

## Tutorial de Active Directory – Parte 4

### Introdução

Prezados leitores, esta é a quarta parte de uma série de tutoriais sobre o Active Directory. O Active Directory foi a grande novidade introduzida no Windows 2000 Server e que também faz parte do Windows Server 2003. Mais do que fazer parte, o Active Directory é o elemento principal de uma rede baseada no Windows 2000 Server ou Windows Server 2003, a partir do qual é possível criar redes de grandes proporções, como por exemplo a rede da empresa onde eu trabalho, a qual tem mais de 20 mil estações de trabalho em rede. Toda a rede é baseada no Windows 2000 Server e no Active Directory. Nesta série de tutoriais, mostrarei ao amigo leitor o que é exatamente o Active Directory, quais as suas funções, quais os elementos que compõem o Active Directory e qual a utilização de Cada um.

**Para um curso completo sobre o Active Directory, no Windows 2000 Server, consulte o livro de minha autoria, indicado a seguir:**



**MANUAL DE ESTUDOS PARA O EXAME 70-217 – 752 páginas**

Um curso completo de Active Directory no Windows 2000 Server

➔ Para acessar o índice do livro, use o endereço a seguir:

<http://www.juliobattisti.com.br/livros/70-217.asp>

➔ Para comprar o livro, use o endereço a seguir:

<http://www.juliobattisti.com.br/loja/vendalivro.asp?CODIGO=70217>

**Para um curso completo sobre o Active Directory, no Windows Server 2003, consulte o livro de minha autoria, indicado a seguir:**



**WINDOWS Server 2003 – CURSO COMPLETO – 1568 páginas**

Aprenda sobre o DNS, DHCP, WINS, RRAS, Active Directory, etc.

➔ Para acessar o índice do livro, use o endereço a seguir:

<http://www.juliobattisti.com.br/livros/windows2003.asp>

➔ Para comprar o livro, use o endereço a seguir:

<http://www.juliobattisti.com.br/loja/vendalivro.asp?CODIGO=WIN3K>

Esta série de tutoriais é especialmente indicada para quem está iniciando os seus estudos sobre o Active Directory e precisa entender, em detalhes, como funcionam as redes baseadas no Windows 2000 Server ou Windows Server 2003 e no Active Directory.

## Active Directory

Lembro de já ter escrito a seguinte frase, em um dos capítulos do meu livro: Windows Server 2003 – Curso Completo, 1568 páginas.

“O Active Directory é, sem dúvidas, a mudança mais significativa incluída no Windows 2000 Server e que também faz parte do Windows Server 2003.”

### **Mas de uma maneira simples, o que é o Active Directory?**

“O Active Directory é o serviço de diretórios do Windows Server 2003. Um Serviço de Diretórios é um serviço de rede, o qual identifica todos os recursos disponíveis em uma rede, mantendo informações sobre estes dispositivos (contas de usuários, grupos, computadores, recursos, políticas de segurança, etc) em um banco de dados e torna estes recursos disponíveis para usuários e aplicações.”

Pode parecer que o Active Directory é, na verdade um banco de dados. Mas não é só isso. Além do banco de dados com informações sobre os elementos (tecnicamente conhecidos como objetos) que compõem o domínio, o Active Directory também disponibiliza uma série de serviços que executam as seguintes funções:

- Replicação entre os Controladores de domínio
- Autenticação
- Pesquisa de objetos na base de dados
- Interface de programação para acesso aos objetos do diretório

Pela descrição formal, é possível inferir que o Active Directory é um serviço de rede, no qual ficam armazenadas informações sobre dados dos usuários, impressoras, servidores, grupos de usuários, computadores e políticas de segurança. Cada um desses elementos são conhecidos como objetos.

O Active Directory além de armazenar uma série de informações sobre os objetos disponíveis no domínio (contas de usuários, grupos de usuários, contas de servidores, contas de computadores, políticas de segurança, etc), torna fácil para o administrador localizar e fazer alterações nos objetos existentes, bem como criar novos objetos ou excluir objetos que não sejam mais necessários. Em resumo, com o conjunto de serviços oferecidos pelo Active Directory, a administração da rede torna-se uma tarefa bem mais gerenciável.

Os recursos de segurança são integrados com o Active Directory, através do mecanismo de logon e autenticação. Todo usuário tem que fazer o logon (informar o seu nome de usuário e senha), para ter acesso aos recursos da rede. Durante o logon o Active Directory verifica se as informações fornecidas pelo usuário estão corretas e então libera o acesso aos recursos para os quais o usuário tem permissão de acesso.

Os recursos disponíveis através do Active Directory, são organizados de uma maneira hierárquica, através do uso de Domínios. Uma rede na qual o Active Directory está instalado, pode ser formada por um ou mais Domínios. Com a utilização do Active Directory um usuário somente precisa estar cadastrado em um único Domínio, sendo que este usuário pode receber permissões para acessar recursos em qualquer um dos Domínios, que compõem a árvore de domínios da empresa.

A utilização do Active Directory simplifica, em muito, a administração da rede, pois fornece um local centralizado, através do qual todos os recursos da rede podem ser administrados. Todos os Controladores de Domínio (DCs), possuem o Active Directory instalado. A maneira de criar um domínio é instalar o Active Directory em um Member Server e informar que este é o primeiro Controlador de Domínio, de um novo domínio que está sendo criado. Depois de criado

o domínio (a parte prática da criação de domínios será vista nas últimas partes desta série de tutoriais). você pode criar DCs adicionais, simplesmente instalando o Active Directory em outros servidores da rede. Ao instalar o Active Directory em um servidor, você torna-o um DC.

O Active Directory utiliza o DNS (Domain Naming System) como serviço de nomeação de servidores e recursos e de resolução de nomes. Por isso um dos pré-requisitos para que o Active Directory possa ser instalado e funcionar perfeitamente é que o DNS deve estar instalado e corretamente configurado em um dos servidores da rede (não é obrigatório que o DNS esteja instalado no mesmo servidor onde o Active Directory será instalado).

**Novidade:** No Windows Server 2003, o assistente de instalação do Active Directory é capaz de instalar e configurar o DNS, caso ele não encontre um servidor DNS adequadamente configurado na rede. Esta não chega a ser exatamente uma novidade. O que ocorre na prática, é que o assistente de instalação do Active Directory, no Windows Server 2003, consegue na maioria das vezes configurar o DNS corretamente, o que não ocorria no Windows 2000 Server.

O Agrupamento de objetos em um ou mais Domínios permite que a rede de computadores reflita a organização (quer seja a organização física, quer seja a organização lógica e funcional) da sua empresa. Para que um usuário cadastrado em um domínio, possa receber permissões para acessar recursos em outros domínios, o Windows Server 2003 cria e mantém, automaticamente, relações de confiança entre os diversos domínios. As relações de confiança são bidirecionais e transitivas. Isso significa se o Domínio A confia no Domínio B, o qual por sua vez confia em um Domínio C, então o Domínio A também confia no Domínio C. Isso é bastante diferente do que acontecia até o NT Server 4.0, uma vez que as relações de confiança tinham que ser criadas e mantidas manualmente pelos administradores dos domínios, uma a uma. Era um trabalho e tanto, o que dificultava a implementação de relações de confiança em uma rede com muitos domínios.

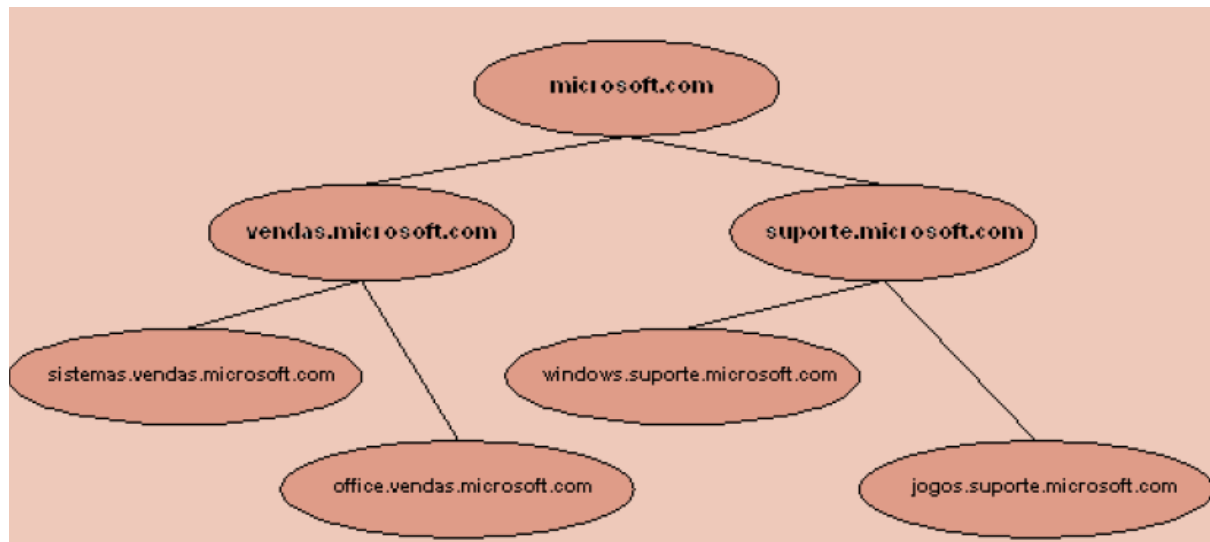
**Todo Domínio possui as seguintes características:**

- Todos os objetos de uma rede (contas de usuários, grupos, impressoras, políticas de segurança, etc) fazem parte de um único domínio.
- Cada domínio somente armazena informações sobre os objetos do próprio domínio.
- Cada domínio possui suas próprias políticas de segurança.

## Árvore de domínios

Quando existem diversos domínios relacionados através de relações de confiança, criadas e mantidas automaticamente pelo Active Directory, temos uma Árvore de domínios. Uma árvore nada mais é do que um agrupamento ou arranjo hierárquico de um ou mais domínios do Windows Server 2003, os quais “compartilham um espaço de nome.”

Vou explicar em detalhes o que significa a expressão “compartilham um espaço de nome”. Primeiramente observe a Figura a seguir:



**Figura - Todos os domínios de uma árvore compartilham um espaço de nomes.**

Observe que é exibida uma árvore com 7 domínios. Mas o que significa mesmo “compartilham um espaço de nome”?

Observe que o domínio inicial, também conhecido como domínio pai ou domínio root, é microsoft.com. Os domínios seguintes são: vendas.microsoft.com e suporte.microsoft.com. Quando é formada uma hierarquia de domínios, compartilhar um espaço de nomes, significa que os nomes dos objetos filho (de segundo nível, por exemplo: vendas.microsoft.com e suporte.microsoft.com), contém o nome do objeto pai (microsoft.com). Por exemplo, vendas.microsoft.com contém microsoft.com. Descendo mais ainda na hierarquia, você pode observar que este fato continua verdadeiro. Por exemplo o objeto filho sistemas.vendas.microsoft.com contém o nome do objeto Pai vendas.microsoft.com.

Com isso uma árvore de diretórios deste tipo forma um espaço de nomes contínuo, onde o nome do objeto filho sempre contém o nome do objeto pai.

## Unidades Organizacionais

Você pode ainda dividir um Domínio em "Unidades Organizacionais". Uma Unidade Organizacional é uma divisão lógica do domínio, a qual pode ser utilizada para organizar os objetos de um determinado domínio em um agrupamento lógico para efeitos de administração. Isso resolve uma série de problemas que existiam em redes baseadas no NT Server 4.0.

No Windows NT Server 4.0 se um usuário fosse adicionado ao grupo Administradores (grupo com poderes totais sobre qualquer recurso do domínio), ele poderia executar qualquer ação em qualquer servidor do domínio. Com a utilização de Unidades Organizacionais, é possível restringir os direitos administrativos apenas a nível da Unidade Organizacional, sem que com isso o usuário tenha poderes sobre todos os demais objetos do Domínio.

Cada domínio pode implementar a sua hierarquia de Unidades Organizacionais, independentemente dos demais domínios, isto é, os diversos domínios que formam uma árvore, não precisam ter a mesma estrutura hierárquica interna de unidades organizacionais.

No exemplo da Figura anterior, o domínio vendas.microsoft.com, poderia ter uma estrutura hierárquica de Unidades Organizacionais, projetada para atender as necessidades do domínio vendas. Essa estrutura poderia ser completamente diferente da estrutura de Unidades Organizacionais do domínio suporte.microsoft.com, a qual seria projetada para atender as necessidades do domínio suporte. Com isso tem-se uma flexibilidade bastante grande, de tal forma que a árvore de domínios e a organização dos domínios em uma hierarquia de Unidades Organizacionais, possa atender perfeitamente as necessidades da empresa. A utilização de Unidades Organizacionais não é obrigatória, porém altamente recomendada, conforme mostrarei em alguns exemplos mais adiante.

### Quando devo utilizar Unidades Organizacionais:

- Você quiser representar a estrutura e organização da sua companhia em um domínio. Sem a utilização de Unidades Organizacionais, todas as contas de usuários são mantidas e exibidas em uma única lista, independente da localização, departamento ou função do usuário.
- Você quiser delegar tarefas administrativas sem para isso ter que dar poderes administrativos em todo o Domínio. Com o uso de Unidades Organizacionais, você pode dar permissões para um usuário somente a nível da Unidade Organizacional.
- Quiser facilitar e melhor acomodar alterações na estrutura da sua companhia. Por exemplo, é muito mais fácil mover contas de usuários entre Unidades Organizacionais do que entre domínios, embora no Windows Server 2003 seja bem mais fácil mover uma conta de um domínio para outro, do que era no Windows 2000 Server.

Com a apresentação destes conceitos, você já está habilitado a estudar os elementos do Active Directory em mais detalhes. Mas este já é assunto para as próximas partes desta série de tutoriais, onde passarei a tratar sobre os objetos do Active Directory.

## **Conclusão**

Nesta parte do tutorial apresentei mais alguns conceitos de fundamental importância para entender o Active Directory: tratei sobre o que é o Active Directory e o que ele representa em uma rede, falei sobre domínios, espaço de nomes e Unidades Organizacionais. A partir da próxima parte, passarei ao estudo dos elementos que compõem o Active Directory, denominados "objetos do Active Directory".

**IMPORTANTE:** Se você preferir, poderá ter acesso a todas as partes do tutorial, já no formato .PDF, com permissão de impressão. Esta série de tutoriais, corresponde ao Módulo 2, de um dos seguintes e-books de minha autoria:

<b>Manual de Estudos Para o Exame MCDST – 70-271 – 892 páginas</b>	
<b>7 0 - 2 7 1</b>	<b>Um Manual Completo Para o Exame 70-271</b>  Um curso completo de Active Directory no Windows 2000 Server  ➔ Para acessar o índice do manual, use o endereço a seguir: <a href="http://www.juliobattisti.com.br/cursos/70271/indice.asp">http://www.juliobattisti.com.br/cursos/70271/indice.asp</a>  ➔ Para comprar o livro, use o endereço a seguir: <a href="http://www.juliobattisti.com.br/ebooksdoautor/default.asp">http://www.juliobattisti.com.br/ebooksdoautor/default.asp</a>
<b>Manual de Estudos Para o Exame MCSE – 70-290 – 1020 páginas</b>	
<b>7 0 - 2 9 0</b>	<b>Um Manual Completo Para o Exame 70-290</b>  Um Curso de Administração do Windows Server 2003  ➔ Para acessar o índice do manual, use o endereço a seguir: <a href="http://www.juliobattisti.com.br/cursos/70290/indice.asp">http://www.juliobattisti.com.br/cursos/70290/indice.asp</a>  ➔ Para comprar o livro, use o endereço a seguir: <a href="http://www.juliobattisti.com.br/ebooksdoautor/default.asp">http://www.juliobattisti.com.br/ebooksdoautor/default.asp</a>