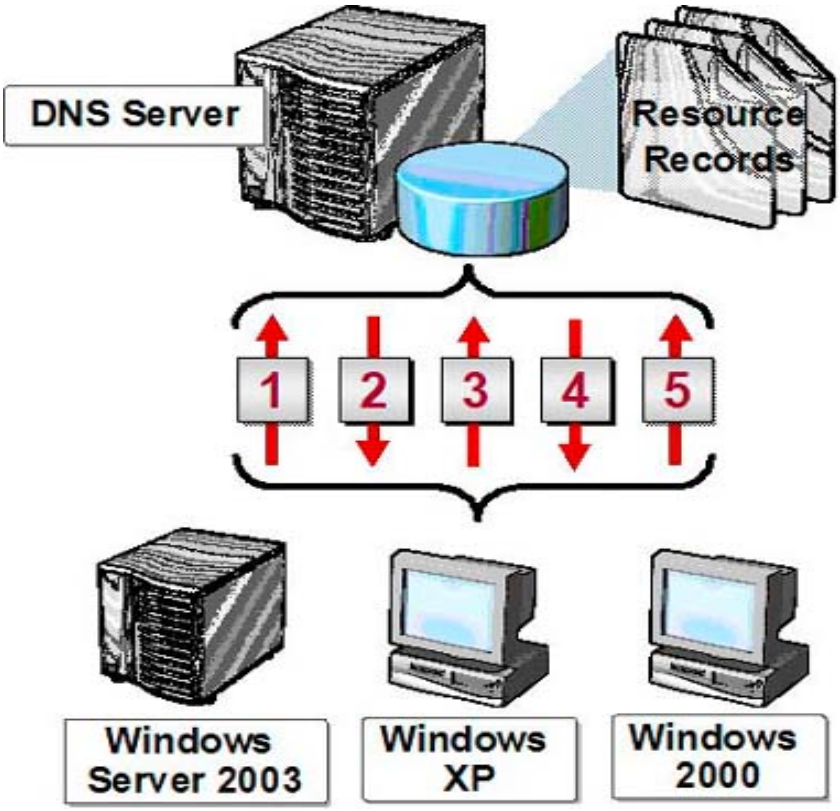
***O processo de transferência de zona se inicia quando uma das seguintes situações ocorre:***

- Um servidor mestre envia ao servidor ou servidores secundários uma notificação informando que ocorreu uma modificação na zona. Quando o servidor secundário recebe a notificação, ele verifica as modificações no Servidor Mestre.
- Cada servidor secundário verifica periodicamente um servidor mestre para comprovar se houve modificação no arquivo de zona, mesmo que ele não tenha sido notificado sobre


© 2003 Microsoft Corporation. Todos os direitos reservados.

nenhuma modificação. Isso ocorre quando o serviço de Servidor DNS é iniciado no servidor secundário ou durante o intervalo de atualização no servidor secundário.

## 3.10. Introdução às atualizações dinâmicas




Você pode configurar servidores DHCP para atribuir automaticamente endereços IP para máquinas clientes. Quando um cliente recebe um novo endereço IP de um servidor DHCP, ele deve atualizar as informações de atribuições de nomes a endereços IP armazenados no servidor DNS. No Windows 2003, os servidores e os clientes DHCP podem registrar e atualizar dinamicamente as informações dos servidores DNS configurados para permitir atualizações dinâmicas.

### 3.10.1 Protocolo de atualização dinâmica

O protocolo de atualização dinâmica permite que a máquinas clientes atualizem automaticamente seus registros de recursos em um servidor DNS, sem necessidade de intervenção do administrador. As máquinas com Windows 2000, Windows XP e Windows Server 2003 são configuradas para realizar atualizações dinâmicas quando são configuradas com um endereço IP estático também.

### 3.10.2 Processo de atualização dinâmica

Quando um servidor DHCP atribui um endereço IP a um cliente DHCP baseado no Windows 2000 ou no Windows Server 2003, o seguinte processo é executado:

1. O cliente inicia uma mensagem de solicitação de DHCP ao servidor DHCP, na qual ele solicita um endereço IP. Essa mensagem inclui o nome de domínio completo.
2. O servidor DHCP devolve ao cliente uma mensagem de confirmação de DHCP na qual ele fornece uma concessão de endereço IP.


© 2003 Microsoft Corporation. Todos os direitos reservados.

3. O cliente envia ao servidor DNS uma solicitação de atualização de DNS do seu próprio registro de pesquisa direita, o registro de recursos A (endereço).
4. O servidor DHCP envia atualizações para o registro de pesquisa inversa do cliente DHCP, o registro de recursos PTR (ponteiro). Para realizar essa operação, o servidor DHCP utiliza o nome do domínio completo obtido no primeiro passo.

### 3.10.3. Atualizações dinâmicas para clientes com versões anteriores do Windows

As máquinas clientes que executam versões anteriores do Windows não permitem atualizações dinâmicas. É preciso configurar o servidor DHCP para que ele sempre atualize os registros de recursos A e PTR desses clientes. Nesse caso, o processo a seguir tem início:

1. O cliente inicia uma mensagem de solicitação de DHCP ao servidor DHCP, na qual ele solicita um endereço IP. Ao contrário das mensagens de solicitação de DHCP dos clientes DHCP baseados no Windows 2000, a solicitação não inclui um nome de domínio completo.
2. O servidor devolve ao cliente uma mensagem de confirmação de DHCP na qual ele fornece uma concessão de endereço IP.
3. O servidor DHCP envia ao servidor DNS atualizações dos registros de recursos A e PTR do cliente.

### 3.10.4. Configuração do Servidor DNS para permitir atualizações dinâmicas

Para configurar um servidor DNS para permitir atualizações dinâmicas, abra a caixa de diálogo ***Propriedades*** da zona no servidor DNS que deseja configurar. Na guia ***Geral***, na caixa de listagem ***Permitir atualizações dinâmicas?***, clique em ***Sim***. Na tabela seguinte, estão descritas as opções disponíveis para as atualizações dinâmicas.

***Não*** Desativa as atualizações dinâmicas nesta zona
***Sim*** Ativa as atualizações dinâmicas nesta zona
***Apenas atualizações seguras*** Permite atualizações dinâmicas seguras de uma zona integrada do Active Directory realizadas a partir de máquinas clientes autorizadas.

Para obter mais informações sobre o DNS:

http://www.microsoft.com/Windows2000/technologies/communications/dns/default.asp

http://support.microsoft.com/default.aspx?scid=kb;en-us;814591

http://support.microsoft.com/default.aspx?scid=kb;en-us;323445

http://support.microsoft.com/default.aspx?scid=kb;en-us;323380

http://support.microsoft.com/default.aspx?scid=kb;en-us;323383

http://support.microsoft.com/default.aspx?scid=kb;en-us;323419

http://support.microsoft.com/default.aspx?scid=kb;en-us;324259

http://support.microsoft.com/default.aspx?scid=kb;en-us;324260

http://support.microsoft.com/default.aspx?scid=kb;en-us;323417

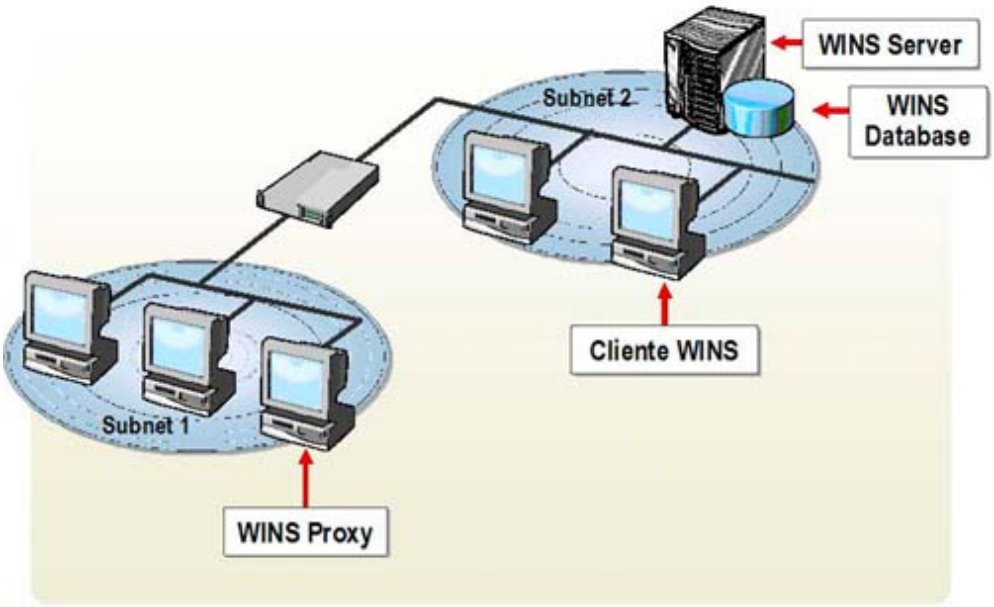

© 2003 Microsoft Corporation. Todos os direitos reservados.

http://support.microsoft.com/default.aspx?scid=kb;en-us;816518

http://support.microsoft.com/default.aspx?scid=kb;en-us;816567

http://support.microsoft.com/default.aspx?scid=kb;en-us;323418

## 4. Descrição do WINS (Windows Internet Name System)




O método mais comum para resolver nomes NetBIOS remotos e locais é o uso de um servidor de nomes NetBIOS.

Quando um usuário executa determinados comandos, como ***net use***, um aplicativo NetBIOS interage com a rede e o processo de resolução de nomes NetBIOS é iniciado. No cache de nomes NetBIOS, é possível comprovar se existe a atribuição de nome NetBIOS no endereço IP do host de destino. Se o nome NetBIOS não estiver no cache, o cliente tentará determinar o endereço IP do host de destino através de outros métodos.

Se o nome não puder ser resolvido com o cache, o nome NetBIOS do host de destino é enviado ao servidor de nomes NetBIOS configurado para o host de origem. Quando o nome é convertido em um endereço IP, ele é devolvido ao host de origem.

O WINS é a implementação da Microsoft de um servidor de nomes NetBIOS.

***Para que o WINS funcione corretamente em uma rede, cada cliente deve:***

- Registrar seu nome no banco de dados WINS. Ao iniciar um cliente, ele registra seu nome no servidor WINS configurado.
- Renovar o registro em intervalos configuráveis. Os registros dos clientes são temporários e, por isso, os clientes WINS devem renovar regularmente seu nome ou a sua concessão será expirada.
- Liberar os nomes dos bancos de dados ao fechar. Se o cliente WINS não precisar mais do nome, por exemplo, quando ele é excluído, é enviada uma mensagem para pedir ao servidor WINS que esse nome seja liberado.

***Depois de ter configurado o WINS como método de resolução de nomes, o cliente também o usa para finalizar as consultas de nomes NetBIOS. Para eles, as seguintes ações devem ser realizadas:***


© 2003 Microsoft Corporation. Todos os direitos reservados.

1. Se o cliente não puder resolver o nome do seu cache, envie uma consulta de nome ao seu servidor WINS principal. Se ele não responder, o cliente enviará a solicitação mais duas vezes.
2. Se o cliente não receber uma resposta do servidor WINS principal, ele envia outra solicitação a todos os servidores WINS adicionais, configurados no cliente. Se um servidor WINS resolver o nome, ele responderá ao cliente com o endereço IP do nome NetBIOS solicitado.
3. Caso nenhuma resposta seja recebida, o servidor WINS enviará uma mensagem indicando que o nome não foi encontrado e o cliente passará para o método seguinte de resolução de nomes configurado.

## 4.1 Exercício 10: Instalação do WINS

Para criar um servidor WINS, instale o WINS em uma máquina onde o ***Windows Server 2003*** esteja sendo executado.

***Para instalar o WINS:***

1. Clique duas vezes em ***Adicionar ou Remover Programas*** no Painel de controle.
2. Clique em ***Adicionar ou remover componentes do Windows***.
3. Clique em Serviços de Rede e em Detalhes na página ***Componentes do Windows*** do Assistente para ver os componentes do Windows, em ***Componentes***.
4. Selecione a caixa ***Serviço WINS*** na caixa de diálogo ***Serviços de rede*** em ***Subcomponentes*** e clique em ***Ok***.
5. Clique em ***Avançar***.

## 4.2. Estudo de registros do banco de dados WINS

A opção WINS do Microsoft Management Console (MMC) permite que o usuário veja o conteúdo do banco de dados WINS e busque entradas específicas.

**Abertura do banco de dados WINS**

***Para abrir o banco de dados WINS:***

1. Expanda o nome do servidor em WINS e clique em ***Registros ativos***.
2. Clique com o botão direito do mouse em ***Registros ativos*** e depois clique em ***localizar por proprietário***.
3. Clique em ***Todos os Proprietários*** na caixa de diálogo ***localizar por proprietário***, na guia ***Proprietários***, e depois clique em ***Localizar***.

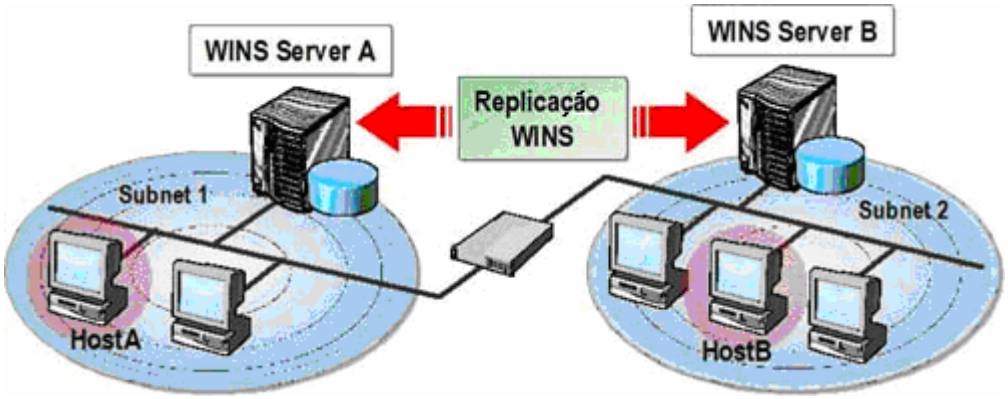
### 4.2.1. Estudo das informações de registro do WINS

O WINS mostra todos os registros do banco de dados e organiza as informações de registro do WINS nas colunas seguintes:

- ***Nome de registro:*** O nome NetBIOS registrado, que pode ser um nome único ou pode representar um grupo, um grupo da Internet ou uma máquina com múltiplas placas.
- ***Tipo.*** O serviço que registrou a entrada, incluindo o identificador de tipo hexadecimal.
- ***Endereço IP.*** O endereço IP correspondente ao nome registrado.
- ***Estado.*** O estado da entrada do banco de dados, que pode ser Ativo, Liberado ou Recusado. Se o estado da entrada for Recusado, ela não está ativa e será removida do banco de dados.
- ***Proprietário.*** O servidor WINS de onde a entrada se originou. Devido à replicação, não é necessariamente o mesmo servidor que está sendo visto no banco de dados.
- ***Versão*** Número hexadecimal único, atribuído pelo servidor WINS durante o registro de nomes. Os associados do servidor o utilizam para identificar novos registros durante a replicação.
- ***Expiração.*** Mostra a data de expiração da entrada. Quando uma replicação é armazenada no banco de dados, os dados de expiração correspondentes são estabelecidos conforme a hora no servidor WINS de recebimento e o intervalo de renovação estabelecido no cliente.


© 2003 Microsoft Corporation. Todos os direitos reservados.

### 4.3. Replicação do WINS




Embora um servidor WINS possa aceitar mais de 5.000 clientes em condições normais de carga de trabalho, é possível instalar um segundo servidor para proporcionar tolerância a falhas na resolução dos nomes NetBIOS. Esse servidor permitirá, ao mesmo tempo, localizar o tráfego de resolução. Dessa forma, se ocorrer um erro em um dos servidores WINS, o outro continuará executando a resolução de nomes NetBIOS na rede.

Cada servidor WINS de uma rede mantém seu próprio banco de dados WINS. Portanto, se houver vários servidores WINS na rede, eles devem ser configurados para replicar os registros de seus bancos de dados nos outros servidores WINS. A replicação dos bancos de dados WINS garante que um cliente WINS configurado para usar um servidor WINS diferente possa solucionar os nomes registrados em outro servidor WINS.

***Por exemplo:***

- O host A da subrede 1 registra-se no servidor WINS A da subrede 1.
- O host B da subrede 2 registra-se no servidor WINS B da subrede 2.
- Quando ocorre uma replicação do WINS, cada servidor WINS atualiza seu banco de dados com a nova entrada proveniente do banco de dados do outro servidor.

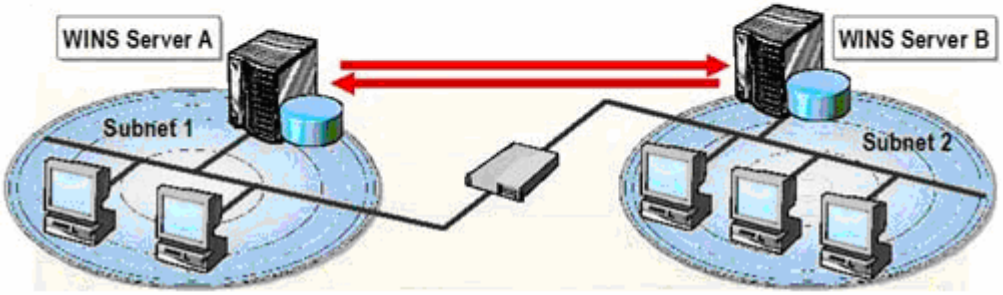
Como resultado da replicação, os dois servidores WINS dispõem de informações sobre os dois hosts, e os hosts A e B podem solucionar mutuamente seus nomes se entrarem em contato com seu servidor WINS local.

Para que seja produzida uma replicação, cada servidor WINS deverá se configurar com um parceiro de replicação, no mínimo. Ao configurar um parceiro de replicação para um servidor WINS, é possível especificá-lo como parceiro de extração, como parceiro de inserção ou como parceiro de extração e inserção para o processo de replicação.

#### 4.3.1 Como funciona a replicação de envio?


© 2003 Microsoft Corporation. Todos os direitos reservados.

O parceiro Push notifica os parceiros de replicação quando a base de dados chega a quantidade de alterações configurada.
A replicação Push mantém um alto nível de sincronização em links rápidos




1. O servidor WINS A chega a 50 alterações em sua base
2. O servidor WINS A notifica o servidor B que chegou ao valor
3. O servidor WINS B responde ao servidor A com um pedido de replicação
4. O servidor WINS A envia a réplica das entradas novas em sua base de dados

#### 4.3.1.1. Definição

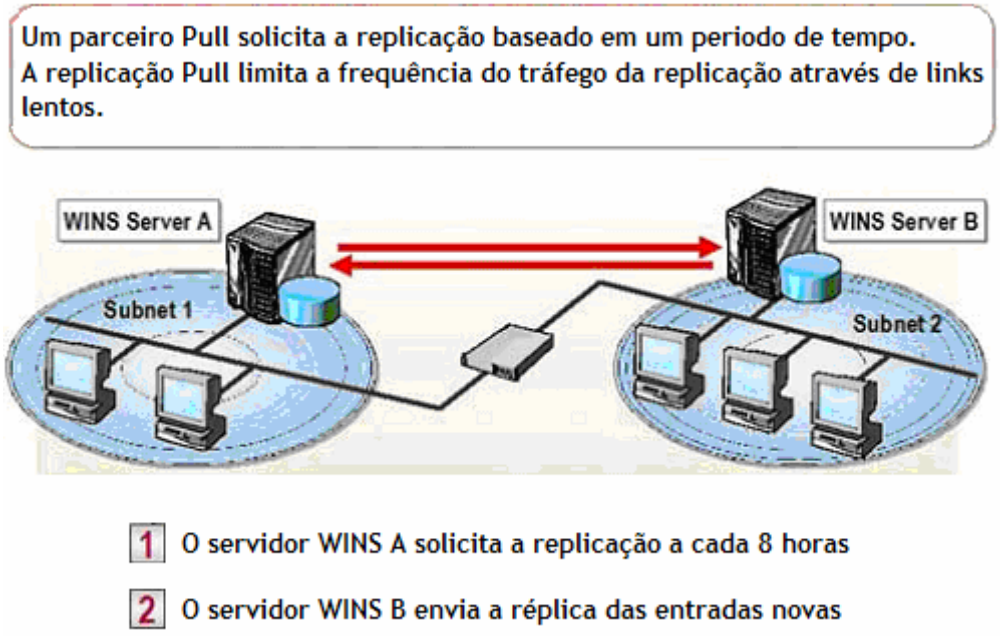
A replicação de envio ***Push*** é o processo de cópia dos registros atualizados de um Servidor WINS para outros, sempre que o Servidor WINS que contém dados atualizados alcança um valor específico de modificações.

***O processo de replicação de envio funciona da seguinte forma:***

1. O Parceiro de envio notifica seus Parceiros de Replicação sempre que o número de modificações no seu banco de dados do WINS ultrapassa um valor específico configurável. Por exemplo, você pode configurar o Parceiro de Envio para notificar os Parceiros de Replicação quando ocorrerem 50 modificações no banco de dados.
2. Quando os Parceiros de Replicação respondem à notificação com um pedido de replicação, o Parceiro de Envio envia a replicação das entradas novas no banco de dados.

### 4.3.2 Como funciona uma replicação de recepção?


© 2003 Microsoft Corporation. Todos os direitos reservados.




#### 4.3.2.1. Definição

A replicação de recepção ***Pull*** é o processo de cópia dos registros atualizados a partir de um servidor WINS para outros servidores WINS, em intervalos específicos de tempo.

***O processo de replicação de recepção funciona da seguinte forma:***

1. O Parceiro de recepção solicita as mudanças do banco de dados do WINS em intervalos de tempo. Por exemplo, você pode configurar um Parceiro de Recepção para solicitar as mudanças a cada 8 horas.
2. Os Parceiros de Replicação respondem enviando as novas entradas do banco de dados.

Também existe a possibilidade de configurar Parceiros de Replicação de modo Envio/Recepção. Isso garante que quando não ocorre uma determinada quantidade de mudanças, seja gerada uma replicação em intervalos de tempo.

### 4.4. Prática 11: Como configurar uma replicação WINS?

Para poder fazer este exercício, você precisará de duas instalações do Windows Server 2003 com o serviço de WINS instalado.

Por padrão, os Parceiros de Replicação do WINS são configurados como Push/Pull Partners (Parceiros de Envio/Recepção). Para modificar essa configuração e satisfazer às necessidades da sua rede, você pode especificar os parâmetros Push e Pull para cada Parceiro de Replicação.

***Para configurar uma Replicação WINS:***

1. Selecione, no console WINS, o Servidor WINS ao qual você quer adicionar um Parceiro de Replicação e clique em ***Parceiros de Replicação***.
2. Clique em ***Novo Parceiro de Replicação*** no menu ***Ação.***
3. Insira no campo ***Servidor WINS*** o nome ou o IP do Servidor WINS para adicionar como Parceiro de Replicação. (Segundo Computador)


© 2003 Microsoft Corporation. Todos os direitos reservados.

4. Clique em ***OK***.

***Para modificar o tipo de Parceiro de Replicação:***

1. Expanda o servidor WINS no console de WINS.
2. Clique em ***Parceiros de Replicação*** do console WINS.
3. Clique com o botão direito do mouse no servidor apropriado da caixa de detalhes e depois clique em ***Propriedades***.
4. Selecione uma das seguintes opções na caixa ***Propriedades*** do servidor e em ***Avançado***, no campo: ***Tipo de parceiro de replicação:***
   - ***Push.***
   - ***Pull.***
   - ***Push/Pull.***
5. Clique em ***OK*** na caixa ***Propriedades do Servidor***.
6. Feche o console de WINS.

Para obter mais informações sobre o WINS:

http://support.microsoft.com/default.aspx?scid=kb;en-us;323416

## 4.5. Manutenção

### 4.5.1. Backup

Você deve realizar tarefas de manutenção em períodos de tempo específicos. Para ajudá-lo nessa tarefa, o Servidor WINS pode ser configurado para realizar os backups automaticamente. Lembre-se de que nem todos os softwares de backup realizam essa tarefa porque o banco de dados é um arquivo com privilégios exclusivos do sistema operacional sempre que o serviço é iniciado.

***Para especificar o diretório de backup do WINS:***

1. Clique com o botão direito do mouse no Servidor WINS do console WINS e depois em ***Propriedades***.
2. Insira o diretório onde quiser realizar os backups do Servidor WINS, em ***Geral*** no campo ***Caminho padrão do backup***.

**Nota:** O Servidor WINS realizará um backup automaticamente a cada 24 horas.

### 4.5.2. Compactar o banco de dados

Para realizar as operações de reparo e/ou compactação, é preciso utilizar as ferramentas apropriadas: o banco do WINS, que é um arquivo localizado em \Windows\system32\Wins e seu nome é Wins.mdb. A ferramenta que você deve utilizar é o jetpack, e o comando é:

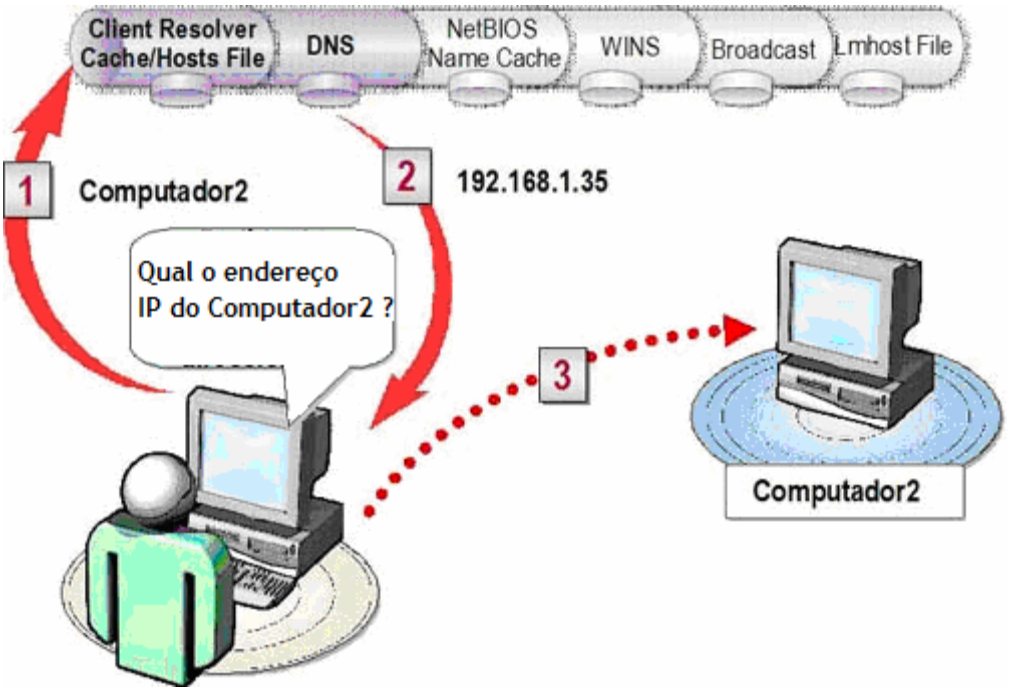
***jetpack %Systemroot%\System32\Wins\Wins.mdb Temp.mdb***

Onde %systemroot% é o diretório de instalação do sistema operacional e temp.mdb é um banco temporário.
Em seguida, exclua o arquivo Wins.mdb e renomeie o banco temporário com o nome Wins.mdb. Lembre-se de que, para realizar essa tarefa, o serviço do Servidor WINS precisa estar suspenso.

## 4.6. Processos de resolução de nomes e integração WINS / DNS

### 4.6.1. Resolução de nomes de host


© 2003 Microsoft Corporation. Todos os direitos reservados.




***O processo de resolução de nomes de HOST em um cliente cumpre o diagrama a seguir:***

1. O cliente verifica se já obteve a resolução em outra oportunidade. Se esse for o caso, a resolução é localizada no cache local DNS do cliente e o processo é finalizado. Se a resolução não for obtida, vai para o passo seguinte.
2. O cliente realiza uma consulta ao DNS primário. Se o DNS resolver a consulta, o processo é finalizado. Se a resolução não for obtida, vai para o passo seguinte.
3. O cliente verifica se já obteve a resolução em outra oportunidade. Nesse caso, a resolução é localizada no cache local do NetBIOS do cliente e o processo é finalizado. Se ainda não tiver obtido a resolução, vai para o passo seguinte.
4. O cliente realiza uma consulta ao WINS primário. Se o WINS resolver a consulta, o processo é finalizado. Se não conseguir a resolução, vai para o passo seguinte.
5. Se ainda assim não conseguir resolver o nome, o cliente realiza um broadcast local. Se a consulta for resolvida, o processo é finalizado. Se ainda assim não obtiver obtido a resolução, vai para o passo seguinte.
6. Por último, ele terá que consultar o arquivo HOST local localizado em systemroot\system32\drivers\etc. Esse arquivo é um banco estático de resolução; não tem extensão e também não é atualizado. Se esse último processo não obtiver êxito, o cliente não consegue a resolução.


© 2003 Microsoft Corporation. Todos os direitos reservados.

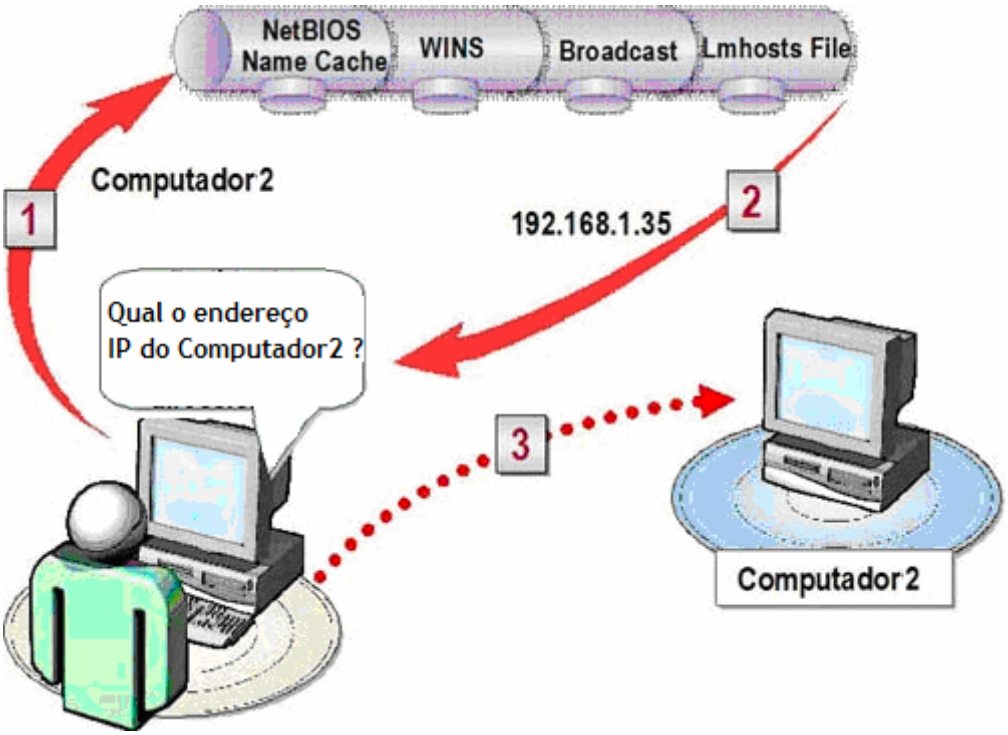
**Exemplo de arquivo HOST**

```
# Copyright (c) 1993-1999 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#      102.54.94.97     rhino.acme.com          # source server
#       38.25.63.10     x.acme.com              # x client host

127.0.0.1       localhost
```

### 4.6.2. Resolução de nomes NetBIOS


© 2003 Microsoft Corporation. Todos os direitos reservados.

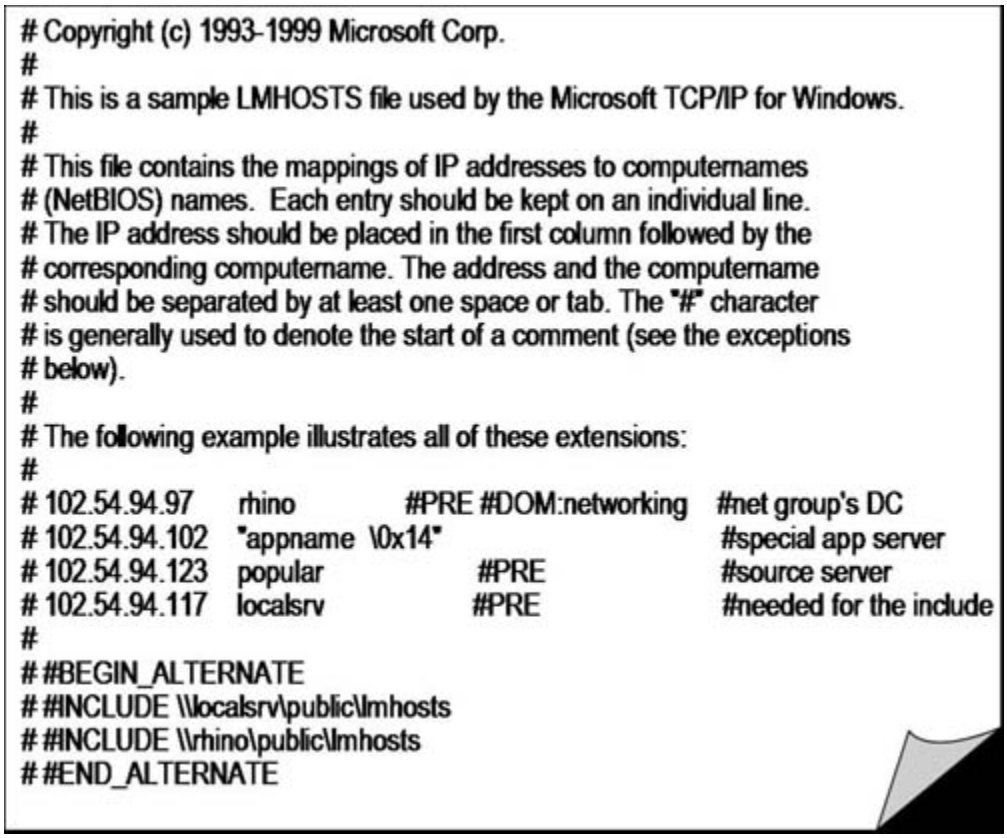



***O processo de resolução de nomes NetBIOS em um cliente segue o diagrama abaixo:***

1. O cliente verifica se já obteve a resolução em outra oportunidade. Se esse for o caso, a resolução é localizada no cache local do NetBIOS do cliente e o processo é finalizado. Se ainda não tiver obtido a resolução, vai para o passo seguinte.
2. O cliente realiza uma consulta ao WINS primário. Se o WINS resolver a consulta, o processo será finalizado. Se ainda não tiver obtido a resolução, vai para o passo seguinte.
3. Se ainda assim não conseguir resolver o nome, o cliente realiza um broadcast local. Se a consulta for resolvida, o processo é finalizado. Se não tiver conseguido a resolução, vai para o passo seguinte.
4. Por último, será preciso consultar o arquivo LMHOST local encontrado no systemroot\system32\drivers\etc. Esse arquivo é um banco estático de resolução; não tem extensão e também não se atualiza. Se esse último processo não obtiver êxito, o cliente não obterá a resolução.

**Exemplo de arquivo LMHOST**

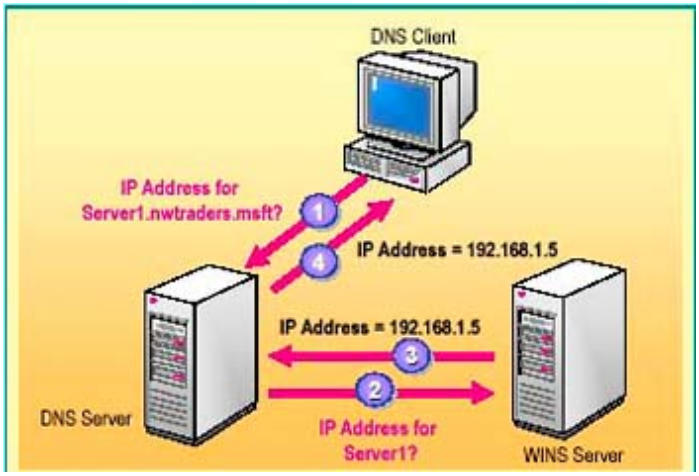

© 2003 Microsoft Corporation. Todos os direitos reservados.



```
# Copyright (c) 1993-1999 Microsoft Corp.
#
# This is a sample LMHOSTS file used by the Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to computernames
# (NetBIOS) names.  Each entry should be kept on an individual line.
# The IP address should be placed in the first column followed by the
# corresponding computername. The address and the computername
# should be separated by at least one space or tab. The "#" character
# is generally used to denote the start of a comment (see the exceptions
# below).
#
# The following example illustrates all of these extensions:
#
# 102.54.94.97     rhino          #PRE #DOM:networking   #net group's DC
# 102.54.94.102    "appname  \0x14"                      #special app server
# 102.54.94.123    popular              #PRE             #source server
# 102.54.94.117    localsrv             #PRE             #needed for the include
#
# #BEGIN_ALTERNATE
# #INCLUDE \\localsrv\public\lmhosts
# #INCLUDE \\rhino\public\lmhosts
# #END_ALTERNATE
```


© 2003 Microsoft Corporation. Todos os direitos reservados.

### 4.6.3. Introdução à integração WINS e DNS




A integração de WINS com DNS habilita os clientes a usarem exclusivamente DNS para a resolução de nomes. Os clientes poderão acessar os dados do WINS através do servidor DNS. No entanto, o Servidor DNS não pode localizar recursos sem realizar uma consulta ao WINS. No Windows Server 2003, você pode configurar a integração entre o WINS e o DNS para permitir que os clientes sem WINS resolvam nomes NetBIOS, usando um Servidor DNS.

Você pode configurar o DNS integrado com Servidores WINS.

***Para configurar uma zona DNS para uso de uma pesquisa WINS:***

1. Abra o DNS no menu ***Ferramentas Administrativas***.
2. Expanda, no console DNS, o servidor onde está a zona a configurar, expanda ***Zonas de pesquisa direta*** e depois clique na zona.
3. Clique com o botão direito da mouse na zona e depois em ***Propriedades***.
4. Selecione a caixa ***Use pesquisa direta WINS***, da caixa ***Propriedades***, em ***WINS***.
5. Insira o endereço IP do Servidor WINS, da caixa ***Endereço IP*** e depois clique em ***Adicionar***.


© 2003 Microsoft Corporation. Todos os direitos reservados.

# Capítulo 4
# Active Directory

## 1. Introdução

Durante este capítulo, você obterá conhecimentos sobre os serviços de diretório (Active Directory Services) do Windows Server 2003, em particular, sobre alguns dos novos recursos deste serviço.

Para a realização dos exercícios contidos nesta unidade, será preciso instalar o Windows Server 2003 no exercício 1 do capítulo 2 e fazer uma instalação adicional.

***Ao finalizar este capítulo, você será capaz de:***

- Descrever as características do serviço de diretório Active Directory.
- Identificar estruturas lógicas e físicas.
- Instalar e configurar o Active Directory na rede.
- Identificar características referentes à replicação.
- Solucionar problemas do Active Directory.

### 1.1. Definição

Em uma rede do Microsoft® Windows® Server 2003, o serviço de diretório Active Directory® proporciona a estrutura e as funções para organizar, administrar e controlar o acesso aos recursos de rede. Para implementar e administrar uma rede do Windows Server 2003, você deverá compreender o objetivo e a estrutura do Active Directory.

O Active Directory também permite administrar de forma central a rede do Windows Server 2003. Esse recurso significa que é possível armazenar de forma central informações sobre a empresa, por exemplo, informações de usuários, grupos e impressoras, e que os administradores podem administrar a rede de um único lugar.

O Active Directory permite delegar o controle administrativo de seus objetos. Essa delegação permite que os administradores atribuam a um grupo determinado de administradores permissões administrativas específicas para objetos, como contas de usuários ou de grupos.

O Active Directory é o serviço de diretório de uma rede do Windows Server 2003. Um ***serviço de diretório*** armazena informações sobre os recursos da rede e permite que os mesmos estejam acessíveis aos usuários e aos aplicativos. Os serviços de diretório proporcionam uma forma coerente de nomear, descrever, localizar, obter acesso, administrar e proteger as informações relativas aos recursos da rede.

### 1.2. A funcionalidade

O Active Directory oferece a funcionalidade de serviço de diretório para organizar, administrar e controlar de forma centralizada o acesso aos recursos de rede. Também faz com que a topologia física da rede e os seus protocolos passem despercebidos para que o usuário de uma rede possa ter acesso a qualquer recurso sem saber onde ele está ou como está conectado fisicamente à rede. Um exemplo deste tipo de recurso é uma impressora.

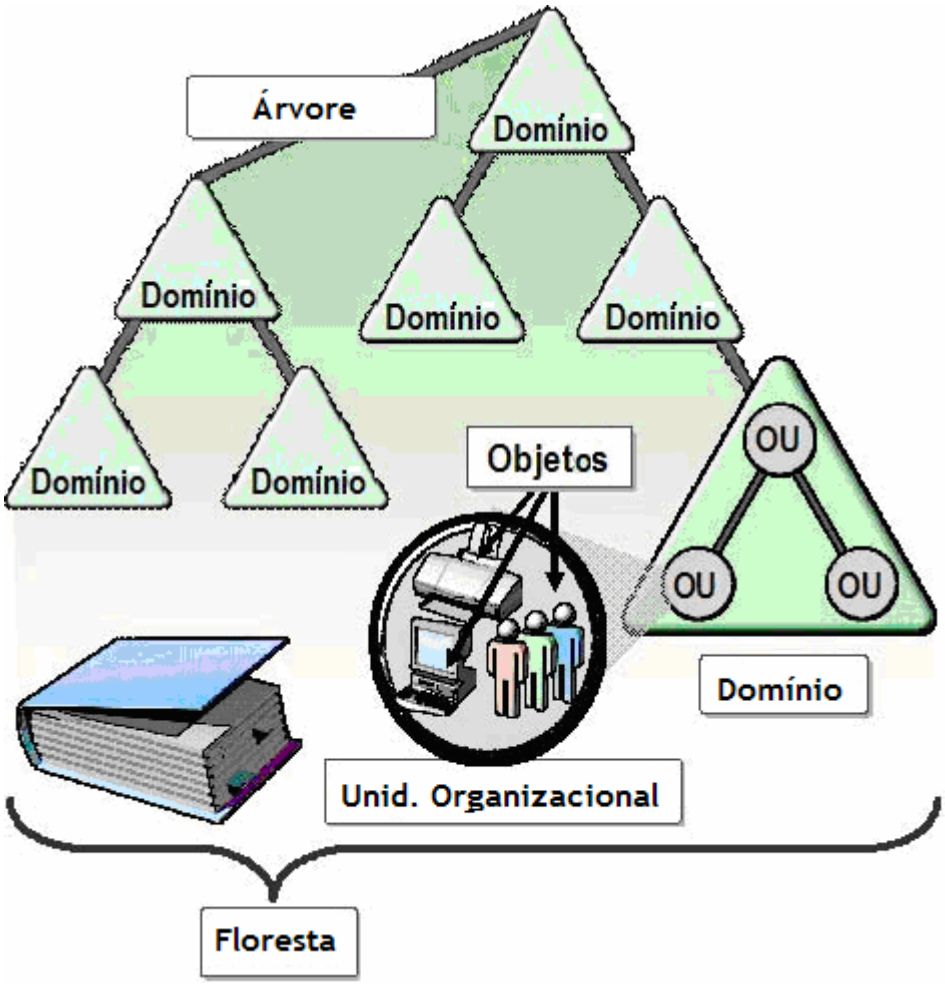
O Active Directory está organizado em seções que permitem o armazenamento de uma grande quantidade de objetos. Dessa forma, é possível ampliar o Active Directory à medida que a organização cresce, permitindo que uma organização que tenha um único servidor com centenas de objetos se expanda e chegue a ter milhares de servidores e milhões de objetos.


© 2003 Microsoft Corporation. Todos os direitos reservados.

Um servidor que executa o Windows Server 2003 armazena a configuração do sistema, as informações dos aplicativos e as informações sobre a localização dos perfis de usuário no Active Directory. Em combinação com as diretivas de grupo, o Active Directory permite que os administradores controlem escritórios distribuídos, serviços de rede e aplicações de um local central, ao mesmo tempo em que utilizam uma interface de administração coerente.

Além disso, o Active Directory proporciona um controle centralizado do acesso aos recursos de rede, ao permitir que os usuários só iniciem a sessão uma única vez para obter pleno acesso aos recursos através do Active Directory.

### 1.3. Estrutura Lógica do Active Directory




O Active Directory possibilita o armazenamento seguro de informações sobre objetos na sua estrutura hierárquica lógica. Os objetos do Active Directory representam usuários e recursos como, por exemplo, os computadores e as impressoras. Alguns objetos podem funcionar como contêineres para outros objetos.

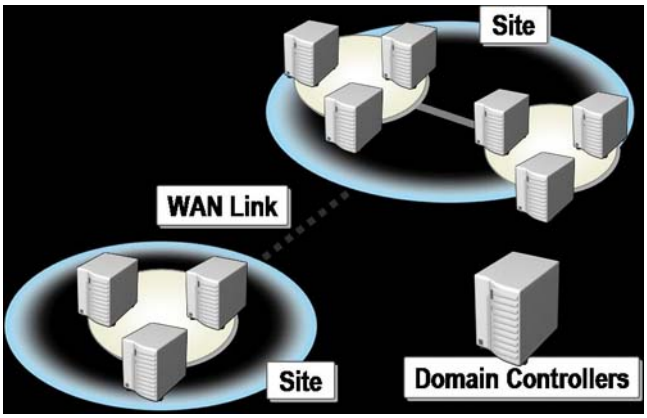
Compreendendo o objetivo e a função desses objetos, você poderá realizar uma variedade de tarefas, incluindo a instalação, a configuração, a administração e a resolução de problemas do Active Directory.


© 2003 Microsoft Corporation. Todos os direitos reservados.

***A estrutura lógica do Active Directory inclui os seguintes componentes:***

- ***Objetos.*** Eles são os componentes básicos da estrutura lógica.
- ***Classes de objeto.*** São os modelos de tipos de objetos que podem ser criados no Active Directory. Cada classe de objeto é definida por um grupo de atributos que estabelece os valores que podem ser associados a um objeto. Cada objeto tem uma combinação única de valores de atributos.
- ***Unidades Organizacionais*** Você pode utilizar esses contêineres de objetos para organizar outros objetos com propósitos administrativos. Organizando os objetos por Unidade Organizacional é mais fácil localizar e administrar objetos. Você também pode delegar autoridade para administrar as Unidades Organizacionais. Elas podem conter outras Unidades Organizacionais para simplificar a administração de objetos.
- ***Domínios.*** São as unidades funcionais básicas da estrutura lógica do Active Directory e, portanto, é uma coleção de objetos administrativos definidos que compartilham, através de um banco de dados comum do diretório, diretivas de segurança e relações de confiança com outros Domínios. Os domínios oferecem as 3 funções a seguir:
  - Um limite administrativo para os objetos
  - Meios de administrar a segurança dos recursos compartilhados
  - Uma unidade de replicação para os objetos
- ***Árvores de domínio.*** São Domínios agrupados em estruturas hierárquicas. Quando um segundo domínio é adicionado a uma árvore, ele é convertido em Filho da árvore Raiz do Domínio. O domínio ao qual um Filho do Domínio é adicionado é chamado de Domínio Pai. O Domínio Filho pode ter seus próprios Domínios Filhos e seu nome é combinado com o nome do seu Domínio Pai para formar o seu próprio nome exclusivo, o DNS (Domain Name System). Um exemplo seria corp.nwtraders.msft. Desse modo, uma árvore tem um Nome de Espaço contínuo.
- ***Florestas.*** Uma Floresta é uma instância completa do Active Directory, e consiste em uma ou mais árvores. Em uma única árvore de 2 níveis, recomendável para a maioria das organizações, todos os Domínios Filhos são filhos do Domínio Raiz da Floresta para formar uma árvore contígua. O primeiro domínio na floresta é chamado de Domínio Raiz da Floresta e o nome desse domínio faz referência à floresta, por exemplo, nwtraders.msft. Por padrão, as informações no Active Directory só são compartilhadas dentro da floresta. Dessa forma, a segurança da floresta estará contida em uma única instância do Active Directory.

## 1.4. Estrutura física do Active Directory




Em comparação com a estrutura lógica e os requisitos administrativos dos modelos, a estrutura física do Active Directory otimiza o tráfego da rede, determinando como e quando ocorre a replicação e o tráfego do logon. Para otimizar o uso da largura de banda da rede Active Directory, você precisa entender a sua estrutura física.


© 2003 Microsoft Corporation. Todos os direitos reservados.

***Os elementos da estrutura física do Active Directory são:***

- ***Controladores de domínio.*** Estes computadores executam o Microsoft® Windows® Server 2003 ou o Windows 2000 Server e o Active Directory. Cada Controlador de Domínio realiza funções de armazenamento e replicação e, além disso, oferece suporte a apenas um domínio. Para garantir uma disponibilidade contínua do Active Directory, cada domínio deve ter mais de um controlador de domínio.

- ***Sites do Active Directory*** Os sites são grupos de computadores conectados. Quando você estabelece sites, os Controladores de Domínios que estão dentro de um mesmo site podem se comunicar com freqüência. Essa comunicação reduz ao mínimo o estado de latência dentro do site, isso é, o tempo necessário para que uma modificação realizada em um Controlador de Domínio seja duplicada nos outros controladores de domínio. Você cria sites para otimizar o uso da largura de banda entre controladores de domínio em diversos locais.

- ***Partições do Active Directory*** Cada Controlador de Domínio contém as seguintes partições do Active Directory:

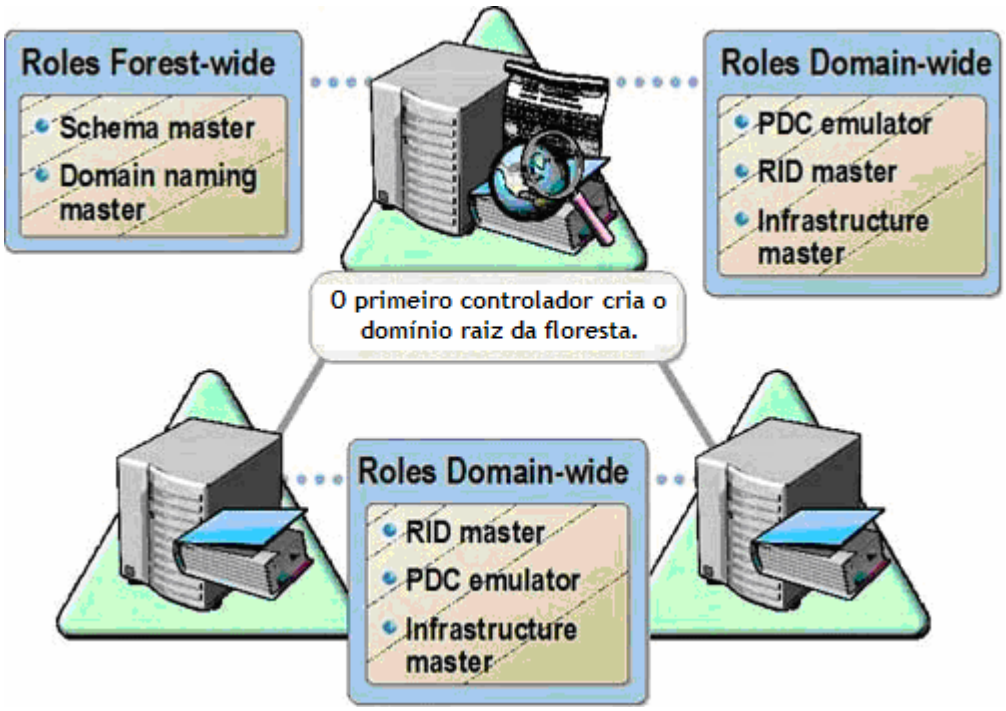
  - Partições de Domínio, que contêm a replicação de todos os objetos neste domínio. Essa partição é duplicada apenas para outros Controladores de Domínio do mesmo domínio.

  - Partição de Configuração, que contém a topologia da floresta. A topologia registra todas as conexões dos Controladores de Domínio na mesma floresta.

  - Partição de Esquema, que contém o esquema da floresta. Cada floresta tem um esquema de modo que a definição de cada classe do objeto seja constante. As partições de Configuração e Esquema de Partições são duplicadas para cada Controlador de Domínio na floresta.

- Opções de Partição de Aplicativos que contêm os objetos relacionados à segurança e são utilizados por um ou mais aplicativos. As partições de aplicativos são duplicadas em Controladores de Domínio específicos na floresta.

## 1.5. O que são Mestre de Operações?





© 2003 Microsoft Corporation. Todos os direitos reservados.

### 1.5.1. Single Master Replication e MultiMaster Replication

Quando é realizada uma modificação em um domínio, essa modificação é duplicada em todos os seus controladores de domínio. Algumas modificações, como as feitas no esquema, são duplicadas em todos os domínios na floresta. Este tipo de replicação é chamado de ***Multimaster Replication***.

Durante a replicação multimaster, é possível que ocorra um conflito de replicação que gere atualizações simultâneas no mesmo atributo do objeto e em dois Controladores de Domínio. Para evitar conflitos de replicação, você pode utilizar **Single Master Replication**, que designa um Controlador de Domínio como o único onde é possível realizar modificações de diretório.

Dessa maneira, as modificações não podem ocorrer em diversos lugares da rede ao mesmo tempo. O Active Directory usa o Single Master Replication para modificações importantes, por exemplo, o acréscimo de um novo domínio ou modificações no esquema da floresta.

### 1.5.2. Funções de Mestre de Operações

As operações que utilizam Replicação Mestre Única são realizadas junto com funções específicas na floresta ou no domínio. Essas funções se chamam ***Funções de Mestre de Operações.*** Para cada Função de Mestre de Operação, somente o Controlador de Domínio que tem a função pode realizar as modificações associadas ao diretório. O Controlador de Domínio responsável pela função em particular é chamado de ***Mestre de Operações desta função***. O Active Directory, por sua vez, armazena as informações sobre o Controlador de Domínio que executa uma função específica.

As Funções de Mestre de Operações são realizadas no nível da floresta ou do domínio, e o Active Directory define cinco delas, que possuem uma localização padrão.

***As funções Únicos na floresta são:***

- ***Mestre de Esquema.*** Controla todas as atualizações do esquema. O esquema contém a definição de objetos e atributos que são utilizados para criar todos os objetos do Active Directory, como usuários, computadores e impressoras.

- ***Mestre de Nomeação de Domínio*** Controla o acréscimo e a retirada de domínios da floresta. Quando se deseja adicionar um novo domínio à floresta, apenas o Controlador de Domínio com a função de Mestre de Nomeação de Domínio poderá adicionar o novo domínio. Só há um Mestre de Esquema e um Mestre de Nomeação de Domínio por floresta.

***As funções para cada domínio da floresta são:***

- ***O emulador de controlador de domínio primário (PDC).*** Atua como um PDC do Windows NT para oferecer suporte aos Backup Domain Controllers (BDCs) que executam o Microsoft Windows® NT em domínios, de modo misto. Esse tipo de domínio tem Controlador de Domínio que executa o Windows NT 4.0. O emulador de PDC é o primeiro Controlador de Domínio a ser criado em um novo domínio.

- ***Mestre de Identificador relativo.*** Quando se cria um novo objeto, o Controlador de Domínio cria um novo Objeto de Segurança que representa o objeto, atribuindo-lhe um Identificador de Segurança Único (SID). O SID consiste em um Domínio SID que é igual para todos os Objetos de Segurança criados no domínio e um identificador relativo (RID), único para cada objeto de segurança criado no domínio. O RID Mestre designa blocos de RIDs para cada Controlador de Domínio no domínio. O Controlador de Domínio designa o RID aos objetos criados do bloco designado dos RIDs.

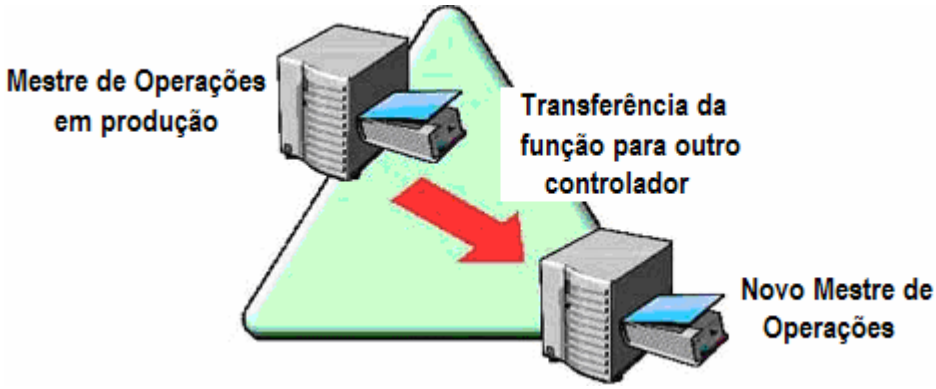
- ***Mestre de Infra-estrutura.*** Quando os objetos são transferidos de um domínio para outro, a Infra-estrutura Mestre atualiza as referências ao objeto nesse e no outro domínio. A referência do objeto contém o Object Globally Unique Identifier (GUID), o Nome Distinto e o SID. O Active Directory


© 2003 Microsoft Corporation. Todos os direitos reservados.

atualiza periodicamente o Nome Distinto e o SID, na referência ao objeto para refletir as modificações realizadas no objeto real, por exemplo, movimentos em e entre domínios ou a eliminação do objeto.

Cada domínio na floresta contém seu próprio Emulador de PDC, Mestre RID e o Mestre de Infra-estrutura.

### 1.5.3. Transferência de Funções de Mestre de Operações




Você colocará as Funções de Mestre de Operações em uma floresta quando implementar uma estrutura de floresta e domínio. As Funções de Mestre de Operações só são transferidas quando é feita uma modificação importante na estrutura do domínio. Essas modificações incluem a desmontagem de um Controlador de Domínio que já teve uma função e o acréscimo de um novo Controlador de Domínio que satisfaça melhor às operações de uma função específica.

A transferência de Funções de Mestre de Operações implica mover a função de um Controlador de Domínio para outro. Para transferir funções, os dois Controladores de Domínio devem estar ativos e conectados à rede.

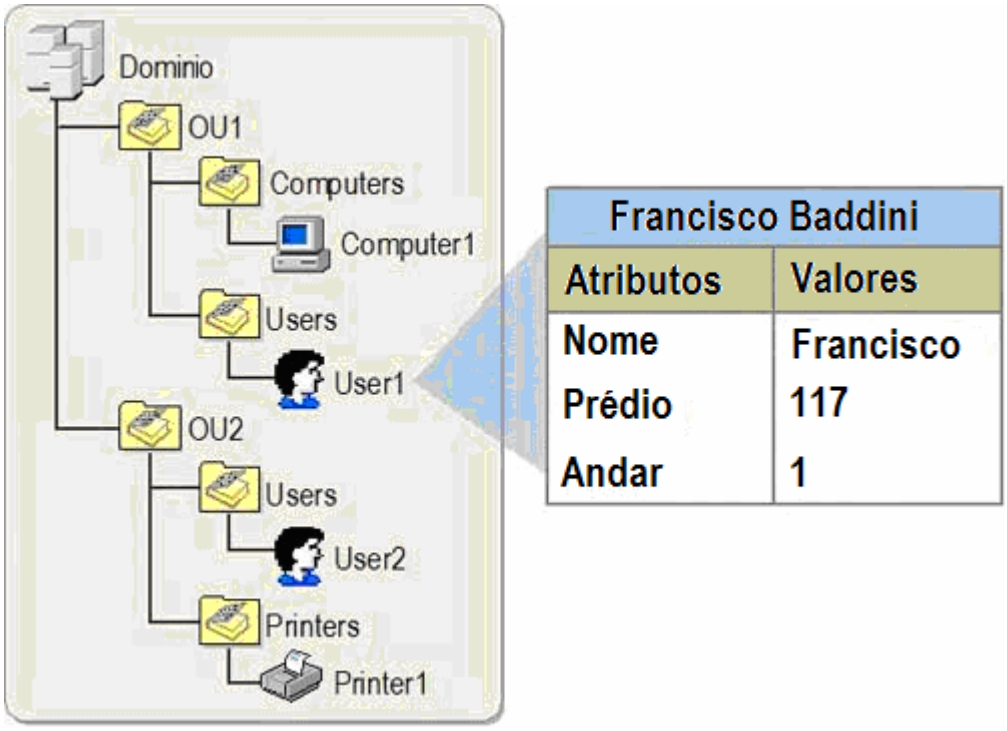
Não ocorre nenhuma perda de dados quando você transfere a Função de Mestre de Operações. O Active Directory duplica a Função de Mestre de Operações real para o novo Controlador de Domínio, assegurando que a nova Função de Mestre de Operações obterá as informações necessárias para essa função. Essa transferência utiliza o mecanismo da replicação do diretório.

Para obter informações sobre o processo de transferência:

http://support.microsoft.com/default.aspx?scid=kb;en-us;324801


© 2003 Microsoft Corporation. Todos os direitos reservados.

## 2. O que é o serviço de diretório?




Um serviço de diretório é um depósito estruturado de informações sobre pessoas e recursos em uma organização. Em uma rede do Windows Server 2003, o serviço de diretório é o Active Directory.

### 2.1. O Active Directory tem os seguintes recursos:

- ***Permite que usuários e aplicativos tenham acesso a informações sobre objetos.*** Essas informações são armazenadas na forma de valores de atributos. Você pode procurar objetos por classe, atributo, valor do atributo, localização na estrutura do Active Directory ou qualquer combinação desses valores.

- ***Torna a topologia e os protocolos físicos da rede transparentes.*** Dessa forma, um usuário em uma rede pode ter acesso a qualquer recurso, por exemplo, a uma impressora, sem saber onde está o recurso ou onde ele está conectado fisicamente com a rede. Ele permite o armazenamento de um número muito grande de objetos. Como é organizado por partições, o Active Directory pode ser ampliado à medida que a organização cresce. Por exemplo, um diretório pode ser ampliado de um único servidor com alguns objetos para milhares de servidores e milhões de objetos.

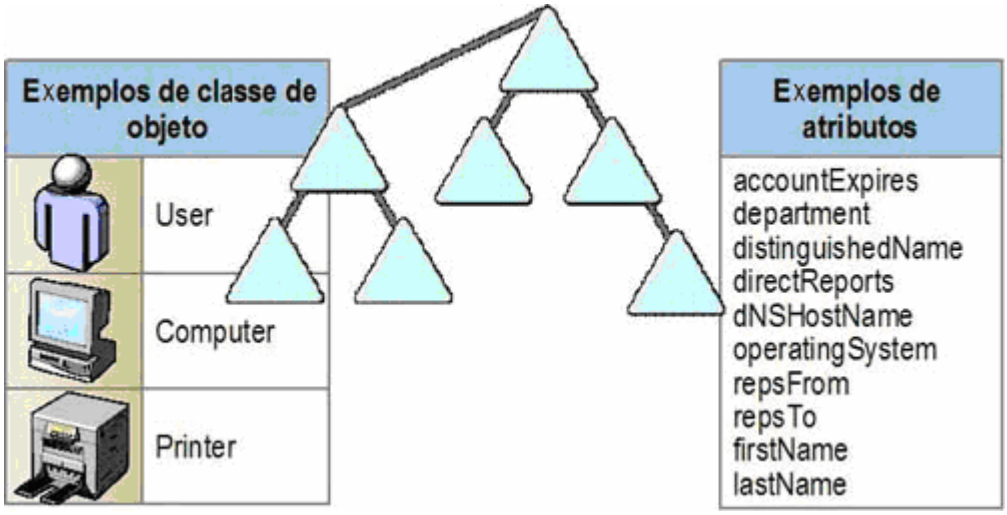
- new! ***É possível funcionar como serviço de sistema não-operacional*** O Active Directory no Modo de Aplicação (AD/AM) é um novo recurso do Microsoft Active Directory e atua em cenários de aplicativos em diretórios. O AD/AM funciona como serviço de Sistema Não-Operacional e, como tal, não exige instalação em um Controlador de Domínio. Executar serviços de Sistema Não-Operacional significa que múltiplas instâncias de AD/AM podem funcionar simultaneamente em um único servidor, sendo cada instância configurável de forma independente.

  Para obter mais informações sobre o ADAM (Modo de Aplicativo do Active Directory):

  http://www.microsoft.com/windowsserver2003/techinfo/overview/adam.mspx


© 2003 Microsoft Corporation. Todos os direitos reservados.

## 2.2. O que é o esquema?




O esquema do Active Directory contém as definições de todos os objetos, como, por exemplo, usuários, computadores e impressoras armazenados no Active Directory. Nos Controladores de Domínio que executam o Windows Server 2003, só existe um esquema para toda a floresta. Dessa forma, todos os objetos criados no Active Directory seguem as mesmas regras.

O Esquema tem dois tipos de definições: classes de objeto e atributos. Um exemplo de Classes de Objeto são os usuários, o computador e a impressora, que descrevem os objetos que podem ser criados no diretório. Cada Classe de Objeto é uma coleção de atributos. Os atributos são definidos separadamente das Classes de Objeto. Cada atributo é definido somente uma vez e pode ser utilizado em várias Classes de Objeto. Por exemplo, o atributo da descrição é utilizado em várias Classes de Objetos, mas só é definido uma única vez no Esquema para garantir a consistência.

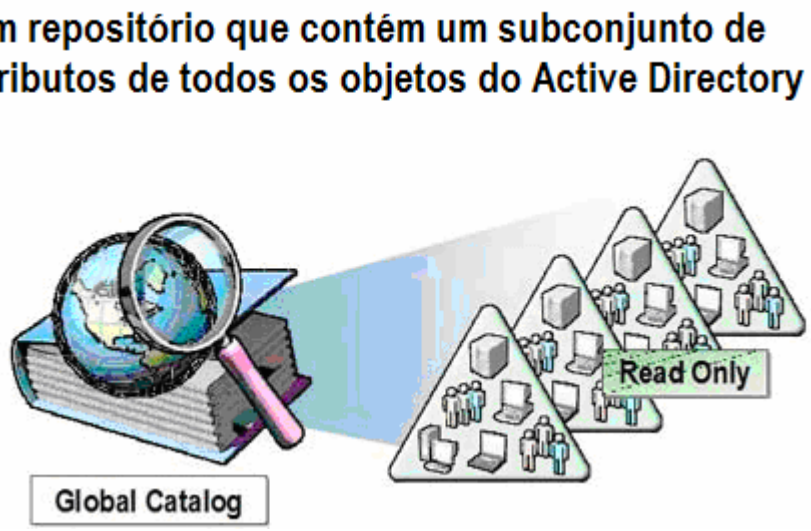
Você também pode criar novos tipos de objetos no Active Directory estendendo o Esquema. Por exemplo, para um aplicativo de Servidor de E-mail, é possível ampliar a Classe de Usuário no Active Directory com atributos de diretório que contenham informações adicionais, como o endereço e o e-mail dos usuários.

new! Nos Controladores de Domínio do Windows Server 2003, você pode reverter modificações de esquema desativando-os e permitindo que as organizações; desta forma, melhorem o uso dos recursos de extensão do Active Directory.

new! Também é possível redefinir uma classe ou atributo do Esquema, por exemplo, modificar a sintaxe da seqüência de Unicode do atributo chamado Gerenciador de Vendas para um Nome Distinto.


© 2003 Microsoft Corporation. Todos os direitos reservados.

## 2.3 O que é o Catálogo Global?




O ***Catálogo Global*** é um repositório de informações que contém um subconjunto de atributos de todos os objetos no Active Directory. Os membros do grupo Administradores de Esquema podem modificar os atributos armazenados no Catálogo Global, dependendo das necessidades da organização.

***O Catálogo Global contém:***

- Os atributos utilizados com mais freqüência em consultas, por exemplo, nome, sobrenome e nome de logon dos usuários.
- As informações necessárias para determinar as localizações de qualquer objeto no diretório.
- Um subconjunto padrão dos atributos de cada tipo de objeto.
- As permissões de acesso para cada objeto e atributos armazenados no Catálogo Global. Se você estiver pesquisando um objeto e não tiver permissão apropriada para vê-lo, o objeto não aparecerá nos resultados da pesquisa. As permissões de acesso garantem que os usuários só localizem os objetos aos quais eles têm acesso.

O ***Servidor de Catálogo Global*** é um Controlador de Domínio que processa de forma eficiente consultas entre florestas do Catálogo Global. O primeiro Controlador de Domínio que você cria no Active Directory é automaticamente convertido em Servidor de Catálogo Global. Você pode configurar Servidores de Catálogo Global adicionais para equilibrar o tráfego para logon e consultas.

***O Catálogo Global permite que os usuários realizem duas funções importantes:***

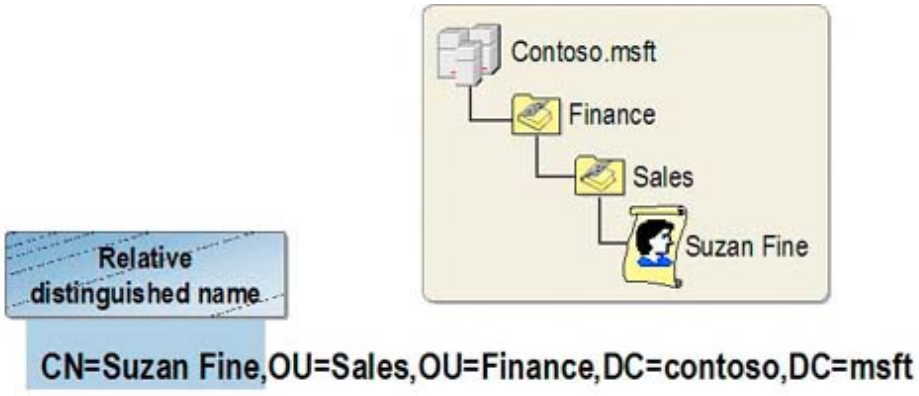
- Pesquisar informações no Active Directory em toda a floresta, independente da localização dos dados.
- Usar informações de associação do Grupo Universal no processo de logon na rede.

new! Os servidores de catálogo global duplicam seu conteúdo em um esquema de replicação. Até o Windows 2000, essas duplicações eram do tipo sincronização total, mas a partir do Windows Server 2003 é possível fazer a sincronização de modo parcial, ou seja, replicando as modificações apenas, em vez de enviar o catálogo completo.

new! Para poder utilizar esse novo recurso do Windows Server 2003, você pode ter o nível de funcionalidade do modo Windows 2000 ou Windows Server 2003, mas só podem ser feitas duplicações parciais entre os servidores de Catálogo Global que executam o Windows Server 2003.


© 2003 Microsoft Corporation. Todos os direitos reservados.

## 2.4 O Que São Nomes Distintos e Relativos?




O LDAP utiliza um nome que representa objetos no Active Directory por uma série de componentes relacionados com a sua estrutura lógica. Essa representação é chamada ***Nome Distinto*** do objeto e identifica o domínio onde está localizado o objeto e a trajetória completa até chegar a ele. O Nome Distinto deve ser único na floresta Active Directory.

O ***Nome Distinto Relativo*** de um objeto o identifica de modo único no seu contêiner. Dois objetos no mesmo contêiner não podem ter o mesmo nome. O Nome Distinto Relativo sempre é o primeiro componente do Nome Distinto, mas pode não ser sempre um Nome Comum.

Para uma usuária chamada Suzan Fine da Unidade Organizacional Sales (Vendas) no domínio Contoso.msft, cada elemento da estrutura lógica está representando no seguinte nome distinto:

**CN=Suzan Fine,UO=Sales,DC=contoso,DC=msft**

- CN é o Nome Comum do objeto no seu contêiner.
- UO é a Unidade Organizacional que contém o objeto. Pode haver mais de um valor de UO se o objeto residir em uma Unidade Organizacional aninhada em mais níveis.
- DC é o Componente do Domínio, por exemplo, .com. ou .msft.. Sempre há, pelo menos, dois Componentes de Domínio, mas pode haver mais se o domínio for um domínio filho.

Os componentes de domínio dos Nomes Distintos baseiam-se no Domain Name System (DNS).

## 2.5. Ferramentas e snap-ins do Active Directory

O Windows Server 2003 oferece diversos snap-ins e ferramentas de linha de comando para administrar o Active Directory. Você também pode administrar o Active Directory usando o Active Directory Service Interfaces (ADSI). O ADSI é uma interface simples de grande alcance para criar scripts reutilizáveis para administrar o Active Directory.

**Nota:** A ferramenta ADSI Edit pode ser instalada a partir do CD do Windows Server 2003. Ela pode ser encontrada na pasta \Support\Tools.


© 2003 Microsoft Corporation. Todos os direitos reservados.

*A tabela a seguir descreve os snap-ins administrativos comuns para administração do Active Directory.*

| Snap-in | Descrição |
|---|---|
| Usuários e computadores do Active Directory | É um Microsoft Management Console (MMC) utilizado para administrar e publicar informações no Active Directory. Você pode administrar as contas de usuário, grupos e contas de computador, adicionar computadores ao domínio, administrar diretivas de contas, direitos de usuário e diretivas de auditoria. |
| Domínios e Relações de Confianças do Active Directory | É um MMC utilizado para administrar Relações de Confianças de Domínio e Relações de Confianças de Floresta, adicionar sufixos de nome principal de usuário e modificar níveis de funcionamento de domínios e floresta. Os Sites e Serviços do Active Directory são um MMC que você utiliza para administrar a replicação do diretório. |
| Esquema do Active Directory | É um MMC utilizado para administrar o esquema. Não está disponível por padrão no menu. |
| Ferramentas Administrativas | Você deve adicioná-las manualmente. |

*A tabela seguinte descreve as ferramentas de linha de comando para utilizar quando se quer administrar o Active Directory.*

| Ferramenta | Descrição |
|---|---|
| Dsadd | Adiciona objetos ao Active Directory, como computadores, usuários, grupos, unidades organizacionais e contatos. |
| Dsmod | Modifica objetos no Active Directory, como computadores, servidores, usuários, grupos, unidades organizacionais e contatos. |
| Dsquery | Executa consultas no Active Directory segundo critérios especificados. Você pode executar consultas em servidores, computadores, grupos, usuários, sites, unidades organizacionais e partições. |
| Dsmove | Move objetos dentro de um domínio para uma nova localização no Active Directory ou renomeia um único objeto sem movê-lo. |
| Dsrm | Exclui um objeto do Active Directory. |
| Dsget | Mostra atributos selecionados de um computador, contato, grupo, unidade organizacional, servidor ou usuário do Active Directory. |
| Csvde | Importa e exporta dados do Active Directory usando formato separado por vírgulas. |
| Ldifde | Cria, modifica e exclui objetos do Active Directory. Também pode estender o Esquema do Active Directory e exportar informações de usuários e grupos para outros aplicativos ou serviços. |

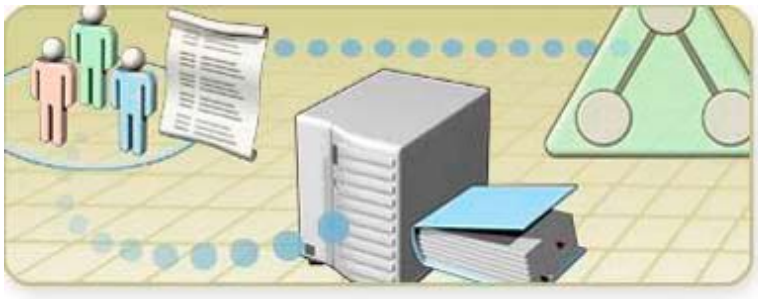
Para obter mais informações sobre ferramentas de linha de comando:

http://support.microsoft.com/default.aspx?scid=kb;en-us;322684


© 2003 Microsoft Corporation. Todos os direitos reservados.

## 3. Instalação do Active Directory:

### 3.1. Requisitos para instalar o Active Directory



Antes de instalar o Active Directory, você deve garantir que o computador esteja preparado para ser um Controlador de Domínio, cumprindo requisitos de hardware e do sistema operacional. Além disso, o Controlador de Domínio deverá ter acesso ao servidor de DNS, que deve cumprir determinados requisitos para oferecer suporte à integração com o Active Directory.

***A lista a seguir identifica os requisitos para a instalação do Active Directory:***

- Um computador executando o Microsoft® Windows® Server 2003 Standard Edition, Enterprise Edition ou Datacenter Edition. O Windows Server 2003 Web Edition não oferece suporte ao Active Directory.

- Um mínimo de 250 megabytes (MB) de espaço no disco. 200 MB para o banco de dados do Active Directory e 50 MB para o log de transações do Active Directory. Os requisitos de tamanho do arquivo para a base do Active Directory e os arquivos de registro, dependem do número e do tipo de objetos no domínio. Será necessário ter espaço de disco adicional se o Controlador de Domínio também for Servidor de Catálogo Global.

- Uma partição ou um volume com formato NTFS e com sistema de arquivos. A partição NTFS é exigida para a pasta SYSVOL.

- Os privilégios administrativos necessários para criar um domínio em uma rede existente do Windows Server 2003.

- TCP/IP instalado e configurado para utilizar o DNS.

- Um Servidor DNS de autorização para o Domínio de DNS e suporte para os requisitos enumerados na tabela seguinte.

- ***Registros de Recursos do Servidor (Obrigatório) – Recursos Localizador de Serviço (SRV).*** São registros de DNS que identificam os serviços específicos oferecido nos computadores de uma rede do Windows Server 2003. O Servidor DNS que oferece suporte à instalação do Active Directory precisa de suporte a Registros de Recursos de Servidor. Caso contrário, você deve configurar o DNS localmente durante a instalação do Active Directory ou configurar o DNS manualmente após a instalação do Active Directory.

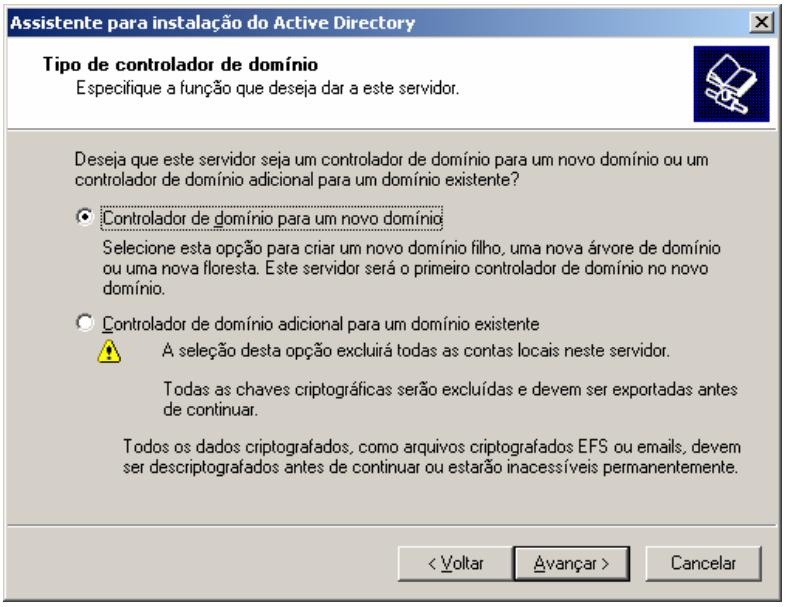
- ***Atualizações Dinâmicas (Opcionais).*** A Microsoft recomenda que os servidores DNS também permitam atualizações dinâmicas. O protocolo dinâmico de atualização permite que os servidores e os clientes em um ambiente DNS adicionem e atualizem o banco de dados do DNS automaticamente, o que diminui os esforços administrativos. Se você utilizar software DNS que oferece suporte aos Registros de Recursos de Servidor, mas que não oferece suporte ao protocolo dinâmico de atualização, é preciso inserir os Registros de Recursos de Servidor manualmente no banco de dados DNS.

- ***Transferências de zona incremental (Opcional)*** Em uma transferência de zona incremental, as modificações realizadas em uma zona no Servidor de DNS Mestre devem ser duplicadas nos servidores DNS


© 2003 Microsoft Corporation. Todos os direitos reservados.

secundários dessa zona. As transferências incrementais da zona são opcionais, mas são recomendáveis porque economizam largura de banda da rede, duplicando apenas os registros novos ou modificados entre os Servidores DNS, em vez do arquivo do banco de dados inteiro da zona.

## 3.2 O processo de instalação do Active Directory




***O processo de instalação realiza as seguintes tarefas:***

- ***Inicia o protocolo de autenticação Kerberos versão 5***

- ***Aplica a diretiva de Autoridade de Segurança Local (LSA).*** Essa configuração indica que o servidor é um Controlador de Domínio.

- ***Cria as partições do Active Directory.*** Uma partição do diretório é uma parte do Espaço de Nomes do Diretório. Cada partição do diretório contém uma hierarquia ou sub-árvore dos objetos do diretório na árvore de diretórios. Durante a instalação, foram criadas as seguintes partições no primeiro controlador de domínio da floresta.

    - Partição de Diretório do Esquema
    - Partição de Diretório de Configurações
    - Partição de Diretório de Domínios
    - Zona DNS da Floresta
    - Partição de Zona de DNS do Domínio


© 2003 Microsoft Corporation. Todos os direitos reservados.

Depois as partições são atualizadas através da replicação, em cada um dos Controladores de Domínio criados de forma subseqüente na floresta.

- ***Cria o banco de dados e os logs do Active Directory.*** A localização padrão do banco de dados e dos arquivos de logs é systemroot\Ntds.

- ***Cria o domínio raiz da floresta.*** Se o servidor for o primeiro Controlador de Domínio na rede, o processo de instalação cria o Domínio de Raiz de Floresta e atribui as Funções de Mestre de Operações ao Controlador de Domínio, incluindo:

    - Emulador de Controle de Domínio Primário (PDC)
    - Mestre de Operações de Identificador Relativo (RID)
    - Mestre de Nomeação de Domínio
    - Mestre de Esquema
    - Mestre de Infra-estrutura

- ***Cria a pasta compartilhada do volume do sistema.*** Essa estrutura de pastas reside em todos os Controladores de Domínio do Windows Server 2003 e contém as seguintes pastas:

- A pasta compartilhada SYSVOL, que contém informações de Diretiva de Grupo.
- A pasta compartilhada de Logon de Rede, que contém os scripts de logon para computadores que não executam o Windows Server 2003.

- ***Configura propriedade ao site apropriado para o Controlador de Domínio.*** Se o IP do servidor que você está promovendo a Controlador de Domínio estiver em uma sub-rede definida no Active Directory, o assistente colocará o Controlador de Domínio no site associado com a sub-rede. Se não for definido nenhum objeto de sub-rede ou se o IP do servidor não estiver dentro do intervalo da sub-rede do Active Directory, o servidor será colocado no Primeiro Site Padrão. O primeiro site é instalado automaticamente quando você cria o primeiro Controlador de Domínio na floresta. O assistente de instalação do Active Directory cria um servidor de objeto do Controlador de Domínio no site apropriado. O servidor de objetos contém as informações necessárias para a replicação e também contém uma referência ao objeto do computador nos Controladores de Domínio OU, indicando que o Controlador de Domínio está sendo criado.

- ***Aplica segurança no Serviço de Diretório e nas Pastas de Replicação de Arquivo*** Isso implica controlar o acesso de usuário a objetos do Active Directory.

- ***Aplica a senha à conta do administrador.*** Você utiliza a conta para iniciar o Controlador de Domínio no Modo de Restauração de Serviços de Diretório.

### 3.2.1. Exercício 1: Como criar a estrutura de Floresta e Domínio?

Você utiliza o Assistente para Instalação do Active Directory para criar a estrutura de floresta e domínio. Quando instala o Active Directory pela primeira vez em uma rede, você tem que criar o Domínio Raiz da Floresta e depois utilizar o assistente para criar árvores e domínios filhos adicionais.

O Assistente para Instalação do Active Directory orientará você no processo de instalação e lhe solicitará as informações necessárias, que variam conforme as opções selecionadas.


© 2003 Microsoft Corporation. Todos os direitos reservados.

***Para criar o Domínio Raiz da Floresta, você deve seguir os passos abaixo:***

1. Clique em ***Iniciar*** e depois em ***Executar*** e escreva ***dcpromo***. Em seguida, pressione Enter. O assistente verificará:
   - Se o usuário validado é membro do grupo de administradores locais.
   - Se o computador está executando um sistema operacional que ofereça suporte ao Active Directory.
   - Se foi realizada uma instalação ou remoção de uma versão anterior do Active Directory sem reiniciação do computador, ou se não há uma instalação ou uma retirada do Active Directory em andamento. Se qualquer uma dessas quatro verificações falhar, uma mensagem de erro aparecerá e você sairá do assistente.
2. Na página ***Bem-vindo***, clique em ***Avançar***.
3. Na página ***Compatibilidade do Sistema operacional***, clique em ***Avançar***.
4. Na página ***Tipo de Controlador de domínio***, clique em ***Controlador de domínio para um novo domínio***, e depois clique em ***Avançar***.
5. Na página ***Criar novo domínio***, clique no ***Domínio em uma nova floresta*** e depois em ***Avançar***.
6. Na página ***Novo nome de domínio***, insira o Nome do DNS para o novo domínio (nwtraders.msft) e depois clique em ***Avançar***.
7. Na página ***Nome de domínio NetBIOS*** verifique o Nome NetBIOS (NWTRADERS) e depois clique em ***Avançar***. O nome NetBIOS identifica o domínio nos computadores de cliente executando versões anteriores do Windows e do Windows NT. O assistente verifica se o nome NetBIOS é único. Se não for, ele pedirá para que você modifique o nome.
8. Na página ***Pastas do banco de dados e log***, especifique a localização em que deseja instalar as pastas do banco de dados e dos logs. Em seguida, clique em ***Avançar.***
9. Na página ***Volume de Sistema Compartilhado***, especifique o local onde você deseja instalar a pasta SYSVOL ou clique em ***Procurar...*** para escolher um local e depois clique em ***Avançar***.
10. Na página ***Diagnóstico de registro de DNS*** verifique se há um servidor DNS de autorização para essa floresta; se necessário, clique em ***Instalar e configurar o servidor DNS neste computador e definir este computador para usar o servidor DNS como seu servidor DNS***, e depois clique em ***Avançar***.
11. Na página ***Permissões***, especifique se foram atribuídas permissões padrão aos objetos de usuário e grupo compatíveis com os servidores que executam versões anteriores do Windows ou do Windows NT, ou somente com os servidores do Windows Server 2003.
12. Quando for perguntado, especifique a senha para o modo de restauração dos serviços de. Os controladores de domínio do Windows Server 2003 mantêm uma versão pequena do banco de dados de contas do Microsoft Windows NT 4.0. A única conta nesse banco de dados é a conta do administrador e ela é exigida para autenticação quando o computador é ligado no Modo Directory Services Restore porque o Active Directory não é iniciado deste modo.
13. Reveja a página ***Sumário*** e depois clique em ***Avançar*** para começar a instalação.
14. Quando solicitado, reinicie o computador.


© 2003 Microsoft Corporation. Todos os direitos reservados.

### 3.2.2 Exercício 2 (Opcional): Como adicionar um Controlador de Domínio adicional?

Para concluir esse exercício, você precisará de dois computadores ou dois PCs Virtuais, com um Controlador de Domínio instalado (Exercício 1) e um Windows Server 2003.

O procedimento é semelhante à criação de um novo Controlador de Domínio, com exceção de que é preciso selecionar na primeira tela do assistente a opção ***Adicionar controlador de domínio adicional para um domínio***. O restante do processo pode ser realizado de duas formas:

1. ***Através da rede:*** Se você tiver uma grande quantidade de objetos, essa opção exige uma conexão com largura de banda ou tempo suficientes para a replicação inicial.
2. new! ***Duplicar a partir da mídia:*** Essa nova característica do Windows Server 2003 permite realizar a replicação inicial por meio de um backup, da seguinte forma:
   - Primeiro faça um backup do Estado do Sistema no Controlador de Domínio existente.
   - Em seguida, envie esse backup para o computador de destino.
   - No computador de destino, realize a operação de restauração em um outro local (Escolha uma pasta, por exemplo: C:\NTDSRestore)
   - Por último, execute o assistente ***dcpromo /adv***
   - O assistente lhe permitirá selecionar a opção ***A partir da mídia***

## 3.3. new! Como renomear um Controlador de Domínio?

No Windows Server 2003, você pode renomear um Controlador de Domínio depois que ele já tiver sido instalado. Para renomear um Controlador de Domínio, você deve ter direitos de Administrador do Domínio.

Quando você renomeia um Controlador de Domínio, é preciso adicionar o novo nome do Controlador de Domínio e remover o nome antigo nos bancos de DNS e Active Directory. A renomeação de um Controlador de Domínio só é possível se o Nível Funcional do Domínio for configurado como Windows Server 2003. Esta configuração será abordada mais a frente neste capítulo.

***Para renomear um Controlador de Domínio, você deve seguir os passos abaixo:***

1. No Painel de Controle, clique duas vezes em ***Sistema***.
2. Na caixa ***Propriedades do Sistema***, em ***Nome do Computador***, clique em ***Alterar***.
3. Quando solicitado, confirme se deseja renomear o Controlador de Domínio.
4. Incorpore o nome completo do computador (incluindo o sufixo de DNS primário) e depois clique em ***OK***.

Você poder trocar o sufixo de DNS Primário de um Controlador de Domínio quando renomeia o Controlador de Domínio. No entanto, ao modificar o sufixo do DNS Primário, não mova o Controlador de Domínio para um novo domínio do Active Directory. Por exemplo, se você renomear dc2.nwtraders.msft para dc1.contoso.msft, o computador continua sendo um Controlador de Domínio do nwtraders.msft, embora seu sufixo de DNS primário seja contoso.msft. Para mover um Controlador de Domínio para outro domínio, você deve primeiro rebaixar o Controlador de Domínio e depois promovê-lo no novo domínio.

Obtenha informações sobre a instalação do Active Directory

http://support.microsoft.com/default.aspx?scid=kb;en-us;324753

http://support.microsoft.com/default.aspx?scid=kb;en-us;814591

http://support.microsoft.com/default.aspx?scid=kb;en-us;814591

http://support.microsoft.com/default.aspx?scid=kb;en-us;814591


© 2003 Microsoft Corporation. Todos os direitos reservados.

### 3.4. Como solucionar problemas na instalação do Active Directory?

Ao instalar o Active Directory, você pode ter problemas. Eles podem ser credenciais inadequadas de segurança, uso de nomes que não são únicos, uma rede não confiável ou falta de recursos.

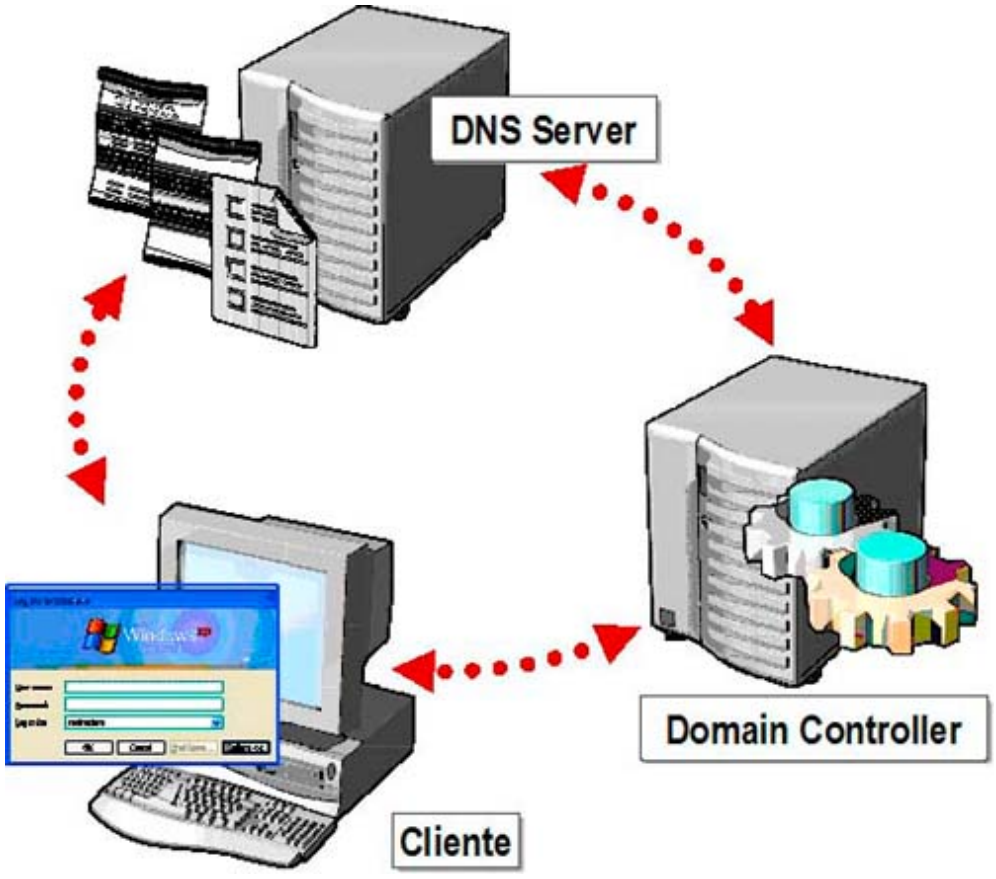
Em seguida, são descritos alguns problemas comuns que você pode encontrar enquanto instala o Active Directory e algumas estratégias para resolvê-los.

***Acesso negado enquanto cria ou adiciona os Controladores de Domínio.*** Feche a sessão e depois reinicie com uma conta que pertença ao grupo local de administradores. As credenciais devem ser de um usuário que é membro do Admins de Domínio ou Admins da empresa.

***O nome de DNS ou NetBIOS do domínio não é único*** Troque o nome para um nome único.

***O domínio não pode ser contatado*** Verifique se há conexão de rede entre o servidor que você está promovendo a Controlador de Domínio e se há, pelo menos, um Controlador de Domínio no domínio. Use o comando ping do prompt de comando para testar a conexão com qualquer Controlador de Domínio do domínio. Verifique se o DNS proporciona a resolução de nomes, pelo menos, a um Controlador de Domínio no domínio.

## 4. O Que São Zonas Active Directory de DNS Integradas?





© 2003 Microsoft Corporation. Todos os direitos reservados.

## 4.1. Introdução

Uma vantagem de integrar o DNS e o Active Directory é a capacidade de integrar as zonas de DNS no banco de dados do Active Directory. Uma zona é parte do Espaço de Nome de Domínio que agrupa registros de forma lógica, permitindo transferências de zona desses registros para funcionar como uma unidade.

## 4.2. Zona do Active Directory Integrado

Os Servidores DNS da Microsoft armazenam as informações que são utilizadas para resolver os nomes de host em endereços IP e endereços IP em nomes de host, usando um banco de dados em formato de arquivo que tenha uma extensão .dns para cada zona.

***As Zonas do Active Directory Integradas*** são primárias e stub, e armazenadas como objetos no banco de dados do Active Directory. Você pode armazenar objetos da zona na Partição de Aplicativos do Active Directory ou na Partição de Domínio do Active Directory. Se os objetos de zona estiverem armazenados na Partição de Aplicativos do Active Directory, somente os Controladores de Domínio sob essa Partição de Aplicativo podem participar na replicação desta partição. No entanto, se os objetos de zona forem armazenados na Partição de Domínio do Active Directory, todos os Controladores de Domínio serão duplicados no domínio.

## 4.3. Vantagens das Zonas do Active Directory Integrada

***As Zonas do Active Directory Integrado oferecem as seguintes vantagens.***

- ***Replicação multimaster.*** Quando você configura Zonas no Active Directory Integrado, as atualizações dinâmicas do DNS baseiam-se no modelo multimaster. Neste modelo, qualquer servidor de autorização do DNS, por exemplo, um Controlador de Domínio executando o Servidor DNS, é primário para a zona. Considerando que a Cópia Mestre da zona se mantém na base do Active Directory (que é duplicado completamente para todos os Controladores de Domínio), a zona pode ser atualizada pelos Servidores DNS funcionando em qualquer Controlador de Domínio do domínio.

- ***Atualizações dinâmicas de segurança*** Como as zonas do DNS são objetos do Active Directory nas Zonas do Active Directory Integrado, você pode aplicar permissões aos registros dentro dessas zonas e também pode controlar que computadores podem atualizar seus registros. Dessa maneira, as atualizações que utilizam o protocolo dinâmico de atualização só podem ser recebidas dos computadores autorizados.

Para obter mais informações sobre as Zonas do Active Diretory Integrado:

http://support.microsoft.com/default.aspx?scid=kb;en-us;816101

## 4.4. Exercício 3: Verificação da Zona Integrada com o Active Directory

Durante esse exercício, você verificará se o seu Servidor DNS tem a zona integrada com o Active Directory.

***Para verificar o DNS:***

1. Abra o console de DNS.
2. Clique no nome do servidor.
3. Clique na zona a verificar.
4. Clique com o botão direito do mouse na zona e depois em ***Propriedades***.
5. Na caixa ***Tipo da zona*** selecione ***Integrada ao Active Directory***
6. Para trocar o tipo de zona, clique em ***Alterar***.


© 2003 Microsoft Corporation. Todos os direitos reservados.

## 5. Qual é a funcionalidade de Floresta e Domínio?

| Ambiente de rede | Domain functional levels | Forest functional levels |
|---|---|---|
| Windows 2000 mixed-mode domain | ✓ | |
| Windows 2000 native-mode domain | ✓ | ✓ |
| Windows Server 2003 Domain | ✓ | ✓ |
| Windows Server 2003 Interim | ✓ | |

### 5.1. Introdução

No Windows Server 2003, a funcionalidade de floresta e domínio proporciona uma maneira de permitir os novos recursos em toda a floresta ou domínio do Active Directory no seu ambiente de rede. Diversos níveis da funcionalidade da floresta e do domínio estão disponíveis, dependendo do seu ambiente de rede.

### 5.2. Qual é a funcionalidade do Domínio?

A funcionalidade do domínio ativa os recursos que afetarão o domínio inteiro e somente esse domínio. Quatro níveis funcionais de domínio estão disponíveis:

- ***Windows 2000 mista.*** Esse é o nível operacional padrão. Você pode elevar o nível de funcionamento do domínio para Windows 2000 nativo ou Windows Server 2003. Os domínios de modo misto podem conter os Controladores de Domínio de backup do Windows NT 4.0, mas não é possível utilizar grupos de segurança universais, aninhamento de grupos ou recursos do Identificador de Segurança (SID) History.
- ***Windows 2000 nativo.*** Você pode utilizar esse nível funcional se o domínio contiver somente os Controladores de Domínio do Windows 2000 e do Windows Server 2003. Embora os Controladores de Domínio funcionem no Windows 2000 Server, eles não estão preparados para a funcionalidade de domínio. Características do Active Directory, como grupos de segurança universais, aninhamento de grupos e recursos do Histórico do Identificador de Segurança (SID), estão disponíveis.
- ***Windows 2003 Server*** Esse é o nível funcional mais alto para um domínio. Você só pode utilizá-lo se todos os Controladores de Domínio do domínio funcionarem no Windows Server 2003. Todos os recursos do Active Directory para o domínio estão disponíveis para uso.
- new! ***Windows 2003 Interim.*** É um nível funcional especial que suporta Controladores de Domínio do Windows NT 4.0 e do Windows Server 2003.

### 5.3. new! O que é a funcionalidade da floresta?

A funcionalidade da floresta ativa os recursos através de todos os domínios dentro da sua floresta. Dois níveis funcionais de floresta estão disponíveis: o Windows 2000 e o Windows Server 2003. Por padrão, as florestas funcionam no nível funcional do Windows 2000. Você pode elevar o nível funcional da floresta ao Windows Server 2003 para ativar os recursos que não estão disponíveis no nível funcional do Windows 2000, incluindo:


© 2003 Microsoft Corporation. Todos os direitos reservados.

- Relações de confiança entre florestas
- Replicação melhorada

**Importante:** Você não pode rebaixar o nível funcional do domínio ou da floresta depois que ele tiver sido elevado.

## 5.4. new! Requisitos para ativar novos recursos no Windows Server 2003

| Requisito | Dominio | Floresta |
|---|---|---|
| Controladores de domínio executando: | Windows Server 2003 | Windows Server 2003 |
| O nível funcional do domínio deve ser: | Elevado a Windows Server 2003 | Capaz de ser elevado a Windows Server 2003 |
| Privilégios: | Administrador do dominio para elevar o nível funcional do dominio | Enterprise administrator para elevar o nível funcional da floresta |

### 5.4.1 new! Introdução

Além dos recursos básicos do Active Directory nos Controladores de Domínio individuais, os novos recursos em toda a floresta (forest-wide) e em todo o domínio (domain-wide) estão disponíveis quando determinadas condições são cumpridas.

Para ativar os novos recursos de todo o domínio, todos os Controladores de Domínio no domínio devem executar o Windows Server 2003, e o nível funcional do domínio deve ser elevado para o Windows Server 2003. Você precisa ser administrador do domínio para elevar o nível funcional do domínio.

Para ativar os novos recursos de toda a floresta, todos os Controladores de Domínio na floresta devem executar o Windows Server 2003, e o nível funcional da floresta deve ser elevado ao Windows Server 2003. Você precisa ser administrador Enterprise para elevar o nível funcional da floresta.

Para obter mais informações sobre os níveis de funcionalidade:

http://support.microsoft.com/default.aspx?scid=kb;en-us;322692

### 5.4.2 Exercício 4: Como elevar o nível funcional?

Elevar a funcionalidade da floresta e do domínio ao Windows Server 2003 ativa determinados recursos, por exemplo, confianças de floresta, que não estão disponíveis em outros níveis funcionais. Você pode elevar a funcionalidade da floresta e do domínio usando a ferramenta Domínios e Relações de Confianças do Active Directory.

***Para elevar o nível funcional do domínio, é preciso executar os passos a seguir:***

1. Abra a ferramenta Domínios e Relações de Confiança do Active Directory.
2. Clique com o botão direito do mouse no domínio que você deseja elevar e depois clique em ***Aumentar o nível funcional do domínio***.


© 2003 Microsoft Corporation. Todos os direitos reservados.

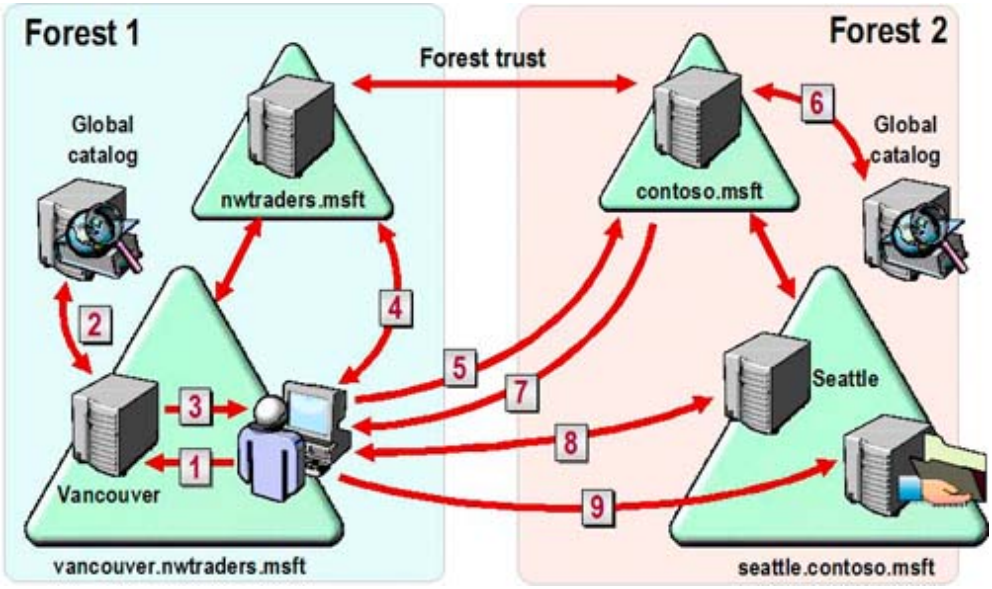
3. Selecione o nível funcional do Windows Server 2003 na caixa ***Selecione um nível funcional de domínio disponível*** e depois clique em ***Aumentar***.

***Para elevar o nível funcional da floresta, é preciso executar os passos a seguir:***

1. Na ferramenta Domínios e Relações de Confianças do Active, no console, clique com o botão direito do mouse em ***Active Directory Domains and Trusts***, e depois clique em ***Aumentar nível funcional da floresta***.
2. Na caixa ***Selecione um nível funcional de floresta disponível***, selecione ***Windows Server 2003*** e depois clique em ***Aumentar***.

**Nota:** Você deve elevar o nível funcional de todos os domínios em uma floresta ao Windows 2000 nativo ou mais alto, antes de elevar o nível funcional da floresta.

## 6. Como funcionam as Relações de Confianças entre Florestas?




### 6.1. Introdução

O Windows Server 2003 suporta confianças entre florestas que permite que os usuários na floresta tenham acesso a recursos em outra floresta. Quando um usuário tenta obter acesso a um recurso em uma floresta confiável, o Active Directory primeiro localizará o recurso.

Depois de localizar o recurso, o usuário poderá ser autenticado e ter acesso ao recurso. Entender como este processo funciona o ajudará a identificar problemas que possam se apresentar com confianças entre florestas.

### 6.2. Como é concedido um recurso?

A seguir temos uma descrição de como um cliente do Windows 2000 Professional ou Windows XP Professional localiza e tem acesso a um recurso em outra floresta que tenha o Windows 2000 Server ou o Windows Server 2003.

1. Um usuário que inicie a sessão no domínio vancouver.nwtraders.msft tenta ter acesso a uma pasta compartilhada na floresta contoso.msft. O computador do usuário entra em contato com o KDC em


© 2003 Microsoft Corporation. Todos os direitos reservados.

um controlador de domínio no vancouver.nwtraders.msft e solicita um solicitação de serviço usando o SPN do computador, onde reside o recurso. Um SPN pode ser o nome DNS de um host ou domínio ou pode ser o Nome Distinto de um Objeto de Ponto de Conexão do Serviço.

2. O recurso não está em vancouver.nwtraders.msft e o Controlador de Domínio de vancouver.nwtraders.msft faz consultas no Catálogo Global para ver se o recurso está situado em outro domínio da floresta. Considerando que o Catálogo Global contém apenas informações sobre sua própria floresta, ele não encontra o SPN. O Catálogo Global testa seu banco de dados para saber se há informações sobre relações de confianças de floresta estabelecidas com a sua floresta. Se o Catálogo Global encontrar uma, compare os sufixos de nome que estão listados na confiança da floresta TDO com o sufixo de destino SPN. Se encontrar um ponto em comum, o Catálogo Global fornece as informações de encaminhamento sobre como localizar o recurso ao Controlador de Domínio em vancouver.nwtraders.msft.
3. O Controlador de Domínio em vancouver.nwtraders.msft envia uma referência para seu domínio Pai nwtraders.msft, no computador do usuário.
4. O computador do usuário entra em contato com o Controlador de Domínio nwtraders.msft pela referência ao Controlador de Domínio do Domínio da Floresta Raiz da floresta contoso.msft.
5. Usando a referência do Controlador de Domínio em nwtraders.msft, o computador entra em contato com o controlador de domínio na floresta contoso.msft para solicitar uma permissão de serviço.
6. O recurso não está situado no Domínio da Floresta Raiz da floresta contoso.msft e, por isso, o Controlador de Domínio entra em contato com seu Catálogo Global para pesquisar o SPN. O Catálogo Global busca o SPN e o envia ao Controlador de Domínio.
7. O Controlador de Domínio envia a referência seattle.contoso.msft ao computador do usuário.
8. O computador do usuário entra em contato com o KDC no controlador de domínio em seattle.contoso.msft e negocia a permissão para acesso do usuário ao recurso no domínio seattle.contoso.msft.
9. O computador envia a permissão de serviço do servidor ao computador onde está o recurso compartilhado e onde são lidas as credenciais de segurança do usuário e é criado o token de acesso que permite o acesso do usuário ao recurso.

**Nota:** Lembre-se de que para poder utilizar esse novo recurso, é preciso ter as duas florestas no nível funcional do Windows Server 2003. As relações de confianças entre florestas no Windows Server 2003 lhe permitem validar os usuários usando o Kerberos v5, utilizando a segurança própria do protocolo. Também é permitido que as confianças transitem entre duas florestas, e não em múltiplas florestas. Por exemplo: A floresta A estabeleceu uma confiança com a floresta B, e todos os domínios nas duas florestas podem utilizar essa confiança. No entanto, se, por sua vez, a floresta B tem uma confiança na floresta C, não existe nenhum tipo de relação entre a floresta A e a floresta C.

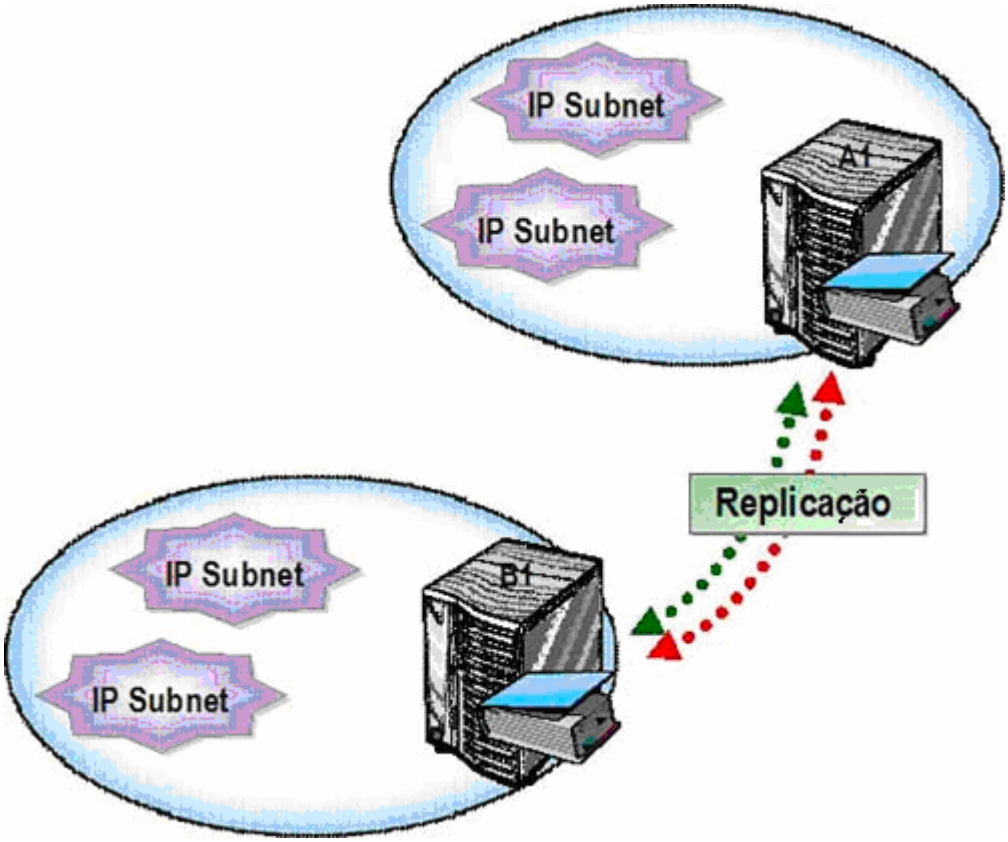
Para obter mais informações sobre relações de confiança:

http://support.microsoft.com/default.aspx?scid=kb;en-us;325874

http://support.microsoft.com/default.aspx?scid=kb;en-us;816101


© 2003 Microsoft Corporation. Todos os direitos reservados.

## 7. Replicação no Active Directory




### 7.1. Replicação dentro dos sites

***Os pontos dominantes da replicação do Active Directory dentro do site são:***

- ***A replicação ocorre quando há:***

  - Um acréscimo de um objeto ao Active Directory.
  - Uma modificação dos valores de um atributo de objeto.
  - Uma mudança do nome de um contêiner de objetos.
  - Uma eliminação de um objeto de diretório.

- ***Notificação da modificação.*** Quando ocorre uma mudança em um controlador de domínio, o controlador de domínio notifica seus parceiros da replicação no mesmo site. Esse processo é chamado de notificação de alteração.

- ***Latência da replicação.*** Tempo de espera entre a hora em que ocorre a modificação e a hora em que a atualização atinge todos os controladores de domínio no site. Por padrão, a latência da replicação é de 15 minutos.

- ***Replicação urgente.*** Em vez de esperar os 15 minutos padrão, os atributos confidenciais fornecem uma mensagem imediata de notificação de alteração quando são atualizados.


© 2003 Microsoft Corporation. Todos os direitos reservados.

- ***Convergência.*** Cada atualização no Active Directory é propagada a todos os Controladores de Domínio no site que contêm a partição na qual a atualização foi realizada. Essa propagação completa é chamada de convergência.

- ***Propagation dampening.*** O processo de evitar uma replicação desnecessária. Cada Controlador de Domínio atribui a cada modificação de atributo ou objeto um Número de Seqüência de Atualização (USN) para evitar a replicação desnecessária.

- ***Conflitos.*** Quando atualizações simultâneas originadas em dois mestres de replicações diferentes são inconsistentes, podem ocorrer conflitos. O Active Directory resolve três tipos de conflitos: atributo, contêineres eliminados e conflitos de Nome Distinto Relativo (RDN).

- ***Carimbo global único.*** O Active Directory mantém um carimbo que contém o número da versão, carimbo de hora, e identificador global exclusivo (GUID) de servidor que o Active Directory criado durante a atualização originaria.

## 7.2. new! Linked Multivalued Attributes

***O processo pelo qual os atributos de múltiplos valores vinculados são duplicados varia, dependendo do nível funcional da floresta:***

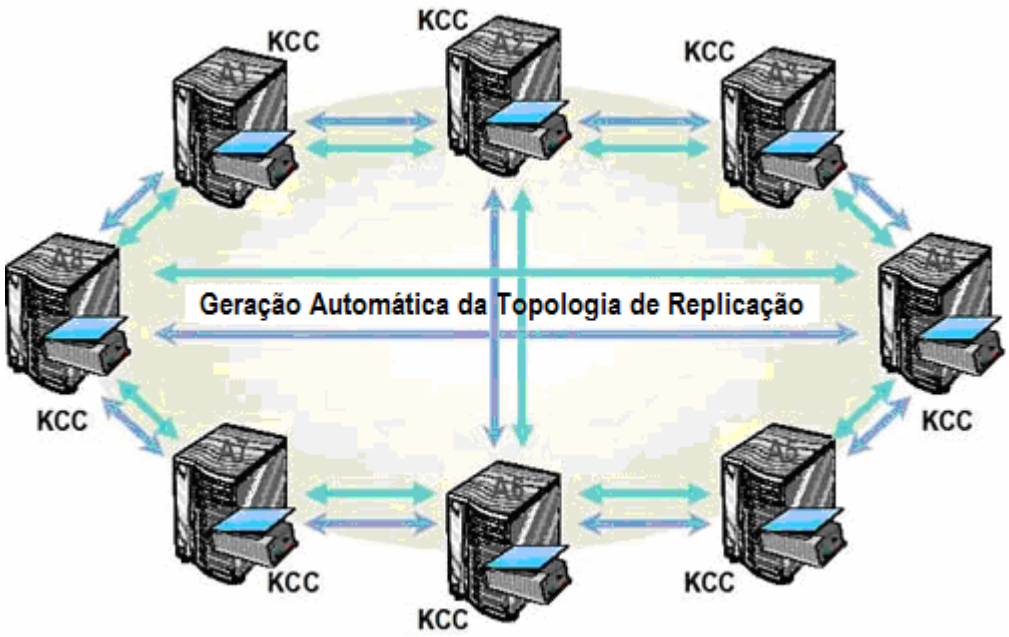
Quando o nível funcional da floresta é inferior ao Windows Server 2003, qualquer modificação realizada em um atributo de membros de grupo inicia a replicação da lista inteira do atributo membro. O atributo **membro** de múltiplos valores é considerado um único atributo com o fim da replicação nesse caso. Essa replicação aumenta a probabilidade de substituir uma modificação do atributo membro que outro administrador realizou em outro controlador de domínio, antes da primeira modificação ter sido duplicada.

Quando o nível funcional da floresta é modificado para o Windows Server 2003, um valor individual duplica as modificações de atributos de múltiplos valores vinculados. Essa funcionalidade aprimorada duplica apenas modificações do atributo membro do grupo, e não a lista inteira do atributo de membro.

Desta forma, elimina-se a restrição de um máximo de 5000 usuários por grupo. Essa restrição era fornecida no Windows 2000 pelo valor máximo que o atributo de membro de um grupo podia ter.

## 7.3. new! Geração automática da topologia de replicação


© 2003 Microsoft Corporation. Todos os direitos reservados.




Quando você adiciona Controles de Domínio a um site, o Active Diretory usa o Knowledge Consistency Checker (KCC) para estabelecer um caminho de replicação entre os Controladores de Domínio.

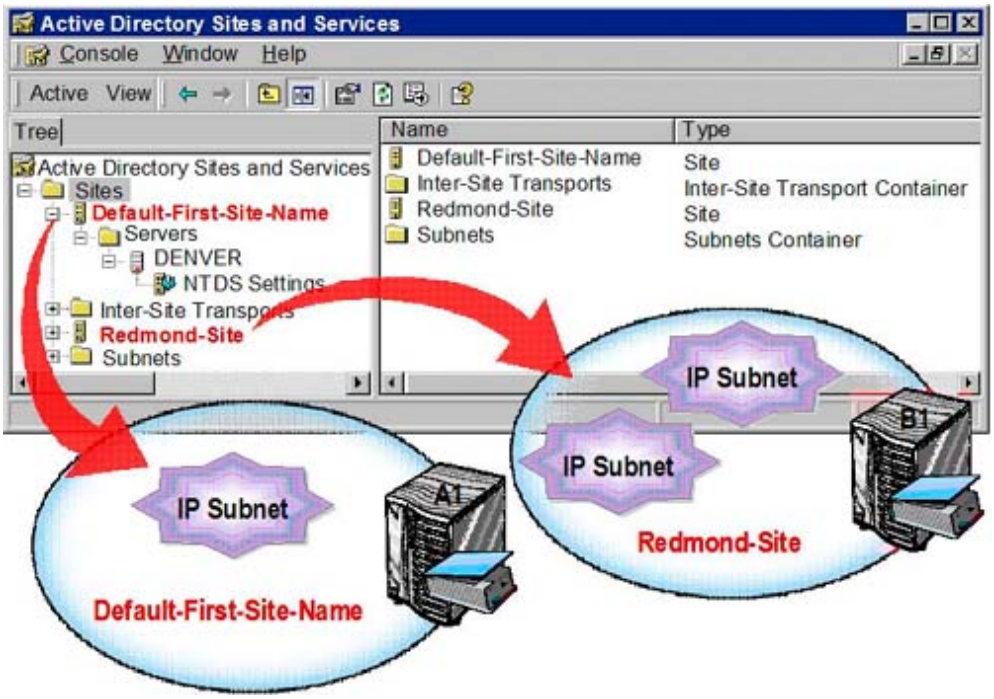
O KCC é um processo que funciona em cada Controlador de Domínio e gera a topologia da replicação para todas as partições do diretório contidas nesse Controlador de Domínio. O KCC é executado em intervalos específicos, a cada 15 minutos por padrão, e define os caminhos de replicação entre Controladores de Domínio nas conexões mais favoráveis disponíveis no momento.

Este processo foi melhorado com relação ao processo do Windows 2000, fazendo com que essa nova característica elimine a limitação existente de um máximo de 500 sites no Active Directory. Atualmente já foram testados até 3000 sites e o suporte máximo é de 5000 sites.

**Nota:** Para aproveitar essa característica, você deve ter a floresta no nível funcional do Windows Server 2003 ou do Windows Server 2003 Interim.

### 7.4. Criando e Configurando Sites


© 2003 Microsoft Corporation. Todos os direitos reservados.




Você utiliza sites para controlar o tráfego de replicações, o tráfego de logins e as consultas do cliente ao Servidor de Catálogo Global.

### 7.4.1. O que são os sites?

No Active Directory, os sites ajudam a definir a estrutura física de uma rede. Uma ou mais sub-redes TCP/IP em um intervalo específico de endereços define um site, no qual são definidos alternadamente um grupo de Controladores de Domínio que tem velocidade e custos semelhantes. Os sites consistem em servidores de objetos, que contêm objetos de conexão que permitem a replicação.


© 2003 Microsoft Corporation. Todos os direitos reservados.

### 7.4.2. O que são os objetos sub-rede?

Os objetos de sub-rede identificam os endereços de rede que utilizam os computadores nos sites. Uma sub-rede é um segmento de uma rede TCP/IP ao qual é atribuído um sistema de endereços IP lógicos. Considerando que os objetos da sub-rede representam a rede física, eles formam sites. Por exemplo, se 3 sub-redes estiverem situadas em 3 campos em uma cidade e esses campos estiverem conectados com conexões de alta velocidade e alta disponibilidade, você pode associar cada uma dessas sub-redes a um site.
Um site pode consistir em uma ou mais sub-redes. Por exemplo, em uma rede que tem 3 sub-redes em Redmond e 2 em Paris, você pode criar um site em Redmond, um site em Paris e depois adicionar as sub-redes nos respectivos sites.

### 7.4.3. O que são os links de sites?

***Os Links de Site são conexões que você pode estabelecer entre sites para***:

- Ativar a replicação
- Controlar os horários em que você quer fazer a replicação
- Controlar o custo de acordo com o enlace que você está utilizado e o protocolo de replicação IP (RPC) ou SMTP.

Para obter mais informações sobre os sites:

http://support.microsoft.com/default.aspx?scid=kb;en-us;323349

### 7.4.4 Exercício 5: Criar e Configurar Sites e Sub-redes

***Para criar um site, você deve seguir os passos abaixo:***

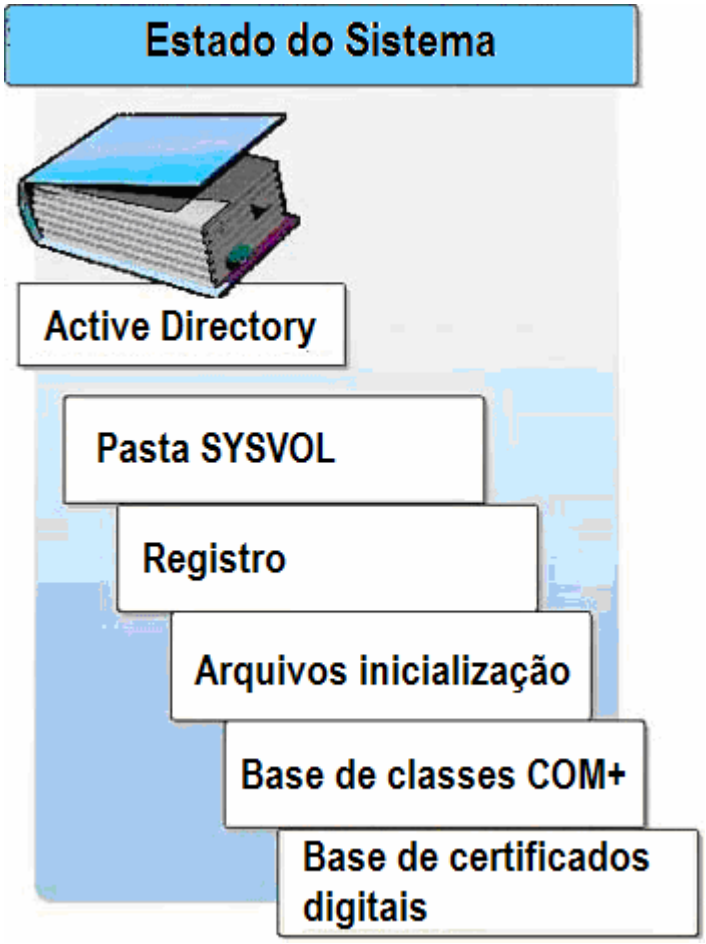
1. Abra os Sites e Serviços do Active Directory no menu ***Ferramentas Administrativas***.
2. Clique com o botão direito em ***Sites*** no console e depois clique em ***Novo Site***.
3. Insira o nome do novo site na caixa ***Nome***.
4. Clique em um objeto de link do site e depois clique em ***OK*** duas vezes.

***Para criar um objeto de sub-rede, você deve seguir os passos abaixo:***

1. Em Sites e Serviços do Active Directory, no console, clique duas vezes em ***Sites***, clique com o botão direito em ***Sub-redes*** e depois clique em ***Nova Sub-rede***.
2. Na caixa ***Endereço***, insira o endereço IP da sub-rede.
3. Na caixa ***Máscara***, insira a máscara de sub-rede que descreve o intervalo de endereços da sub-rede.
4. Selecione o site para associar à sub-rede e depois clique em ***OK***.


© 2003 Microsoft Corporation. Todos os direitos reservados.

### 8. Fazer backup do Active Directory.




Fazer o backup do Active Directory é essencial para manter o banco de dados do Active Directory. Você pode fazer o backup do Active Directory usando uma interface de usuário gráfica (GUI) e ferramentas de linha de comando fornecidas pelo Windows Server 2003.

Você deve com freqüência fazer backup dos dados do Estado do Sistema nos Controladores de Domínio para que seja possível restaurar os dados mais atuais. Estabelecendo um cronograma regular de backup, você tem mais chances de recuperação de dados quando necessário.

***Os Dados de Estado do Sistema no Controlador de Domínio incluem os seguintes componentes:***

***Active Directory*** Os Dados do Estado do Sistema não contêm o Active Directory, a menos que o servidor no qual você está fazendo backup dos Dados de Estado do Sistema seja um Controlador de Domínio. O Active Directory só está presente nos Controladores de Domínio.
***A pasta compartilhada SYSVOL.*** Esta pasta compartilhada contém arquivos de Diretivas de Grupo e scripts de login. A pasta compartilhada SYSVOL está presente somente em controladores de domínio.
***O registro.*** Este repositório de banco de dados contém as informações sobre a configuração dos computadores.
***Arquivos de inicialização do sistema.*** O Windows Server 2003 exige esses arquivos durante sua fase de inicialização. Eles incluem os arquivos do sistema e inicializações que estão protegidos pela proteção do arquivo do Windows.
***O banco de dados COM+ Registro de Classe.*** O banco de dados do Registro de Classe contém informações sobre aplicativos de Serviços de Componente.
***O banco de dados dos Serviços de Certificado.*** Este banco de dados contém os certificados do servidor que o

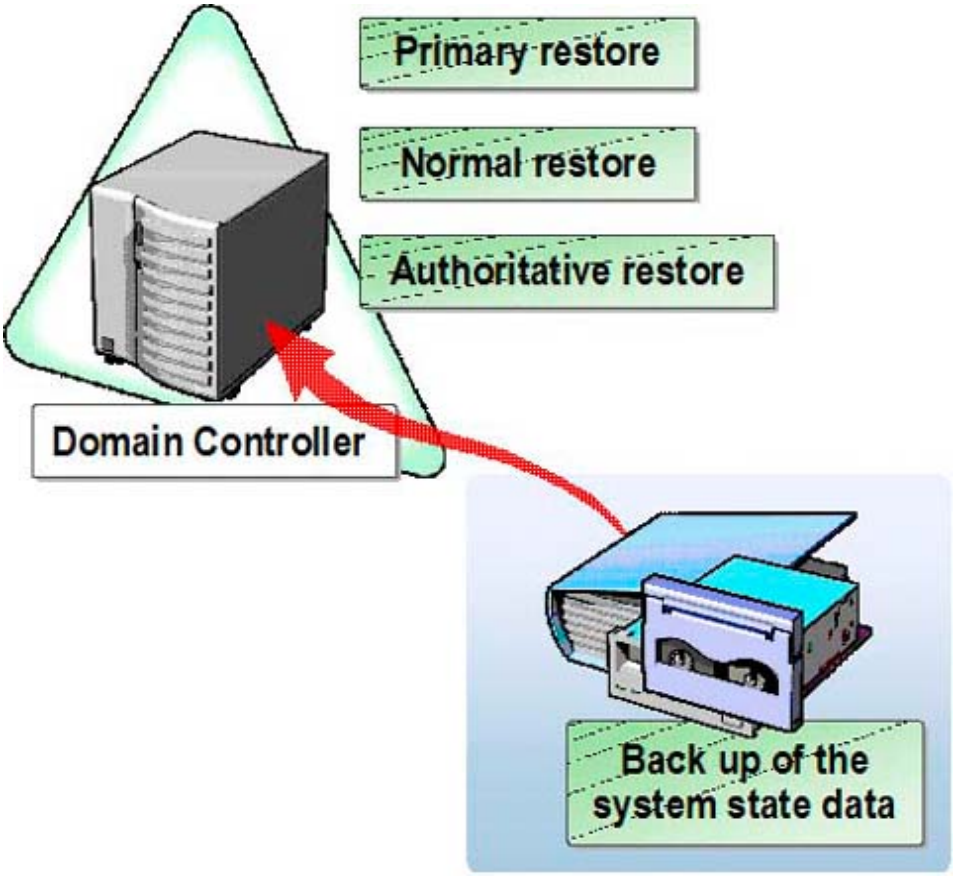

© 2003 Microsoft Corporation. Todos os direitos reservados.

Windows Server 2003 utiliza para autenticar usuários. Esse banco só está presente se o servidor estiver funcionando como servidor de certificados.

***Para realizar a operação de backup, você pode utilizar a ferramenta prevista pelo Windows Server 2003:***

1. Clique em ***Backup*** no menu ***Iniciar***, ***Todos os Programas***, ***Acessórios***, ***Ferramentas do Sistema***.
2. Clique em ***Avançar*** na página ***Bem-vindo ao Assistente de Backup ou Restauração***.
3. Na página ***Faça backup ou restaure***, clique em ***Fazer backup de arquivos e confgurações*** e depois clique em ***Avançar***.
4. Na página ***Backup***, clique em ***Eu escolherei os itens para backup*** e depois clique em ***Avançar***.
5. Na página ***Itens para backup***, expanda ***Meu computador***, selecione ***Estado do Sistema***, e depois clique em ***Avançar***.
6. Na página ***Tipo, destino e nome do backup***, clique em ***Procurar***, selecione um local para backup, clique em ***Salvar*** e depois clique em ***Avançar***.
7. Na página ***Concluindo o Assistente para backup ou restauração***, clique em ***Concluir***.
8. Após o backup ser realizado, na página ***Progresso do Backup*** clique em ***Fechar.***

## 8.1 Restauração do Active Directory





© 2003 Microsoft Corporation. Todos os direitos reservados.

Você pode utilizar um dos três métodos para restaurar o Active Directory de meios de backup: restauração primária, restauração normal (sem autoridade) e restauração com autoridade.

1. ***Restauração primária.*** Este método reconstrói o primeiro controlador de domínio no domínio quando não há outra maneira de reconstruir o domínio. Faça uma restauração primária somente quando todos os controladores de domínio em um domínio estiverem perdidos e você quiser reconstruir o domínio usando o backup.

2. ***Restauração Normal.*** Este método reinstala os dados do Active Directory no estado antes do backup e atualiza os dados com o processo normal de replicação. Realize uma restauração normal quando quiser restaurar um único controlador de domínio a um estado previamente conhecido.

3. ***Restauração com autoridade.*** Você executa esse método junto com uma restauração normal. Uma restauração com autoridade marca os dados específicos e evita que a replicação substitua esses dados. Os dados autorizados são replicados através do domínio.

***Para realizar uma restauração primária do Active Directory, siga os passos abaixo:***

1. Reinicie seu controlador de domínio no Modo Restauração do Serviço de Diretório.
2. Inicie o utilitário de Backup.
3. Clique em ***Modo Avançado*** na página ***Bem-vindo ao Assistente para Backup ou Restauração***.
4. Na página ***Bem-vindo ao modo avançado do utilitário de backup***, em ***Restaurar e gerenciar mídia***, selecione o que deseja restaurar e depois clique em ***Iniciar Restauração***.
5. Clique em ***Cuidado*** e depois em ***OK***.
6. Na caixa ***Confirmar Restauração***, clique em ***Avançado***.
7. Na caixa ***Opções Avançadas de Restauração*** clique em ***Ao restaurar dados replicados, marcar os conjuntos de dados como primários para todas as replicações*** e depois clique em ***OK*** duas vezes.
8. Na caixa ***Progresso da Restauração***, clique em ***Fechar***.
9. Na caixa ***Utilitário de Backup***, clique em ***Sim***.


© 2003 Microsoft Corporation. Todos os direitos reservados.

# Capítulo 5
# Implementação, Administração e Monitoração da Diretiva de Grupos

Durante este capítulo, você assimilará os conhecimentos necessários para administração, projeto e implementação adequados de Diretiva de Grupos.

Para poder realizar os exercícios dessa unidade, é necessário já ter concluído os exercícios dos capítulos 2 e 3.

## 1. Introdução

Você utiliza a Diretiva de Grupo no Active Directory® para centralizar o controle de usuários e computadores em uma empresa. Configurando a Diretiva de Grupos, é possível centralizar políticas para toda uma organização, domínio, sites ou unidades organizacionais e também descentralizar a configuração da Diretiva de Grupos, configurando-a para cada departamento no nível da unidade organizacional.

Você pode se certificar de que os usuários dispõem dos ambientes necessários para realizar seus trabalhos e fazer cumprir as políticas das organizações, incluindo normas, metas e requisitos de segurança da empresa. Além disso, é possível baixar o Custo Total da Propriedade controlando ambientes de usuário e de computadores, de forma que a necessidade de ajuda técnica e o prejuízo à produtividade decorrentes de erros seja reduzido.

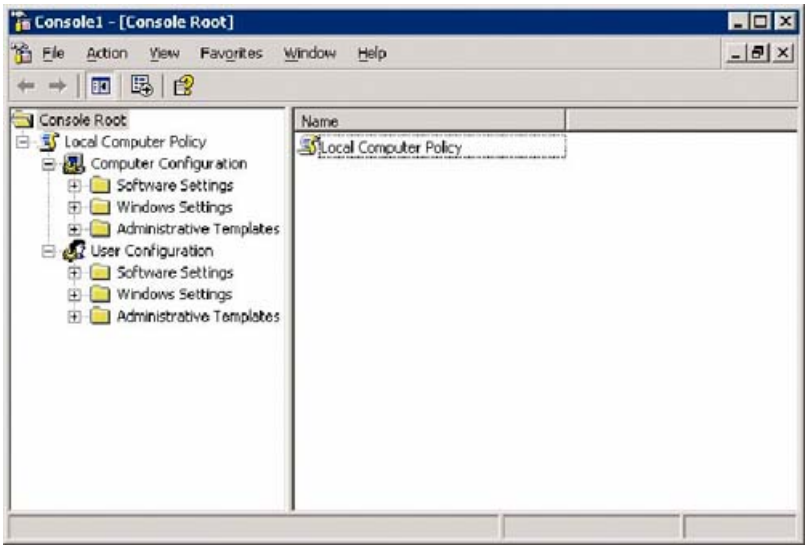
***Ao concluir este capítulo, você poderá:***

- Criar e configurar objetos de Diretivas de Grupos (GPOs).
- Configurar intervalos de atualização da Diretiva de Grupos e configurações da Diretiva de Grupos.
- Administrar GPOs.

### 1.1. O que é a Diretiva de Grupos?

A Diretiva de Grupos lhe concede o controle da administração sobre os usuários e os computadores da sua rede; portanto, lhe permite definir o estado do ambiente de trabalho dos usuários uma única vez, confiando no Microsoft® Windows® Server 2003 para implementar continuamente a configuração de Diretiva de Grupo que foi definida. Também será possível aplicar configurações da Diretiva de Grupos através de uma organização inteira ou grupos específicos de usuários e computadores.


© 2003 Microsoft Corporation. Todos os direitos reservados.




Para obter mais informações sobre a Diretiva de Grupo:

Microsoft IntelliMirror®.

Visão Geral de Configurações de Diretiva de Grupo.

## 1.2. O Que São as Definições de Configuração de Usuário e Computador?

Você pode executar as Configurações de Diretiva de Grupos para os computadores e os usuários usando Configuração de Computador e Configuração de Usuário na Diretiva de Grupo.

***Configurações de Diretiva de Grupo*** para usuários incluem configurações específicas do sistema operacional, configurações de área de trabalho, configurações de segurança, opções de aplicativos atribuídas e publicadas, configurações de aplicativos, opções de redirecionamento de pasta e script de logon e logoff de usuários. As Configurações de Diretiva de Grupo de usuário são aplicáveis quando os usuários iniciam a sessão no computador e durante um ciclo de atualização periódica.

As Configurações de Diretiva de Grupos modificam o ambiente da área de trabalho do usuário conforme requisitos específicos ou aplicam as diretivas de bloqueio em usuários e estão contidas em ***Configuração do usuário*** no editor de Objeto de Diretiva de Grupos.

***Em Configuração do Usuário, também é possível selecionar:***

- A pasta Configurações de Software: contém configurações de software que são aplicadas aos usuários, independente do computador em que a sessão foi iniciada. Essa pasta também contém configurações que são incluídas conforme os provedores de software independentes (ISVs).

- A pasta Configurações do Windows: contém configurações do Windows que são aplicadas aos usuários, independe do computador em que a sessão foi iniciada. Esta pasta também contém os seguintes pontos: **Redirecionamento de Pastas, Configurações de Segurança e Scripts**.

As Configurações de Diretiva de Grupo para os computadores incluem a forma como o sistema operacional se comporta, o comportamento da área de trabalho, as configurações de segurança, os scripts de inicialização e desligamento, as opções de aplicativos atribuídas ao computador e as configurações de aplicativos. As Diretivas de Grupo relacionadas ao computador são aplicadas quando o sistema operacional é iniciado e durante um ciclo periódico de atualização. Normalmente, em caso de conflito, as configurações da Diretiva de Grupo do computador têm prioridade em relação à Diretiva de Grupo do usuário.


© 2003 Microsoft Corporation. Todos os direitos reservados.

As Configurações de Diretiva de Grupo, que modificam o ambiente conforme requisitos particulares da área de trabalho e para todos os usuários de um computador ou que aplicam as diretivas de segurança nos computadores de uma rede, podem ser encontradas em ***Configuração do Computador*** no editor de Objeto de Diretivas de Grupo.

***Em Configuração do Computador, também é possível encontrar:***

- A pasta Configurações de Software: contém configurações de software aplicadas a todos os usuários que iniciam a sessão no computador. Essa pasta possui configuração de instalação do software e pode conter outras configurações inseridas pelo ISVs.

- A pasta Configurações do Windows: contém as configurações do Windows aplicadas a todos os usuários que iniciam a sessão no computador. Esta pasta também contém os seguintes pontos: **Configurações de Segurança e Scripts**.


© 2003 Microsoft Corporation. Todos os direitos reservados.

***Configurações de Segurança*** está disponível na pasta Configurações do Windows localizada em Configuração do Computador e Configuração do usuário no editor de Objeto de Diretiva de Grupo. As Configurações de Segurança ou as Diretivas de Segurança são regras que você configura em um ou vários computadores para proteger recursos em um computador ou em uma rede. Com Configurações de Segurança você pode especificar Diretivas de Segurança de uma unidade organizacional, domínio ou site.

Para mais informações sobre o extensor de Diretiva de Grupo, veja os métodos Avançados estendendo Diretiva de Grupo em:

http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windowsserver2003/proddocs/server/sag_SPconcepts_30.asp

## 1.3. Exercício 1: Configurar Definições de Diretiva de Computador Local:

***Para adicionar o Editor de Objeto de Diretiva de Grupos a um CustomMMC, é preciso:***

1. Abrir um CustomMMC. (execute mmc em Executar...)
2. Adicionar o snap-in do Editor de Objeto de Diretiva de Grupo.
3. Salvar o CustomMMC.

***Para evitar que os usuários desativem o servidor usando Configuração de Diretiva Local, é preciso:***

1. Expandir, no CustomMMC, o snap-in ***Diretiva de Segurança Local***.
2. Expandir, no console, ***Configuração do usuário***. Expandir ***Modelos Administrativos*** e depois clicar no menu ***Iniciar*** e em ***Barra de Tarefas***.
3. Clicar duas vezes em ***Remover e prevenir acesso ao comando Desligar***, no painel de detalhes
4. Clicar em ***Habilitar*** na caixa ***Remover e prevenir acesso às propriedades do comando*** e depois clicar em ***OK***.
5. Fechar e salvar todos os programas e fazer logoff.

***Para testar a diretiva, é preciso:***

1. Iniciar a sessão como ***User*** com uma senha.
2. Clicar em ***Iniciar*** e verificar se o botão ***Desligar*** foi removido do menu ***Iniciar***.
3. Fechar e salvar todos os programas e fazer logoff.

## 1.4. As ferramentas usadas para criar os GPOs

- ***Usuários e Computadores do Active Directory***

Você pode abrir o editor de Objeto de Diretiva de Grupo de Usuários e Computadores do Active Directory para administrar GPOs para domínios e unidades organizacionais. Na caixa Propriedades de um domínio ou unidade organizacional, temos a guia Diretiva de Grupo, onde é possível controlar os GPOs de domínio ou unidade organizacional.

- ***Sites e Serviços do Active Directory***

Você pode abrir o editor de Objeto de Diretiva de Grupo de Sites e Serviços do Active Directory para controlar GPOs de sites. Na caixa Propriedades do site, temos a guia Diretiva de Grupo, onde é possível controlar os GPOs do site.

- ***Group Policy Management Console***

O Console de Gerenciamento de Diretiva de Grupo é um sistema de interfaces programáveis para o controle de Diretiva de Grupo, assim como os snap-ins MMC, que são criados nessas interfaces programáveis também. Os componentes de Gerenciamento de Diretiva de Grupo, por sua vez, consolidam a administração da Diretiva de Grupo em toda a empresa.


© 2003 Microsoft Corporation. Todos os direitos reservados.

O Group Policy Management Console combina a funcionalidade de múltiplos componentes em uma única interface de usuário (UI). A UI é estruturada conforme o modo como a Diretiva de Grupo é utilizada e controlada. Ela também incorpora a funcionalidade relacionada com a Diretiva de Grupo das ferramentas seguintes em um único snap-in MMC:

- Usuários e Computadores do Active Directory
- Sites e Serviços do Active Directory
- Conjunto de Diretivas Resultantes (RSoP)

O Gerenciamento de Diretivas de Grupos também proporciona os seguintes recursos ampliados que não estavam disponíveis em ferramentas anteriores de Diretiva de Grupos. Com o Gerenciamento de Diretiva de Grupos, você pode:

Fazer backup e restauração de GPOs.

- Copiar e importar GPOs.
- Usar filtros de Windows Management Instrumentation (WMI).
- Gerar relatórios de GPO e RSoP.
- Pesquisar para GPOs.

- ***Group Policy Management vs. ferramentas padrão de Diretiva de Grupos***

Antes do Group Policy Management, você administrava a Diretiva de Grupo usando diversas ferramentas do Windows, incluindo Usuários e Computadores do Active Directory, Sites e Serviços do Active Directory e RSoP. Mas agora o Gerenciamento de Diretiva de Grupo consolida a administração de todas as tarefas baseadas em Diretiva de Grupo em uma única ferramenta. Graças a essa administração consolidada, a funcionalidade de Diretiva de Grupo não é exigida em outras ferramentas.

Depois de instalar o Group Policy Management, você ainda utiliza cada uma das ferramentas do Active Directory para seus objetivos específicos de administração de diretórios, por exemplo, criar um usuário, computador e grupo. No entanto, você pode utilizar o Gerenciamento de Diretivas de Grupo para realizar todas as tarefas relacionadas a Diretivas de Grupo. A funcionalidade de Diretiva de Grupo não estará mais disponível nas ferramentas do Active Directory quando o Group Policy Management for instalado.

O Group Policy Management não substitui o editor do Objeto de Diretiva de Grupo. No entanto, você deve editar os GPOs, usando o editor de Objeto de Diretiva de Grupos. O Group Policy Management integra a funcionalidade de edição proporcionando acesso direto ao editor de Objeto de Diretiva de Grupo.

**Nota:** O Console do Group Policy Management não é fornecido com o Server 2003.

**Você deve fazer o download a partir de:**

http://www.microsoft.com/downloads/details.aspx?FamilyId=F39E9D60-7E41-4947-82F5-3330F37ADFEB&displaylang=en


© 2003 Microsoft Corporation. Todos os direitos reservados.

### 1.5. Exercício 2: Como criar um GPO?

Utilize os procedimentos a seguir para criar um novo GPO ou um link para um GPO existente, usando o Active Directory Users and Computers, e para criar um GPO em um site, domínio ou unidade organizacional.

***Para criar um GPO novo ou estabelecer um link para um GPO existente usando Usuários e Computadores do Active Directory:***

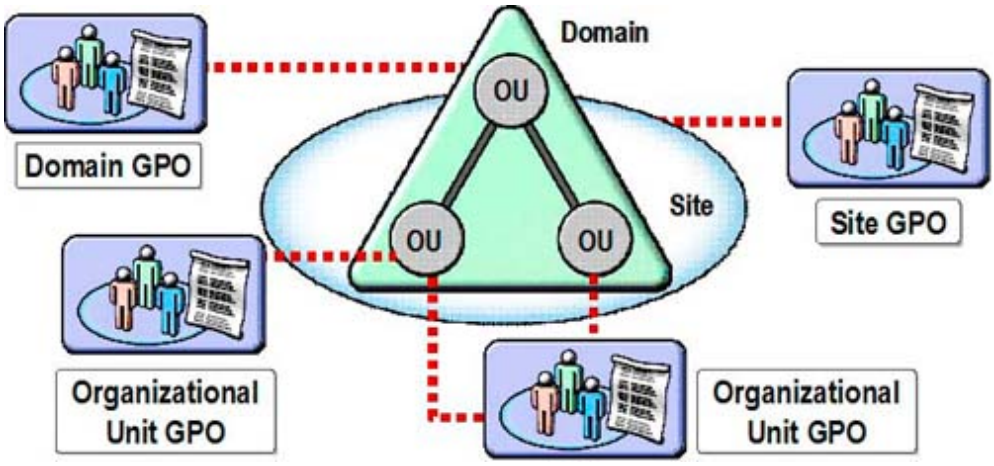
1. Clique com o botão direito no ***contêiner do Active Directory*** (domínio ou unidade organizacional), que está em Usuários e Computadores do Active Directory, para criar um GPO. Depois clique em ***Propriedades***.
2. Escolha uma das opções a seguir, na caixa ***Propriedades***, da guia ***Diretiva de Grupo***:

   - ***Para criar um novo GPO***, clique em Novo, insira um nome para o novo GPO e pressione ENTER.

   - ***Para criar um link a um GPO existente***, clique em Adicionar e selecione o GPO da lista.

O GPO ou o link que você cria são exibidos na lista de GPOs que estão vinculados ao contêiner do Active Directory.

### 1.6. O que é um Link de GPO?




Todo os GPOs são armazenados em um contêiner do Active Directory chamado Objetos de Diretiva de Grupo. Quando um GPO é utilizado por um site, domínio ou unidade organizacional, o GPO é vinculado ao contêiner de Objetos de Diretiva de Grupos. Conseqüentemente, você pode centralizar a administração e a implementação de GPOs em muitos domínios ou unidades organizacionais.

Quando cria um link de GPO em um site, domínio ou unidade organizacional, você pode realizar duas operações diferentes: criar o novo GPO e vinculá-lo ao site, domínio ou unidade organizacional. Ao delegar permissões e vincular um GPO ao domínio, à unidade organizacional ou ao site, você poderá modificar as permissões para o domínio, a unidade organizacional ou o site que deseja delegar.

Por padrão, somente os membros dos grupos de Admins de Domínio e Admins da Empresa têm as permissões necessárias para vincular GPOs a domínios e unidades organizacionais. Somente os membros do grupo Admins da Empresa têm permissões para vincular GPOs a sites. Membros dos Proprietários Criadores de Diretiva de Grupo podem criar GPOs, mas não podem vinculá-los.

Quando você cria um GPO no contêiner de Objetos de Diretiva de Grupo, o GPO não é aplicado a nenhum usuário ou computador até que o link de GPO seja criado. Você pode criar um GPO desvinculado usando o


© 2003 Microsoft Corporation. Todos os direitos reservados.

Group Policy Management e também pode criar GPOs desvinculados em uma organização de grande porte, onde um grupo cria GPOs e outro cria links de GPOs para site, domínio ou unidade organizacional.

## 1.7. Exercício 3: Como criar um Link de GPO?

Para fazer esse exercício, você deverá instalar previamente o GPMC. (Veja o item 4.3 a seguir.) Utilize os procedimentos seguintes para criar e vincular GPOs.

- Para vincular um GPO quando ele é criado:

1. No Group Policy Management Console, expanda a floresta que contém o domínio no qual você deseja criar e vincular o GPO. Expanda ***Domínios*** e siga os passos abaixo:

- ***Para criar um GPO e vinculá-lo ao domínio***, clique com o botão direito no domínio e depois em ***Criar e conectar uma diretiva aqui***.

- ***Para criar um GPO e vinculá-lo a uma unidade organizacional***, expanda o domínio que contém a unidade organizacional, clique com o botão direito da unidade organizacional e depois clique em ***Criar e conectar uma diretiva aqui***

2. Na caixa ***Nova diretiva*** (Novo GPO), insira o nome do novo GPO e depois clique em ***OK***.

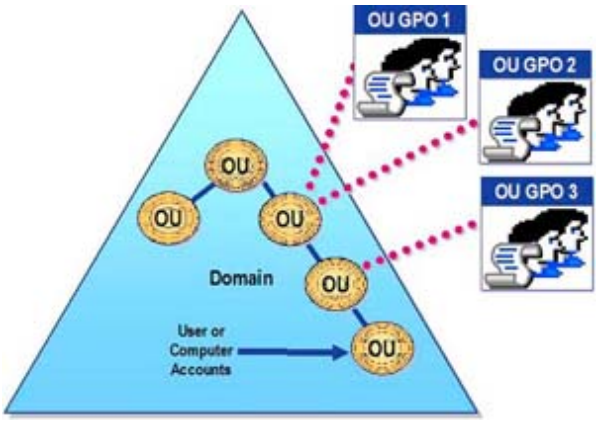
- Para vincular o GPO existente ao site, domínio ou unidade organizacional.

1. No Group Policy Management Console, expanda a floresta contendo o domínio ao qual você deseja vincular um GPO existente. Expanda ***Domínios*** e o domínio.
2. Clique com o botão direito no domínio, site ou unidade organizacional. Depois de clicar no ***Conectar a uma diretiva existente***.
3. Na caixa ***Selecionar diretiva***, clique no GPO que deseja vincular e depois clique em ***OK***.

## 1.8. Como foram herdadas as permissões de Diretiva de Grupo no Active Directory?

A ordem em que o Windows Server 2003 aplica GPOs depende do contêiner do Active Directory ao qual é vinculado o GPO. Os GPOs são aplicados primeiro ao site e depois aos domínios e, por último, às unidades organizacionais nos domínios.

Um contêiner filho herda GPOs do contêiner pai. Isso significa que um contêiner filho pode ter várias Configurações de Diretiva de Grupo aplicadas a seus usuários e computadores, sem ter um GPO vinculado a ele. No entanto, não há hierarquia de domínios como nas unidades organizacionais, por exemplo, unidades organizacionais pai e filhas.




Os GPOs são cumulativos visto que são herdados. A herança da Diretiva de Grupo é a ordem na qual o Windows Server 2003 aplica os GPOs. Essa ordem e a herança de GPOs determinam, em última instância, que configurações afetam usuários e computadores. Se houver múltiplos GPOs definindo o mesmo valor, por padrão, o GPO aplicado por último terá prioridade.

Você também pode ter múltiplos GPOs vinculados aos mesmos contêineres. Por exemplo, é possível ter três GPOs vinculados a um único domínio. A ordem em que são aplicados os GPOs pode afetar o resultado da


© 2003 Microsoft Corporation. Todos os direitos reservados.

configuração da Diretiva de Grupo. Também há uma ordem ou prioridade de Diretiva de Grupos e de GPOs para cada contêiner.

## 1.9. O que ocorre quando há conflito de GPOs?

As combinações complexas de GPOs podem criar conflitos e conseqüentemente exigir a modificação do comportamento de herança padrão. Quando uma configuração de Diretiva de Grupos é definida para uma unidade organizacional pai e a mesma configuração não é configurada para a unidade organizacional filha, os objetos dessa última herdam a configuração de Diretiva de Grupos da unidade organizacional pai.

Quando você configura uma Diretiva de Grupo para unidades organizacionais pais e filhas, as configurações para essas unidades são aplicadas. Se as configurações forem incompatíveis, a unidade organizacional filha conserva sua própria configuração de Diretiva de Grupo. Por exemplo, uma configuração de Diretiva de Grupo para a unidade organizacional aplicada por último ao computador ou ao usuário substitui a que estava causando o conflito de configuração de Diretiva de Grupo em um contêiner, que é de um nível de hierarquia mais alto no Active Directory.

Se a ordem de hierarquia padrão não atender às necessidades da organização, você pode modificar as regras de herança em GPOs específicos. O Windows Server 2003 proporciona as duas opções a seguir para trocar a ordem padrão da herança:

- ***Não Substituir***

  Essa opção é utilizada para impedir que contêineres filhos não sejam priorizados em relação a um GPO com prioridade mais alta de configuração. Essa alternativa é útil para fazer cumprir os GPOs que representam normas de negócios da organização. A opção ***Não Substituir*** é fixada em uma base individual do GPO. Você pode definir essa opção em um ou mais GPOs conforme as necessidades. Quando é definido mais de um GPO em ***Não Substituir***, o GPO mais alto da hierarquia do Active Directory definido em ***Não Substituir*** terá prioridade.

- ***Bloquear herança de diretiva***

  Essa opção é utilizada em contêineres filhos para bloquear a hierarquia de todos os contêineres pai. É útil quando uma unidade organizacional exige uma única configuração de Diretiva de Grupo. ***Bloquear herança de diretiva*** é definida com base no contêiner. Em caso de conflito, a opção ***Não Substituir*** sempre tem prioridade sobre a opção ***Bloquear herança de diretiva***.

## 1.10. Bloqueio de Implementação de GPO

Você pode evitar que um contêiner filho herde GPOs dos contêineres pai, ativando ***Bloquear herança de diretiva*** no contêiner filho. Dessa forma, ele evita que o contêiner herde todas as configurações de Diretiva de Grupos. Isso é útil quando um contêiner do Active Directory exige configurações únicas de Diretiva de Grupo e você deseja garantir que as configurações de diretiva de grupos não sejam herdadas. Por exemplo, é possível utilizar ***Bloquear herança de diretiva*** quando o administrador de uma unidade organizacional precisa controlar todos os GPOs de um determinado contêiner.

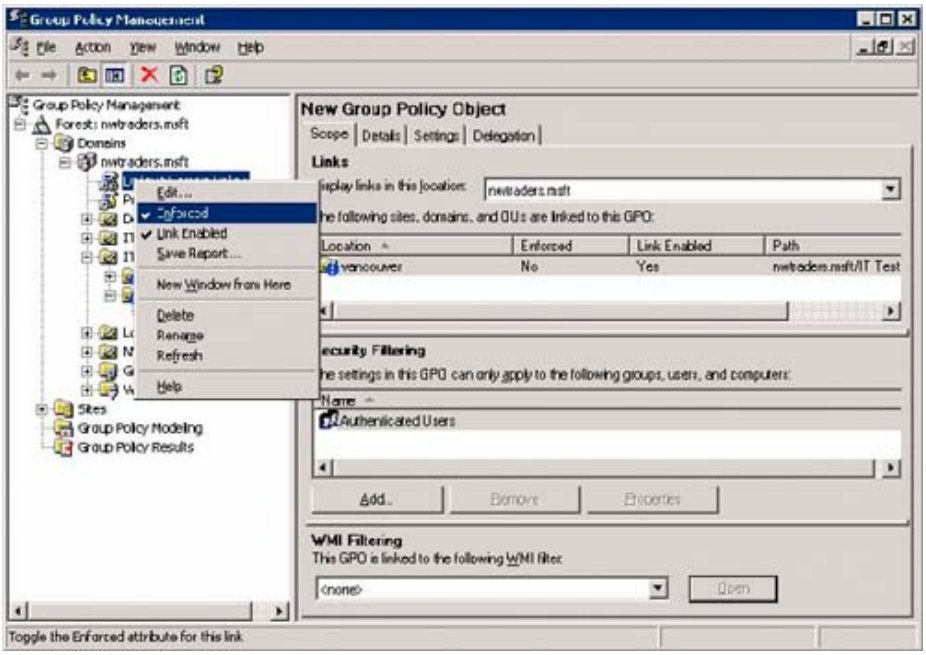

© 2003 Microsoft Corporation. Todos os direitos reservados.

***Ao usar Bloquear herança de diretiva, ele deverá considerar o seguinte:***

- Não é possível escolher seletivamente o que os GPOs bloqueiam. ***Bloquear herança de diretiva*** afeta todos os GPOs de todos os contêineres pai, exceto os GPOs configurados com a opção ***Não Substituir***, sem GPMC instalada e ***Forçado*** com GPMC instalada.

- ***Bloquear herança de diretiva*** não bloqueia a herança de um GPO vinculado a um contêiner pai se o vínculo for configurado com a opção ***Não Substituir***.

## 1.11. Como configurar a Aplicação de Diretiva de Grupo?




**Importante:** Antes de instalar o Group Policy Management Console, a opção ***Forçado (Enforced)*** é chamada Não Substituir em Usuários e Computadores do Active Directory.

***Para configurar a aplicação de link de GPO, é preciso:***

1. No Group Policy Management Console, expanda a floresta contendo o link no qual você deseja configurar a aplicação. Depois siga um dos passos abaixo:

   - ***Para configurar a aplicação do link de GPO a um domínio,*** expanda Domínios e o domínio que contém o link de GPO.

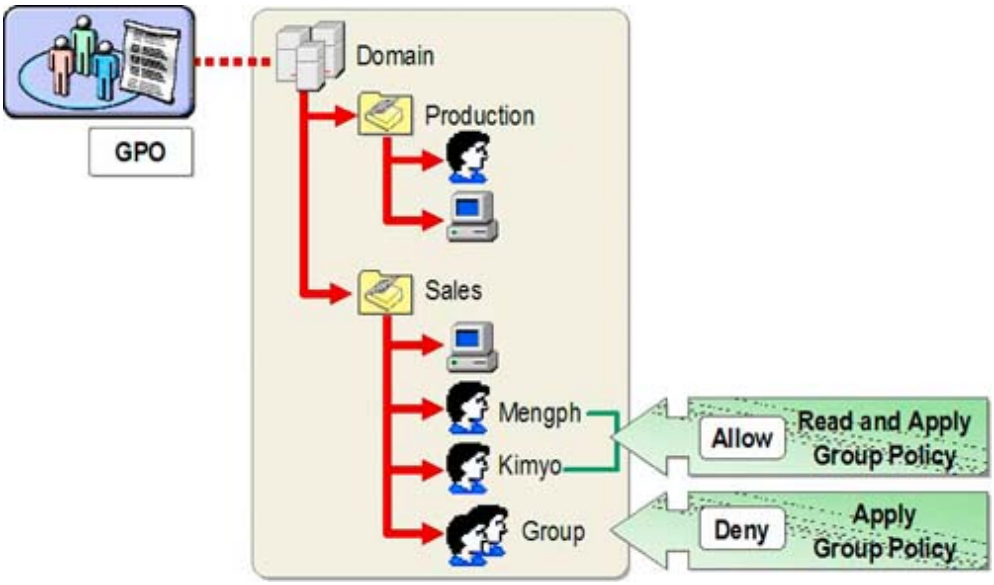
   - ***Para configurar a aplicação do link de GPO a uma unidade organizacional,*** expanda Domínios e o domínio que contém a unidade organizacional. Depois de expandir a unidade organizacional que pode incluir unidade organizacional pai ou filha e que contenha o link de GPO.

   - ***Para configurar a aplicação do link de GPO a um site,*** expanda Sites e depois o site que contém o link de GPO.

2. Clique com o botão direito do mouse no link de GPO e depois clique em ***Forçado*** para ativar ou desativar a aplicação.

## 1.12. Filtro de Implementação de GPO


© 2003 Microsoft Corporation. Todos os direitos reservados.




Por padrão, todas as Configurações de Diretiva de Grupos contidas nos GPOs afetam o contêiner e são aplicadas a usuários e computadores desse contêiner, o que não produz os resultados que você deseja. Usando o recurso de filtro, é possível determinar se as configurações se aplicam aos usuários e aos computadores no contêiner específico.

Você pode filtrar a implementação do GPO definindo permissões no link de GPO para determinar o acesso de leitura ou negar a permissão no GPO. Para que as Configurações de Diretiva de Grupo sejam aplicadas a uma conta de usuário ou de computador, a conta deve ter, pelo menos, permissão de leitura para um GPO. Por padrão, as permissões para um novo GPO têm as seguintes Access Control Entries (ACEs):

- Usuários Autenticados. Permitir leitura e aplicar Diretiva de Grupo
- Admins de Domínio, Adminis da Empresa e SYSTEM. Permitir leitura, Permitir gravação, Permitir criar todos os objetos filhos, Permitir excluir todos os objetos filhos

***Você pode utilizar os seguintes métodos de filtro:***

- ***Negar explicitamente***

Este método é utilizado para negar o acesso à diretiva de grupo Por exemplo, você poderia negar explicitamente a permissão ao grupo de segurança dos administradores, que avisaria os administradores da unidade organizacional sobre a recepção de Configurações de GPO.

- ***Remover usuários autenticados***

Você pode remover os administradores da unidade organizacional do grupo de segurança, o que significa que não há nenhuma permissão explícita para o GPO.

Para mais informações sobre a Diretiva de Grupo:

http://support.microsoft.com/default.aspx?scid=kb;en-us;324753

http://microsoft.com/downloads/details.aspx?FamilyId=D26E88BC-D445-4E8F-AA4E-B9C27061F7CA&displaylang=en

http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windowsserver2003/management/gp/default.asp

## 2. Administração do ambiente de usuário


© 2003 Microsoft Corporation. Todos os direitos reservados.

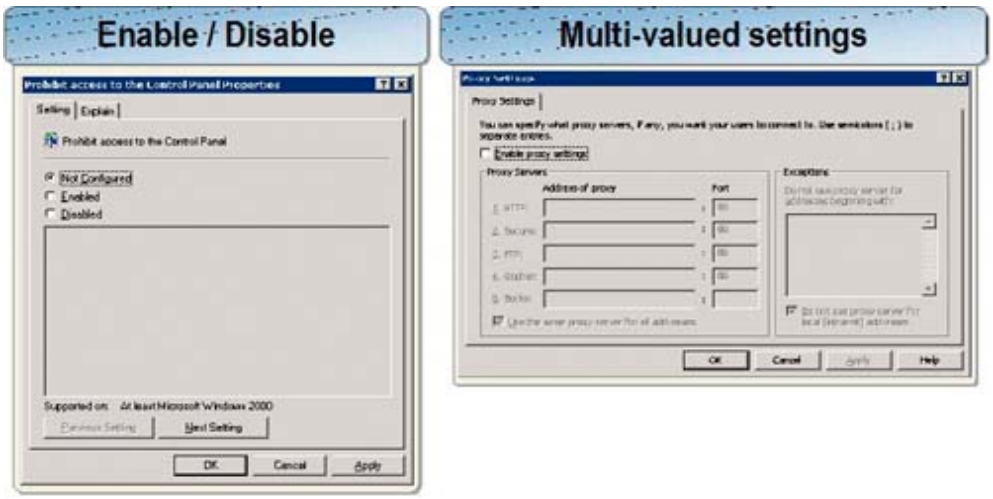
A administração do ambiente de usuário significa controlar o que eles podem fazer quando iniciam a sessão na rede. Isso é feito através da Diretiva de Grupo, controlando os computadores do escritório, as conexões de rede e as interfaces de usuário. Você controla os ambientes de usuário para garantir que eles tenham apenas o acesso necessário para realizarem seus trabalhos. Dessa forma, eles não podem corromper ou configurar incorretamente seus ambientes.

***Quando você configura ou controla ambientes de usuário de forma centralizada, é possível realizar as seguintes tarefas:***

- ***Controlar os usuários e os computadores:*** Isso é possível controlando-se a configuração da área de trabalho do usuário com diretivas baseadas no registro. Dessa forma, você garante que os usuários tenham os mesmos ambientes, mesmo quando iniciam a sessão em computadores diferentes. Assim, você pode controlar como o Microsoft Windows® Server 2003 administra seus perfis de usuário, que especificam a forma como os dados pessoais de um usuário estão disponíveis. Redirecionando pastas de usuário dos discos rígidos locais do usuário para um local central de um servidor, você pode garantir que os dados dos usuários estejam disponíveis para eles, independente do computador onde a sessão foi iniciada.

- ***Implementar software.*** O software é instalado nos computadores ou nos usuários com serviço de diretório Active Directory®. Com a instalação do software, você pode garantir que os usuários tenham seus programas, service packs e hotfixes exibidos.

## 2.1. O que é Ativar ou Desativar as Configurações de Diretiva de Grupo?




Se você desativar uma configuração de diretiva, estará desativando a ação da configuração de diretiva. Por exemplo, os usuários, por padrão, podem ter acesso ao Painel de Controle. Para eles, você não precisa desativar a configuração de diretiva ***Restringir acesso ao Painel de Controle***, a menos que tenha previamente aplicado uma configuração de diretiva ativando-a. Nessa situação, você terá que definir outra configuração de diretiva para desativar a que foi aplicada previamente.

Isso é útil quando configurações de diretiva são herdadas e não se deseja usar filtros para aplicar configurações de diretiva a grupos específicos. Você pode aplicar um GPO que permita uma configuração de diretiva na unidade organizacional pai e outra definição de diretiva que desative o GPO na unidade organizacional filha.

Quando você aceita uma definição de diretiva, está consentindo a ação dessa configuração de diretiva. Por exemplo, para negar a alguém acesso ao Painel de Controle, você pode permitir a configuração de diretiva ***Restringir acesso ao Painel de Controle***.

Um GPO executa valores que modificam o registro dos usuários e dos computadores que estão em conformidade com o GPO. Por padrão, a configuração de uma diretiva é ***Não Configurado***. Se quiser


© 2003 Microsoft Corporation. Todos os direitos reservados.

redefinir uma configuração de diretiva de um computador ou um usuário para o valor predefinido ou para a diretiva local, você deverá selecionar a opção ***Não Configurado***. Por exemplo, você pode permitir uma configuração de diretiva para alguns clientes e, ao usar a opção ***Não Configurado***, a diretiva inverterá a diretiva padrão ou a definição de diretiva local.

Alguns GPOs exigem que sejam fornecidas determinadas informações adicionais depois de permitir o objeto. Algumas vezes, pode ser necessário selecionar um grupo ou um computador se a configuração de diretiva precisar voltar a fornecer ao usuário uma determinada informação. Outras vezes, para permitir configurações proxy, você deverá fornecer o nome ou o endereço IP do servidor proxy e o número da porta. Se a configuração de diretiva tiver múltiplos valores e as configurações estiverem em conflito com outra configuração de diretiva, as configurações com múltiplos valores em conflito são substituídas pela última configuração de diretiva aplicada.

## 2.2. Exercício 4: Como editar Configuração de Diretiva de Grupo?

Como administrador de sistemas, você deve editar as configurações de diretiva de grupo. Utilize o procedimento a seguir para realizar essa tarefa.

1. No Group Policy Management Console, navegue para os ***Group Policy Objects***.
2. Clique com o botão direito do mouse no GPO e depois em ***Edit***.
3. No editor de Objeto de Diretiva de Grupo, pesquise a configuração de Diretiva de Grupo que deseja editar e depois clique duas vezes nela.
4. Na caixa ***Properties***, defina a configuração de Diretiva de Grupo e depois clique em ***OK***.

## 2.3. Quais são os scripts de Configurações de Diretiva de Grupo?

Você pode utilizar os scripts de Diretiva de Grupo para configurar scripts centralizados que sejam executados automaticamente quando o computador é iniciado e desligado, e também quando os usuários iniciam e fecham uma sessão. Você pode especificar qualquer script que execute o Windows Server 2003, incluindo arquivos em lote, programas executáveis e scripts suportados pelo Windows Script Host (WSH).

***Para ajudar o usuário a controlar e configurar seus ambientes, é preciso:***

- Executar os scripts que realizam as tarefas que você não pode realizar com outras configurações de Diretiva de Grupos. Por exemplo, configurar o ambiente de usuário com conexões de rede, conexões de impressora, atalhos para aplicativos e documentos corporativos.

- Limpar as áreas de trabalho quando os usuários fecham a sessão e desligam o computador. Você pode remover as conexões adicionadas aos scripts de logon ou inicialização, para que o computador permaneça no mesmo estado de quando o usuário o ligou.

- Executar scripts pré-existentes, definidos para controlar os ambientes de usuário até que eles sejam configurados com outras Diretivas de Grupo que substituam esses scripts.

**Nota:** Com o Active Directory Users and Computers, você pode atribuir scripts de login individualmente para as contas de usuário na caixa ***Propriedades*** de cada uma. Por isso, a Diretiva de Grupo é o melhor método para executar scripts porque é possível controlar esses scripts centralizados junto com os scripts de inicialização e logoff.

Para mais informações sobre os scripts, veja TechNet Script Center em:

http://www.microsoft.com/technet/treeview/default.asp?url=/technet/scriptcenter/default.asp

## 2.4. Exercício 5: Como atribuir scripts com Diretiva de Grupo?


© 2003 Microsoft Corporation. Todos os direitos reservados.

Para implementar o script, você utiliza a Diretiva de Grupo e o adiciona à configuração apropriada em um modelo de Diretiva de Grupos. Isso indica que o script pode ser executado na inicialização, desligamento, logon ou logoff.

***Para adicionar um script ao GPO, é preciso:***

1. No Group Policy Management Console, edite o GPO.
2. No editor de Objeto de Diretiva de Grupo do console, procure User Configuration/Windows Settings/Scripts (Logon/Logoff).
3. No painel de detalhes, clique duas vezes em ***Logon***.
4. Na caixa ***Logon Properties***, clique em ***Add***.
5. Na caixa ***Add a Script***, defina todas as configurações seguintes que quiser utilizar. Depois, clique em ***OK.***
   - ***Script Name.*** Insira o caminho do script ou clique em ***Browse*** para localizar o arquivo de script na pasta compartilhada Netlogon do Controlador de Domínio.
   - ***Script Parameters.*** Insira os parâmetros que quiser utilizar, da mesma forma que os inseriria na linha de comando.
6. Na caixa ***Logon Properties***, defina todas as configurações a seguir que você queira utilizar.
   - ***Logon Scripts for.*** Esta lista enumera todos os scripts que estão atribuídos atualmente ao GPO selecionado. Se forem atribuídos múltiplos scripts, eles serão processados na ordem especificada. Para mover o script na lista, clique no script e depois em ***Up*** ou ***Down***.

## 2.5. O que é o Redirecionamento de Pastas?

Quando você redireciona pastas, modifica a localização das pastas do disco rígido local do computador do usuário, a uma pasta compartilhada em um servidor da rede. Depois de redirecionar uma pasta a um servidor, ela continuará aparecendo como local para o usuário. O perfil de usuário é formado por quatro pastas de perfil de usuário e que podem ser redirecionadas: Meus Documentos, Dados de Aplicativos, Desktop e Menu Iniciar.

***Armazenando dados na rede, o benefício para os usuários está na disponibilidade crescente e os backup freqüentes de seus dados. O redirecionamento de pastas oferece os seguintes benefícios:***

- Os dados nas pastas estão disponíveis para o usuário; independente do computador cliente onde o usuário inicia a sessão.
- Os dados nas pastas estão armazenados em pontos centrais e, por isso, é mais fácil administrá-los e fazer backup de segurança.
- Os arquivos dentro das pastas redirecionadas, como os arquivos de um perfil de usuário móvel, não são copiados e não são salvos no computador do usuário que inicia a sessão. Isso significa que quando o usuário inicia a sessão no computador cliente, não é utilizado espaço de armazenamento para esses arquivos e os dados, que podem ser confidenciais, nesse computador.
- Os dados são armazenados em uma pasta compartilhada da rede que pode ser parte das áreas de rotinas de backup. Isso é mais seguro porque não exige nenhuma ação por parte do usuário.
- Como administrador, você pode utilizar a Diretiva de Grupo para configurar cotas de disco, limitando a quantidade de espaço ocupado pelos usuários.


© 2003 Microsoft Corporation. Todos os direitos reservados.

## 2.6. Pastas que podem ser redirecionadas

Você pode redirecionar as pastas Meus Documentos, Dados de Aplicativos, Desktop e Menu Iniciar. Uma organização deve redirecionar essas pastas para preservar dados e configurações importantes do usuário. Existem várias vantagens do redirecionamento de cada uma dessas pastas, que variam conforme as necessidades da organização.

***Você pode utilizar o redirecionamento para qualquer das seguintes pastas no perfil de usuário:***

***Meus Documentos***
O redirecionamento de Meus Documentos é particularmente vantajoso porque a pasta tende a realizá-lo a longo prazo.
A tecnologia de Arquivos Offline permite que os usuários tenham acesso a Meus Documentos, mesmo quando não estão conectados à rede. Isso é particularmente útil para quem utiliza computadores portáteis.

***Dados de aplicativos***
As configurações de Diretiva de Grupos controlam o comportamento dos Dados de Aplicativos quando o cache do cliente está ativado. Essa configuração sincroniza os dados de aplicativos centralizados em um servidor da rede com o computador local. Conseqüentemente, o usuário pode trabalhar on-line ou offline. Se forem realizadas modificações de dados de aplicativos, a sincronização atualiza os dados do aplicativo sobre o cliente e o servidor.

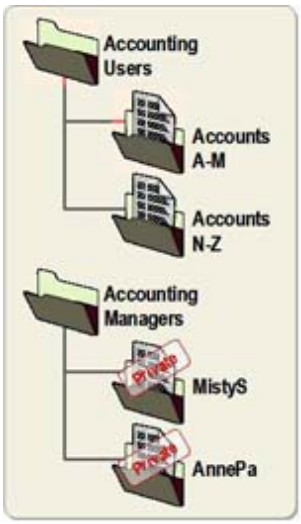
***Desktop***
Você pode redirecionar a área de trabalho e todos os arquivos, atalhos e pastas a um servidor centralizado.

***Menu Iniciar***
Quando o menu Iniciar é redirecionado, suas subpastas também são redirecionadas.

## 2.7. Configurações necessárias para definir o Redirecionamento de Pasta

Existem 3 configurações disponíveis para Redirecionamento de Pasta: nenhum, básico e avançado. O Redirecionamento de Pasta Básico é para usuários que devem redirecionar suas pastas a uma área comum ou para os usuários que precisam manter a privacidade de seus dados.

***Você tem as seguintes opções básicas para Redirecionamento de Pastas:***




- ***Redirecione as pastas para um local***
  Todos os usuários redirecionam suas pastas a uma área comum onde é possível ver ou utilizar outros dados em pastas redirecionadas. Para fazer isso, escolha a configuração ***Básico*** e configure ***Redirecionar pastas para o seguinte local.*** É aconselhável utilizar essa opção para todas as pastas que contenham dados que não são privados.

- ***Crie uma pasta para cada usuário no caminho raiz***
  Para os usuários que precisam que suas pastas sejam redirecionadas com dados privados, escolha a configuração ***Básico*** e configure ***Criar uma pasta para cada usuário no caminho raiz.*** É aconselhável utilizar essa opção para os usuários que precisam manter seus dados privados, como gerentes que guardam dados pessoais sobre funcionários.

Quando você seleciona ***Avançado – Especifica os locais dos vários grupos de usuários***, as pastas são redirecionadas a locais diferentes, baseadas em grupos de segurança dos usuários.


© 2003 Microsoft Corporation. Todos os direitos reservados.

***As opções avançadas para Redirecionamento de Pasta são as seguintes:***

***Selecionar um grupo.*** Especifique aqui para quem aplicar o redirecionamento.
***Caminho.*** Aqui é possível escolher uma das opções a seguir:

- ***Criar uma pasta para cada usuário no caminho raiz.*** Utilize para dados confidenciais.
- ***Redirecionar para o seguinte local.*** Utilize para dados compartilhados.
- ***Redirecionar para o seguinte local.*** Para usuários que utilizam uma combinação de computadores clientes que não são parte do Active Directory por um lado e por outro sim.

***Caminho.*** Nessa caixa, especifique o servidor e o nome da pasta compartilhada para a qual deseja redirecionar.

## 2.8. Exercício 6: Como configurar Redirecionamento de Pasta?

Você configura Redirecionamento de Pasta usando o editor do Objeto de Diretiva de Grupos.

***Para configurar Redirecionamento de Pasta, é preciso:***

1. No Group Policy Management, edite ou crie o GPO.
2. No editor de Objeto de Diretiva de Grupo do console, expanda ***Configuração do usuário***, expanda ***Configurações do Windows*** e depois ***Redirecionamento de Pasta***. Os ícones para as quatro pastas que podem ser redirecionadas são exibidos.
3. Clique com o botão direito do mouse na pasta que deseja redirecionar e depois clique em ***Propriedades***.
4. Na caixa ***Propriedades***, na guia ***Geral***, clique em uma das seguintes opções:
   - ***Básico – Redirecionar pastas de todos os usuários para o mesmo local.***
   Todas as pastas afetadas por esse GPO são armazenadas na mesma pasta compartilhada da rede.
   - ***Avançado – Especifica os locais de vários grupos de usuários.***
   As pastas são redirecionadas para outras partições da rede e baseadas nos membros de grupos de segurança. Por exemplo, as pastas pertencentes aos usuários do grupo de contabilidade são redirecionados ao servidor de contabilidade e
   as pastas que pertencem aos usuários no grupo de comercialização se redirecionam ao servidor de comercialização.
5. Na caixa ***Propriedades***, clique em ***Adicionar***.
6. Em ***Local da pasta de destino***, na caixa ***Caminho da raiz***, insira o nome da pasta compartilhada na rede e clique em ***Procurar*** para localizá-la.
7. Na guia ***Configurações***, configure as opções que você queria utilizar e depois clique em ***OK***.

## 2.9. *O que é o Gpupdate?*

```
gpupdate [/Target:{Computer | User}] [/Force]
[/Wait:Value] [/Logoff] [/Boot] [/Sync]
```

***Gpupdate*** é uma ferramenta de linha de comando que atualiza as configurações de Diretiva de Grupo locais e configurações de Diretiva de Grupo armazenadas no Active Directory, incluindo as configurações de segurança. Por padrão, as configurações de segurança são atualizadas a cada 90 minutos em uma estação de trabalho ou um servidor, e a cada 5 minutos em um Controlador de Domínio. Você pode executar gpupdate para testar uma configuração de Diretiva de Grupo ou aplicá-la diretamente.


© 2003 Microsoft Corporation. Todos os direitos reservados.

***Os exemplos a seguir demonstram como você pode utilizar o comando gpupdate:***

```
C:\gpupdate
C:\gpupdate /target:computer
C:\gpupdate /force /wait:100
C:\gpupdate /boot
```

**Gpupdate tem os parâmetros a seguir.**

- ***/Target:{Computador | Usuário}*** Especifica a atualização somente de usuários ou computadores para suas configurações de diretiva. Por padrão, a diretiva de usuário e computador é atualizada.

- ***/Force*** Replica todas as configurações de diretiva. Por padrão, somente as configurações de diretiva que foram modificadas são replicadas.

- ***/Wait:{Valor}*** Defina o número de segundos a aguardar o processamento da diretiva. O padrão é 600 segundos. O valor ' 0 ' indica que não há espera. O valor ' -1 ' indica uma espera indefinidamente.

- ***/Logoff*** Faz logoff depois de atualizar a configuração de definições de Diretiva de Grupos.

- ***/Boot*** Faz com que o computador seja reiniciado depois da atualização das configurações de Diretiva do Grupo.

- ***/Sync*** Faz como que a próxima configuração de definição de diretiva seja aplicada de forma síncrona.

## 2.10. *O que é o Gpresult?*

```
gpresult [/s Computer [/u Domain\User /p Password]]
[/user TargetUserName] [/scope {user|computer}] [/v]
[/z]
```

Como você pode aplicar níveis sobrepostos das configurações de diretivas a qualquer computador ou usuário, a Diretiva de Grupo gera um relatório da aplicação das diretivas no logon. ***Gpresult*** exibe o relatório da aplicação da diretiva no computador para o usuário especificado no logon.

O comando ***gpresult*** exibe as configurações de Diretiva de Grupo e o Conjunto de Diretivas Resultante (RSoP) para um usuário ou um computador. Você pode utilizar ***gpresult*** para verificar se as configurações de GPO estão em vigor e localizar problemas no aplicativo.

***Os exemplos a seguir demonstram como você pode utilizar o comando gpresult:***

```
C:\gpresult /user targetusername /scope computer
C:\gpresult /s srvmain /u maindom/hiropln /p p@ssW23 /user targetusername /scope USER
C:\gpresult /s srvmain /u maindom/hiropln /p p@ssW23 /user targetusername /z >policy.txt
C:\gpresult /s srvmain /u maindom/hiropln /p p@ssW23
```

**Gpresult tem os seguintes parâmetros.**

- ***/s Computador*** Especifica o nome ou o endereço IP de um computador remoto. Por padrão, é o computador local.

- ***/u Domínio/Usuário*** O comando funciona com as permissões da conta de usuário específicas de Usuário ou Domínio/Usuário. O padrão é utilizar as permissões de usuário que foram autenticadas no computador e que executam o comando.

- ***/p Senha*** Especifica a senha da conta de usuário que é especificada no parâmetro /u.


© 2003 Microsoft Corporation. Todos os direitos reservados.

- ***/usuário TargetUserName*** Especifica o nome de usuário de quem são exibidos os dados RSoP.

- ***/scope {usuário|computador}*** Exibe as configurações de diretiva de usuário ou computador. Os valores válidos para o parâmetro /scope são usuário ou computador. Se não for incluído o parâmetro /scope, o gpresult exibe usuário e computador.

- ***/v*** Especifica que a saída exibirá informações detalhadas da diretiva.

- ***/v*** Especifica que a saída exibirá todas as informações disponíveis sobre a Diretiva de Grupo. Como esse parâmetro gera mais informações que o parâmetro /v, é preciso redirecionar a saída para um arquivo de texto quando esse parâmetro é utilizado (por exemplo, s pode ser gravado em ***gpresult /z >policy.txt***).

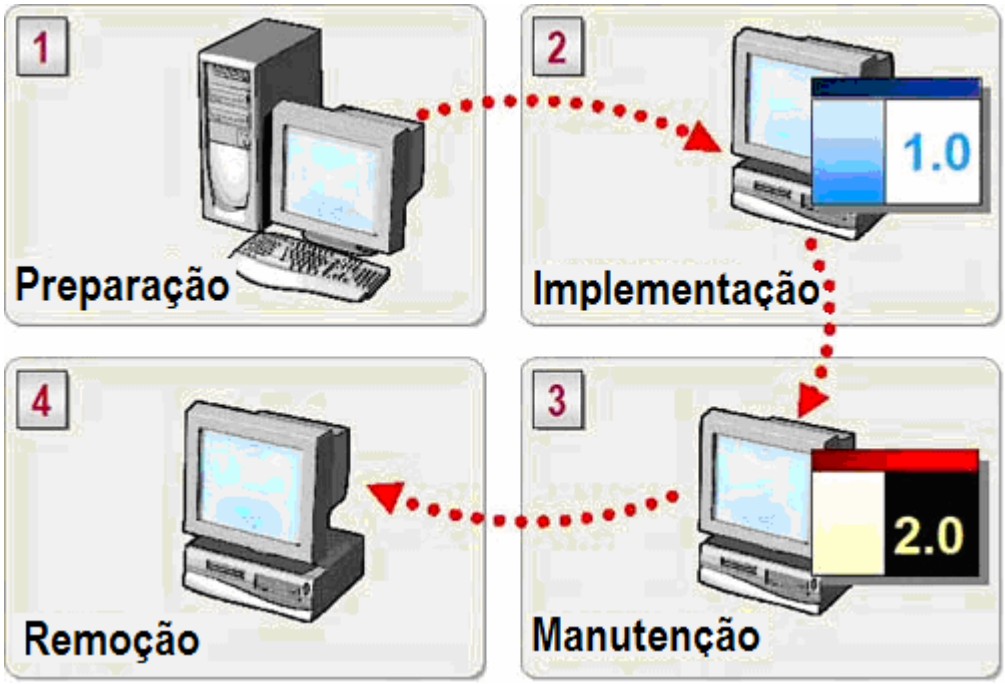
- ***/?*** Exibe a ajuda na janela de comandos.


© 2003 Microsoft Corporation. Todos os direitos reservados.

## 3. Administração de instalação do software

O Microsoft® Windows® Server 2003 inclui uma característica chamada instalação e manutenção de software que utiliza o serviço do Active Directory®, Diretiva de Grupo e Microsoft Windows Installer para instalar, manter e desligar software nos computadores da sua organização. Usando o método de administração e instalação de software baseado em diretivas, é possível garantir que os programas de que os usuários precisam para realizar seus trabalhos estejam disponíveis sempre e onde necessário.

### 3.1. A instalação do Software e o processo de manutenção




No Windows Server 2003, você pode utilizar a Diretiva de Grupo para controlar o processo de instalação do software centralizado a partir de uma localização. Além disso, as configurações de Diretiva de Grupo podem ser aplicadas aos usuários ou computadores em um site, domínio ou unidade organizacional para instalar, atualizar ou remover automaticamente o software. Aplicando as configurações de Diretiva de Grupo no software, você pode controlar várias fases de instalação do software sem instalar software em cada computador individualmente.

***A lista a seguir descreve cada fase da instalação do software e o seu processo de manutenção:***

1. ***Preparação.*** Primeiro, é preciso instalar o software usando a estrutura atual do Objeto de Diretiva de Grupo (GPO), e também identificar os riscos de usar a infra-estrutura atual para instalar o software. Para preparar arquivos que permitam que um programa seja instalado com a Diretiva de Grupo, você deve copiar os arquivos do pacote do Windows Installer em um programa de um ponto de distribuição de software, que pode ser uma pasta compartilhada em um servidor. Da mesma forma, é possível adquirir o arquivo do pacote do Windows Installer do fornecedor do programa ou criar o pacote de arquivo usando um utilitário de terceiros.
2. ***Implementação*****.** Nesse caso, é preciso criar um GPO que instale o software em um computador e vinculá-lo a um contêiner apropriado do Active Directory. O software estará instalado quando o computador for ligado ou quando o usuário iniciar o programa.
3. ***Manutenção*** O software é atualizado com uma nova versão ou reinstalando o software com um service pack ou uma atualização de software. Dessa forma, o software será automaticamente atualizado ou reinstalado quando o computador for ligado ou quando o usuário iniciar o programa.


© 2003 Microsoft Corporation. Todos os direitos reservados.

4. ***Remoção.*** Para eliminar programas de software que não sejam necessários, é preciso remover a configuração de pacote de software do GPO que instalou o software originalmente. O software será automaticamente removido quando o computador for ligado ou quando um usuário iniciar a sessão.

## 3.2. O que é o Windows Installer?

Para ativar a Diretiva de Grupo para instalação e administração de software, o Windows Server 2003 usa o Windows Installer. Este componente automatiza a instalação e a remoção de programas, aplicando um sistema de regras definidas de forma centralizada durante o processo de instalação.

***O Windows Installer possui dois componentes:***

***Serviço do Windows Installer*** Este serviço no cliente automatiza completamente a instalação do software e o processo de configuração. O serviço Windows Installer também pode modificar ou reparar um programa instalado existente. Um programa pode ser instalado diretamente do CD-ROM ou usando a Diretiva de Grupo. Para isso, o serviço do Windows Installer exige um pacote do Windows Installer.

***Pacote do Windows Installer*** Esse pacote de arquivo contém todas as informações que o serviço do Windows Installer exige para instalar ou remover o software. O arquivo contém:

- Um arquivo do Windows Installer com uma extensão .msi.
- Arquivos fonte externos, necessários para instalar ou remover o software.
- Informações padrão sobre o software e o pacote.
- Arquivos do produto ou uma referência a um ponto de instalação onde residem os arquivos do produto.

***As vantagens de usar a tecnologia do Windows Installer são:***

***Instalações personalizadas.*** Recursos opcionais de um aplicativo. Por exemplo, clipart ou dicionário, pode ser visualizado em um programa sem que o recurso seja instalado. Embora os comandos de menu estejam acessíveis, o recurso não é instalado até que o usuário acesse o menu de comandos. Este método de instalação ajuda a reduzir a complexidade e a quantidade de espaço de disco rígido que o programa utiliza.

***Aplicativos flexíveis.*** Se um arquivo crítico for excluído ou corrompido, o programa automaticamente obtém uma nova cópia do arquivo da fonte de instalação, sem exigir a intervenção do usuário.

***Remoção de limpeza.*** O Windows Installer remove aplicativos sem deixar arquivos órfãos ou inadvertidamente danificar outro aplicativo, por exemplo, quando um usuário apaga um arquivo compartilhado necessário para outro aplicativo. O Windows Installer remove todas as configurações de registro relacionadas e armazena as transações de instalação em um banco de dados e arquivos de registro subseqüentes.


© 2003 Microsoft Corporation. Todos os direitos reservados.

### 3.3. Descrição do processo de Implementação de Software

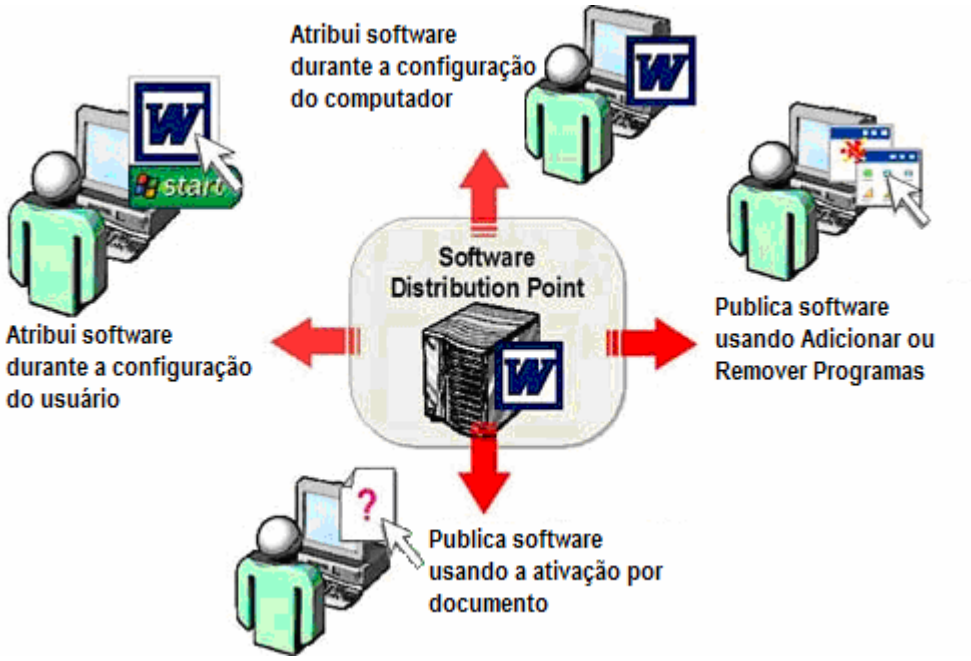
Quando você instala o software, está especificando como os aplicativos são instalados e mantidos na sua organização.

***Para instalar um novo software, utilizando a Diretiva de Grupo, é preciso:***

1. ***Criar um ponto de distribuição de software*****.** Esta pasta compartilhada no seu servidor contém o pacote e os arquivos do software para instalá-la. Quando o software é instalado em um computador local, o Windows Installer copia arquivos no computador.
2. ***Utilizar o GPO para instalar software.*** Você deve criar ou realizar as modificações necessárias no GPO para o contêiner onde é preciso instalar o aplicativo. Ao mesmo tempo, é preciso configurar o GPO para instalar software para a conta de usuário ou de computador. Esta tarefa também inclui selecionar o tipo de instalação necessário.
3. ***Modificar os recursos da instalação do software.*** Dependendo das suas necessidades, você pode modificar as características que foram definidas durante a instalação inicial do software.

### 3.4. Atribuir Software vs. Publicar Software


© 2003 Microsoft Corporation. Todos os direitos reservados.




**Os dois tipos de instalação são:** atribuir e publicar software

Usando a atribuição de software, você garante que o software esteja sempre disponível para o usuário. Quando ele inicia a sessão, os atalhos do menu ***Iniciar*** e os ícones da área de trabalho do aplicativo são exibidos. Por exemplo, se o usuário abrir um arquivo que utilize o Microsoft Excel em um computador que não tenha Excel, mas o Excel tiver sido atribuído ao usuário, o Windows Installer instala o Excel no computador quando abre o arquivo. Além disso, a atribuição de software o torna flexível. Se, por qualquer motivo, o usuário remover o software, ele será reinstalado pelo Windows Installer na próxima vez em que o usuário iniciar a sessão e iniciar o aplicativo.

Usando a publicação de software, você garante que o software esteja disponível para que os usuários o instalem em seus computadores. O Windows Installer não adiciona atalhos na área de trabalho do usuário ou no menu ***Iniciar*** e não insere entradas no registro local. Como os usuários precisam instalar o software publicado, você pode publicar software somente para os usuários e não para os computadores.

***Você pode atribuir e publicar software usando um dos métodos da tabela a seguir:***

| Método de instalação | Método 1 | Método 2 |
|---|---|---|
| Atribuição | Configurando o usuário. Quando um software é atribuído a um usuário, ele é exibido na sua área de trabalho sempre que ele inicia uma sessão. A instalação não terá início até que o usuário clique duas vezes no início do aplicativo ou em um arquivo associado ao aplicativo. Esse é um método chamado de ativação por documento. Se o usuário não ativar o aplicativo, o software não é instalado. Dessa forma, economiza-se espaço no disco rígido e tempo. | Configurando o computador. Quando você atribui software a um computador, não é exibido nenhum aviso. No entanto, o software é instalado automaticamente quando o computador é ligado. Atribuindo software a um computador, você garante que determinados aplicativos estejam sempre disponíveis nesse computador, independente de quem o utiliza. Você não pode atribuir software a um computador que seja controlador de domínio. |


© 2003 Microsoft Corporation. Todos os direitos reservados.

| | | |
|---|---|---|
| Publicação | Usando Adicionar ou Remover Programas. Um usuário pode abrir o Painel de Controle e clicar duas vezes em Adicionar ou Remover Programas para exibir os aplicativos disponíveis. O usuário pode selecionar um aplicativo e depois clicar em Adicionar. | Usando a ativação por documentos. Se você publicar um aplicativo no Active Directory, as extensões de nome de arquivo dos documentos suportados pelo aplicativo serão associadas no diretório. |

## 3.5. Exercício 7: Como utilizar um GPO para instalar software?

Depois de criar um ponto de distribuição de software, você deverá criar um GPO que instale esses aplicativos, e depois vincular o GPO ao contêiner que contenha os usuários ou computadores onde deseja instalar o software.

**Importante:** Não atribua ou publique um pacote do Windows Installer mais de uma vez no mesmo GPO. Por exemplo, se atribuir o Microsoft Office XP a computadores que sejam afetados por um GPO, você não deverá atribuir ou publicar nos usuários afetados por esse mesmo GPO.

***Para utilizar um GPO para instalar software, você deverá seguir os passos abaixo:***

1. Crie ou edite o GPO.
2. Em ***Configuração do usuário*** ou ***Configuração do computador*** (dependendo de você estar atribuindo o software aos usuários ou aos computadores ou publicando-os para os usuários), expanda ***Configurações de Software***, clique com o botão direito do mouse em ***Instalação de Software***, selecione ***Novo*** e depois clique em ***Pacote***.
3. Na caixa ***Abrir arquivo***, procure o ponto de distribuição de software usando o nome Universal Naming Convention (UNC). Por exemplo, **\\NomeServidor\NomeCompartilhado**, selecione o arquivo do pacote e depois clique em ***Abrir***.
4. Na caixa ***Implantar software***, selecione o método de instalação e depois clique em ***OK***.

## 3.6. Exercício 8: Como modificar as opções para instalação de Software?

Um GPO pode conter várias configurações que afetam como um aplicativo é instalado, controlado e removido. Você pode definir as configurações padrão para os novos pacotes de GPO e também modificar algumas dessas configurações futuramente, editando as propriedades do pacote durante a instalação do software. Depois de instalar um pacote de software, você poderá modificar as características da instalação que foram definidas durante a instalação inicial do software. Por exemplo, você pode impedir que os usuários instalem o pacote de software usando a ativação do documento.

***Para configurar as opções implícitas para a instalação do software, é preciso executar os seguintes passos:***

1. Criar ou editar o GPO.
2. Em ***Configuração do usuário*** ou ***Configuração do computador***, expandir ***Configurações de Software***, clicar com o botão direito do mouse em ***Instalação de Software*** e depois em ***Propriedades***.
3. Na guia ***Geral***, configure as seguintes opções de instalação de software:

   - ***Local padrão do pacote***
   - ***Ao adicionar novos pacotes às configurações de usuário***
   - ***Opções de interface do usuário da instalação***

4. Na guia ***Avançado***, selecione a opção ***Desinstalar o aplicativo quando eles ficarem fora do escopo de gerenciamento***.

***Para modificar os recursos da instalação de software, é preciso:***

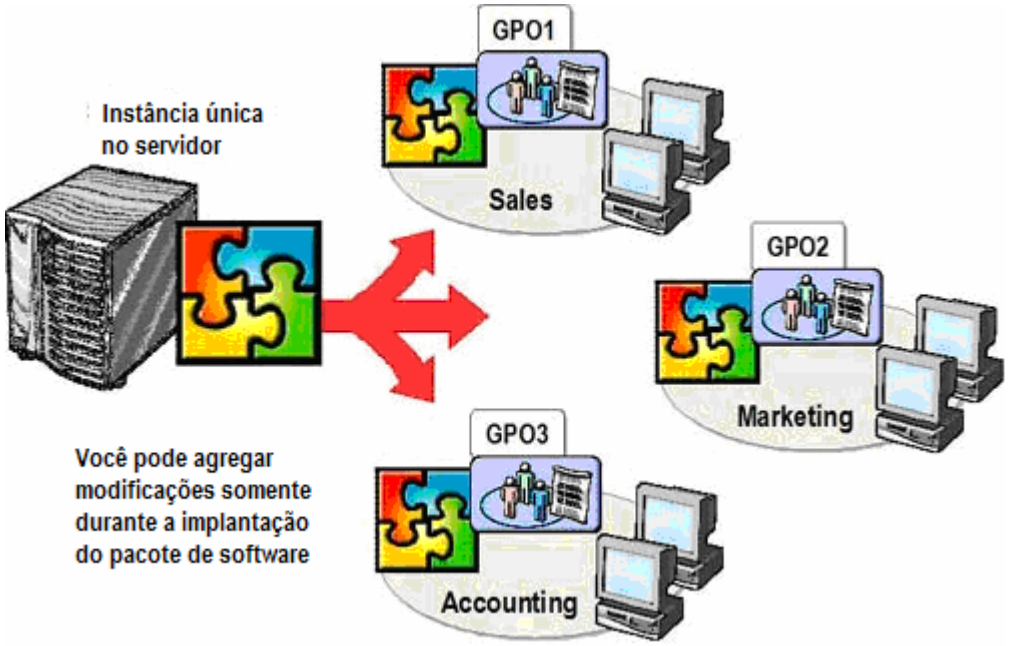

© 2003 Microsoft Corporation. Todos os direitos reservados.

1. Na Instalação do Software, clique com o botão direito do mouse no pacote instalado e depois clique em ***Propriedades***.
2. Na caixa ***Propriedades*** da guia ***Implantação***, modifique as seguintes opções:

- ***Tipo de implantação***
- ***Opções de implantação***
- ***Opções da interface do usuário da instalação***


© 2003 Microsoft Corporation. Todos os direitos reservados.

### 3.7. Qual é a modificação do software?




As modificações são associadas a um pacote do Windows Installer na instalação anterior que utilize esse pacote do Windows Installer para instalar ou modificar o aplicativo.

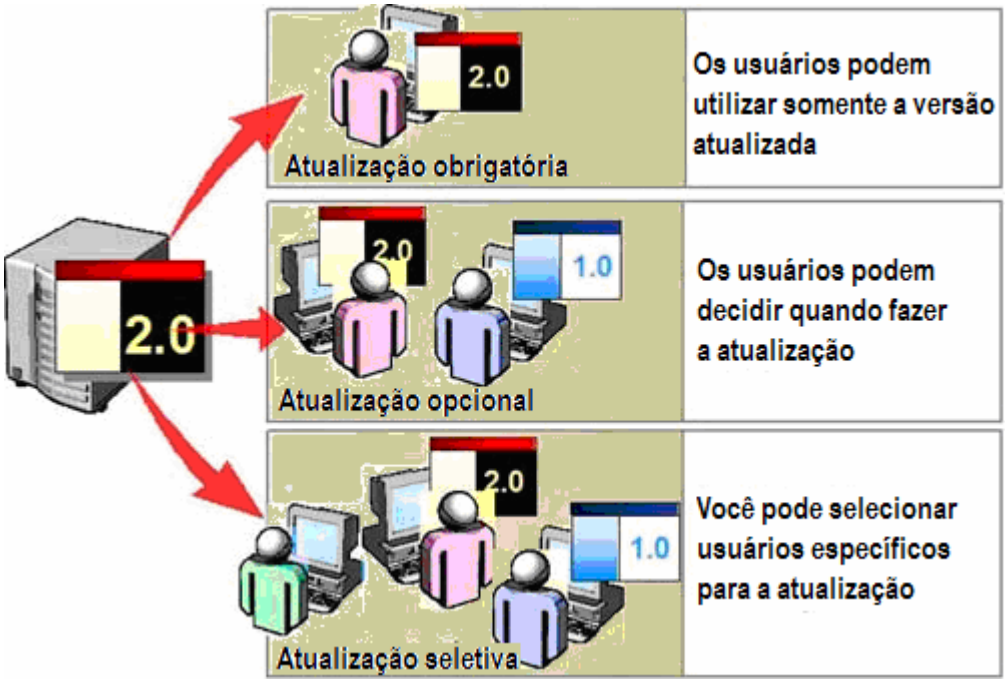
Instalar várias configurações de um aplicativo permite que vários grupos da sua organização utilizem um pacote de software de várias formas diferentes. Você pode utilizar modificações de software ou arquivos ***.mst*** (também chamado de ***arquivos de transformação***) para instalar várias configurações de um aplicativo. Um arquivo .mst é um pacote de software personalizado que modifica como o Windows Installer instala o pacote ***.msi*** associado.

O Windows Installer aplica modificações nos pacotes conforme as suas especificações. Para salvar modificações em um arquivo .mst, é preciso executar o assistente de instalação personalizada e escolher o arquivo .msi no qual basear a transformação. Você deverá determinar em que ordem aplicar as transformações aos arquivos antes de atribuir ou publicar o aplicativo.

**Exemplo:** Uma empresa de grande porte, por exemplo, pode querer instalar o Microsoft Office XP, mas as necessidades do Office de cada departamento variam significativamente na organização. Em vez de configurar manualmente cada um dos departamentos, você pode utilizar GPOs e arquivos .mst diferentes combinados com os arquivos .msi padrão, para que cada departamento instale várias configurações do Office XP. Nesse exemplo, você pode executar o assistente de instalações personalizadas do Office XP do Office Resource Kit para criar o arquivo de transformação.


© 2003 Microsoft Corporation. Todos os direitos reservados.

### 3.8. Tipos de atualização do Software




As tarefas em uma organização são dinâmicas e variadas. Você pode utilizar a Diretiva de Grupo para instalar e administrar atualizações de software que atendam às necessidades de cada departamento na sua organização. As atualizações normalmente envolvem mudanças importantes no software e têm novos números de versão. Em geral, um número substancial de arquivos é modificado em uma atualização.

***Vários acontecimentos no ciclo de vida do aplicativo podem desencadear a necessidade de uma atualização, incluindo o seguinte:***

- Uma nova versão do software é lançada e contém recursos novos e aprimorados.
- Patches de segurança ou aprimoramentos de funções foram implementados no software desde o último lançamento.
- A organização decide utilizar um software de diversos fornecedores

***Existem três tipos de atualizações:***

***Atualizações obrigatórias.*** Essas atualizações substituem automaticamente uma versão antiga do software pela nova versão. Por exemplo, se os usuários utilizam atualmente a versão do programa 1.0, eles removem essa versão e a versão do programa 2.0 é instalada na próxima vez em que o computador é ligado ou o usuário inicia a sessão.

***Atualizações opcionais.*** Essas atualizações permitem que os usuários decidam quando atualizar para a nova versão. Por exemplo, os usuários podem determinar se desejam atualizar para a versão 2.0 do software ou continuar usando a versão 1.0.

***Atualizações seletivas.*** Se alguns usuários precisarem de uma atualização e outros não, você pode criar múltiplos GPOs para que sejam aplicados aos usuários que exigem a atualização e criar pacotes de software apropriados a eles.


© 2003 Microsoft Corporation. Todos os direitos reservados.

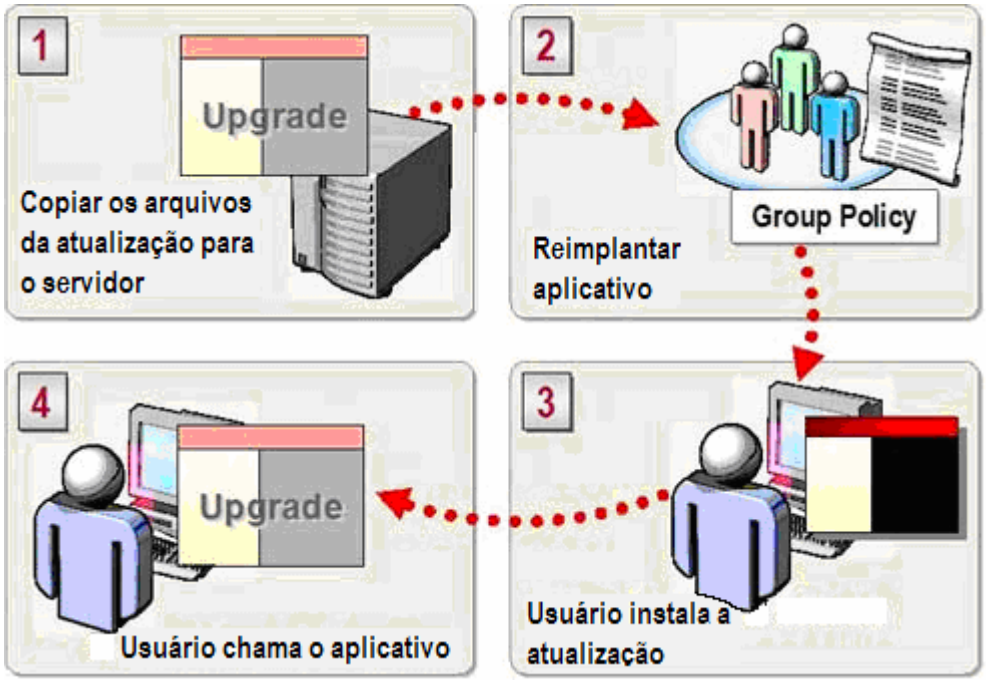
### 3.9. Exercício 9: Como atualizar o Software instalado?

Você utiliza a instalação de software para estabelecer o procedimento de atualização de software para a versão atual.

***Para instalar uma atualização:***

1. Instale a versão seguinte do software.
2. Abra Instalação de software, clique com o botão direito do mouse na nova versão e depois clique em ***Propriedades***.
3. Na caixa ***Propriedades*** na guia ***Atualizações***, na seção ***Pacotes que este pacote vai atualizar***, clique em ***Adicionar*** e depois selecione a versão anterior (atual) do software. Você pode atualizar um aplicativo usando o GPO atual ou selecionando um GPO específico. Se as duas versões do programa tiverem um Pacote do Windows Installer nativo, esse passo será realizado automaticamente.
4. Clique em ***Atualizar o pacote sobre o existente*** ou ***Desinstalar o pacote existente e instalar o pacote de atualização*** e depois clique em ***OK***.
5. Selecione o tipo de atualização:
   - Para realizar uma atualização obrigatória, selecione a caixa ***Atualização necessária para pacotes existentes*** e depois clique em ***OK***.
   - Para realizar uma atualização opcional, limpe a caixa ***Atualização necessária para pacotes existentes*** e depois clique em ***OK***.

### 3.10. Como funciona a reinstalação de software?




***Reimplantação*** é a aplicação de service packs e atualizações de software ao software instalado. Você pode instalar um pacote instalado forçando a reinstalação do software. A reinstalação pode ser necessária se o pacote de software instalado previamente tiver sido atualizado, mas continuar na mesma versão, ou se houver algum problema de interoperabilidade ou vírus que a reinstalação do software possa corrigir.

Quando você marca um pacote de arquivos para reinstalação, o software é anunciado em todos os que têm acesso ao aplicativo, seja através de atribuição ou publicação. Sendo assim, dependendo de como o pacote original tenha sido instalado, um desses 3 cenários ocorrerá:


© 2003 Microsoft Corporation. Todos os direitos reservados.

- Quando você atribui software a um usuário, o menu ***Iniciar***, os atalhos da área de trabalho e a configuração de registro serão relevantes ao software e atualizados na próxima vez em que o usuário iniciar a sessão. Na próxima vez em que o usuário iniciar o software, o service pack ou a atualização de software serão aplicados automaticamente.

- Quando você atribui o software a um computador, o service pack ou a atualização de software é aplicado automaticamente na próxima vez em que o computador é ligado.

- Quando você publica e instala o software, o menu ***Iniciar***, os atalhos da área de trabalho e a configuração de registro refletirão o software e serão atualizados da próxima vez em que o usuário iniciar a sessão. Na próxima vez em que o usuário iniciar o software, o service pack ou a atualização de software serão aplicados automaticamente.

## 3.11. Exercício 10: Como reinstalar o software?

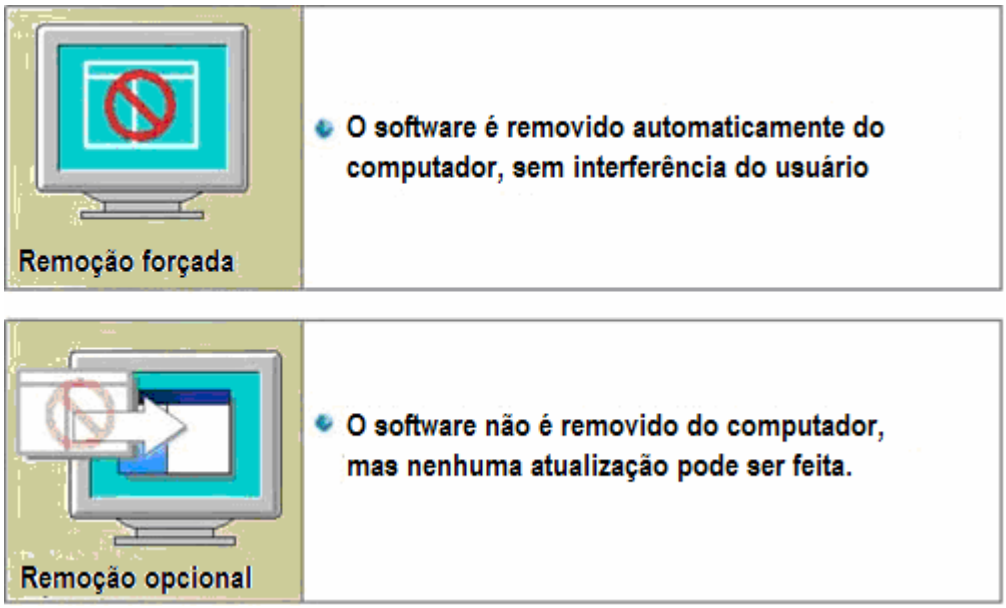
Você utiliza a instalação de software para estabelecer o procedimento da sua reinstalação. Antes de reinstalar, certifique-se de que o serviço inclui um novo arquivo do pacote do Windows Installer (.msi ). Caso contrário, você não poderá reinstalar o software porque somente o novo pacote de arquivo contém instruções para instalar os arquivos novos do service pack ou da atualização de software.

***Para reinstalar um software, é preciso:***

Obter o service pack ou a atualização de software do fornecedor do aplicativo e colocar os arquivos nas pastas apropriadas de instalação.

1. Editar o GPO que originalmente instalou o software.
2. Na Instalação do Software, clicar com o botão direito do mouse no nome do pacote de arquivos, selecionar ***Todas as Tarefas*** e depois clicar em ***Reinstalar aplicativo***.
3. Na caixa de diálogo, clicar em ***Sim***.

## 3.12. Métodos para remover o Software instalado




Pode ser preciso remover o software se uma versão não for mais suportada ou se os usuários não precisarem mais dele. Você pode forçar a remoção do software ou dar aos usuários a opção de continuar usando o software antigo.


© 2003 Microsoft Corporation. Todos os direitos reservados.

**Existem dois métodos de remoção:**

***Remoção forçada.*** Você pode forçar a remoção do software, o que removerá o software automaticamente do computador na próxima vez em que ele for ligado ou na próxima vez que um usuário iniciar a sessão, em caso de uma configuração de Diretiva de Grupo do usuário. O software será removido antes de aparecer na área de trabalho do usuário.

***Remoção opcional*** Você pode remover o software da instalação do mesmo sem forçar a retirada física do software. O software não é realmente removido dos computadores. O software não aparece mais em ***Adicionar ou Remover Programas***, mas os usuários podem utilizá-lo. Se os usuários removerem manualmente o software, ele não poderá ser reinstalado.

## 3.13. Exercício 11: Como remover o software instalado?

Quando você utiliza a Diretiva de Grupo para instalar o software, é possível configurar o GPO para remover o software antigo se ele não for mais necessário na sua organização. Também é possível remover software antigo configurando o GPO que permite aos usuários uma atualização opcionalmente a um pacote de software novo.

***Para remover um software instalado, é preciso:***

1. Abrir o GPO que foi utilizado originalmente para instalar o software.
2. Na Instalação do Software, clicar com o botão direito do mouse no nome do pacote, selecionar ***Todas as Tarefas*** e depois clicar em ***Remover***.
3. Na caixa ***Remover Software***, clicar em uma das opções seguintes e depois em ***OK***.

- ***Desinstalar imediatamente o software dos usuários e computadores***

- ***Permitir que os usuários continuem a usar o software, mas impedir novas instalações***

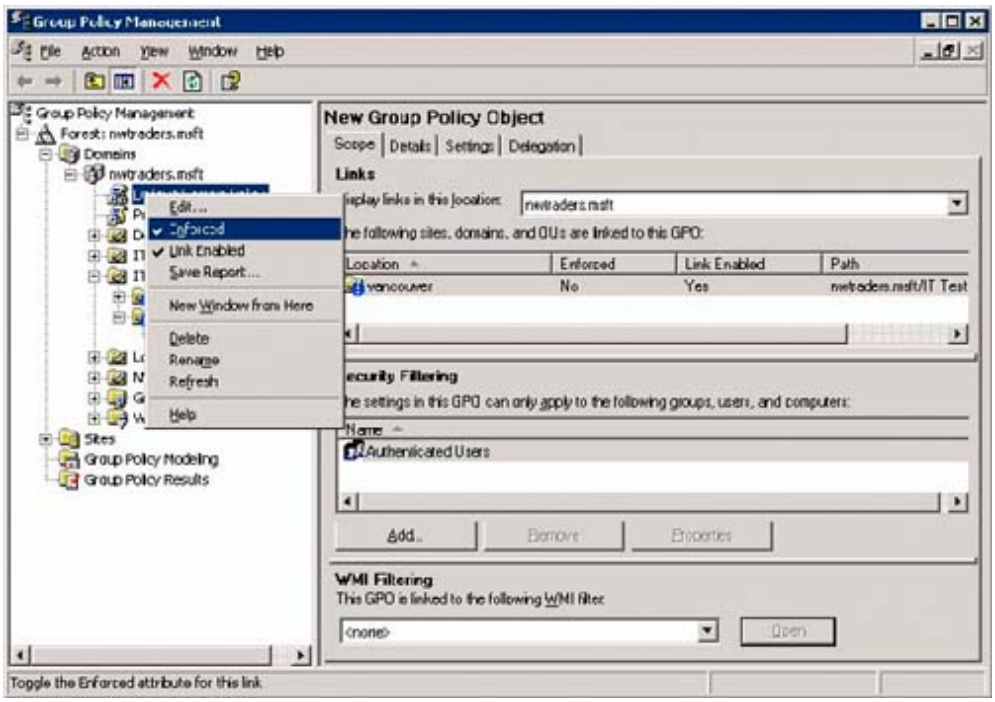
**Nota:** Você deve garantir que os usuários reiniciem seus computadores se a modificação afetar o computador ou iniciem a sessão novamente se a modificação afetar o usuário.


© 2003 Microsoft Corporation. Todos os direitos reservados.

## 4. new! Group Policy Management Console (GPMC)

Juntamente com o Microsoft® Windows Server. 2003, a Microsoft está lançando uma nova ferramenta Group Policy Management, que unifica a administração da Diretiva de Grupo. O Microsoft Group Policy Management Console (GPMC) proporciona uma única solução para controlar todas as áreas relacionadas à Diretiva de Grupo. Consiste em um novo snap-in do Microsoft Management Console (MMC) e um sistema de interfaces de scripts para a administração de Diretiva de Grupo. A GPMC ajuda a gerenciar com mais eficácia uma empresa.

### 4.1. O que é o Group Policy Management Console?




O Group Policy Management Console (GPMC) é uma ferramenta nova para controlar a Diretiva de Grupo no Windows Server 2003.

***O GPMC:***

- Permite que você controle a Diretiva de Grupo para diferentes florestas, domínios e unidades organizacionais a partir de uma interface constante.
- Exibe os links, herança e delegação da Diretiva de Grupo
- Mostra os contêineres aos quais a diretiva se aplica
- Proporciona relatórios em HTML das configurações.
- Proporciona ferramentas para mostrar o Conjunto de Diretivas Resultantes (RSoP) e experimenta combinações propostas de diretivas.

**Nota:** O GPMC não vem com o Windows Server 2003. Você pode fazer o download de

http://www.microsoft.com/windowsserver2003/gpmc/default.mspx


© 2003 Microsoft Corporation. Todos os direitos reservados.

## 4.2. Requisitos do Sistema de GPMC

O GPMC ajuda a controlar ambos os domínios baseados no Windows 2000 e no Windows Server 2003 com o serviço do Active Directory®.

***Em qualquer caso, o computador que executa o GPMC deve ter um dos sistemas operacionais a seguir:***

- Windows Server 2003

- Windows XP Professional com Service Pack 1 (SP1) e Microsoft .NET Framework. Além disso, é necessário um hotfix pós-SP1 (QFE Q326469). Este QFE atualiza sua versão de gpedit.dll para a versão 5.1.2600.1186, que é exibida para o GPMC. Este QFE é incluído com o GPMC e a instalação do GPMC pergunta sobre sua instalação. Entretanto, se o idioma do GPMC não corresponder ao idioma do seu sistema operacional, o GPMC não instalará o QFE e será necessário obter e instalar separadamente este QFE, que será incluído no Windows XP Service Pack 2.

## 4.3. Instalação do GPMC

A instalação do GPMC é um processo simples que inclui a execução de um pacote Windows Installer (.MSI). Os arquivos necessários serão instalados na pasta **\Arquivos de Programas\GPMC**.

***Para eles:***

1. Clique duas vezes no pacote ***gpmc.msi*** e em ***Avançar***.
2. Aceite o Contrato de Licença de Usuário Final (EULA) e clique em ***Avançar***.
3. Clique em ***Fechar*** para concluir a instalação.

Após a conclusão da instalação, a guia Diretiva de Grupo que era exibida nas páginas de propriedades de sites, domínios e unidades organizacionais (OUs) nos snap-ins do Active Directory é atualizada para proporcionar um acesso direto ao GPMC. A funcionalidade que existia previamente na guia original da Diretiva de Grupo não estará mais disponível, toda a funcionalidade para controlar a Diretiva de Grupo estará disponível através do GPMC.

***Para abrir o snap-in do GPMC diretamente, utilize alguns dos métodos a seguir:***

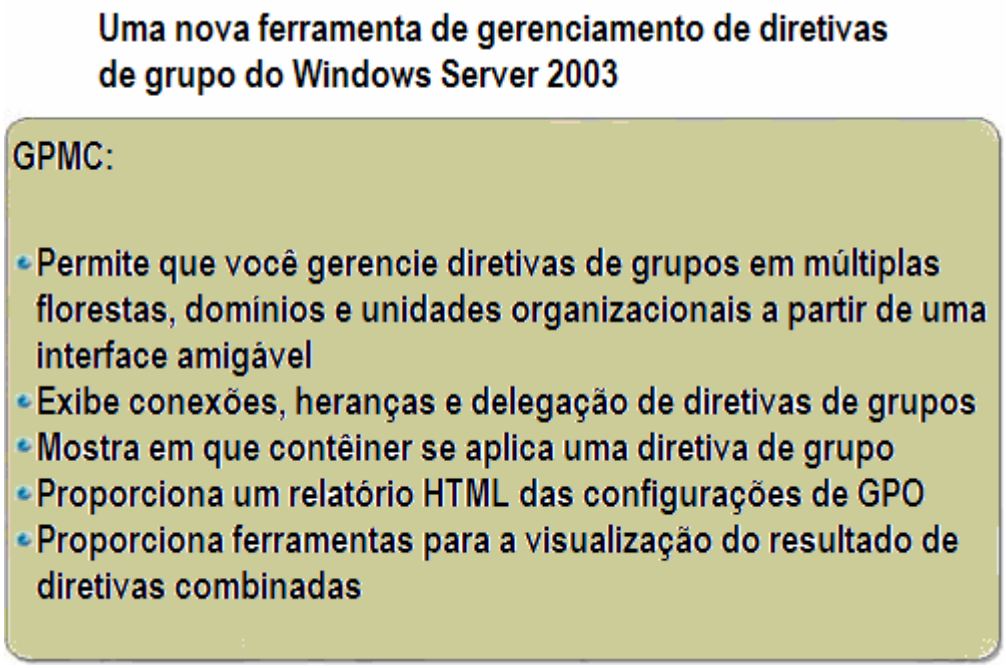
- Clique em ***Iniciar***, clique em ***Executar***, insira ***GPMC.msc*** e depois clique em ***OK***.
- Clique no acesso ***Group Policy Management*** na pasta ***Ferramentas Administrativas*** do menu Iniciar ou no Painel de Controle.
- Crie um console personalizado MMC

1. Clique em ***Iniciar***, clique em ***Executar***, insira ***MMC*** e depois clique em ***OK***.
2. No menu ***Arquivo***, clique em ***Adicionar/remover snap-in,*** clique em ***Adicionar***, selecione ***Group Policy Management***, clique em ***Adicionar***, em ***Fechar***, e depois em ***OK***.

- Para reparar ou remover o GPMC, use ***Adicionar ou Remover Programas*** no Painel de Controle. Você também pode executar o pacote gpmc.msi, selecionar a opção apropriada e clicar em ***Concluir***.


© 2003 Microsoft Corporation. Todos os direitos reservados.

## 4.4. Modelagem de Diretiva de Grupo e Resultados de Diretiva de Grupo




### *Modelagem de Diretiva de Grupo*

O Windows Server 2003 traz um novo recurso de grande alcance: o Group Policy Management Ele permite que o usuário simule a aplicação de diretivas que seriam aplicadas aos usuários e aos computadores antes de aplicá-las realmente. Esse recurso é conhecido como Conjunto de Diretivas Resultante (RSoP). O modo de planejamento no Windows Server 2003 integra-se no GPMC como Modelagem de Diretiva de Grupo. Isto exige um controlador de domínio do Windows Server 2003 na floresta porque a simulação é realizada por um serviço que só está presente nos controladores de domínio do Windows Server 2003.

Entretanto, usando esta característica, você pode simular o conjunto de diretivas resultantes para qualquer computador na floresta, incluindo aqueles que usam o Microsoft Windows® 2000.

### *Diretiva de Grupo Resultantes*

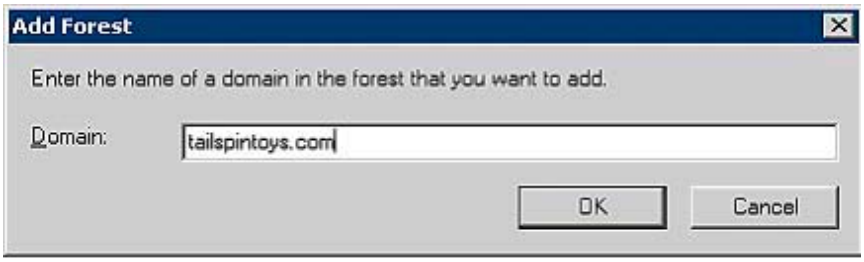
Este recurso permite que os administradores determinem o conjunto de políticas resultante que foi aplicado a um computador específico e (opcionalmente) o usuário que iniciou a sessão nesse computador. Os dados que se apresentam são semelhantes aos dados de Modelagem de Política de Grupo. Entretanto, são diferentes uma Modelagem de Diretivas de Grupo, considerando que não são uma simulação. É o resultado real do conjunto de diretivas resultante obtido do computador de destino. Também é diferente da Modelagem de Diretiva de Grupo, os dados dos Resultados de Diretiva de Grupo são obtidos do cliente e não são simulados no controlador de domínio. O cliente precisa executar o Windows XP, o Windows Server 2003 ou posterior. Não é possível obter Resultados de Diretiva de Grupo em um computador que execute o Windows 2000 ou versão anterior.


© 2003 Microsoft Corporation. Todos os direitos reservados.

## 4.5. Administrar múltiplas florestas

***Múltiplas florestas podem ser adicionadas facilmente ao console. Para isso, é preciso:***

1. Clicar com o botão direito no nó da raiz ***Group Policy Management*** e selecionar ***Add Forest...***




2. Especificar o nome DNS ou NetBIOS do domínio criado na floresta que não foi carregado no GPMC, e clicar em ***OK***.

A floresta especificada aparecerá como um nó secundário no console e será carregada no console com o domínio que foi incorporado na caixa ***Add Forest***.

Para remover um nó de floresta, basta clicar com o botão direito no nó e selecionar ***Remove***. Por padrão, você pode adicionar somente a floresta ao GPMC se houver uma confiança bidirecional com a floresta do usuário que executa o GPMC.

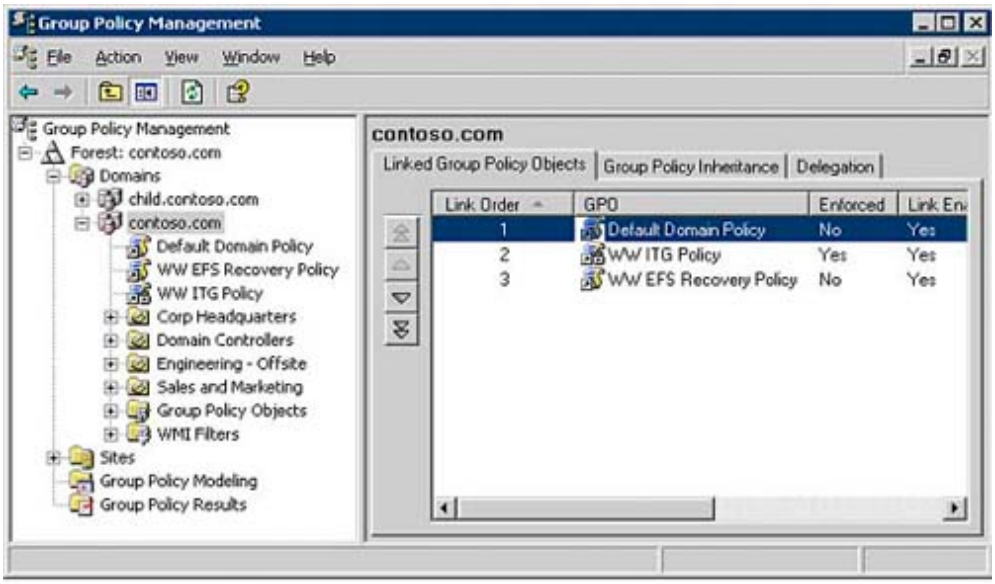
## 4.6. Conteúdo de Domínios

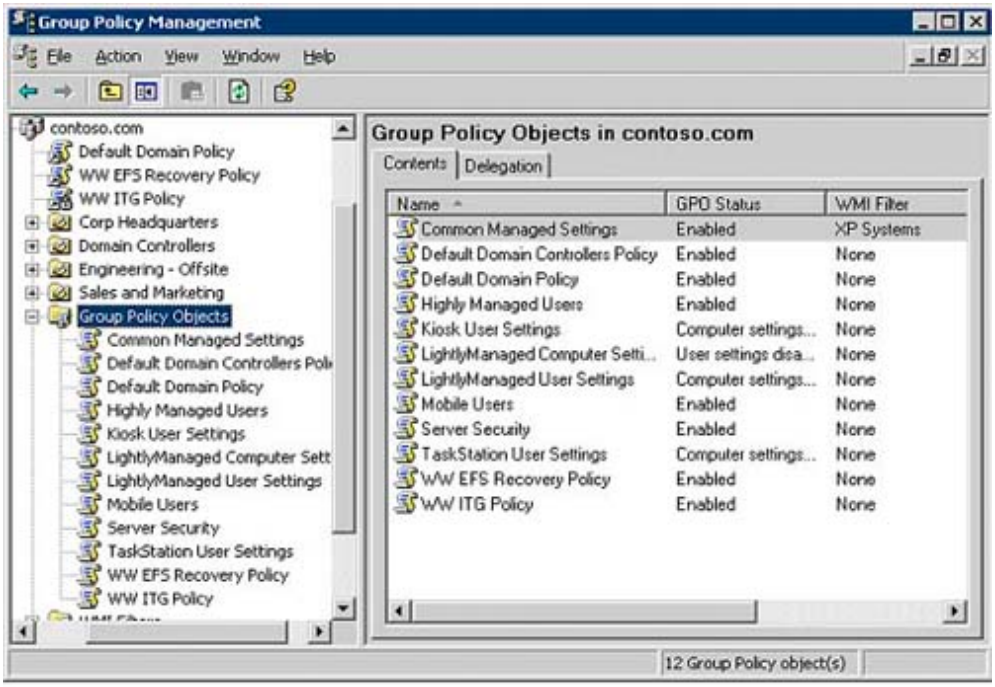
Dentro de cada domínio, o GPMC proporciona uma vista baseada nas diretivas do Active Directory e nos componentes associados à Diretiva de Grupo, por exemplo, GPOs, filtros WMI e links de GPO. A visão no GPMC é semelhante à visão em snap-in do MMC de Usuários e Computadores do Active Directory que mostra a hierarquia da Unidade Organizacional. No entanto, o GPMC difere desse snap-in porque em vez de mostrar usuários, computadores e grupos das Unidades Organizacionais, exibe os GPOs que estão vinculados a cada contêiner.

***Cada nó de domínio no GPMC exibe os seguintes pontos:***

- Todos os GPOs vinculados ao domínio.
- Todas as Unidades Organizacionais de alto nível e uma vista de árvore das Unidades Organizacionais e dos GPOs vinculados a elas.
- Os contêineres de ***Group Policy Objects*** mostram todos os GPOs no domínio.
- O contêiner ***WMI Filters*** mostra todos os Filtros WMI no domínio.


© 2003 Microsoft Corporation. Todos os direitos reservados.



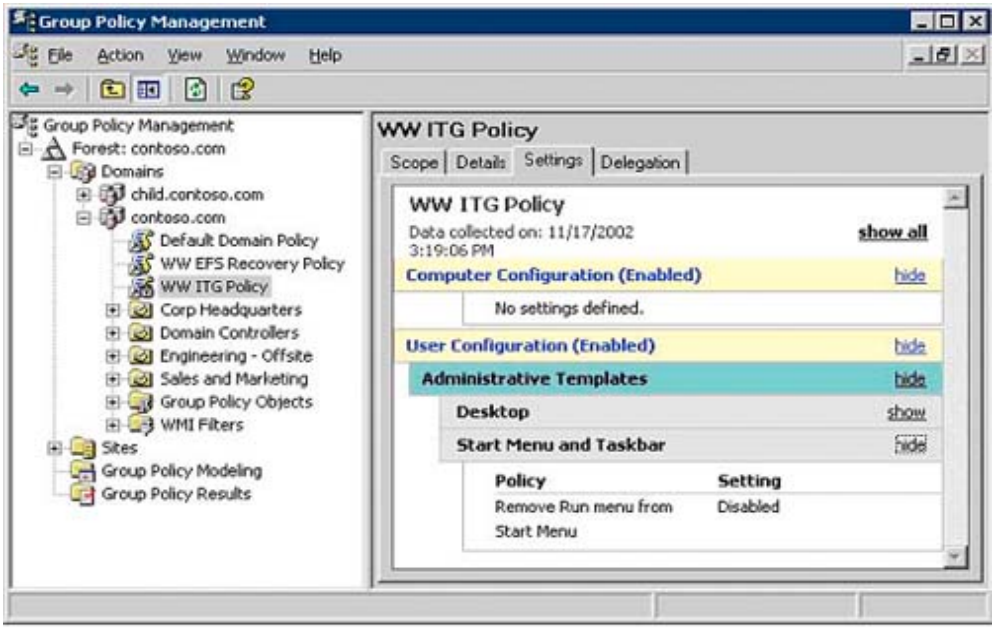

## 4.7. Relatórios de configuração de GPO

A guia de configuração de GPO ou link de GPO no GPMC mostra um relatório em HTML que exibe todas as configurações definidas no GPO. Clique nesta guia para gerar um relatório das configurações no GPO. Este relatório pode ser gerado por qualquer usuário com acesso de leitura ao GPO. Sem GPMC, os usuários que não tinham acesso de gravação a um GPO não podem ler e revisar configurações com esse GPO. Isso ocorre porque o editor de Objeto de Diretiva de Grupo exige que o usuário tenha permissão de leitura e gravação ao abrir o GPO.


© 2003 Microsoft Corporation. Todos os direitos reservados.

Os relatórios de HTML também facilitam que o administrador tenha visão de todas as configurações contidas em um GPO de uma visualização. Selecionando a opção ***Show All*** acima do relatório, ele é completamente ampliado e mostra todas as configurações.

Para ver ou salvar um relatório diretamente em um navegador da Web, você deve utilizar o Internet Explorer 6 ou o Netscape 7. O Netscape 7 não aceita a funcionalidade que permite mostrar ou ocultar dados nos relatórios.




## 4.8. Operações com o GPO

As operações de GPO referem-se aos recursos de ***backup*** (exportar), ***restaurar***, ***importar*** e copiar GPOs. Fazer um backup de GPO consiste em copiar os dados do GPO no sistema de arquivos. Observe que a função ***Backup*** também serve como a função de exportação para GPOs.

A Restauração de GPO restaura um backup existente e recria o GPO no domínio. O objetivo da restauração é reajustar um GPO específico de novo ao estado idêntico que tinha quando foi realizado o backup. Portanto, a operação de restauração não pode ser utilizada para transferir GPOs através de domínios. Para essa operação, é preciso utilizar a importação de GPO ou a operação de cópia.

### 4.8.1. Backup

***O Backup de GPO coloca uma cópia de todos os dados relevantes de GPO em uma localização especificada do sistema de arquivos. Os dados relevantes incluem:***

- O GUID de GPO e domínio.
- Configurações de GPO.
- A Discretionary Access Control List (DACL) do GPO.
- O link de filtro do WMI.

A operação de backup só faz backup de componentes do GPO que estão no Active Directory e na estrutura dos arquivos do GPO em SYSVOL. A operação não captura dados armazenados fora do GPO, por exemplo, filtros WMI e diretivas de Segurança IP. Esses são objetos separados com seus próprios sistemas de permissões e é possível que um administrador qualquer faça o backup ou a restauração. Ele pode não ter as permissões exigidas nesses outros objetos.


© 2003 Microsoft Corporation. Todos os direitos reservados.

***Os administradores podem fazer backup de uma ou mais de GPOs usando os métodos seguintes:***

- Clique com o botão direito do mouse no GPO no nó ***Group Policy objects*** e escolha ***Back up...*** do menu de contexto.

- Clique com o botão direito do mouse em um ou mais GPOs na guia ***Contents*** do nó ***Group Policy objects*** e escolha ***Back up...*** do menu de contexto. Isso faz backup dos GPO(s) selecionados.

- No nó ***Group Policy Objects***, clique no botão direito do mouse e escolha a opção ***Back Up All...***
Isso faz backup de todos os GPOs no domínio.

- Use os scripts de backup do GPO. Você pode escrever seus próprios scripts ou utilizar a amostra de scripts incluída com o GPMC na pasta GPMC\scripts . Existem dois scripts ***BackupGPO.wsf*** e ***BackupAllGPOs.wsf*** que são incluídos com o GPMC, que você pode utilizar para fazer backup de GPOs.

### 4.8.2. Restauração

A operação de Restauração de GPO restaura o GPO a um estado anterior e pode ser utilizado nos casos seguintes: foi feito o backup no GPO, mas ele foi removido ou o GPO está ativo e você quer voltar a um estado anterior.

***A operação de restauração substitui os componentes seguintes de um GPO:***

- Configurações de GPO.
- ACLs no GPO.
- Os links de filtro de WMI.


© 2003 Microsoft Corporation. Todos os direitos reservados.

***Você pode realizar uma restauração de GPOs usando qualquer dos métodos a seguir:***

- Para restaurar um GPO existente, clique com o botão direito do mouse no GPO no contêiner ***Group Policy objects*** e selecione ***Restore from Backup...*** Ele abre ***Restore Group Policy Object Wizard***.

- Use os scripts de restauração do GPO. Você pode gravar seus próprios scripts ou utilizar as amostras de scripts incluídas com o GPMC na pasta **GPMC\scripts**
  Existem dois scripts ***RestoreGPO.wsf*** e ***RestoreAllGPOs.wsf***.

### 4.8.3. Importar

A operação de importação transfere a configuração em um GPO existente do Active Directory, usando um backup de GPO na localização do sistema de arquivos como sua origem. As operações de importação podem ser utilizadas para transferir configurações através de GPOs dentro do mesmo domínio, através de domínios na mesma floresta ou em florestas separadas.

As operações de importação são ideais para imigrar a Diretiva de Grupo em ambientes de onde não há confiança.

***As operações de importação podem ser realizadas usando qualquer dos métodos a seguir:***

- Clique com o botão direito do mouse no GPO no nó Objetos de Diretiva de Grupo e clique em Import Settings. Isso inicia um assistente que o orientará no processo de selecionar o backup e especificar uma tabela de migração se apropriado.

- Use qualquer dos scripts ***ImportGPO.wsf*** ou ***ImportAllGPOs.wsf*** incluídos no GPMC.

### 4.8.4. Copiar

1. Uma operação de cópia transfere configurações usando um GPO existente no Active Directory como origem e cria um GPO novo como seu destino.

2. Uma operação de cópia pode ser utilizada para transferir configurações para um novo GPO qualquer no mesmo domínio, em outros domínios, na mesma floresta ou em florestas separadas. Considerando que uma operação de cópia utiliza um GPO existente no Active Diretory como origem, é exigida confiança entre a origem e os domínios do destino.

***As operações de cópia podem ser realizadas usando qualquer dos métodos a seguir:***

- Clique com o botão direito do mouse na origem de GPO, escolha a cópia e clique com o botão direito no contêiner ***Group Policy Object***s do domínio desejado de destino. Escolha a opção Colar.

- Use Arrastar e soltar para arrastar o GPO da origem ao contêiner ***Group Policy Objects*** no destino de domínio.

- Use o script ***CopyGPO.wsf*** de linha de comando incluído com o GPMC.

Para obter mais informações:

http://www.microsoft.com/windowsserver2003/gpmc/default.mspx
http://www.microsoft.com/windowsserver2003/gpmc/migrgpo.mspx
http://www.microsoft.com/grouppolicy
http://www.microsoft.com/technet/grouppolicy


© 2003 Microsoft Corporation. Todos os direitos reservados.

# Capitulo 6
# Implementação e Administração do Terminal Server no Windows Server 2003.

O Terminal Server do Microsoft® Windows Server 2003 permite diversificar o hardware do escritório através da emulação de terminais.

***Ele também oferece suporte a uma ampla gama de clientes e melhora os ambientes de computação ao:***

- Tornar a família do Windows mais escalável para empresas que queiram implementar a solução “thin client” para oferecer Windows de 32 bits a uma grande variedade de dispositivos de hardware do legado.

- Combinar o baixo custo de um terminal com os benefícios de um ambiente gerenciado, baseado no Windows. Também oferece o mesmo ambiente de baixo custo e administração central de um ***mainframe*** tradicional com terminais, mas acrescenta a familiaridade, a facilidade de uso e a variedade de suporte a aplicativos proporcionados por uma plataforma de sistema operacional do Windows.

***Ao concluir este capítulo, você poderá:***

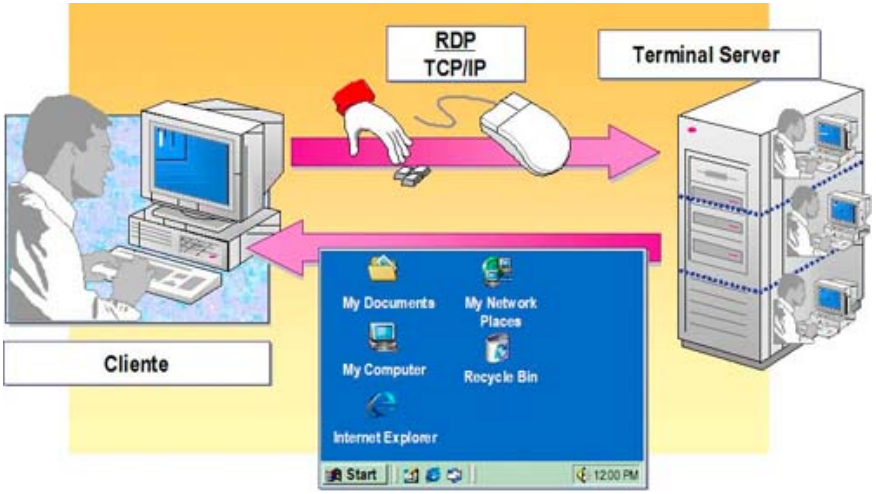
- Implementar a Área de Trabalho Remota para administração
- Instalar o Terminal Server
- Administrar um ambiente Terminal Server

## 1. Introdução

Os Terminal Services permitem o acesso de múltiplos usuários ao Windows Server 2003, permitindo que várias pessoas iniciem sessões em um único computador simultaneamente. Os administradores podem instalar aplicativos baseados no Windows do Terminal Server e colocá-los à disposição de todos os clientes conectados com o servidor. Embora os usuários possam ter diversos hardware e sistemas operacionais, a sessão Terminal que é aberta na área de trabalho do cliente conserva o mesmo aspecto e funcionalidade para todos.


© 2003 Microsoft Corporation. Todos os direitos reservados.

### 1.1. Como funciona o Terminal Services?




***O Terminal Server do Windows Server 2003 é composto por quatro componentes:***

- ***Terminal Server:*** Este núcleo de servidor multiusuário permite manter várias sessões simultâneas de clientes no Windows Server 2003 e em versões futuras do Windows Server. Também é possível ter de forma direta áreas de trabalho de cliente multiusuários compatíveis que executem diversos equipamentos de hardware baseados ou não no Windows. Os aplicativos padrão baseados no Windows, se forem desenvolvidos adequadamente, não precisam de nenhuma modificação para executar no Terminal Server, e é possível utilizar todas as infra-estruturas de administração e tecnologias padrão baseadas no Windows Server 2003 para administrar as áreas de trabalho do cliente.

- ***Remote Display Protocol (RDP):*** Este protocolo é um componente chave do Terminal Server e permite que o cliente se comunique com o Terminal Server em uma rede. Baseia-se no protocolo T.120 da União Internacional de Telecomunicações (UIT) e é um protocolo de múltiplos canais que estão ajustados para ambientes corporativos de largura de banda elevada e que oferece suporte a três níveis de criptografia.

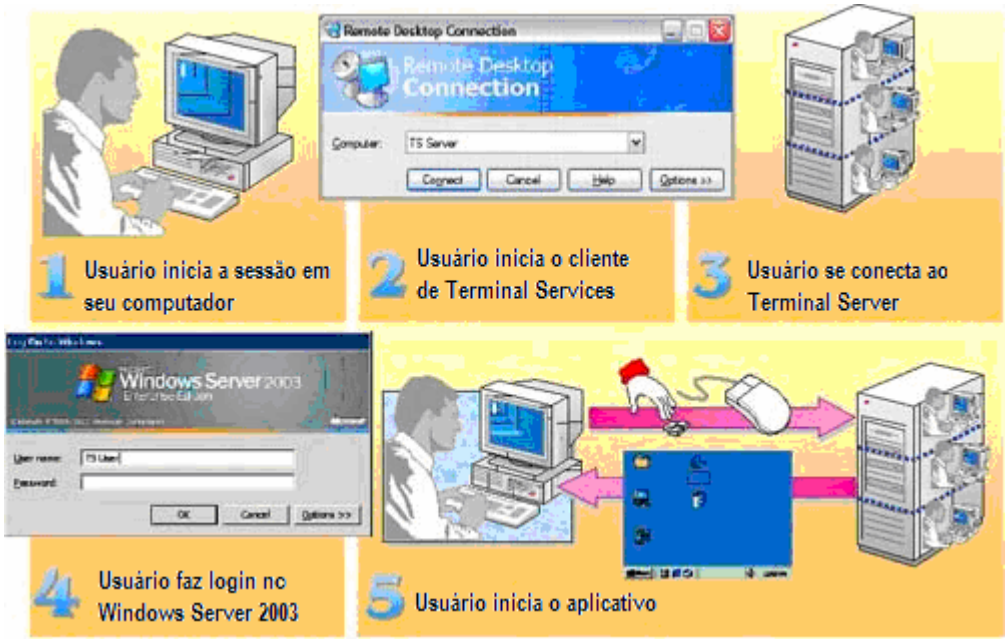
- ***Cliente do Terminal Server:*** É o software de cliente que apresenta uma interface familiar do Windows de 32 bits em uma grande variedade de hardware de área de trabalho:

    - Novos dispositivos Terminal baseados no Windows (em clusters).
    - Computadores pessoais que executam o Windows 95, o Windows 98 e o Windows NT Workstation 3.51 ou 4.0, o Windows 2000 ou XP Professional.
    - Computadores pessoais que executam o Windows for Workgroups 3.11.

- ***Ferramentas de administração***: Além de todas as ferramentas de administração familiares do Windows Server 2003, o Terminal Server acrescenta um administrador de licenças de Terminal Services, a configuração do Terminal Server (MMC) e ferramentas de administração para Terminal Server e para sessões de clientes. Também disso, foram adicionados novos objetos ao monitor de desempenho de sessão e usuário, para permitir ajustá-los ao servidor em um ambiente de múltiplos usuários.

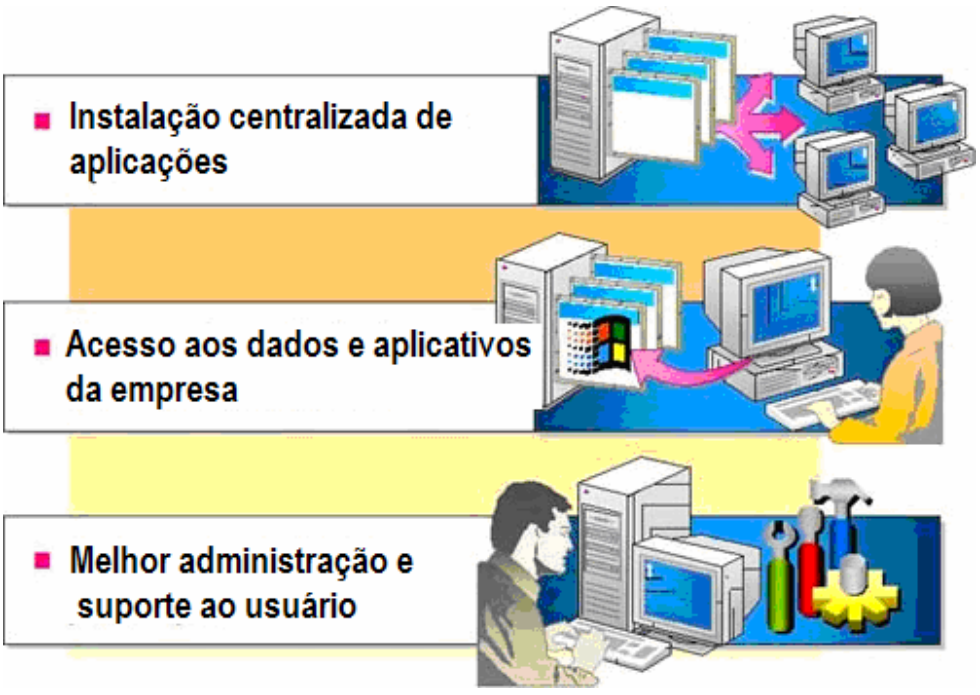

© 2003 Microsoft Corporation. Todos os direitos reservados.

### 1.2. Ambientes de Usuário




Depois de instalar o software do cliente, os usuários acessam o Terminal Server abrindo o Cliente de Conexão de Área de Trabalho Remota do menu ***Todos os Programas/Acessórios/ Comunicações.*** Quando um usuário conecta e inicia a sessão no Terminal Server, a área de trabalho do Windows Server 2003 é exibida na área de trabalho do cliente. Quando um usuário inicia um programa, é fácil perceber se o programa não estiver funcionando de forma local.

### 1.3. Recursos e vantagens





© 2003 Microsoft Corporation. Todos os direitos reservados.

Os recursos do Terminal Server proporcionam várias vantagens que uma organização pode utilizar como instalação, acesso e controle dos aplicativos de negócios.

## Instalação Centralizada

As organizações podem instalar aplicativos de negócios, considerando que o funcionamento dos programas ocorrerá inteiramente no servidor. O Terminal Server tem o menor TCO para um único dispositivo de aplicativo que funciona em uma linha de negócio, por exemplo, um sistema de reservas ou uma Central de Atendimento ao Cliente.

### *Oferece também as seguintes vantagens:*

- ***Menos hardware de alto custo.*** Funcionários que realizem trabalhos que exigem acesso apenas a um programa da empresa e que possam usar terminais ou computadores menos caros.

- ***Acesso fácil a software novo ou atualizado.*** Quando o Terminal Server está ativado no Windows Server 2003, os administradores não precisam instalar os aplicativos em cada computador do escritório. O aplicativo já está instalado no servidor e os clientes possuem acesso automático à versão nova ou atualizada do software.

## Acesso à área de trabalho do Windows Server 2003

O Terminal Server pode estender o Windows Server 2003 e os aplicativos baseados no Windows a vários clientes.

### *Ao mesmo tempo, também permite:*

- ***Executar aplicativos do Windows:*** O Terminal Server pode disponibilizar aplicativos do Windows a uma ampla variedade de clientes. Esses aplicativos baseados no Windows podem funcionar em vários sistemas, de sistema operacional ou hardware, com pouca ou nenhuma modificação.

- ***Ampliar o uso de um equipamento mais antigo*** A organização pode implementar o Terminal Server como tecnologia transitória para criar uma ponte com os sistemas operacionais antigos, os ambientes da área de trabalho do Windows Server 2003 e aplicativos de 32 bits baseados no Windows.

- ***Substituir terminais de texto*** Como muitos terminais do Windows podem oferecer suporte à conexão por emulação de terminal no mesmo dispositivo, as organizações podem substituir terminais de texto por terminais do Windows. Elas permitem que os usuários trabalhem com dados do sistema, tenham acesso ao software mais novo baseado no Windows como, por exemplo, o Microsoft Outlook.

- ***Segurança e confiabilidade aprimoradas*** Como nenhum programa ou dado de usuário reside no cliente, o Terminal Server pode proporcionar um ambiente mais seguro para dados confidenciais. Também oferece suporte à criptografia em múltiplos níveis, considerando que sempre há risco de interceptação não-autorizada da transmissão na conexão entre o servidor e o cliente. Existem três níveis de criptografia disponíveis: baixo, médio e alto. Todos esses níveis usam o Padrão de Criptografia Rivest-Shamir-Adleman (RSA) RC4. Esse é o padrão de criptografia para os dados que são enviados através de redes públicas como, por exemplo, a Internet.

## Administração e suporte aprimorados

### *O Terminal Server tem vários recursos úteis para a administração e tarefas de suporte, que também podem ajudar a reduzir os custos de administração e de suporte.*

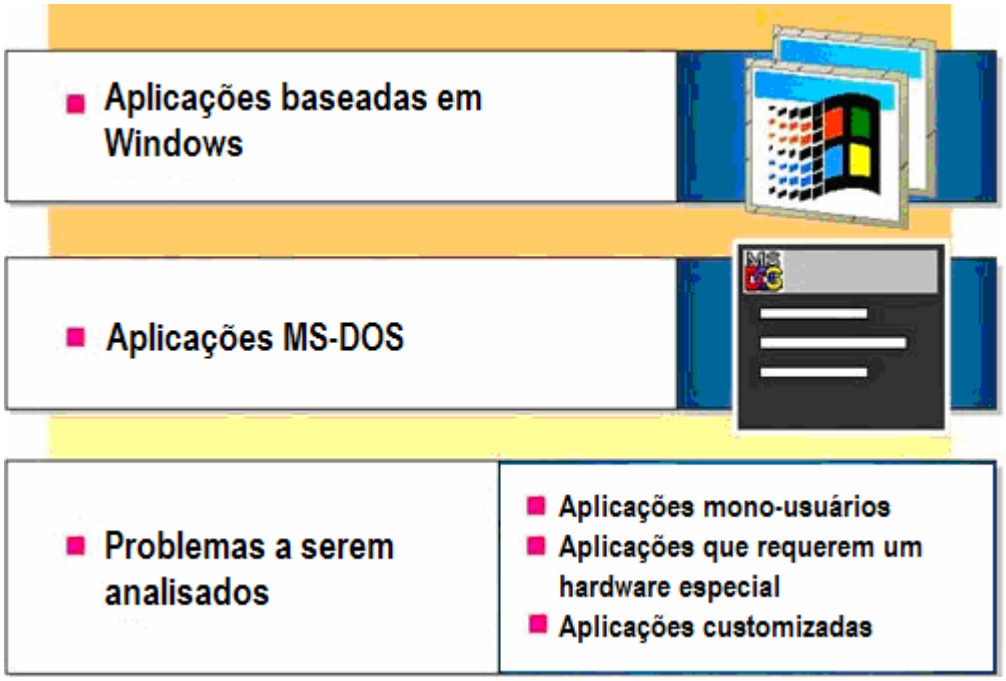
- ***Administração remota***. A Área de Trabalho Remota é um novo recurso do Terminal Server no Windows Server 2003. Ele foi desenvolvido para fornecer aos operadores e administradores acesso remoto aos servidores Microsoft BackOffice® e aos Controladores de Domínio. O administrador tem


© 2003 Microsoft Corporation. Todos os direitos reservados.

acesso às ferramentas de interface gráfica disponíveis no ambiente do Windows, mesmo que não esteja utilizando um computador com Windows para administrar o servidor.

- ***Suporte remoto.*** Os administradores podem oferecer suporte remoto para um usuário que inicie a sessão no Terminal Server, acompanhando a sessão do cliente a partir de outra sessão do cliente. Os administradores ou o pessoal de suporte também podem realizar ações de teclado e mouse por um usuário, usando o Controle Remoto. O Controle Remoto pode ser útil para oferecer treinamento e suporte de usuários nos sistemas ou aplicativos novos.

## 1.4. Planejamento da instalação




### 1.4.1. Identificando aplicativos cliente

Antes de instalar o Terminal Server, identifique os aplicativos que você pretende instalar na área de trabalho do cliente. A maioria dos programas que funciona corretamente no Windows Server 2003 também funciona no Terminal Server.

#### Aplicativos baseados no Windows

Os aplicativos instalados em um Terminal Server devem ser compatíveis com o Windows Server 2003. Se um programa não funcionar no Windows Server 2003, ele não funcionará no ambiente multiusuário do Terminal Server. Os aplicativos de 32 bits funcionam com mais eficiência que os aplicativos de 16 bits, aproveitando completamente o hardware e o sistema operacional de 32 bits. Os aplicativos de 16 bits executados no Terminal Server podem reduzir o número de usuários que o processador aceita em aproximadamente 40%, e aumentar a memória exigida por cada usuário em aproximadamente 50%.

#### Aplicativos do MS-DOS

Considerando que os aplicativos baseados no Microsoft MS-DOS® nunca foram desenvolvidos para ambientes de múltiplas tarefas, executar aplicativos do MS-DOS no Terminal Server pode retardar o funcionamento do sistema com processos ociosos. Se o funcionamento do servidor for retardado de


© 2003 Microsoft Corporation. Todos os direitos reservados.

forma perceptível quando os usuários utilizarem aplicativos do MS-DOS, é preciso ajustar as configurações do sistema.


© 2003 Microsoft Corporation. Todos os direitos reservados.

### 1.4.2. Identificar requisitos de hardware do cliente

Computadores de cliente conectados a um Terminal Server não exigem muito poder de processamento e, por isso, é muito fácil integrar o Terminal Server a uma rede que tenha computadores e equipamentos antigos.

**O Terminal Server oferece suporte às seguintes plataformas**

- Microsoft Windows 2000/XP/2003
- Microsoft Windows NT® versões 3.51 e 4.0
- Microsoft Windows 95
- Microsoft Windows 98
- Microsoft Windows para Workgroups 3.11
- Microsoft Windows CE, Handheld PC Edition 3.0
- Windows CE, Handheld PC Professional Edition 3.0
- Terminais baseados ao Windows

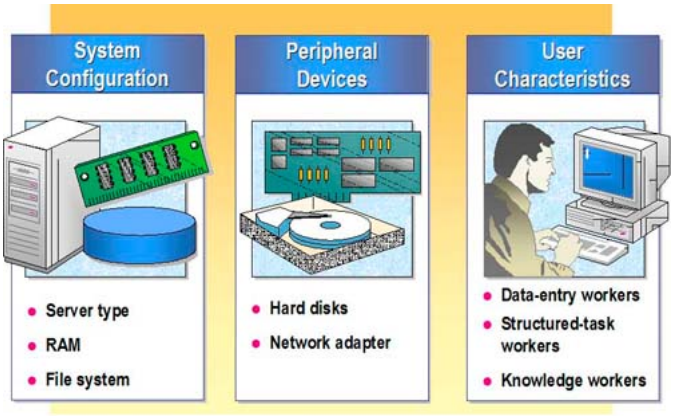
**Requisitos de Hardware**

A tabela a seguir descreve os requisitos de hardware específicos do cliente para Terminal Server.

| Sistema Operacional | RAM | CPU | Vídeo |
|---|---|---|---|
| Windows 2000 | 32 megabytes (MB) | Pentium | VGA |
| Windows NT versões 3.51 ou 4.0 | 16 MB | 486 | VGA |
| Windows 98 | 16 MB | 486 | VGA |
| Windows 95 | 16 MB | 386 | VGA |
| Windows for Workgroups 3.11 | 16 MB | 386 | VGA |
| Windows CE, Handheld PC/PRO | Fornecedor | Fornecedor | Fornecedor |


© 2003 Microsoft Corporation. Todos os direitos reservados.

### 1.4.3. Determinar a configuração do servidor para suporte de usuários




Considerando que todo o processamento dos aplicativos é executado no servidor, o Terminal Server normalmente exige mais recursos de servidor por usuário do que um computador que esteja executando o Windows Server 2003. Certificar-se de que o seu servidor pode acomodar a sua base de usuários é crucial para determinar como o funcionamento do servidor do Terminal Server deve oferecer suporte aos usuários. Além disso, é necessário considerar os seguintes fatores: configuração do sistema, dispositivos periféricos e características de usuário.

#### Configuração do Sistema

***Antes de instalar o Terminal Server, considere as recomendações a seguir:***

- ***Tipos de servidor.*** Recomenda-se instalar o Terminal Server em um Servidor Membro e não em um Controlador de Domínio. A instalação do Terminal Server em um Controlador de Domínio pode criar obstáculos para o funcionamento do servidor devido às necessidades de memória, tráfego da rede e o tempo que o processador precisa para realizar as tarefas de um controlador de domínio no domínio.

- ***RAM.*** Geralmente, um Terminal Server exige um adicional de 4 a 10 MB de RAM para cada sessão do terminal.

- ***Sistema de arquivos.*** Recomenda-se instalar um Terminal Server em uma partição formatada com o Sistema de Arquivo NTFS, visto que ele proporciona segurança para os usuários em um ambiente de múltiplas sessões com acesso às mesmas estruturas de dados.

#### Dispositivos Periféricos

***Os dispositivos periféricos também podem afetar o funcionamento do Terminal Server:***

- ***Discos rígidos.*** A velocidade do disco é crítica para o funcionamento do Terminal Server. As unidades de disco SCSI (Small Computer System Interface), especialmente dispositivos compatíveis com o SCSI e Scsi-2 rápidos, têm um desempenho de processamento bem melhor do que os outros tipos de discos. Isso é menos importante nos sistemas que não armazenam Perfis de Usuário e dados no Terminal Server, mas afeta o tempo de carregamento inicial do programa. Para um melhor desempenho do disco, é importante considerar o uso do Controlador RAID (Redundant Array of Independent Disks) SCSI. O Controlador RAID insere automaticamente os dados em múltiplos discos para aumentar o desempenho e melhorar a confiabilidade dos dados.

- ***Adaptador de rede.*** Recomenda-se usar um adaptador de rede de alto desempenho, especialmente se os usuários exigirem acesso a dados que sejam armazenados nos servidores de rede ou executem aplicativos cliente/servidor. Usando múltiplos adaptadores, é possível aumentar de forma perceptível o rendimento da rede e também a segurança do sistema na separação do acesso do cliente de serviços back-end.


© 2003 Microsoft Corporation. Todos os direitos reservados.

### Características de Usuário

Os padrões de uso dos usuários de computadores podem ter um impacto importante no funcionamento do Terminal Server.

***O teste de funcionamento do Microsoft simula usuários nas três categorias seguintes:***

- ***Funcionário de entrada de dados:*** Esses funcionários trabalham somente com um único aplicativo utilizado na entrada de dados (por exemplo, aplicativos de negócios desenvolvidos no Microsoft Visual Basic®).

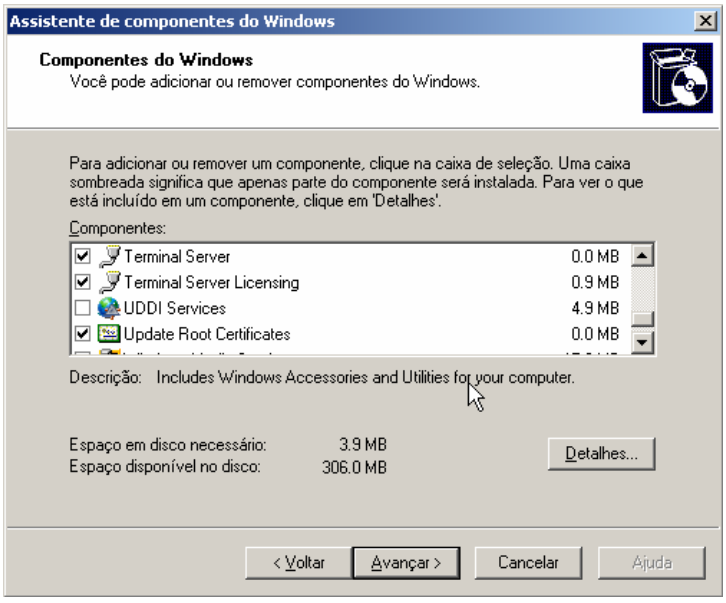
- ***Funcionário de tarefa estruturada.*** Esses funcionários executam um ou dois programas ao mesmo tempo. Os usuários típicos executam programas que não exigem muito do sistema (por exemplo, um processador de texto e um navegador). Os programas são abertos e fechados com freqüência.

- ***Funcionário de conhecimento.*** Os funcionários que trabalham com conhecimento executam três ou mais programas simultaneamente e geralmente deixam seus programas abertos. Os funcionários que utilizam conhecimentos também podem executar programas que exijam processamento intenso do sistema (por exemplo, consultas detalhadas em grandes bancos de dados).

## *1.5. Instalar o Terminal Server*

Para instalar o Terminal Server, é preciso ativar o componente do Terminal Server durante a instalação, usando o assistente de Componentes do Windows. Você pode ativar o Terminal Server de duas formas: com o Servidor de Aplicativos do Terminal ou Administração de Área de Trabalho Remota. Esse último não exige licença e permite somente 3 conexões. A licença do Terminal Server pode ser instalada com o Terminal Server ou sozinha em outro computador. Quando a Licença do Terminal Server é instalada, é preciso especificar se o servidor de licenças servirá ao domínio, ao grupo de trabalho ou ao site.

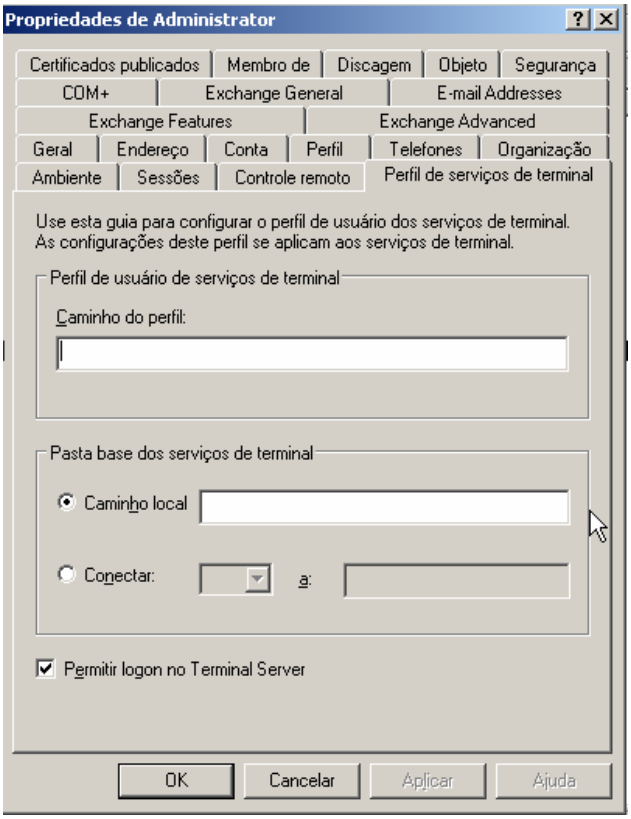
new! Para ativar o Terminal Server (Aplicativo), o processo é realizado através do assistente de componentes do Windows. Por sua vez, para ativar a Área de Trabalho Remota (instalado por padrão), é preciso ir para a guia “Remoto” nas propriedades do sistema e selecionar a opção "Permitir que usuários se conectem remotamente a este computador".




O Terminal Server é ativado adicionando-se o componente "Terminal Server" e usando Componentes do Windows no assistente de ***Adicionar ou Remover Programas.***


© 2003 Microsoft Corporation. Todos os direitos reservados.

### 1.6. Configurar Acesso de Usuário




Os usuários que têm contas em um Terminal Server são habilitados para iniciar a sessão no servidor por padrão.

Para desabilitar o processo de conexão para um usuário, é preciso limpar a caixa ***Permitir logon no Terminal Server*** na guia ***Perfil de serviços de terminal*** na caixa Propriedades para a conta do usuário e depois clicar em ***Aplicar***. Na guia, você também pode especificar os diretórios iniciais e os perfis de usuário dos usuários.

### 1.7. new! Instalar a Conexão de Área de Trabalho Remota

A Conexão de Área de Trabalho Remota vem incluída no Windows XP e no Windows Server 2003, podendo também ser instalada em outros computadores por vários outros métodos.

- ***Utilizando ferramentas***, por exemplo, o Microsoft Systems Management Server ou o Windows 2000 Group Policy usando publicação/atribuição do RDC (.msi) baseado no Windows Installer.

- ***Compartilhamento de pasta*** %systemroot%\system32\clients\tsclient\win32 no Windows Server 2003. (Isso também pode ser feito com o Windows 2000 Server.)

- ***Instalando diretamente a partir do CD do Windows XP ou do Windows Server 2003***, usando 'Realizar tarefas adicionais' do menu Autoplay. (Não exige a instalação do sistema operacional.)

- ***Fazendo o download do Software RDC a partir de***
http://www.microsoft.com/windowsxp/remotedesktop/


© 2003 Microsoft Corporation. Todos os direitos reservados.

### 1.7.1. new! Interface aprimorada

As sessões remotas que usam a Área de Trabalho Remota podem ser realizadas em vídeo high-color e full-screen com uma barra de conexão para permitir a comutação rápida entre a sessão remota e a área de trabalho local. A conexão remota pode ser modificada de acordo com requisitos particulares e para satisfazer suas necessidades específicas, com opções de tela, recursos locais, programas e experiência. A configuração de experiência permite que você escolha sua velocidade de conexão e opções gráficas, por exemplo, animação de temas ou menu e janela para otimizar o desempenho das conexões com pouca largura de banda.

### 1.7.2. new! Redirecionamento de recursos do cliente

O redirecionamento de recursos está disponível para os clientes do Windows Server 2003 ou do Windows XP Professional e oferece uma variedade de tipos de dados a redirecionar. Para maximizar a segurança, cada tipo de redirecionamento pode ser ativado ou desativado individualmente em cada cliente ou servidor. Também é possível exibir um alerta de segurança quando for solicitado um redirecionamento do sistema de arquivos, portas ou um Cartão Inteligente, permitindo que o usuário negue o redirecionamento ou cancele a conexão se preferir.

A Área de Trabalho Remota permite reprodução de áudio (por exemplo, notificações de "erro" ou "nova mensagem de correio" podem ser redirecionadas ao cliente). Combinações de teclas, como Alt-Tab e Control-Escape, são enviadas à sessão remota por padrão, enquanto o Control-Alt-Delete é mantido sempre pelo computador do cliente para preservar a segurança do servidor. As informações de Fuso Horário também podem ser redirecionadas do servidor para os clientes, permitindo que um servidor gerencie múltiplos usuários em diferentes fusos horários. Os programas com recursos de calendário podem aproveitar o redirecionamento de Fuso Horário.

- **new! Redirecionamento do Sistema de Arquivos**

  A cópia dos arquivos entre cliente e servidor é mais fácil. Os discos do cliente, locais e de rede, agora estão disponíveis dentro da sessão do servidor. Os usuários podem ter acesso a seus próprios discos locais e transferir os arquivos entre o cliente e o servidor sem precisar sair da sessão remota.

- **new! Redirecionamento de portas e impressoras**

  Impressoras locais e de rede instaladas no cliente estão disponíveis na rede remota, com nomes simples. As portas seriais do cliente podem ser mapeadas de forma que o software no servidor possa ter acesso ao hardware conectado. Os clientes que reconhecem cartões inteligentes - Windows 2000, Windows XP e Windows CE .NET- podem fornecer credenciais de Cartões Inteligentes para o início de sessão à sessão remota no Windows Server 2003.


© 2003 Microsoft Corporation. Todos os direitos reservados.

## 1.8. Instalar aplicativos no Terminal Server

Para tornar um aplicativo disponível para múltiplos usuários, a instalação do aplicativo deve copiar os arquivos do programa para um local central do servidor, em vez da Pasta Base dos usuários.

**Nota:** para fins de segurança, recomenda-se a instalação dos aplicativos em uma partição NTFS.

***Existem dois métodos para instalar programas em um Terminal Server:***

- ***Usando Adicionar ou Remover Programas no Painel de Controle ou através do comando Change User do prompt de comando.*** O primeiro executa automaticamente o comando Change User, que é o método preferido para instalar programas em um Terminal Server.

  ***Para instalar um programa usando Adicionar ou Remover Programas, é preciso executar as seguintes etapas:***

  1. Iniciar a sessão no Terminal Server como administrador e fechar todos os programas.
  2. Clicar em ***Iniciar, Configurações*** e depois em ***Painel de Controle***.
  3. No Painel de Controle, clicar duas vezes em ***Adicionar ou Remover Programas***.
  4. Clicar duas vezes em ***Adicionar Novos Programas*** e depois em ***CD ou Floppy***.
  5. Selecionar o arquivo de instalação do aplicativo, clicar duas vezes no executável e depois clicar em ***Avançar***.
  6. Na página ***Opção de alteração de usuário***, verificar se ***Todos os usuários utilizarão configurações comuns para o aplicativo*** está selecionada.
  7. Instalar o programa no disco local segundo as instruções do programa de instalação.
  8. Seguir as instruções no assistente para concluir a instalação.

- ***Usando o comando Change User somente quando não é possível instalar o aplicativo usando Adicionar ou Remover Programas.***

  ***Para instalar um programa usando o comando Change User:***

  1. Inicie a sessão no Terminal Server como administrador e feche todos os programas.
  2. Em uma janela de linha de comando, digite ***change user /install*** e depois pressione ENTER.
  3. Instale o programa no disco local segundo as instruções do programa de instalação.
  4. Em uma janela de linha de comando, digite ***change user /execute*** quando a instalação for concluída.

Para obter mais informações:

http://www.microsoft.com/windowsserver2003/technologies/terminalservices/default.mspx


© 2003 Microsoft Corporation. Todos os direitos reservados.

## 2. Administração Remota com Área de Trabalho Remota

***A Área de Trabalho Remota para administração inclui as seguintes características e vantagens:***

- Administração gráfica dos servidores Windows Server 2003 e Windows 2000 de qualquer cliente Terminal Services. (Os clientes estão disponíveis para computadores que executem Windows para Workgroups, Windows 95, Windows 98, Windows CE 2.11, Windows CE.NET, Windows NT®, Windows 2000, Windows XP Professional e Macintosh OS-X.)

- Atualizações remotas, reinício e promoção / rebaixamento de Controladores de Domínio.

- Acesso aos servidores, utilizando conexões de baixa largura de banda, com até 128 bits de criptografia.

- Instalação e execução remotas de aplicativos, com acesso a discos e mídia locais (por exemplo, quando são copiados arquivos grandes e verificações de vírus).

- Possibilidade dos administradores remotos compartilharem uma sessão para fins de colaboração e suporte.

- Remote Desktop Protocol (RDP). Inclui impressão local e em rede, redirecionamento de sistema de arquivos, mapeamento da área de transferência (recortar, copiar e colar), redirecionamento de Cartão inteligente, redirecionamento de dispositivos em série e suporte a qualquer programa de canal virtual RDP.

### 2.1. Integrar Terminal Services

O componente Terminal Services da família Windows Server 2003 é totalmente integrado no kernel e está disponível em todas as instalações do Windows Server 2003. A ativação da Área de Trabalho Remota não exige espaço adicional no disco e tem um impacto mínimo no desempenho. São necessários apenas aproximadamente 2 megabytes (MB) de memória do servidor, com um impacto insignificante no uso da CPU. O desempenho só é afetado quando é iniciada uma sessão remota, semelhante ao custo do console.

É por esses motivos que a Microsoft recomenda ativar a Área de Trabalho Remota em todos os computadores e no Controlador de Domínio do Windows Server 2003. Isso oferecerá flexibilidade e sensibilidade substanciais na administração dos servidores de uma organização, independente da sua localização.

### 2.2. Exercício 1: Ativar a Área de Trabalho Remota

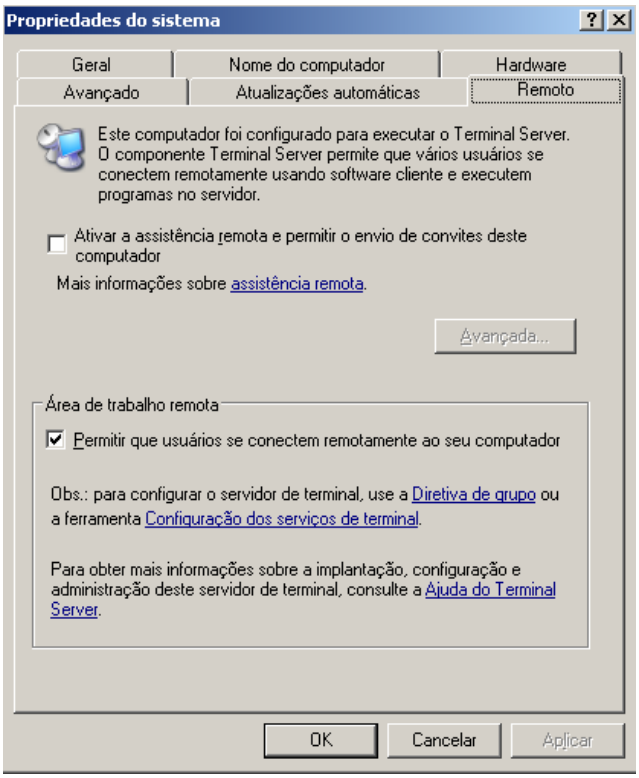
O Terminal Server e a Área de Trabalho Remota agora são configurados separadamente no Windows Server 2003, proporcionando opções mais flexíveis para a administração.

**Área de Trabalho Remota**

A Área de Trabalho Remota é instalada por padrão no Windows Server 2003, mas, por razões de segurança, vem pré-configurada desabilitada. É possível habilitá-lo em ***Sistema*** no ***Painel de Controle***.

Além das duas sessões virtuais disponíveis no modo administrativo do Terminal Services do Windows 2000, um administrador também pode se conectar remotamente ao console verdadeiro de um servidor, através da Área de Trabalho Remota no Windows Server 2003. As ferramentas que antes não funcionariam em uma sessão virtual porque interagiam com a 'sessão 0' agora funcionam remotamente.


© 2003 Microsoft Corporation. Todos os direitos reservados.




***Para ativar a Área de Trabalho Remota:***

1. No Painel de Controle, clique duas vezes em ***Sistema***.
2. Clique na guia ***Remoto*** e depois selecione a caixa ***Permitir que usuários se conectem remotamente a este computador***.
3. Clique em ***Aplicar*** e depois em ***OK***.

***Para realizar uma conexão ao Servidor:***

1. Inicie a sessão normalmente em outro equipamento com Windows XP ou Windows Server 2003.
2. Em ***Iniciar, Executar***, digite ***mstsc.exe*** e depois pressione ***ENTER***.
3. Na caixa ***Computador***, insira o nome do servidor ao qual você deseja se conectar e depois pressione ***ENTER***.

***Para realizar uma conexão ao console:***

1. Inicie a sessão normalmente em outro equipamento com Windows XP ou Windows Server 2003.
2. Em ***Iniciar, Executar***, digite ***mstsc.exe /console /v:<nomedoservidor>*** e depois pressione ***ENTER***.
3. Verifique se, logo ao iniciar a sessão do console, o servidor ao qual você se conectou bloqueou a sessão ativa.

**Lembre-se de que:** Para executar esse exercício, é preciso ter, pelo menos, duas máquinas, já que é impossível conectar o console na mesma sessão.

Para obter mais informações:

http://support.microsoft.com/default.aspx?scid=kb;en-us;323353


© 2003 Microsoft Corporation. Todos os direitos reservados.

## 2.3. Ferramentas de administração

A seguir temos uma amostra limitada das ferramentas de administração que podem ajudá-lo a controlar sessões remotas:

### Conectar com o console

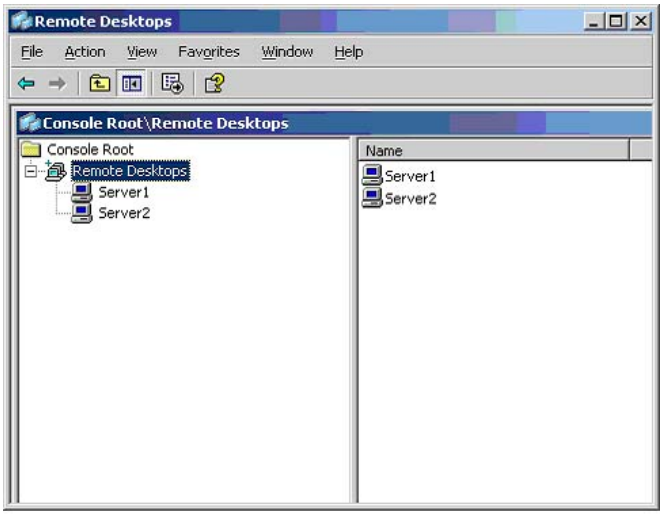
***Para conexão com o console, os administradores podem escolher um dos métodos a seguir:***

- Utilizar o snap-in Remote Desktop Microsoft Management Console (MMC).
- Executar o programa Remote Desktop Connection (mstsc.exe) com o parâmetro /console.
- Criar páginas Remote Desktop Web Connection com a propriedade ConnectToServerConsole.

### Diretiva de Grupo de Serviços de Terminal

A Diretiva de Grupo pode ser utilizada para administrar os serviços de Terminal dos computadores que executam sistemas operacionais do Windows Server. Diretivas de Grupo de Serviços de Terminal podem configurar conexões de Serviços de Terminal, de Diretivas de Usuário e de Clusters do Terminal Server, e administrar sessões de Serviços de Terminal.

### Remote Desktops MMC




O console do snap-in Remote Desktops Microsoft Management Console (MMC) permite que os administradores configurem múltiplas conexões de Serviços de Terminal. Também é útil para gerenciar vários servidores que executem o Windows Server 2003 ou o Windows 2000 Server.

Uma exibição navegável da árvore permite que os administradores vejam, controlem e alternem rapidamente entre as várias sessões de uma única janela. Como na ferramenta Conexão para Área de trabalho Remota, os computadores remotos também podem ser configurados para executar programas específicos através da conexão e para redirecionar discos locais na sessão remota. As informações de logon e a área da janela do cliente podem ser configuradas no snap-in. Da mesma forma, os administradores podem estabelecer conexões remotas para a sessão do console de um computador com sistemas operacionais Windows Server.


© 2003 Microsoft Corporation. Todos os direitos reservados.

### Gerenciador de Serviços de Terminal

Esse utilitário, tsadmin.exe, é utilizado para administrar usuários de Serviços de Terminal, sessões e processos em qualquer servidor da rede que esteja executando Serviços de Terminal. Usando essa ferramenta, você pode conectar e desconectar, fechar sessões, reiniciar e controlar remotamente as sessões. Também é possível utilizá-la para se conectar a outros servidores em domínios confiáveis, controlar sessões em um servidor remoto, enviar mensagens aos usuários ou fechar sessões e concluir processos.

### Configuração de Serviços de Terminal

Este utilitário, tscc.msc, é utilizado para modificar a configuração da criptografia por padrão e para configurar tempos de espera para redefinir e desconectar. Para configurar tempos de espera para reiniciar e desconectar contas individuais, é preciso utilizar a guia das sessões na caixa Propriedades da conta do usuário. Muitas configurações também podem ser determinadas com a Diretiva de Grupo de Serviços de Terminal ou o WMI (Windows Management Instrumentation). Nesse caso, a configuração de Serviços de Terminal é substituída.

### Visualizar Eventos

Use Visualizar Eventos, eventvwr.msc, para pesquisar os acontecimentos que podem ter ocorrido, como caixas de diálogo pop-up no console do servidor.

### Utilitários de Linha de Comando

***Utilitários de linha de comando incluem o seguinte:***

- ***Query User.*** É um utilitário de linha de comando que lista usuários ativos e desconectados.

- ***Disconnect.*** Esse utilitário de linha de comando, tsdiscon, desconecta a sessão. Um procedimento analógico apaga o monitor e deixa o computador em funcionamento. A desconexão também pode ser feita em Iniciar/Desligar. Para reconectar à sessão, inicie-a no servidor, outra vez com o mesmo usuário a partir da Conexão para Área de Trabalho Remota.


© 2003 Microsoft Corporation. Todos os direitos reservados.

## 3. Terminal Server como Servidor de Aplicativos

O componente de Serviços de Terminal do Microsoft® Windows® Server 2003 é estruturado em uma base sólida proporcionada pelo Modo de Servidor de Aplicativo do Windows 2000 Terminal Services, e inclui os novos recursos do cliente e do protocolo no Windows XP. Os Serviços de Terminal permitem fornecer virtualmente aplicativos baseados no Windows ou na área de trabalho do Windows, para qualquer dispositivo, incluindo os que não podem executar o Windows.

Os Serviços de Terminal no Windows Server 2003 podem aperfeiçoar os recursos de instalação do software de uma empresa em uma variedade de cenários, proporcionando uma flexibilidade substancial à infra-estrutura e à administração de aplicativos. Quando um usuário executa um aplicativo no Terminal Server, a execução do aplicativo ocorre no servidor e somente as informações de teclado, mouse e vídeo são transmitidos na rede. Cada usuário vê somente a sua sessão individual, que é administrada de forma transparente pelo sistema operacional do servidor e é independente de qualquer outra sessão do cliente.

### 3.1. Benefícios

Os Serviços de Terminal no Windows Server 2003 fornecem três benefícios importantes:

| Benefício | Descrição |
|---|---|
| Instalação rápida e centralizada de aplicativos | O Terminal Server é ótimo para instalar rapidamente aplicativos baseados no Windows em toda a empresa, especialmente que são utilizados com freqüência ou são de administração difícil. |
| Acesso a dados utilizando conexões de baixa largura de banda | O Terminal Server reduz consideravelmente a largura de banda exigida na rede para ter acesso a dados remotamente. Usar o Terminal Server para executar um aplicativo em conexões de baixa largura de banda, por exemplo, discagem direta ou compartilhamentos de enlaces da WAN, é muito eficaz para fornecer acesso remoto e manipular grandes quantidades de dados, considerando que somente a tela de dados é transferida, e não os próprios dados. |
| Windows em qualquer parte | O Terminal Server ajuda os usuários a serem mais produtivos, possibilitando o acesso aos programas atuais em qualquer dispositivo. |

### 3.2. new! Recursos Adicionais de Administração

***Os recursos a seguir aumentam a flexibilidade dos Serviços de Terminal no Windows Server 2003:***

***Diretiva de Grupo*** A Diretiva de Grupo pode ser atualizada para controlar as propriedades dos Serviços de Terminal. Isso permite a configuração simultânea dos grupos de servidores, incluindo a configuração dos novos recursos, por exemplo, caminho de perfil de Serviços de Terminal por computador, e desabilita o papel de parede, visto que eles estão conectados remotamente.

***Windows Management Interface Provider.*** Um fornecedor completo do Windows Management Instrumentation (WMI) permite a configuração por meio de scripts de Serviços de Terminal. Diversos alias do WMI são incluídos para fornecer um front-end simples de tarefas freqüentes, usando o WMI.

***Gerenciamento de Impressoras. O gerenciamento de impressoras foi aprimorado das seguintes formas:***

- O mapa de drivers de impressora foi aperfeiçoado:
- Quando um driver não corresponde ao cliente, é fornecido um Caminho para Drivers que permite especificar outros drivers de impressora padrão, que são adicionados aos servidores de Terminal.
- O fluxo de impressão é comprimido para melhorar o desempenho em enlaces lentos entre um servidor e um cliente.


© 2003 Microsoft Corporation. Todos os direitos reservados.

### Gerenciador de Serviços de Terminal

O Gerenciador de Serviços de Terminal aprimorado permite uma administração mais fácil de uma grande diversidade de servidores, reduzindo a enumeração automática do servidor. Isso dá acesso direito aos servidores especificados por nome e fornece uma lista dos servidores preferidos.

### Gerenciador do Terminal Server.

O Gerenciador de Licenças do Terminal Server foi aprimorado para facilitar a ativação de um Servidor de Licenças do Terminal Server e atribuir as licenças.

### Diretiva de Sessão Única

Configurando a Diretiva de Sessão Única, o administrador pode limitar os usuários a uma única sessão, independente de ela estar ativa ou não (exatamente como em um grupo de servidores).

### Mensagens de Erro do Cliente

Mais de 40 novas mensagens de erro de cliente facilitam o diagnóstico de problemas da conexão do cliente.

## 3.3. Aprimoramentos na Segurança

O modelo de acesso ao Terminal Server agora se adapta melhor aos paradigmas de administração do Windows Server.

### Grupo de Usuários da Área de Trabalho Remota

Em vez de adicionar usuários a uma lista no programa Configuração dos serviços de Terminal (TSCC), você simplesmente os tornará membros do grupo Remote Desktop Users (RDU). Por exemplo, o administrador pode adicionar o grupo "Usuários do domínio" ao grupo RDU para permitir que todos tenham acesso ao Terminal Server.

Usar um grupo verdadeiro do NT também significa que o acesso aos Terminal Servers pode ser controlado através da Diretiva de Grupo nos grupos de servidores.

### Editor de Diretiva de Segurança.

Para configurações adicionais em Serviços de Terminal, os direitos de usuário podem ser atribuídos a todos os usuários ou a grupos individuais, usando o Editor de Diretiva de Segurança. Dessa forma, você oferece aos usuários a capacidade de iniciar a sessão no Terminal Server, sem precisar ser um membro do grupo Usuários de Área de Trabalho Remota descrita acima.

### Criptografia de 128 bits

Por padrão, as conexões aos Terminal Servers garantem criptografia RC4 bidirecional com 128 bits quando está sendo utilizado um cliente que oferece suporte de 128 bits. (RDC é de 128 bits por padrão). É possível conectar clientes mais antigos com criptografia inferior a 128 bits, a menos que se especifique que somente os clientes de alta criptografia sejam habilitados.

### Diretivas de Restrição de Software

As diretivas de restrição de software no Windows Server 2003 permitem que os administradores utilizem Diretivas de Grupo para simplificar o bloqueio de Terminal Servers, permitindo que apenas determinados programas sejam executados pelos usuários especificados.


© 2003 Microsoft Corporation. Todos os direitos reservados.

Para obter mais informações:

http://www.microsoft.com/windowsxp/pro/techinfo/administration/restrictionpolicies/default.asp

Este recurso do Windows substitui a ferramenta AppSec (Segurança de Aplicativo) utilizada em versões anteriores dos Serviços de Terminal.

### 3.4. Diretório de Sessão

Os Terminal Servers podem ser organizados em grupos. Essa configuração permite clusters utilizando Balanceamento de Carga em Rede (NLB) nos computadores para oferecer a seus usuários um serviço de tolerância a falhas.

O novo recurso Diretório de Sessão nos Serviços de Terminal permite que os usuários reconectem-se a uma sessão específica desconectada do grupo, dirigindo-se a um servidor carregado quando conectada.

O Session Directory pode utilizar o serviço de Equilíbrio de Carga do Windows ou um Equilibrador de Cargas de terceiros e o serviço pode funcionar em qualquer computador com o Windows Server 2003. No entanto, os membros do grupo do Terminal Server devem estar executando o Windows Server 2003, Enterprise Edition.

### 3.5. Exercício 2: Instalação de Aplicativo de Terminal Server

Durante este exercício, você instalará um Terminal Server para executar aplicativos.

1. No Painel de Controle, clique duas vezes em ***Adicionar ou Remover Programas*** e depois em Windows Componentes.
2. Selecione ***Terminal Server*** e depois clique me ***Avançar***.
3. Aceite a configuração padrão e clique em ***Avançar***.
4. Ao finalizar a instalação, clique em ***Concluir***.

Para instalar aplicativos, siga as instruções na seção 1.8 do capítulo. Lembre-se de que é possível instalar, por exemplo, o Microsoft Office XP. Para instalar o Microsoft Office 2000, será necessário o Resource Kit do Office 2000.

### 3.6. new! Windows System Resource Manager

O Windows Server 2003 introduz um novo produto que não é fornecido no CD do Windows Server 2003. Essa ferramenta é compatível apenas com as versões Enterprise e Datacenter.

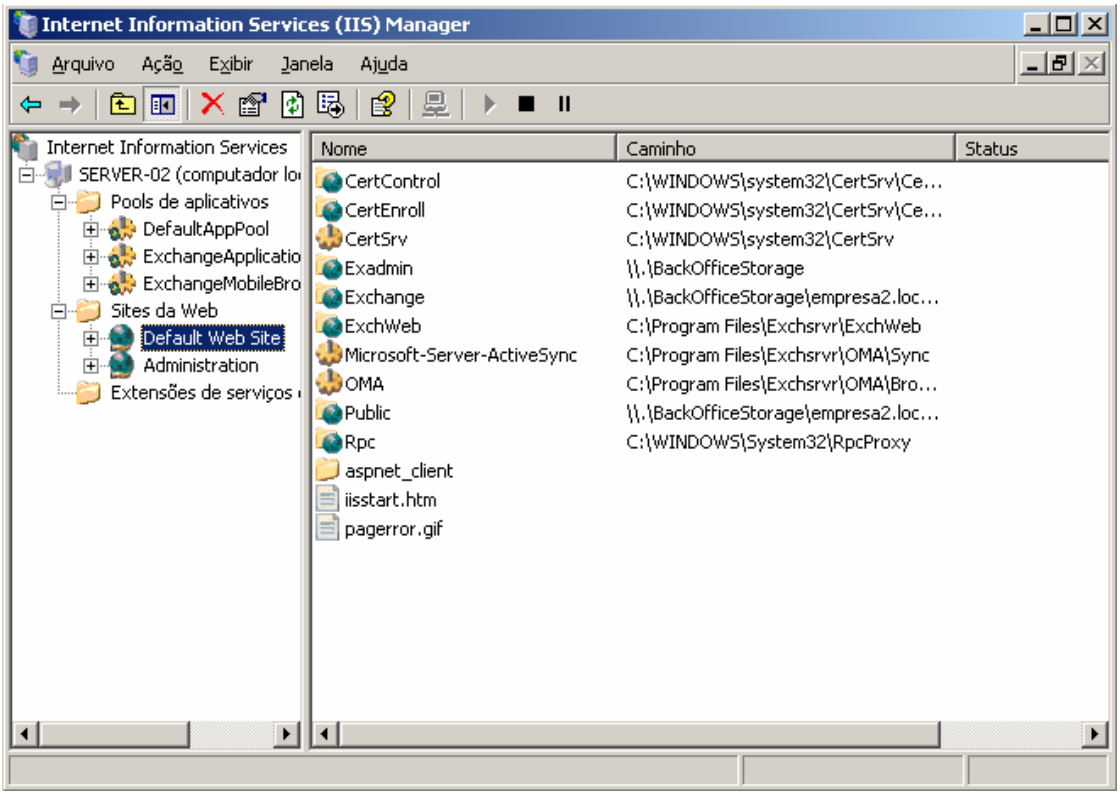
O Windows System Resource Manager (WSRM) permite administrar recursos de hardware, por exemplo, memória e processador, atribuindo aos usuários recursos preestabelecidos. Dessa forma, você pode evitar que um usuário consuma muitos recursos, executando tarefas desnecessárias ou múltiplos processos sem limite de recursos. Também é possível atribuir aos recursos uma agenda de horários, por exemplo, atribuir durante o dia uma quantidade de recursos limitada e, em horário noturno, um limite superior ou nenhum limite, conforme o caso.

Para obter mais informações e fazer o download:

http://www.microsoft.com/windowsserver2003/downloads/wsrm.mspx


© 2003 Microsoft Corporation. Todos os direitos reservados.

# Capitulo 7
# Implementação e Configuração de IIS 6.0




***Neste capitulo, você obterá conhecimentos sobre os serviços Web e, ao concluí-lo, poderá:***

- Implementar Serviços Web
- Instalar o IIS6
- Administrar um ambiente de Serviços Web


© 2003 Microsoft Corporation. Todos os direitos reservados.

## 1. Introdução

Os serviços do Microsoft Internet Information Server (IIS) 6.0 com o Windows Server 2003 fornecem recursos de servidor da Web integrados, confiáveis, escaláveis, seguros e administráveis em uma intranet, uma extranet ou na Internet. O IIS 6.0 incorpora aperfeiçoamentos significativos na arquitetura para atender às necessidades de clientes em várias partes do mundo.

### 1.1. Vantagens

O IIS 6.0 e o Windows Server 2003 introduzem vários recursos novos de administração, disponibilidade, confiabilidade, segurança, rendimento e escalabilidade nos servidores de aplicações da Web. O IIS 6.0 também aprimora o desenvolvimento de aplicativos da Web e a compatibilidade internacional. Juntos, o IIS 6.0 e o Windows Server 2003 proporcionam a solução para servidores da Web mais confiável, produtiva, conectada e integrada disponível.

| Vantagem | Descrição |
|---|---|
| *Confiável e escalável* | O IIS 6.0 proporciona um ambiente de servidor da Web mais inteligente e confiável para fornecer uma confiabilidade ótima. Esse novo ambiente inclui a supervisão do estado dos aplicativos e a sua reciclagem automática. As características de confiabilidade aumentam a disponibilidade e reduzem o tempo que os administradores desperdiçavam para reiniciar os serviços da Internet. O IIS 6.0 está ajustado para proporcionar possibilidades de consolidação e escalabilidade otimizadas que aproveitam ao máximo cada servidor da Web. |
| *Seguro e administrável* | O IIS 6.0 proporciona segurança e capacidade de administração significativamente aprimoradas. Os aprimoramentos de segurança incluem mudanças tecnológicas no processamento de solicitações. Além disso, também foram aprimoradas a autenticação e a autorização. A instalação pré-configurada do IIS 6.0 está completamente bloqueada, o que significa que a configuração padrão oferece segurança máxima. O IIS 6.0 também fornece recursos de administração aprimorados. Uma administração melhor com a metabase XML e novas ferramentas de linha de comandos. |
| *Desenvolvimento e compatibilidade internacionais aprimorados* | Com o Windows Server 2003 e o IIS 6.0, os desenvolvedores de aplicativos beneficiam-se de um único ambiente de armazenamento de aplicativos integrado, com compatibilidade total com os recursos avançados e com o cache em modo de núcleo. Criado no IIS 6.0, o Windows Server 2003 oferece aos desenvolvedores níveis elevados de funcionalidade adicional, incluindo um desenvolvimento de aplicativos rápido e uma ampla seleção de linguagens. O IIS 6.0 também oferece compatibilidade internacional com os padrões Web mais recentes da Web. |


© 2003 Microsoft Corporation. Todos os direitos reservados.

## 1.2. new! Aprimoramentos e novos recursos

***O Windows Server 2003 proporciona novos recursos e aprimoramentos em três áreas principais:***

- Confiabilidade e escalabilidade
- Segurança e capacidade de administração
- Melhor desenvolvimento e compatibilidade internacional

### 1.2.1. Confiabilidade e escalabilidade

O Windows Server 2003 oferece os recursos a seguir para proporcionar uma confiabilidade e uma escalabilidade aprimoradas.

| Recurso | Descrição |
|---|---|
| ***Nova arquitetura de processamento de solicitações*** | Com uma nova arquitetura de processamento de solicitações, o ISS 6.0 detecta automaticamente as perdas de memória, as falhas de acesso e outros erros. Quando ocorrem essas condições, a arquitetura subjacente oferece tolerância a erros e capacidade de reiniciar processos quando necessário. Enquanto isso, o IIS 6.0 continua colocando as solicitações na fila sem interromper a atividade do usuário. |
| ***Detecção do estado*** | O IIS 6.0 é capaz de supervisionar o estado dos processos de trabalho, dos aplicativos e dos sites da Web. Da mesma forma, é possível detectar o estado dos processos de trabalho e reciclá-los conforme diversos fatores, como o rendimento, um planejamento específico, o número de solicitações e o consumo de memória. Também é possível reciclar os processos de trabalho sob demanda. |
| ***Escalabilidade dos sites*** | O IIS 6.0 aprimorou a forma como o sistema operacional utiliza os recursos internos. Por exemplo, o IIS 6.0 não localiza previamente os recursos durante a inicialização. É possível armazenar muitos outros sites em um único servidor que execute o IIS 6.0 e um grande número de processos de trabalho pode estar ativo de forma simultânea. A inicialização e o desligamento de um servidor são processos mais rápidos em comparação a versões anteriores do IIS. Todos esses aprimoramentos contribuem para aumentar a escalabilidade dos sites com o IIS 6.0. |
| ***Novo controlador em modo de núcleo, HTTP.SYS*** | O Windows Server 2003 introduz um novo controlador no modo kernel, o HTTP.SYS, para a análise e o cache de HTTP, melhorando a escalabilidade e o rendimento. O IIS 6.0 foi criado sobre o HTTP.SYS e está ajustado especificamente para aumentar o rendimento do servidor da Web. Além disso, o HTTP.SYS processa diretamente solicitações no kernel, sob determinadas circunstâncias. |


© 2003 Microsoft Corporation. Todos os direitos reservados.

### 1.2.2. new! Segurança e recurso de administração

O Windows Server 2003 traz os seguintes recursos para proporcionar segurança e escalabilidade aprimoradas.

| Recurso | Descrição |
|---|---|
| ***Servidor bloqueado*** | O IIS 6.0 proporciona uma segurança significativamente aprimorada. Para reduzir a superfície de ataque dos sistemas, o IIS 6.0 não é instalado como padrão no Windows Server 2003; os administradores precisam selecioná-lo e instalá-lo de forma explícita. O IIS 6.0 é fornecido em estado bloqueado e serve unicamente ao conteúdo estático. Através do uso do nó da extensão de serviços da Web, os administradores de sites da Web podem ativar ou desativar a funcionalidade do IIS conforme as necessidades individuais da organização. |
| ***Autorização*** | O IIS 6.0 amplia o uso de um novo marco de autorização fornecido com o Windows Server 2003. Além disso, os aplicativos da Web podem utilizar a autorização de endereços URL, formando pares com o Administrador de autorizações para controlar a obtenção de acesso. A autorização delegada e restrita proporciona agora aos administradores de domínio o controle para delegar unicamente serviços e máquinas específicas. |
| ***Metabase XML*** | A metabase de texto do IIS 6.0, com formato XML, proporciona recursos aprimorados de cópia de segurança e restauração para os servidores com erros críticos. Também proporciona recuperação de erros da metabase e uma solução de problemas aprimorada. A modificação direta, mediante ferramentas comuns de modificação de texto, proporciona uma maior capacidade de administração. |

### 1.2.3. new! Desenvolvimento e compatibilidade internacionais aprimorados

O Windows Server 2003 proporciona as características a seguir para obter desenvolvimento e compatibilidade aprimorados.

| Recurso | Descrição |
|---|---|
| ***Integração do IIS e do ASP.NET*** | O Windows Server 2003 oferece uma experiência aprimorada para o desenvolvedor com a integração do IIS e do Microsoft ASP.NET. Criados a partir do IIS 6.0, os aprimoramentos do Windows Server 2003 oferecem aos desenvolvedores níveis elevados de funcionalidade, como o desenvolvimento de aplicativos rápido (RAD) e uma ampla seleção de idiomas. No Windows Server 2003, a experiência de utilizar ASP.NET e Microsoft .NET Framework foi aprimorada porque a arquitetura de processamento de solicitações integra-se ao IIS 6.0. |
| ***Informações compartilhadas através dos limites geográficos*** | Compartilhar informações através de limites geográficos, em uma grande variedade de idiomas, torna-se cada vez mais importante na economia global. Antes, a estrutura no Unicode do protocolo HTTP limitava os desenvolvedores ao sistema das páginas de códigos. Agora com os endereços URL codificados em UTF-8 (Formato de transformação de Unicode 8), o uso de Unicode já é possível. Esse é um aprimoramento que permite trabalhar com idiomas mais complexos, como o chinês. O IIS 6.0 permite que os clientes obtenham acesso às variáveis do servidor em Unicode. Também adiciona novas funções de compatibilidade com o servidor que permitem que o desenvolvedor obtenha acesso à representação em Unicode de um endereço URL e, com isso, melhore a compatibilidade internacional. |

Para obter mais informações:

http://www.microsoft.com/windowsserver2003/iis/default.mspx


© 2003 Microsoft Corporation. Todos os direitos reservados.

## 2. O IIS como servidor de aplicativos

***O servidor de aplicativos é uma nova função do Windows Server 2003, aliado às seguintes tecnologias:***

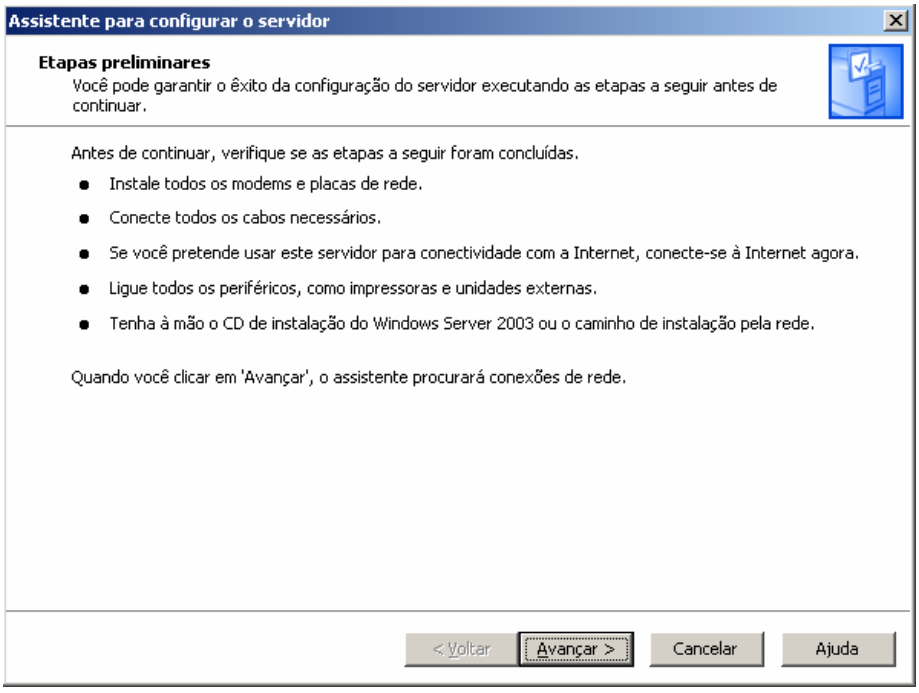
- Internet Information Services (IIS) 6.0
- Microsoft .NET Framework
- ASP.NET
- ASP
- UDDI Services
- COM+
- Microsoft Message Queuing (MSMQ)

A função do servidor de aplicativos combina essas tecnologias em uma experiência coesa, permitindo que os desenvolvedores e administradores da Web disponham de aplicativos dinâmicos, por exemplo, um aplicativo de banco de dados do Microsoft ASP.NET, sem necessidade de instalar qualquer outro software no servidor.

### Configuração do servidor de aplicativos

O servidor de aplicativos é configurável em dois pontos do Windows Server 2003: no assistente Configurar o Servidor e no aplicativo Adicionar ou Remover Componentes.

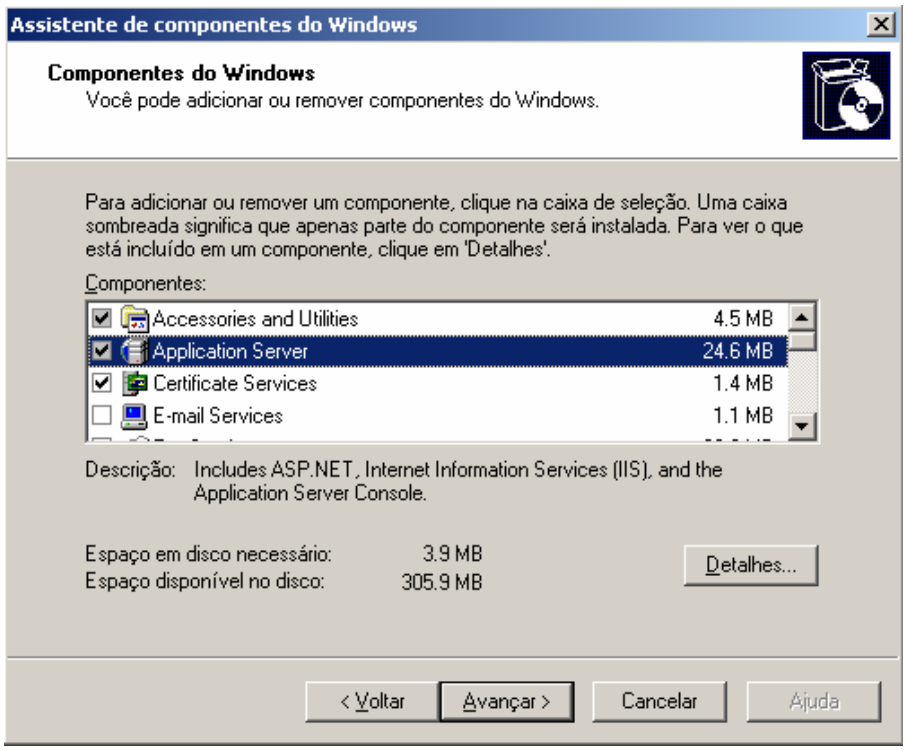
***O assistente para configurar seu servidor***

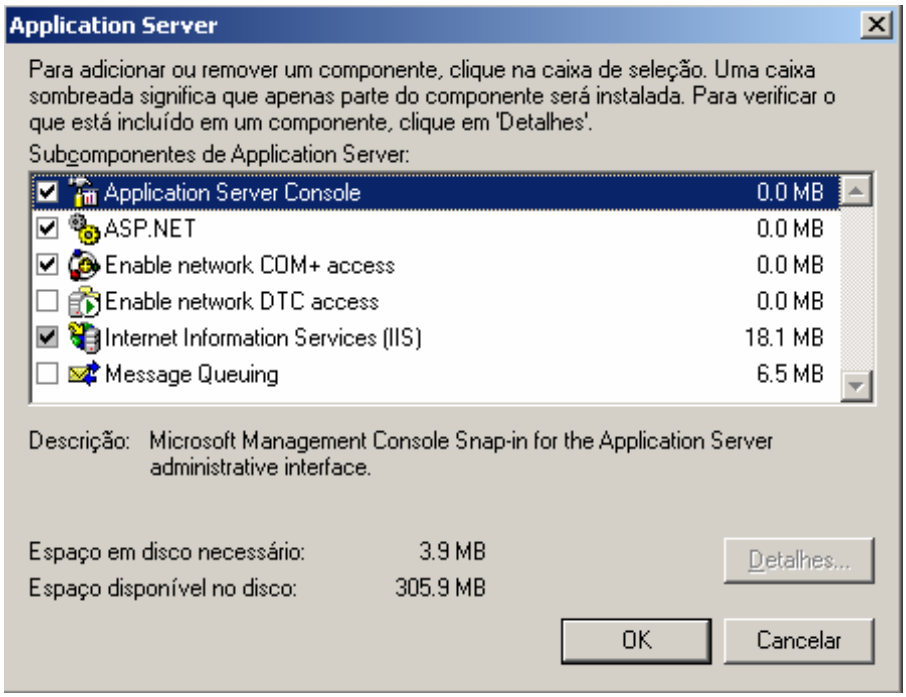



O assistente Configurar o Servidor é o ponto central para configurar funções no Windows Server 2003 e agora inclui a função de servidor de aplicativos. Para ter acesso ao assistente Configurar o Servidor, clique em Adicionar ou Remover Funções no assistente Configurar o Servidor. Essa função substitui a função existente do servidor da Web. Depois de instalar essa nova função, a página Manage Your Server também incluirá uma entrada para a nova função.


© 2003 Microsoft Corporation. Todos os direitos reservados.

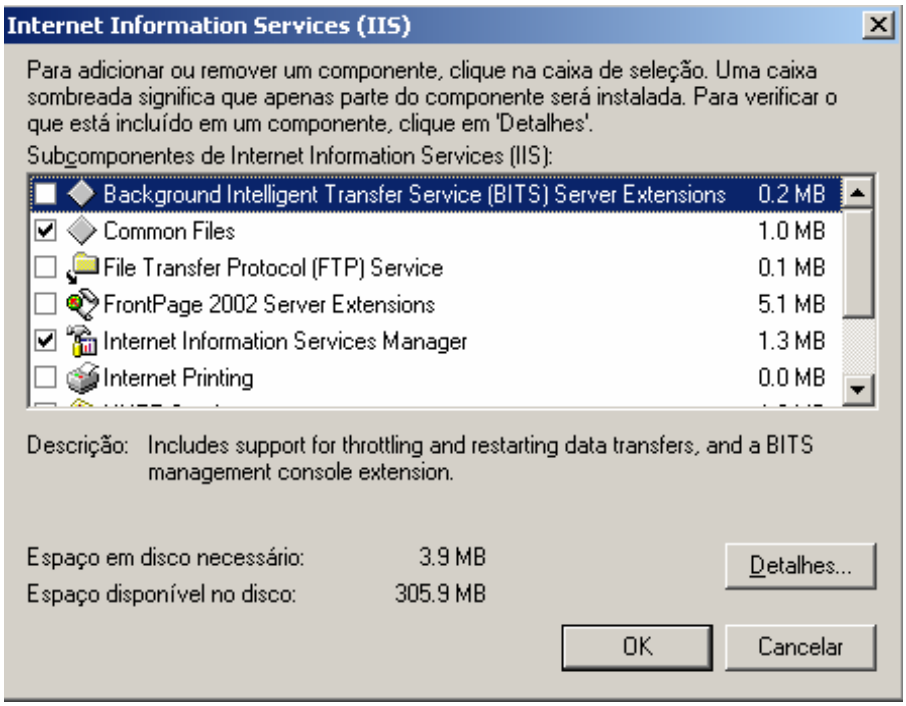
*Adicionar/Remover Componentes do Servidor de Aplicativo*





© 2003 Microsoft Corporation. Todos os direitos reservados.




O servidor de aplicativos também foi incluído no Adicionar ou Remover Componentes do Windows Server 2003 como componente opcional de alto nível. Da mesma forma, os aplicativos do servidor de aplicativos (IIS 6.0, ASP.NET, COM+ e MSMQ) podem ser instalados e configurar os componentes secundários usando Adicionar ou Remover Componentes. Usando Adicionar ou Remover Componentes para configurar o servidor de aplicativos, é possível ter maior controle sobre os componentes secundários específicos que serão instalados.

## 2.1. new! Arquitetura IIS 6.0 - Nova arquitetura de processamento de Solicitação

Os sites da Web e o código de aplicativos estão ficando cada vez mais complexos. Os sites dinâmicos e os aplicativos da Web podem conter código imperfeito que consuma memória ou provoque erros como, por exemplo, violações de acesso. Portanto, um servidor da Web deve ser o responsável ativo pelo ambiente de execução do aplicativo e automaticamente detectar e responder aos erros do aplicativo.

Quando ocorre um erro de aplicativo, o servidor deve ser tolerante a falhas, o que significa que deve reciclar e reiniciar automaticamente o aplicativo responsável, enquanto continua colocando em fila as solicitações para o aplicativo, sem interrupção para o usuário. É por isso que o IIS 6.0 oferece uma nova arquitetura tolerante a falhas de processamento de solicitações que foi desenvolvida para proporcionar um controle ativo do tempo de execução e um aumento expressivo da confiabilidade e da escalabilidade, combinando um novo modelo de processamento isolado chamado *Worker Process Isolation Mode*. Ele traz grandes aprimoramentos no funcionamento como, por exemplo, Fila e Cache em Modo Kernel.

A versão anterior do IIS, o IIS 5.0, foi desenvolvida para ter um processo chamado Inetinfo.exe, que era o processo principal do servidor da Web. Comparativamente, para o IIS 6.0, foram desenvolvidos dois novos componentes: o stack do protocolo http em modo kernel (HTTP.sys) e o componente de administração e monitoramento em modo usuário. Essa arquitetura permite que o IIS 6.0 separe as operações do servidor da Web do processo do site da Web e do código do aplicativo - sem sacrificar o desempenho.

- new! ***HTTP.sys.*** O stack do protocolo http em modo kernel coloca em fila e divide as solicitações HTTP recebidas. Quando chega a vez da solicitação, ela é colocada em cache e retorna o conteúdo do site, e o aplicativo. HTTP.sys não carrega nenhum código de aplicativo, simplesmente divide e encaminha as solicitações.

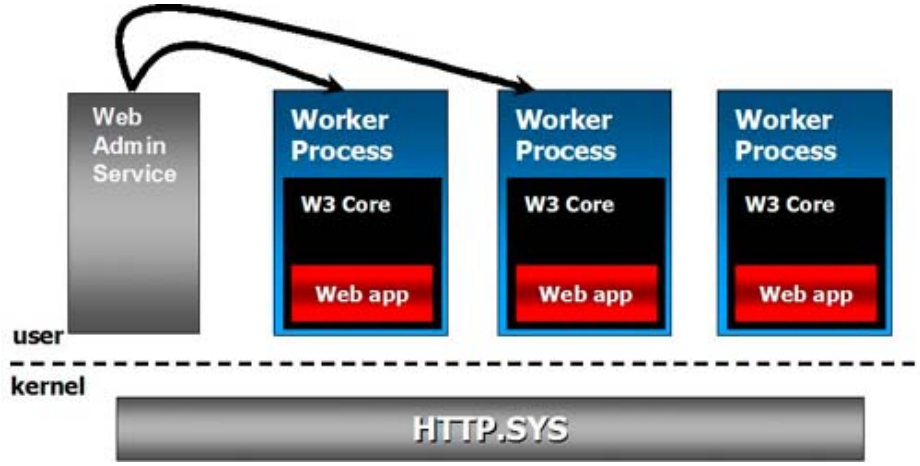

© 2003 Microsoft Corporation. Todos os direitos reservados.

- new! ***Componente de administração e monitoramento do serviço WWW.*** O Gerenciador de Processos e Configurações em modo usuário administra as operações do servidor e supervisiona a execução do código do aplicativo. Como o HTTP.sys, este componente não carrega e nem processa nenhum código de aplicativo.

Antes abordar esses componentes, é importante introduzir os novos conceitos do IIS 6.0: Grupos de Aplicativos e Processos de Trabalho.

new! ***Os grupos (pools) de aplicativos*** são utilizados para administrar sites e aplicativos na Web. Cada Grupo de Aplicativos corresponde a uma fila de solicitação no HTTP.sys e aos processos do Windows responsáveis por executar essas solicitações. O IIS 6.0 pode oferecer suporte a até 2.000 grupos de aplicativos por servidor e pode ter múltiplos Grupos de Aplicação funcionando ao mesmo tempo. Por exemplo, um servidor de departamento pode ter o RH em um Grupo de Aplicativos e o departamento financeiro em outro Grupo. Da mesma forma, um provedor de serviços da Internet (ISP) pode ter sites da Web e aplicativos de um cliente em um grupo de aplicativos e os sites da Web de outro cliente em um Grupo de Aplicativos diferente. Os Grupos de Aplicativos são separados por limites de processamento no Windows Server 2003. Portanto, um aplicativo em um Grupo de Aplicativo não é afetado pelos aplicativos em outros Grupos de Aplicativos, e uma solicitação do aplicativo não pode ser encaminhada a outro grupo de aplicativos. Os aplicativos também podem ser facilmente atribuídos a outros grupos de aplicativos enquanto o servidor está em funcionamento.

new! ***Um Worker Process*** executa pedidos de serviços dos sites da Web e aplicativos em um Grupo de Aplicativos. Todos os processos de aplicativos da Web, incluindo o carregamento dos filtros e das extensões ISAPI, assim como a autenticação e a autorização, são executados por um novo serviço WWW DLL, no qual se carrega um ou mais Worker Processes. O Worker Process executável chama-se W3wp.exe.




## 2.2. HTTP.sys

No IIS 6.0, o HTTP.sys escuta as solicitações e as coloca nas filas apropriadas. Cada fila de solicitações corresponde a um Grupo de Aplicativos. Considerando que nenhum código de aplicativo funciona no HTTP.sys, ele não pode ser afetado por falhas no código do Modo Usuário, que normalmente afetam o estado de Serviços da Web. Se um aplicativo falhar, o HTTP.sys continua aceitando e colocando as novas solicitações na fila apropriada até que um dos seguintes eventos ocorra: o processo seja reiniciado e comece a aceitar solicitações, não haja filas disponíveis, não haja espaço nas filas ou o próprio serviço da Web seja fechado pelo administrador. Como o HTTP.sys é um componente de modo Kernel, a operação realizada é especialmente eficiente, permitindo que a arquitetura do IIS 6.0 combine o isolamento do processo com o alto desempenho ao solicitar processos.

Quando o serviço de WWW notar que o aplicativo falhou, se algum tiver solicitações especiais aguardando para serem inseridas no Worker Process de um Grupo de Aplicativos, um novo Worker Process é iniciado.


© 2003 Microsoft Corporation. Todos os direitos reservados.

Portanto, embora possa haver uma interrupção temporária no processo da solicitação do modo de usuário, o usuário não percebe a falha porque as solicitações continuam sendo aceitas e colocadas em filas.

## 2.3. Componente de Administração e Monitoramento do Serviço WWW

O componente WWW Service Administration and Monitoring melhora uma parte básica do serviço WWW. Como no HTTP.sys, nenhum código do aplicativo funciona no componente WWW Service Administration and Monitoring. Este componente tem responsabilidades primárias: configuração do sistema e administração do Worker Process.

### Configuração de Servidor

Durante a inicialização, o Gerenciador de Configuração do serviço WWW utiliza a configuração na memória da metabase para inicializar a tabela de caminhos do Espaço de Nomes do HTTP.sys. Cada entrada na tabela de caminhos contém informações para direcionar os URLs inseridos no Grupo de Aplicativos do aplicativo associado ao URL. Esses passos de pré-registro informam ao HTTP.sys que há um Grupo de Aplicativos para responder às solicitações em uma parte específica do Espaço para Nomes, e esse HTTP.sys pode solicitar que um Worker Process seja iniciado para um Grupo de Aplicativos quando chegar uma solicitação.

## 2.4. Gerenciamento de Worker Processes

Na função Worker Process Management, o componente de monitoramento e administração do serviço WWW é responsável por controlar o andamento do Worker Process que processa as solicitações. Isso inclui a determinação de quando começar, reciclar ou reiniciar um Worker Process se ele não puder mais processar as solicitações (for bloqueado). Ele também é responsável pela supervisão dos Worker Processes e por detectar quando um deles é finalizado inesperadamente.

## 2.5. Modo de Isolamento do Worker Process

O IIS 6.0 introduz um novo modo de isolamento de aplicativos para controlar o processo de sites da Web e aplicativos: o modo de Isolamento do Worker Process. Ele funciona em todo o código do aplicativo em um ambiente isolado. Os aplicativos podem ser totalmente isolados um do outro, onde um erro em um aplicativo não afeta outro em um processo usando Grupos de Aplicativos. As solicitações são retiradas diretamente do Kernel, em vez de criar um processo Modo de Usuário e encaminhar a outros processos Modo de Usuário. Primeiro, o HTTP.sys encaminha o site da Web e as solicitações do aplicativo ao Grupo de Aplicativos correto. Em seguida, os Worker Processes que servem ao Grupo de Aplicativos enviam as solicitações diretamente da fila do aplicativo em HTTP.sys. Este modelo elimina os saltos de processo desnecessários durante o envio de uma solicitação fora do processo DLLHost.exe (exatamente como no IIS 4.0 e 5.0), e aumenta o desempenho.

O Modo de Isolamento do Worker Process evita que um aplicativo ou site interrompa outro. Além disso, separar os aplicativos ou os sites em Worker Processes diferentes simplifica o número de tarefas administrativas, por exemplo, coloca um site/aplicativo on-line ou offline (independentemente de todos os outros site/aplicativos em execução no sistema).

Para mais informações sobre o IIS 6.0 com servidor de aplicativos:

http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windowsserver2003/proddocs/standard/iiswelcome.asp


© 2003 Microsoft Corporation. Todos os direitos reservados.

## 3. Aprimoramento na Segurança

A segurança sempre foi um aspecto importante do Internet Information Services. Entretanto, nas versões anteriores do produto (ex. O IIS 5.0 no Windows 2000 Server), o servidor não era enviado no estado "bloqueado" por padrão. Muitos serviços desnecessários, por exemplo, impressão pela Internet eram ativados na instalação.

Tornar o sistema mais resistente era um processo manual e muitas organizações simplesmente mantinham os ajustes do servidor sem modificação. Isso provocou uma grande vulnerabilidade a ataques porque, embora os servidores pudessem se tornar seguros, muitos administradores não fizeram o que precisavam ou não tinham as ferramentas para fazê-lo.

É por isso que a Microsoft aumentou significativamente seu foco em segurança desde o desenvolvimento de versões anteriores do IIS. Por exemplo, no início de 2002, o trabalho de desenvolvimento de todos os engenheiros do Windows – mais de 8.500 pessoas – foi suspenso enquanto a companhia realizava um treinamento intensivo sobre segurança. Quando o treinamento terminou, as equipes de desenvolvimento analisaram a base do código do Windows, incluindo o HTTP.sys e o IIS 6.0, para colocar o conhecimento adquirido em prática. Isso representou um investimento substancial no aumento da segurança da plataforma do Windows. Além disso, durante a fase de projeto do produto, a Microsoft realizou um teste de ameaça para garantir que os desenvolvedores de software da empresa tinham entendido o tipo de ataque que o servidor poderia sofrer em implementações do cliente. Da mesma forma, os especialistas de terceiros realizaram análises independentes na segurança do código.

### 3.1. new! Servidor Bloqueado.

Para reduzir a superfície de ataque da infra-estrutura da Web, a instalação do Windows Server 2003 não instala o IIS 6.0 por padrão. Os administradores precisam selecionar e instalar explicitamente o IIS 6.0 em todos os produtos do Windows Server 2003, exceto no Windows Server 2003 Web Edition. Isso significa que agora o IIS 6.0 não precisa ser desinstalado depois que o Windows tiver sido instalado se não for necessário para a função do servidor (por exemplo, se o servidor for instalado para funcionar como servidor de correio ou banco de dados). O IIS 6.0 também será desativado quando um servidor migrar para o Windows Server 2003, a menos que a Ferramenta de Bloqueio do IIS 5.0 esteja instalada antes da migração ou tenha sido configurada uma chave de registro. Além disso, o IIS 6.0 é configurado, por padrão, no estado "bloqueado" quando instalado. Depois da instalação, o IIS 6.0 aceita somente as solicitações de arquivos estáticos até ser configurado para o conteúdo dinâmico. Todos os tempos de espera e ajustes são corrigidos para evitar problemas sérios de segurança. O IIS 6.0 também pode ser desativado usando as Diretivas de Grupo do Windows Server 2003.

### 3.2. new! Múltiplos Níveis de Segurança

A seguinte tabela resume os múltiplos níveis de segurança disponíveis no IIS 6.0.

| Nível de Segurança do IIS 6.0 | Descrição |
|---|---|
| Não instalado por padrão no Windows Server 2003 | Grande parte da segurança deve-se à redução da superfície de ataque do seu sistema. Portanto, o IIS 6.0 não é instalado, por padrão, no Windows Server 2003. Os administradores devem selecionar e instalar explicitamente o IIS 6.0. |
| Instalação no estado bloqueado | Por padrão, a instalação do IIS 6.0 fornece apenas a funcionalidade mínima. Somente os arquivos estáticos funcionam, enquanto outros (por exemplo, o ASP e o ASP.NET) precisam ser ativados explicitamente pelos administradores. |
| Desativação em atualizações | Em atualizações do Windows Server 2003 para servidores com o IIS instalado, se o servidor não instalou e não executou a ferramenta Lockdown Tool e não configurou a chave do registro ***RetainW3SVCStatus*** no servidor que foi atualizado, o IIS 6.0 será instalado no estado desativado. |


© 2003 Microsoft Corporation. Todos os direitos reservados.

| | |
|---|---|
| Desativação via Diretiva de Grupo | Com o Windows Server 2003, os administradores do domínio podem informar os usuários sobre a instalação do IIS 6.0 em seus computadores. |
| Conta com baixo privilégio IIS 6.0 | O Worker Process é executado em usuários com baixo privilégio por padrão. Isso reduz drasticamente o efeito dos possíveis ataques. |
| ASP Seguro de todas as funções | O ASP incorporado sempre é executado em contas de baixo privilégio (usuário anônimo). |
| Extensões de arquivo reconhecidas | Fornece apenas solicitações aos arquivos que reconheceram extensões de arquivos e recusa solicitações de extensões não reconhecidas. |
| Ferramentas de linha de comando acessíveis aos usuários da Web | Os violadores aproveitam bastante as ferramentas de linha de comando executáveis através do servidor da Web. No IIS 6.0, as ferramentas de linha de comando não podem ser executadas pelo servidor da Web. |
| Proteção de gravação para conteúdo | Quando os violadores conseguem acesso a um servidor, eles tentam danificar sites da Web. Impedindo que usuários anônimos da Web substituam o conteúdo da Web, esses ataques podem ser atenuados. |

### 3.3. new! Abrir a funcionalidade com as Extensões de Serviço Web no IIS 6.0

Em um esforço de reduzir a superfície de ataque do seu Servidor da Web, o IIS 6.0 fornece apenas conteúdo estático após uma instalação padrão. A funcionalidade programada proporcionada por Extensões de Internet Server API (ISAPI) ou Interfaces de Gateway Comuns (CGI) deve ser ativada manualmente por um administrador do IIS 6.0 ISAPI. O CGI estende a funcionalidade de suas páginas na Web e, por essa razão, é chamado de Extensões de Serviço da Web. Por exemplo, para executar o Active Server Pages (ASP) nessa versão do IIS 6.0, o ISAPI coloca o ASP.DLL em execução, habilitando-o especificamente como uma Extensão de Serviço Web.

Usando recursos de Extensões de Serviços da Web, os administradores de sites da Web podem ativar ou desativar a funcionalidade do IIS 6.0 conforme as necessidades individuais da organização. Esta funcionalidade global é realizada através do servidor inteiro.

### 3.4. new! Identidade configurável do Worker Process

Os vários aplicativos em execução ou sites em um servidor da Web inserem requisitos adicionais no servidor. Se um ISP receber duas empresas em um servidor (que podem ser concorrentes), é preciso garantir o funcionamento desses dois aplicativos de forma independente. Principalmente o ISP precisa se certificar de que um administrador mal-intencionado de um aplicativo não poderá ter acesso aos dados de outro. O IIS 6.0 proporciona esse nível de isolamento com a identidade configurável pelo Worker Process. Junto com outros recursos de isolamento como largura de banda e uso da CPU ou reciclagem armazenada na memória, o IIS 6.0 proporciona um ambiente aos múltiplos aplicativos em um servidor para que eles sejam totalmente separados.


© 2003 Microsoft Corporation. Todos os direitos reservados.

## 3.5. Aprimoramentos de SSL

***Foram realizados três aprimoramentos principais no Secure Sockets Layer (SSL) do IIS 6.0. Eles são:***

- new! ***Desempenho.*** O IIS 5.0 já proporcionava o software de implementação de SSL mais rápido do mercado. Conseqüentemente, em 50% de todos os sites Web o SSL é executado em IIS 5.0. O SSL do ISS 6.0 é ainda mais rápido. A Microsoft aprimorou a implementação do SSL para fornecer desempenho e escalabilidade ainda maiores.

- new! ***Objeto de Certificação Remota*** No IIS 5.0, os administradores não podiam administrar certificados SSL remotamente porque o provedor de serviços criptográficos e armazenamento certificado não era remoto. Considerando que os clientes controlam centenas ou até alguns milhares de servidores IIS com certificados SSL, eles precisam de uma forma de gerenciar certificados remotamente. Por isso, o CertObject agora permite que os clientes façam isso.

- new! ***Provedor de Serviço Criptográfico.*** Se o SSL estiver ativado, o desempenho cai significativamente porque a CPU precisa realizar diversas operações de criptografia intensas. Por isso, agora existem placas aceleradoras baseadas em hardware que permitem extrair dados dessas criptografias. Os Provedores de Serviços Criptográficos podem inserir seus próprios fornecedores de API de criptografia no sistema. Com o IIS 6.0, é fácil selecionar um provedor de criptografia API de terceiros.

## 3.6. Autorização e autenticação

Se a autenticação faz a pergunta "Quem é você?", a autorização pergunta "O que você pode fazer?". A autorização é permitir ou negar a um usuário o direito de realizar determinada operação ou tarefa. O Windows Server 2003 integra o .NET Passport como mecanismo para a autenticação do IIS 6.0. O IIS 6.0 amplia o uso de um novo framework de autorização fornecido com o Windows Server 2003. Além disso, os aplicativos da Web podem utilizar a autorização de URL junto com o Gerenciador de Autorizações para controlar o acesso.

### new! Integração do .NET Passport com o IIS 6.0

A integração do .NET Passport com o IIS 6.0 proporciona serviços de autenticação .NET Passport no servidor da Web. O .NET Passport 2.0 utiliza as interfaces de aplicativos fornecidas por componentes padrões Passport, por exemplo, o Secure Sockets Layer (SSL) Encryption, Redirecionamentos de HTTP e cookies. Os administradores podem colocar seus sites e aplicativos da Web à disposição da base .NET Passport inteira, que engloba aproximadamente 150.000.000 usuários, sem precisar administrar contas públicas, por exemplo, quanto à expiração ou ao fornecimento de senhas.

Depois de autenticar um usuário com a .NET Passport Unique ID (PUID), é possível mapear uma conta no Microsoft Active Directory® - se esse recurso estiver configurado para seus sites da Web. O token é criado pela Local Security Authority (LSA) para o usuário e o sistema do IIS 6.0 para a solicitação da HTTP.

Para obter mais informações sobre a segurança no IIS 6.0:

http://www.microsoft.com/windowsserver2003/techinfo/overview/iisenhance.mspx


© 2003 Microsoft Corporation. Todos os direitos reservados.

## 4. Exercício 1: Instalar o IIS 6.0 no Windows Server 2003

Para poder realizar este exercício, você terá que instalar o Windows Server 2003.

***Para instalar o IIS 6.0 no Windows Server 2003:***

1. No Painel de Controle, clique duas vezes em ***Adicionar ou Remover Programas***.
2. Clique em ***Componentes do Windows***.
3. Selecione ***Servidor de Aplicativos*** e clique em ***Detalhes***.
4. Selecione a caixa ***Internet Information Services***.
5. Insira o CD do Windows Server 2003, quando solicitado.
6. Faça um teste depois de finalizado o processo de instalação.
7. Abra o ***Internet Explorer*** e escreva **http://localhost**.
8. Verifique a exibição da página de início do IIS 6.0.

Para obter mais informações sobre a instalação:

http://support.microsoft.com/default.aspx?scid=kb;en-us;323384

http://support.microsoft.com/default.aspx?scid=kb;en-us;309506


© 2003 Microsoft Corporation. Todos os direitos reservados.

# Capítulo 8
# Segurança: Novas funcionalidades no Windows Server 2003

Neste capítulo, você assimilará conhecimentos sobre aprimoramentos de segurança introduzidos no Windows Server 2003.

***Ao concluir este capítulo, você poderá:***

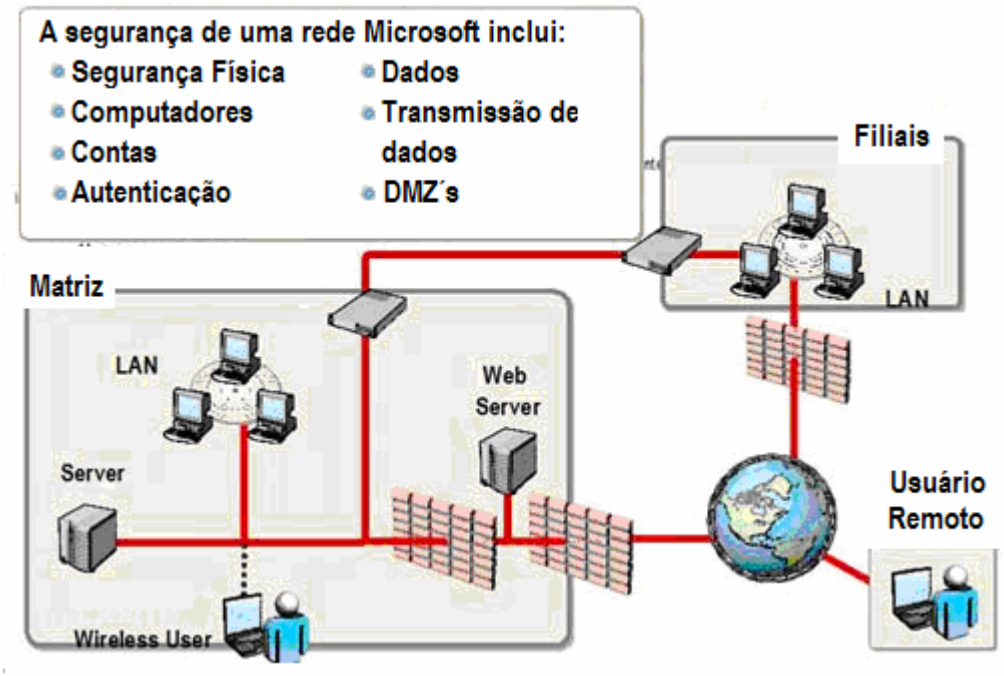
- Descrever as funcionalidades de segurança
- Implementar e verificar as funcionalidades de segurança

**Nota:** Considerando a quantidade de informações sobre temas referentes à segurança e como este capítulo é um resumo das novas funcionalidades, sugerimos que sejam revistos os conhecimentos adquiridos no Windows 2000 e também as publicações do Technet.

Se você quiser receber o boletim de segurança da Microsoft, registre-se no endereço abaixo. O boletim é gratuito e será de grande utilidade para suas tarefas diárias.

http://register.microsoft.com/subscription/subscribeme.asp?id=166

## 1. Introdução




As empresas ampliaram suas redes LAN tradicionais com uma combinação de sites da Internet, intranets e extranets. Conseqüentemente, agora é mais importante do que nunca garantir uma maior segurança nos sistemas. Para proporcionar um ambiente de informática seguro, o sistema operacional Windows Server 2003 traz vários recursos novos e importantes de segurança em relação aos do Windows 2000 Server.


© 2003 Microsoft Corporation. Todos os direitos reservados.

## 1.1. Informática de confiança

Os vírus fazem parte da nossa realidade, por isso, a manutenção da segurança do software é um desafio constante. Para fazer frente a esse desafio, a Microsoft transformou a computação confiável em uma iniciativa chave para todos os seus produtos. A Computação Confiável é um marca para o desenvolvimento de dispositivos baseados em equipamentos e software seguros e confiáveis, como os dispositivos e os equipamentos domésticos que nós utilizamos diariamente. Embora atualmente não exista nenhuma plataforma de computação totalmente confiável, o novo design básico do Windows Server 2003 é um passo sólido para transformar esse conceito em realidade.

## 1.2. Linguagem comum em tempo de execução

O mecanismo do software de linguagem comum em tempo de execução é um elemento chave do Windows Server 2003 que melhora a confiabilidade e facilita a criação de um ambiente seguro de informática. Da mesma forma, também são reduzidos os erros e furos de segurança causados por erros comuns de programação, possibilitando a redução das vulnerabilidades que podem ser exploradas por intrusos.

A linguagem comum em tempo de execução permite que os aplicativos sejam executados sem erros e, por sua vez, verifica se eles possuem permissões de segurança adequadas, garantindo que o código realize exclusivamente as operações autorizadas. Isso é feito testando-se os seguintes aspectos: a localização de onde o código foi obtido por download ou instalado, se o código tem uma assinatura digital de desenvolvedor confiável e se foi alterado após a sua assinatura digital.

## 1.3. Vantagens

O Windows Server 2003 fornece uma plataforma mais segura e econômica para a realização de atividades de empresas.

| Vantagem | Descrição |
|---|---|
| ***Diminuição de custos*** | Engloba processos administrativos de segurança simplificados, como listas de controle de acesso e o administrador de credenciais. |
| ***Implementação de padrões abertos*** | O protocolo IEEE 802.1X facilita a segurança das LANs sem fio frente ao risco de espionagem em um ambiente empresarial. |
| ***Proteção para equipamentos móveis e outros novos dispositivos*** | Os recursos de segurança, como o sistema de arquivos criptografados (EFS), os serviços de certificado e a inscrição automática de cartões inteligentes, facilitam a segurança de uma ampla gama de dispositivos. O EFS é a tecnologia básica para codificar e decodificar arquivos armazenados em volumes NTFS. Somente o usuário que criptografa um arquivo protegido pode abri-lo e trabalhar com ele. Os serviços de certificado são parte do sistema operacional básico que permite que uma empresa atue como entidade emissora de certificados (CA) e emita e administre certificados digitais. A inscrição automática de cartões inteligentes e os recursos de entidade de registro automático proporcionam segurança aos usuários corporativos, adicionando mais um nível de autenticação. Isso é acrescentado aos processos de segurança simplificados, em organizações onde há grande preocupação com segurança. |

## 1.4. Aprimoramentos e novos recursos

***A família do Windows Server 2003 traz os seguintes recursos:***

- Uma plataforma mais segura para realizar atividades corporativas
- A melhor plataforma para a infra-estrutura de chaves públicas
- Uma extensão segura de suas atividades corporativas na Internet


© 2003 Microsoft Corporation. Todos os direitos reservados.

### *Uma plataforma mais segura para realizar atividades corporativas*

O Windows Server 2003 oferece diversos recursos novos e aprimorados combinados para criar uma plataforma mais segura para realizar atividades corporativas.

| Característica | Descrição |
|---|---|
| *Firewall de conexão à Internet* | O Windows Server 2003 proporciona segurança na Internet com uso de um servidor de segurança baseado em software chamado Firewall de Conexão à Internet (ICF). O ICF proporciona proteção às máquinas conectadas diretamente à Internet ou às máquinas localizadas por trás de uma máquina de host de conexão compartilhada à Internet (ICS) e que execute um ICF. |
| *Servidor IAS/RADIUS seguro* | O Servidor de autenticação da Internet (IAS) é um servidor RADIUS que administra a autorização e a autenticação de usuários. Ele também administra conexões com a rede através de diversas tecnologias de conectividade, como o acesso por discagem às redes privadas virtuais (VPN) e aos servidores de segurança. |
| *Redes LAN Ethernet e sem fios seguras* | O Windows Server 2003 permite a autenticação e a autorização de usuários e máquinas conectados a redes LAN Ethernet e sem fio. Isso é possível devido à compatibilidade do Windows Server 2003 com os protocolos IEEE 802.1X. (Os padrões IEEE 802 definem métodos para obter acesso a redes LAN e controlá-las.) |
| *Diretivas de Restrição de Software* | O Windows Server 2003 permite que um administrador de sistemas utilize a exigência de diretivas ou execução para impedir que programas executáveis sejam executados em uma máquina. Por exemplo, aplicativos específicos de âmbito corporativo podem ter sua execução restringida, a menos que sejam executados de um diretório específico. As diretivas de restrição de software também podem ser configuradas para evitar a execução de código mal intencionado ou infectado por vírus. |
| *Aprimoramentos de segurança para servidores em redes LAN Ethernet e sem fio* | O Windows Server 2003 proporciona segurança para redes LAN Ethernet e sem fio baseado nas especificações IEEE 802.11 e compatíveis com os certificados públicos implementados através de inscrição automática ou cartões inteligentes. Esses aprimoramentos na segurança permitem o controle do acesso a redes Ethernet em lugares públicos, como centros comerciais ou aeroportos. A autenticação da máquina também é permitida em um ambiente operacional de protocolo de autenticação extensível (EAP). |
| *Segurança ampliada para servidores Web* | A segurança das informações é um problema de vital importância para as organizações de todo o mundo. Para aumentar a segurança dos servidores da Web, os Serviços do Internet Information Server 6.0 (IIS 6.0) são configurados para proporcionar máxima segurança. A sua instalação padrão é o estado "bloqueado". Os recursos de segurança avançados do IIS 6.0 incluem: serviços criptográficos que podem ser selecionados, autenticação de síntese avançada e controle configurável da obtenção de acesso aos processos. Esses são apenas alguns dos vários recursos de segurança que permitem realizar negócios de forma segura na Web. |
| *Criptografia dos arquivos offline* | Agora é possível criptografar os arquivos offline. Esse é um aprimoramento em relação ao Windows 2000, onde os arquivos no cache não poderiam ser criptografados. Essa característica é compatível com a codificação e decodificação de todos os bancos de dados criptografados offline. São necessários privilégios administrativos para configurar a forma como os arquivos offline são criptografados. |
| *Compatível com o FIPS, modo de núcleo, módulo criptográfico* | Este módulo criptográfico é executado como um controlador no modo de núcleo e implementa algoritmos criptográficos aprovados pelo Padrão Federal de Processamento de Informações (FIPS). Entre os algoritmos |


© 2003 Microsoft Corporation. Todos os direitos reservados.

| | |
|---|---|
| | estão incluídos: SHA-1, DES, 3DES e um gerador de número aleatório aprovado. O módulo criptográfico, compatível com o FIPS de modo de núcleo, permite que as organizações públicas implementem Segurança de Protocolo de Internet (IPSec) compatível com o FIPS 140-1. Para isso, é preciso utilizar:<br>• Servidor e cliente de VPN L2TP (Protocolo de encapsulamento da camada 2)/IPSec.<br>• Encapsulamentos L2TP/IPSec para conexões VPN entre portas de enlace.<br>• Encapsulamentos IPSec para conexões VPN entre portas de enlace.<br>• Tráfego da rede ponto a ponto, criptografado através de IPSec, entre cliente e servidor, e de servidor para servidor. |
| ***Novo protocolo de autenticação extensível protegido*** | O novo protocolo de autenticação extensível protegido (PEAP) é compatível com o protocolo de autenticação extensível (EAP), junto com a RFC 2617 e a RFC 2222. Esste protocolo aumenta a segurança em redes sem fio. |
| ***Administrador de credenciais*** | O administrador de credenciais do Windows Server 2003 oferece um depósito seguro para as credenciais do usuário, incluindo senhas e certificados X.509. Essas credenciais permitem um início de sessão único para os usuários, incluindo os usuários móveis. Uma API de Win32® encontra-se disponível para permitir que os aplicativos baseados no cliente e no servidor obtenham credenciais de usuário. |
| ***Aprimoramentos de autenticação de clientes SSL*** | No Windows Server 2003, o cache da sessão SSL pode ser compartilhado em múltiplos processos. Isso reduz o número de vezes que um usuário precisa retornar para ser autenticado nos aplicativos e também os ciclos de CPU no servidor de aplicativos. |


© 2003 Microsoft Corporation. Todos os direitos reservados.

### *A melhor plataforma para a infra-estrutura de chaves públicas*

O Windows Server 2003 facilita a implementação de uma infra-estrutura de chaves públicas, junto com tecnologias associadas com cartões inteligentes.

| Característica | Descrição |
|---|---|
| *Renovação e inscrição automática de certificados* | Esses novos recursos importantes reduzem de forma drástica a quantidade de recursos necessários para administrar certificados X.509. O Windows Server 2003 possibilita a inscrição e a implementação automática de certificados para os usuários. Da mesma forma, quando o certificado expira, é possível renová-lo automaticamente. A renovação e a inscrição automáticas de certificados facilitam a implementação mais rápida de cartões inteligentes e aumentam a segurança das conexões sem fios (IEEE 802.1X) com expiração e renovação automática de certificados. |
| *Compatibilidade do Windows Installer com a assinatura digital* | A compatibilidade com a assinatura digital permite que os pacotes e os contêineres externos do Windows Installer obtenham uma assinatura digital. Isso proporciona aos administradores de tecnologias de informação, pacotes do Windows Installer mais seguros, o que é de extrema importância se o pacote foi enviado através da Internet. |
| *Aprimoramentos das listas de certificados revogados (CRL)* | O servidor de certificados incluído no Windows Server 2003 agora é compatível com CRLs delta. Uma CRL faz com que a publicação de certificados X.509 revogados seja mais eficaz e facilita que um usuário possa recuperar um certificado novo. E, como agora é possível especificar a localização na qual está armazenada a CRL, fica mais fácil movê-la para atender às necessidades de segurança e específicas da empresa. |

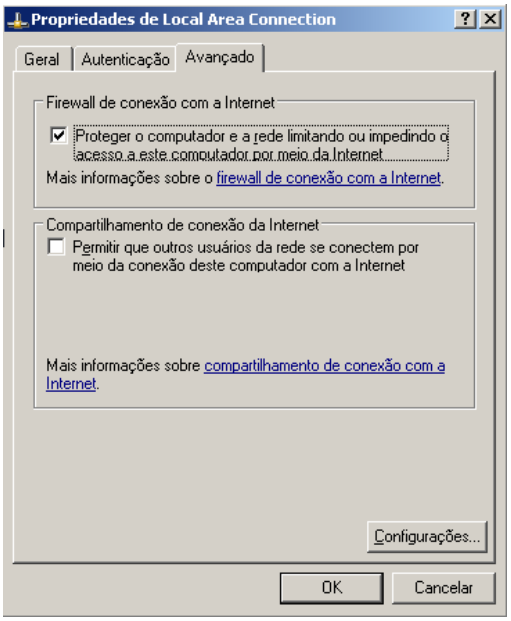
### *Extensão segura das atividades corporativas na Internet*

Uma empresa precisa estabelecer uma forma segura de comunicação com seus funcionários, clientes e parceiros que não estejam dentro da sua intranet. O Windows Server 2003 facilita esse aspecto ampliando de forma segura a obtenção de acesso à rede para pessoas e outras empresas que precisem trabalhar com dados ou recursos de usuário.

| Característica | Descrição |
|---|---|
| *Integração com Passport* | É possível atribuir uma identidade de Passport a uma identidade do Active Directory no Windows Server 2003. Por exemplo, a associação de uma identidade de Passport com uma identidade do Active Directory permite que uma empresa parceira possa ser autorizada a obter acesso aos recursos através do IIS, em vez de precisar iniciar a sessão diretamente em uma rede do Windows. A integração com o Passport possibilita um início de sessão único, através do uso do IIS. |
| *Relações de confiança entre florestas* | Quando se trabalha com um parceiro ou uma empresa que implementou uma floresta do Active Directory, é possível utilizar o Windows Server 2003 para configurar uma relação de confiança entre as florestas do parceiro ou da empresa e suas próprias florestas. Isto lhe permite confiar de forma explícita em alguns usuários, em grupos ou em todos os que pertençam à outra floresta. Também é possível estabelecer permissões por usuário ou grupos que residam em outra floresta. As relações de confiança entre florestas facilitam a realização de negócios com outras empresas através do Active Directory. |


© 2003 Microsoft Corporation. Todos os direitos reservados.

## 2. Personal Firewall (ICF)




O Firewall de Conexão com a Internet (ICF) é uma nova característica no Windows Server 2003, que lhe permite proteger sua conexão à Internet. Utilizando essa ferramenta, você pode determinar que serviços estarão disponíveis da Internet para o servidor que executa o Windows Server 2003 e que serviços estarão disponíveis do seu servidor para a Internet. Esse novo recurso permite proteger suas conexões, sejam as que utilizam adaptadores de rede ou as que utilizam conexões de discagem direta.

**Nota:** Você pode utilizar o ICF para proteger conexões exclusivamente no servidor que está executando o Windows Server 2003. Se for preciso permitir acesso seguro à Internet para clientes internos, uma implementação do Internet Security and Acceleration Server 2000 (Servidor ISA) deverá ser analisada.

***Para obter mais informações sobre o ICF:***

http://support.microsoft.com/default.aspx?scid=kb;en-us;317530

### 2.1. Exercício 1: Ativar o ICF

***Para poder fazer esse exercício, você precisa ter duas instalações do Windows Server 2003.***

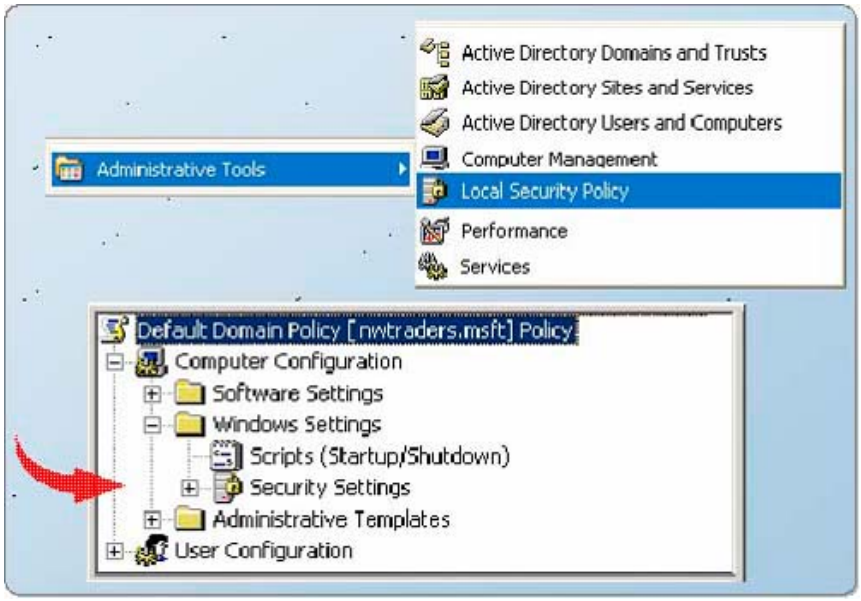
1. A partir do menu ***Iniciar***, clique em ***Conexões de Rede***.
2. Selecione o adaptador de rede, clique com o botão direito do mouse e depois clique em ***Propriedades***.
3. Clique na guia ***Avançado***.
4. Selecione a caixa ***Firewall de Conexão com a Internet***.
5. Clique em ***OK***.

***Para testar a configuração:***

- A partir do computador B, teste uma conexão do tipo **\\nomedoservidor**
- Verifique se a conexão pode ser estabelecida.


© 2003 Microsoft Corporation. Todos os direitos reservados.

## 3. Usar Modelos de Segurança para proteger os Computadores




Você pode usar Modelos de Segurança para criar e alterar Diretivas de Segurança que atendam às necessidades da sua empresa. As Diretivas de Segurança podem ser implementadas de formas diferentes. O método que você usará depende do tamanho e das necessidades de segurança da organização. Dessa forma, as pequenas empresas, que não possuem uma implementação do Active Directory, terão que configurar a segurança manualmente, enquanto as grandes empresas exigirão níveis de segurança elevados. Para elas, é aconselhável usar os Objetos de Diretiva de Grupos (GPOS) para instalar diretivas de segurança.

### 3.1. O que é uma Diretiva de Segurança?

As Diretivas de Segurança são uma combinação de configurações de segurança que afetam a segurança de um computador. Você pode usar a Diretiva de Segurança para estabelecer: Diretivas de Conta e Diretivas Locais no computador local e no Active Directory.

Os Modelos de Segurança a seguir são um conjunto de configurações de segurança predeterminadas. Você pode usar o Snap-in de Modelos de Segurança para modificar os Modelos predefinidos ou criar novos modelos que atendam às suas necessidades. Portanto, na criação ou modificação, é possível utilizar as seguintes ferramentas para aplicar as configurações de segurança: o Snap-in de Configuração e Análise de Segurança, a ferramenta de linha de comando Secedit ou a Diretiva de Segurança Local / Diretiva de Grupo para importar e exportar Modelos de Segurança.

**O Windows Server 2003 fornece os seguintes modelos predefinidos:**

***Segurança Padrão (Setup Security.inf)***

Esse modelo é usado durante a instalação do sistema operacional e representa a configuração básica aplicada durante a instalação, incluindo permissões de arquivos para a Raiz da Unidade do Sistema.


© 2003 Microsoft Corporation. Todos os direitos reservados.

### *Segurança do Controlador de Domínio (DC security.inf)*

Esse Modelo é usado quando um servidor é promovido a controlador de domínio. Contém configurações de segurança necessárias em arquivos, registro e serviços. Você pode aplicar esse modelo usando o snap-in Security Configuration and Analysis ou com a ferramenta Secedit.

### *Compatível (Compatws.inf)*

Este modelo aplica configurações de segurança necessárias para todos os aplicativos que não foram certificados pelo Programa de Logotipo do Windows.

### *Seguro (Secure*.inf)*

Esse Modelo aplica configurações de segurança de alto nível, afetando a compatibilidade dos aplicativos. Por exemplo, Senha Mais Sólida, Bloqueio, Configurações de Auditoria.

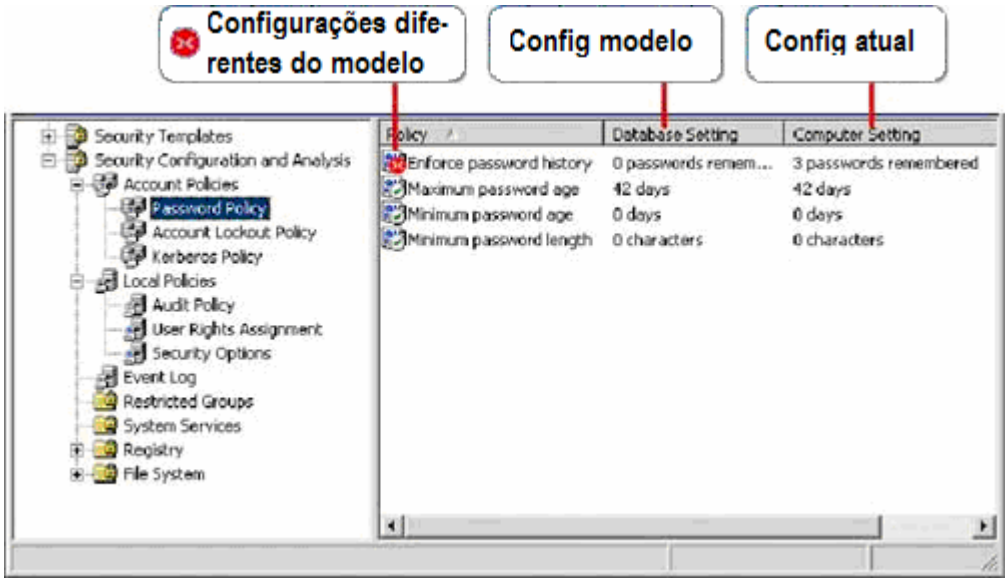
### *Altamente Seguro (Hisec*.inf)*

Este modelo aplica as configurações de segurança mais elevadas possíveis. Para eles, são impostas restrições aos níveis de criptografia e à assinatura de pacotes de dados em canais seguros e entre clientes e servidores nos pacotes Server Message Block (SMB).

Obtenha mais informações sobre ***secedit***:

http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windowsserver2003/proddocs/datacenter/secedit_cmds.asp?frame=true

## 3.2. O que é a ferramenta Security Configuration and Analysis?




A ferramenta Security Configuration and Analysis compara a configuração de segurança do computador local e uma configuração alternativa que é importada do modelo (arquivo .inf ) e armazenada em um banco de dados separado (arquivo .sdb). Quando a análise é concluída, você pode analisar os ajustes da segurança na árvore do console para ver os resultados. As discrepâncias estão marcadas com uma sinalização vermelha, as consistências estão marcadas com uma marca de seleção verde e os ajustes que não estão marcados com uma sinalização vermelha ou uma marca verde não podem ser configurados no banco de dados.


© 2003 Microsoft Corporation. Todos os direitos reservados.

***Depois de analisar os resultados usando a ferramenta Security Configuration and Analysis, você pode realizar várias tarefas, incluindo:***

- Eliminar as discrepâncias entre os ajustes nos bancos de dados e os ajustes atuais do computador. Para configurar ajustes do banco de dados, clique na configuração do painel de detalhes.

- Importar outros modelos, combinando seus ajustes e substituindo ajustes onde houver conflito. Para importar outro modelo, clique com o botão direito em ***Security Configuration and Analysis*** e depois clique em ***Import Template***.

- Exportar os ajustes atuais do banco de dados para um modelo. Para importar outro modelo, clique com o botão direito em ***Security Configuration and Analysis*** e depois clique em ***Export Template***.

***Para mais informações sobre Ferramentas de Segurança:***

***Informações adicionais sobre segurança:***

**Introdução Técnica à Segurança.**

http://www.microsoft.com/windowsserver2003/techinfo/overview/security.mspx

**Guia de Segurança no Windows Server 2003.**

http://www.microsoft.com/security/guidance/prodtech/WindowsServer2003.mspx

**IPsec no Windows Server 2003.**

http://support.microsoft.com/default.aspx?scid=kb;en-us;323342

http://support.microsoft.com/default.aspx?scid=kb;en-us;324269

**Criptografia de Chave Pública**

http://support.microsoft.com/default.aspx?scid=kb;en-us;281557

http://support.microsoft.com/default.aspx?scid=kb;en-us;290760


© 2003 Microsoft Corporation. Todos os direitos reservados.