Active Directory - Implementando um domínio 2003

Abril/2007

Cristiano Paiva Alves
cristiano.paiva@gmail.com

Resumo

O Active Directory surgiu da necessidade de se ter um único diretório, ou seja, ao invés do usuário ter uma senha para acessar o sistema principal da empresa, uma senha para ler seus e-mails, uma senha para se logar no computador, e varias outras senhas, com a utilização do AD, os usuários poderão ter apenas uma senha para acessar todos os recursos disponíveis na rede.Podemos definir um diretório como sendo um banco de dados que armazena as informações dos usuários.

1.Introdução

O Active Directory surgiu com Windows 2000 Server. Objetos como usuários, grupos, membros dos grupos, senhas, contas de computadores, relações de confiança, informações sobre domínio, unidades organizacionais, etc., ficam armazenados no banco de dados do AD. Para que os usuários possam acessar os recursos da rede, estes deverão efetuar o logon.Quando o usuário faz o logon o AD verifica se as informações fornecidas pelos usuários são validas e faz a autenticação.

2.Elementos de um servidor Active Directory:

2.1Domínio

Á semelhança de um grupo de trabalho (Workgroup), um domínio é uma organização lógica de maquinas e recursos. Ele se caracteriza pelo fato de a informação acerca dos recursos pertencentes a essa organização lógica (contas de usuários, máquinas, serviços ativos) permanecer centralizada, em uma base de dados, em servidores que terá um papel específico: os controladores de domínio. Por meio de uma identidade (conta) de usuário válida, um usuário pode ingressar em um domínio a partir de qualquer máquina da rede ligada a esse domínio, e obter acesso a recursos da rede para os quais o

administrador do domínio lhe tenha concedido permissão. Recomenda-se a utilização de domínios em redes cuja gestão de contas e segurança deva ser centralizada e assegurada. Na terminologia do Windows 2000, os domínios são conhecidos como DCs(Domain Controllers).

2.2Workgroup

A inclusão de uma máquina em um grupo de trabalho local ou Workgroup determina que ela possa ser utilizada por um grupo de usuários, que deve requisitar uma autorização local (na próxima máquina) para ter acesso ao sistema operacional. Assim para utilizar dois sistemas ou estações de um Workgroup, um mesmo individuo deve dispor de duas contas de usuário, uma em cada máquina. Isso é necessário porque os bancos de dados de usuários de Workgroup são armazenados localmente na estação, e não em um servidor centralizado, como o DC. Cada usuário e responsável pelos recursos compartilhados em sua máquina, bem como pela segurança do acesso a esses recursos, uma vez, que tais garantias não são gerenciadas por uma administração central. Portanto, esse tio de configuração é recomendado apenas para redes com poucas máquinas, e em que a segurança e a administração centralizada não sejam fatores importantes. No Windows 2003 Server com Active Directory, os grupos de trabalho são definidos como grupos de usuários, agrupados conforme um critério à escolha do administrador. Active Directory Workgroup também pode ser reconhecidos e importados a partir de máquinas ou estações de trabalho (incluindo impressoras de rede, impressoras compartilhadas e volume de rede) existentes em redes compostas de estações Windows XP ou Linux.

2.3Tree

O domínio inicial do Active Directory, que gerencia toda a estrutura de serviços, e denominado, na organização lógica do Active Directory, como tree root domain.Dependendo das necessidades organizacionais, maid domínios podem ser adicionados a essa estrutura, criando uma árvore formada por servidores de domínios ou domínios .Uma tree(ou árvore de domínios)consiste de uma organização de domínios Windows 2003 que compartilham um nome e relações de confiança bidirecionais, e que não precisam ser necessariamente fixas.Uma vez criado o domínio com função de tree root domain, é possível adicionar, à estrutura de serviços, child domains(domínios-filhos).Nessa ocasião, automaticamente são criados relações de confiança entre domínios-filhos e o parent domain, envolvendo o acesso a informação sobre contas de usuários, serviços e grupos de trabalho.

2.4 Forest

O termo forest designa o conjunto de uma ou mais trees.O primeiro domínio da estrutura lógica de domínios windows 2003 cria uma tree é uma forest.Esta última pode ser acrescida de outros domínios, assim como novas trees.Entre o domínio de topo da

tree e o domínio de topo da forest, cria-se uma relação de confiança bidirecional e transitiva,de modo que todos os domínios de uma forest confiem uns nos outros.

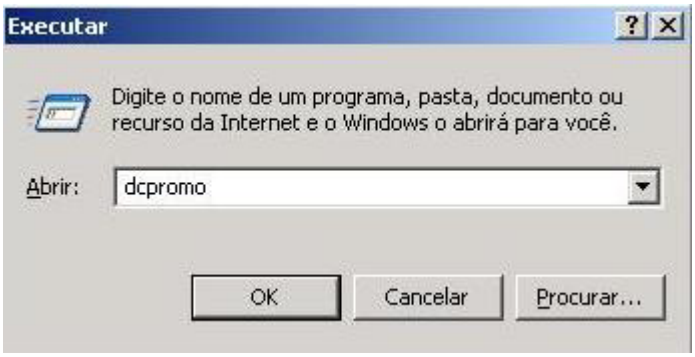
3.Implementação

Nesta seção, vamos implementar a instalação do Active Diretory e a criação do domínio.

3.1 Ambiente usado

O ambiente usado para instalação do AD foi um computador Pentium IV de 2.4 GHz com 256 MB de memória RAM e um Disco rígido de 80 GB. O sistema operacional usado foi o Windows 2003 Server Standard Edition.

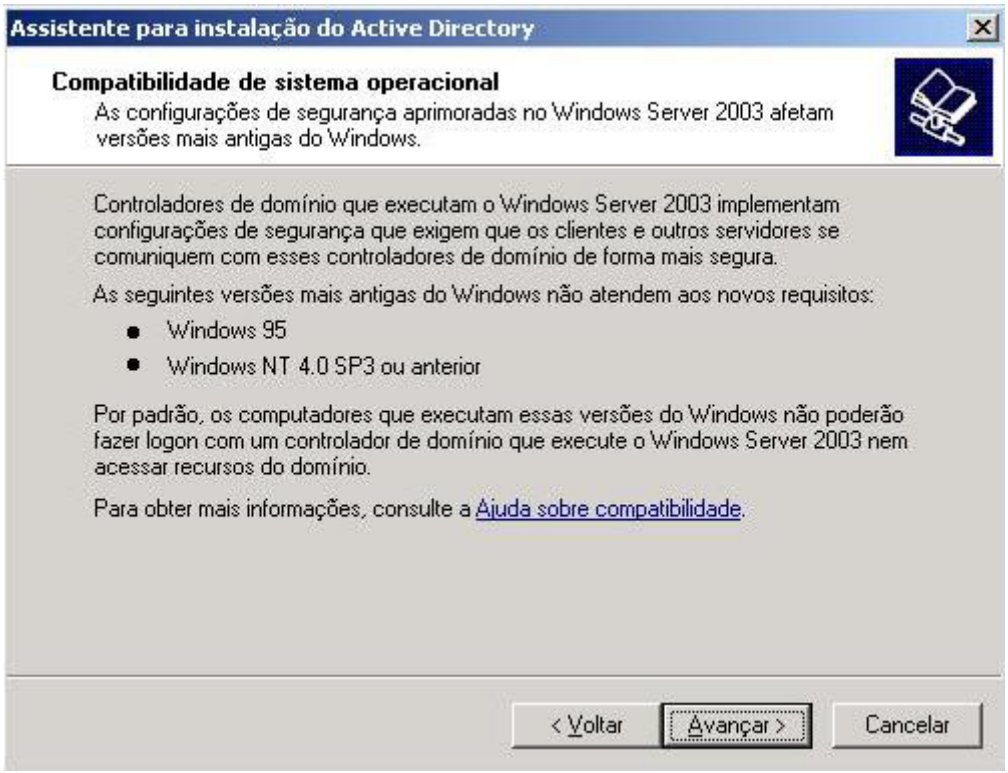
3.2 Instalação do Ad e criação do domínio



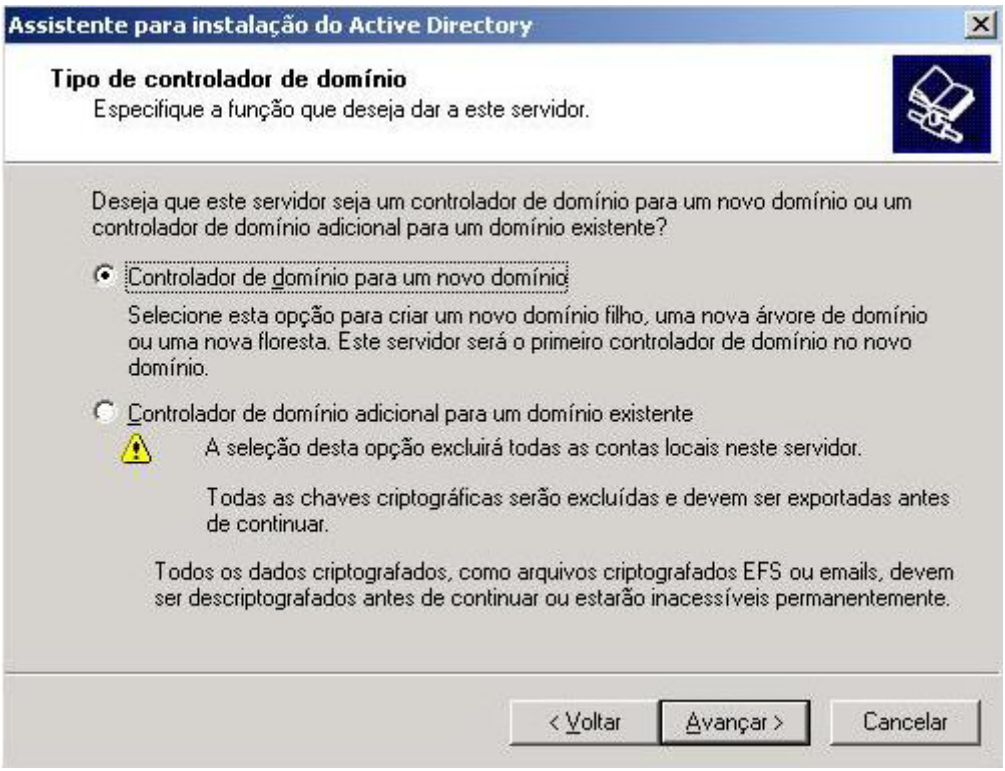
O primeiro passo vá ate o menu iniciar,executar, na linha a seguir digite dcpromo e clique em ok. .

A janela do “Assistente para instalação do Active Directory” irá aparecer. Clique no botão “Avançar”.

Na janela de “Compatibilidade de sistema operacional” leia os requisitos mínimos dos clientes do AD. A seguir, clique no botão “Avançar”.

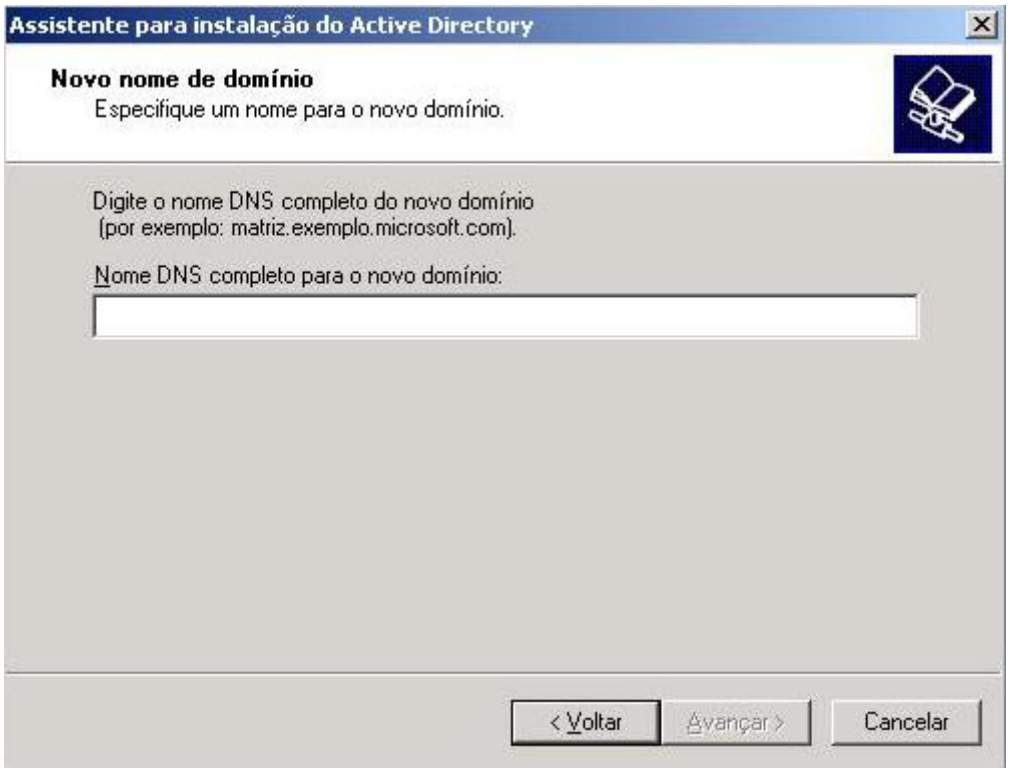


Na janela de “Tipo de controlador de domínio”, selecione a opção “Controlador de domínio para um novo domínio” e clique no botão “Avançar”.

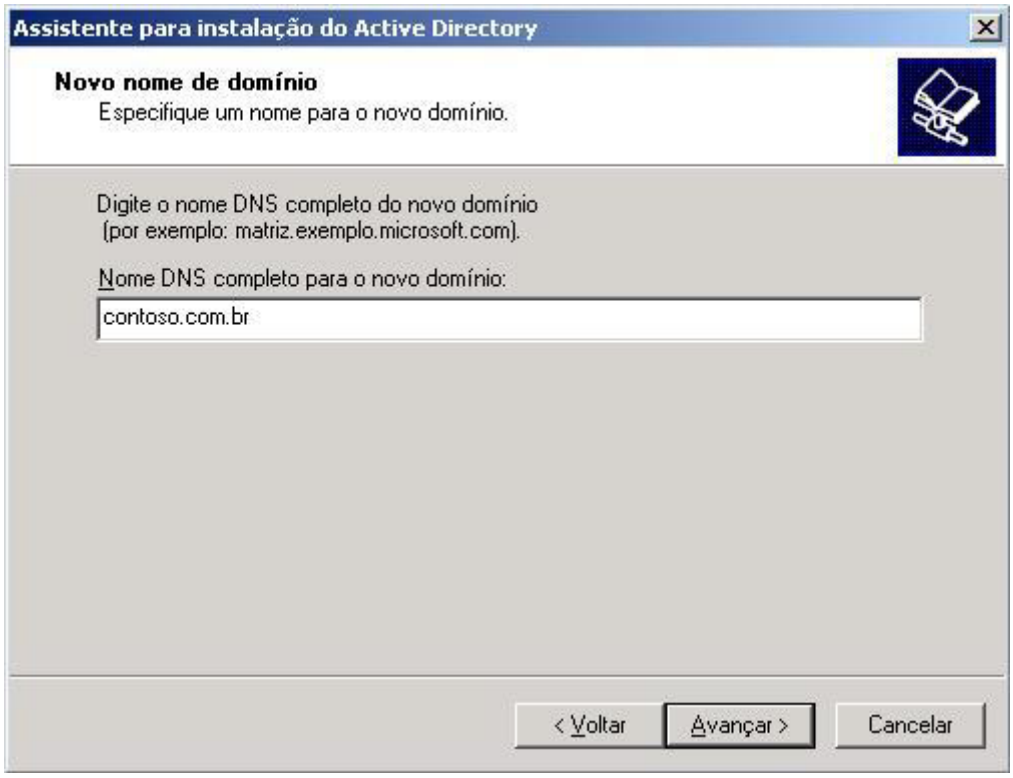


Na janela de “Criar novo domínio”, selecione a opção “Domínio em uma nova floresta” e clique no botão “Avançar”.

A janela de “Novo nome de domínio” é a opção mais importante na criação do AD. Como todo o sistema do AD é baseado no DNS, a criação do nome de domínio irá afetar toda a operação da rede.

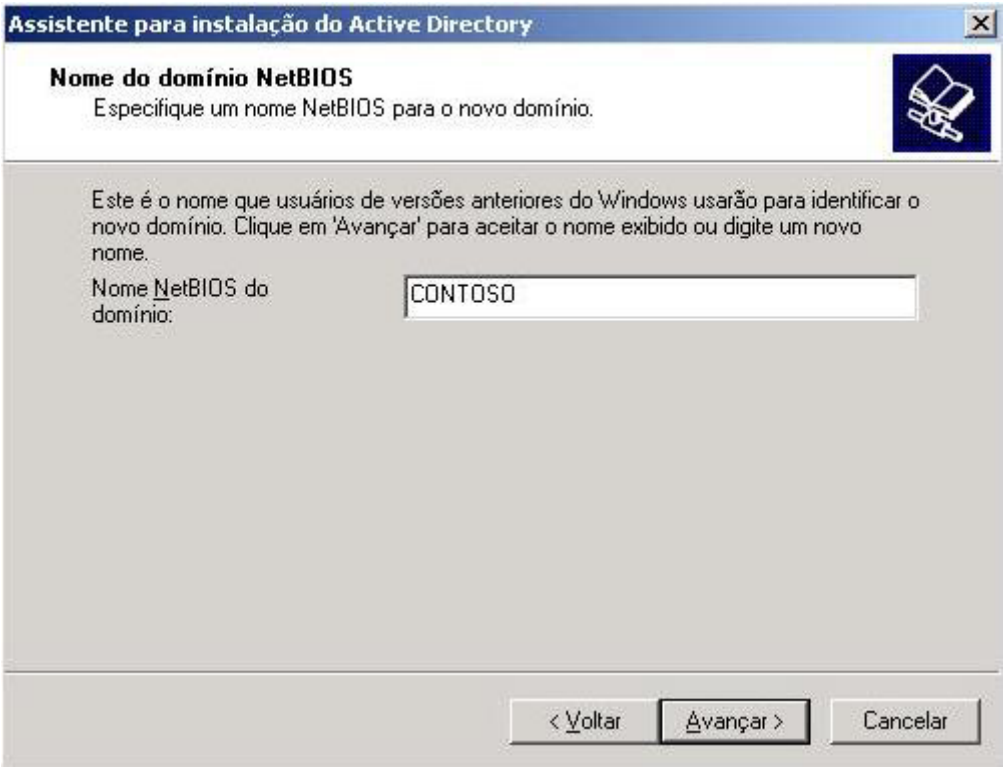


Entre com o nome DNS completo do domínio, por exemplo: contoso.com.br

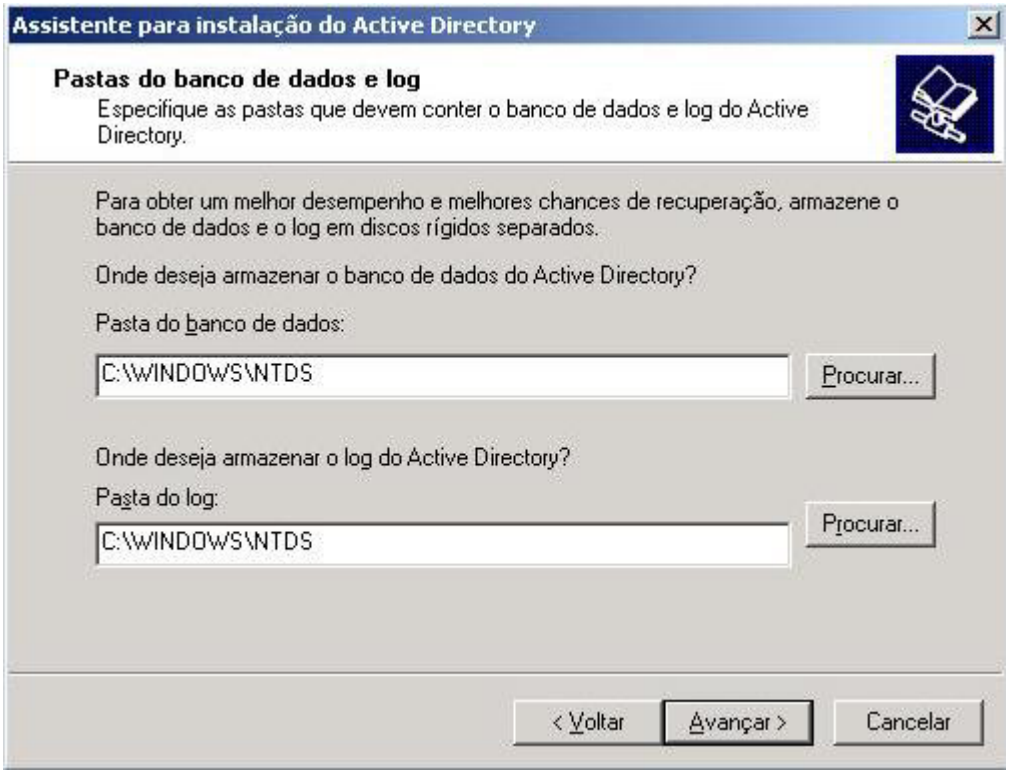


Clique no botão "Avançar".
Este parte poderá demorar alguns minutos, pois o sistema irá procurar pelo servidor DNS e verificar se o nome já existe.

Na janela de "Nome do domínio NetBIOS", aceite a opção padrão (que é o primeiro nome do domínio DNS) e clique no botão "Avançar".

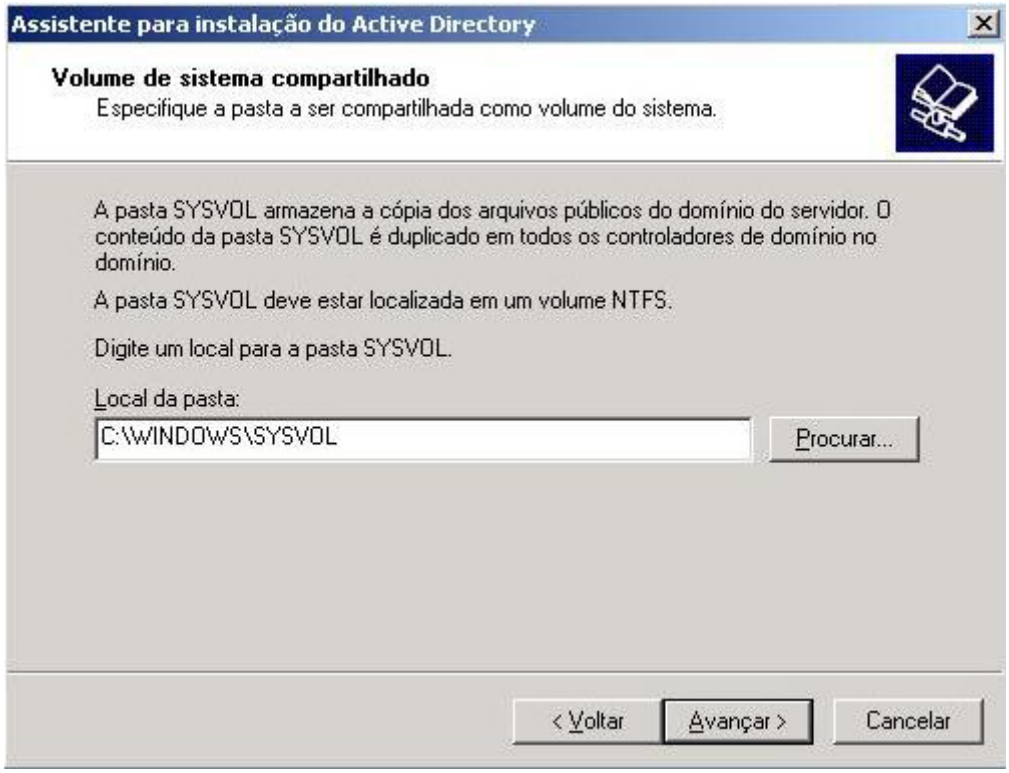


Na janela de “Pastas do banco de dados e log”, lembre-se que a partição deverá ser NTFS e você somente deverá alterar os caminhos padrões por motivos de desempenho. O caminho “\Windows\NTDS” é o local onde serão armazenados os dados do AD. Aceite as opções padrões e clique no botão “Avançar”.

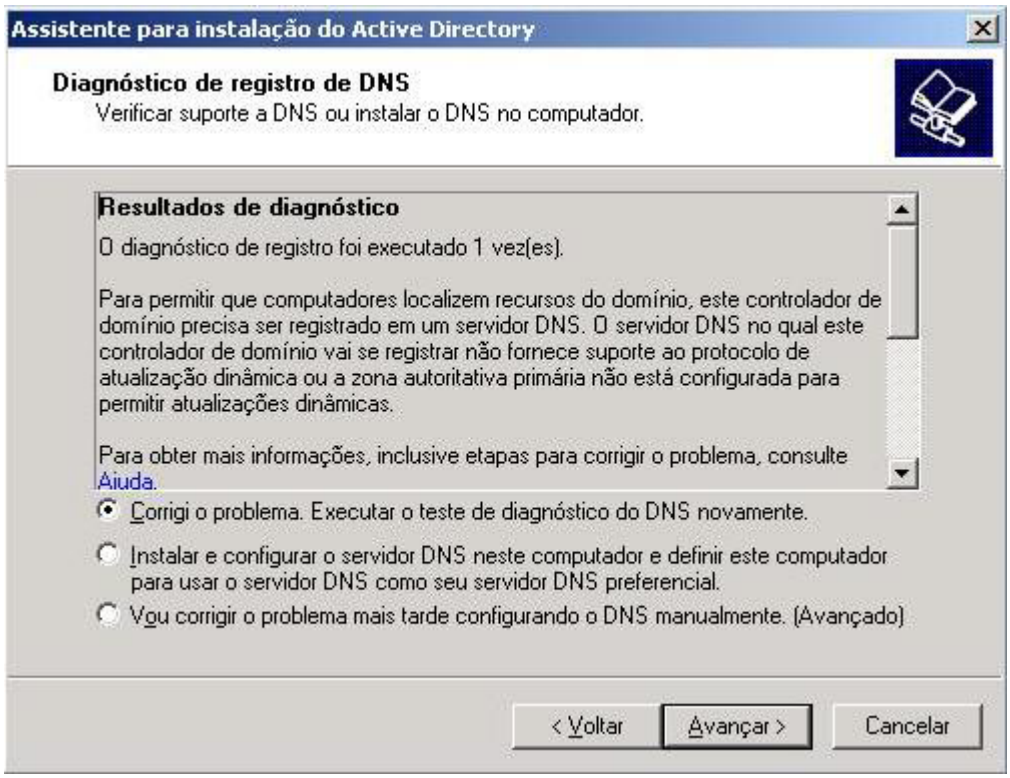


Na janela de “Volume de sistema compartilhado”, a partição também deverá ser NTFS e somente deverá ser alterado caso haja problemas de desempenho. O caminho “\Windows\SYSVOL” é o local onde serão armazenados as GPOs e scripts do AD e esta pasta

é replicada para todos os outros DC. Aceite a opção padrão e clique no botão “Avançar”.



Se o servidor DNS não estiver ativo ou configurado corretamente, você verá o seguinte aviso:

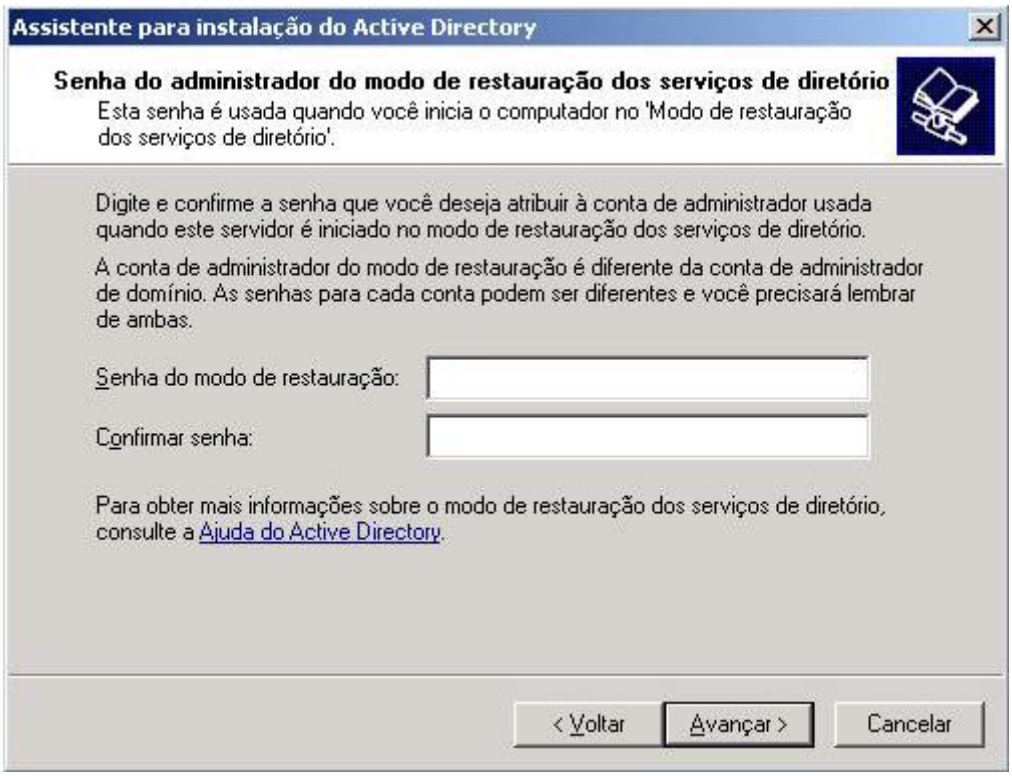


Em geral, o primeiro DC do AD também é o servidor DNS (que é o caso do nosso artigo). Lembre-se que o servidor DNS requerido pelo AD deve aceitar registro SRVs e atualizações dinâmicas.

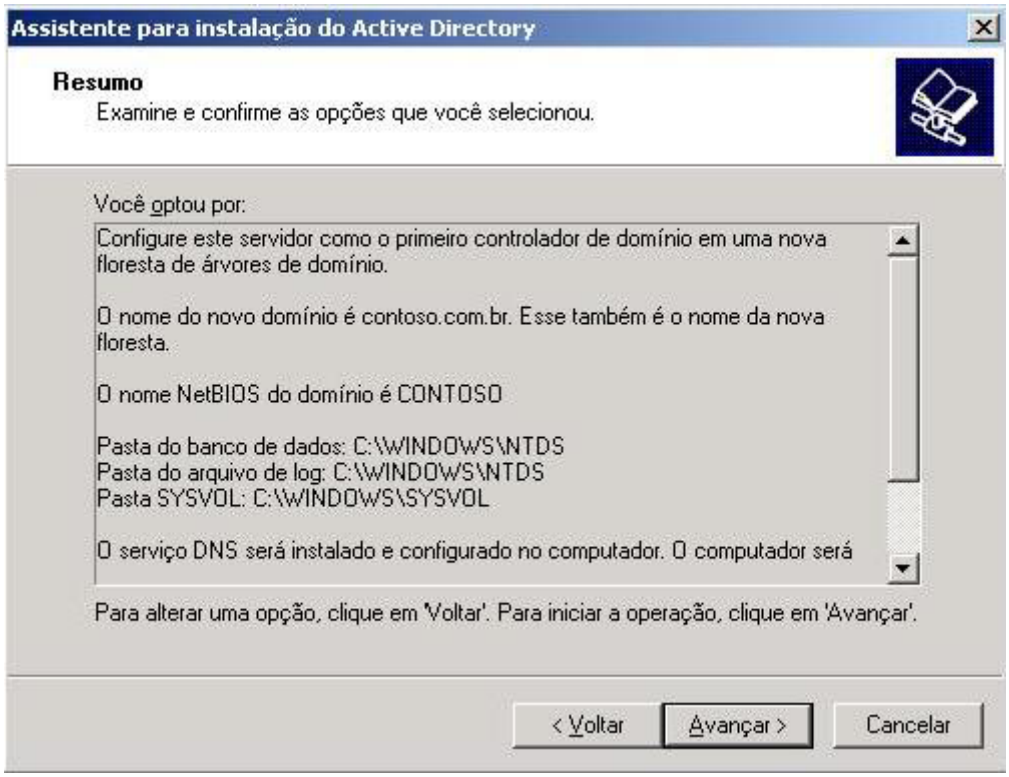
Portanto, o mais recomendável é utilizar o servidor DNS do Windows Server 2003 e deixar que o assistente faça a instalação e configuração do mesmo.
Selecione a opção “Instalar e configurar o servidor DNS neste computador e definir este computador para usar o servidor DNS como seu servidor DNS preferencial” e clique no botão “Avançar”.

Na janela de “Permissões”, selecione a opção “Permissões compatíveis somente com os sistemas operacionais de servidor Windows 2000 ou Windows Server 2003” e clique no botão “Avançar”. Esta opção somente deverá ser alterada caso você tenha DCs rodando em plataforma Windows NT, o que não é o caso do nosso artigo.

Na janela de senha, digite e confirme a senha de administrador do modo de restauração; clique no botão "Avançar".
Esta senha é importante, pois ela não é a mesma senha do administrador do DC e deve ser usada quando houver problemas no DC ou quando o DC for removido do computador.



Na janela de "Resumo", verifique as opções selecionadas. Caso as opções estejam corretas, clique no botão "Avançar".



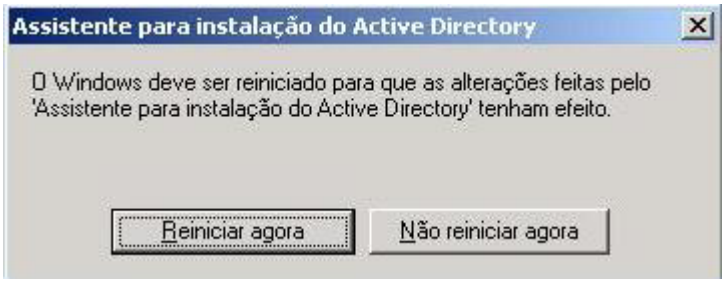
Você irá acompanhar o assistente executando as tarefas solicitadas.

Nunca clique no botão "Cancelar", pois você irá estragar todo o computador! Caso tenha cometido algum erro, aguarde o assistente finalizar e depois o execute novamente para desfazer as alterações.

Caso as tarefas tenham sido realizadas com sucesso, você obterá a seguinte tela:

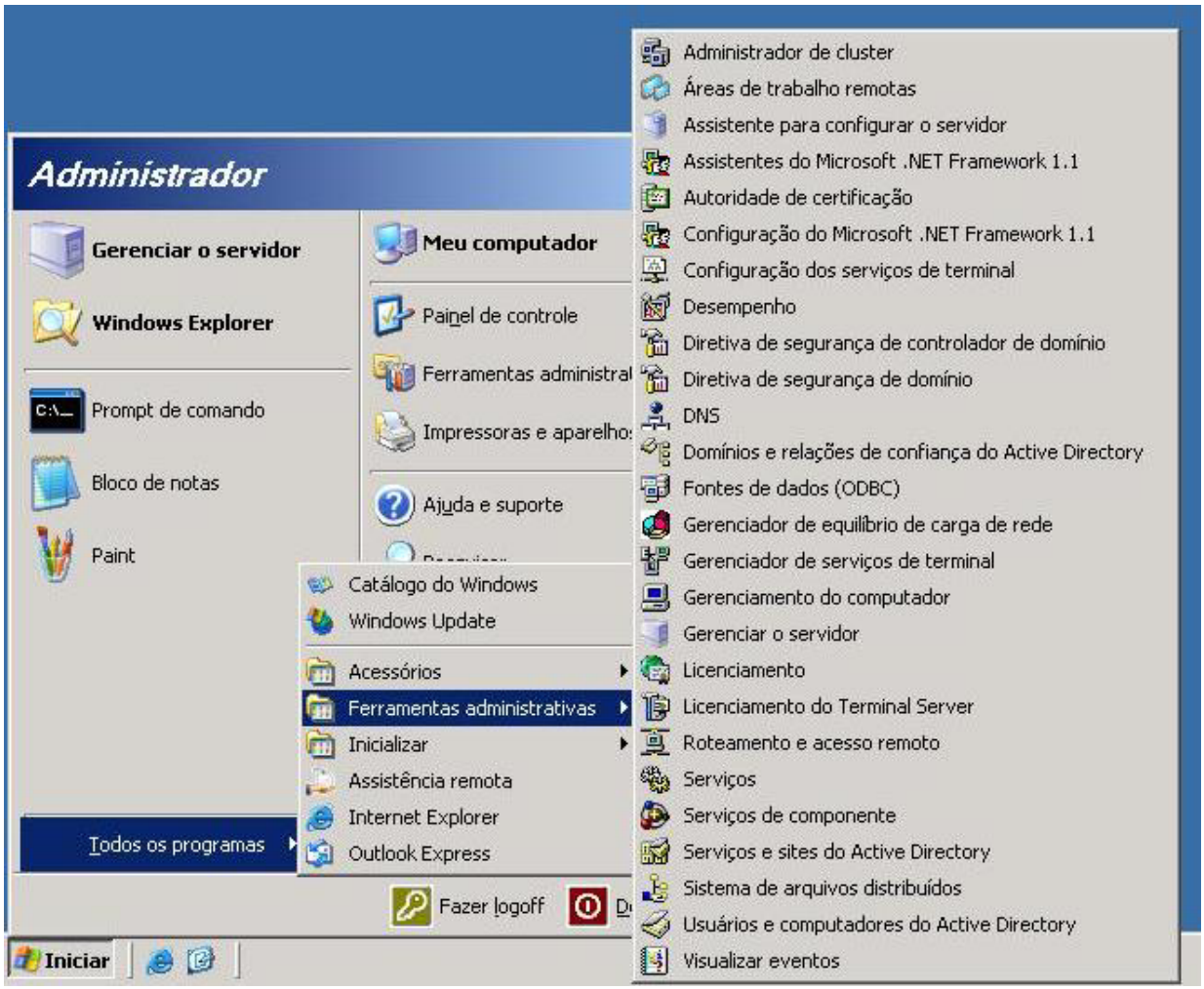
Clique no botão “Concluir”.

Você precisará reiniciar o computador para iniciar o AD. Clique no botão “Reiniciar agora”.



3.3 Verificando a instalação do AD

Nesta etapa iremos verificar se a instalação do AD foi realizada com sucesso.Primeiro, vamos verificar se todas as ferramentas de administração do AD foram instaladas. Clique no menu Iniciar, Todos os programas, Ferramentas administrativas.Como mostra a figura abaixo:



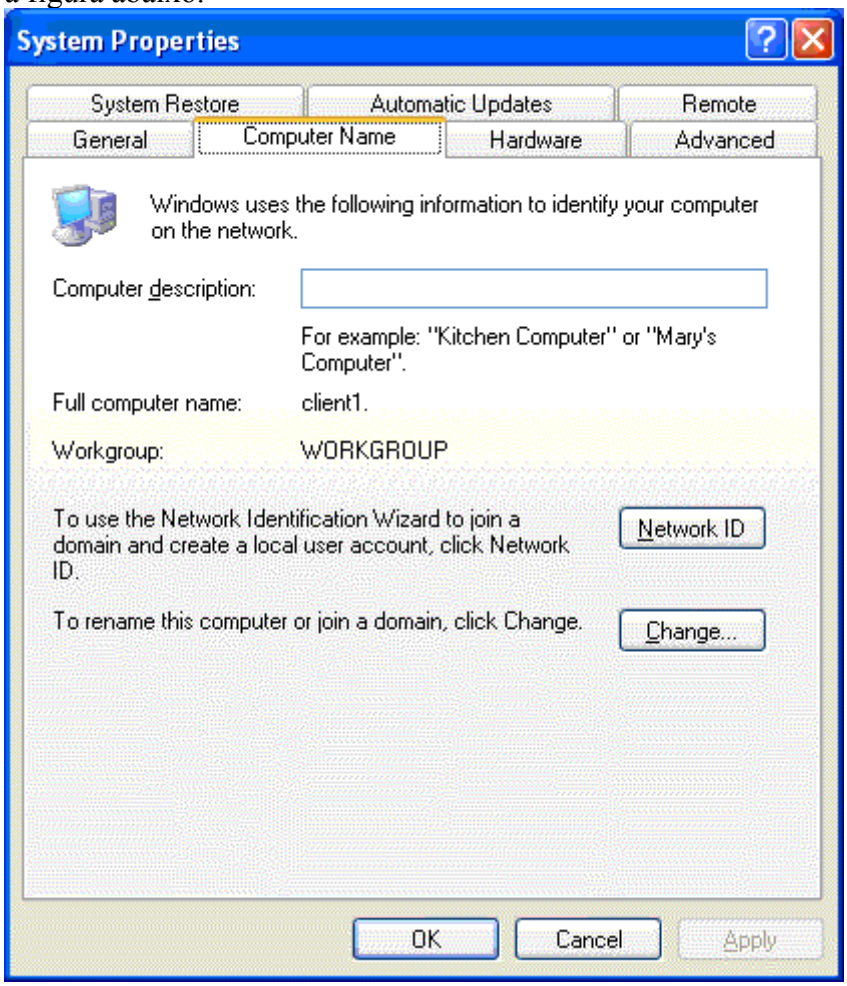
Verifique se aparece o item “Usuários e computadores do Active Directory”. Clique nele e verifique se o domínio “contoso.com. br” foi criado,pronto o Ad já esta em funcionamento.

4. Criando uma base de usuários

Logo depois da instalação eu criei uma base de usuários para fazer os primeiros testes. Para criar uma base de usuários que vão acessar o domínio acesse o item Usuários e computadores do Active Directory,O próximo passo e entrar no diretório Users e adicionar os novos usuários, clicando o botão direito em novo>usuário.Apos nomear a conta do usuário defini a política de inicial de senhas para esse usuário, como por exemplo que o usuário tem que alterar a senha no próximo logon, no meu caso desabilitei esse campo pois estou apenas fazendo testes,ainda aparecem os campos o usuário não pode alterar a senha e a senha nunca expira.Em seguida, inseri os demais usuários criados em grupos, e dessa forma defini suas permissões no sistema,apenas de um clique duplo sobre o grupo que deseja adicionar o usuário como por exemplo grupo alunos,clique sobre a aba membros e em seguida no botão adicionar.

5.Testes

Após a instalação, verificação da instalação do AD e a criação da base de usuários, o próximo passo foi o teste, ou seja, autenticar o meu domínio criado no servidor 2003 numa maquina rodando WINDOWS XP PROFESSIONAL.Para fazer esse teste usei uma máquina com os mesmos recursos de hardware do servidor 2003.O primeiro passo foi configurar a rede com a mesma classe de IP do servidor, no meu caso 192.168.8.1. Logo depois fui ingressar a minha maquina XP ao meu domínio,clicando com o botão direito do mouse em meu computador indo até a aba nome do computador como mostra a figura abaixo.



Logo depois basta clicar no botão alterar, em seguida modifique onde esta marcado membro de, para domínio não mais para grupo de trabalho, digite no campo de domínio o seu domínio criado no servidor nesse caso contoso.com. br,. O computador fará uma busca procurando pelo domínio, quando ele achar aparecera uma janela pedindo para você se logar basta então colocar o nome da conta e senha, pronto agora você já esta logado no Windows XP através do domínio contoso.com. br,De agora em diante cada vez que o computador for acessado na tela inicial aparece uma janela de logon no domínio, onde o usuário terá que digitar seu nome e senha e o domínio no qual está logando.

6.Contas de usuários

Essas informações que foram digitadas na janela de logon no domínio são repassadas para um DC de domínio no Servidor 2003, onde essas informações são verificadas. Se o nome de usuário existir, a senha estiver correta e a conta não estiver bloqueada pelo administrador, o logon será liberado e a área de trabalho será carregada.Uma vez que o usuário fez logon no domínio, ele passou a ser identificado, ou seja, todas a ações que o usuário executar estarão associadas com a sua conta de usuário.Por exemplo, se o usuário Pedro fizer o logon no domínio ABC e tentar acessar um arquivo para o qual ele não tem permissão, ficará registrado nos logs de auditoria do servidor.

Identificação do usuário – no exemplo Pedro.
Data e hora da tentativa de acesso.
Nome do arquivo e/ou pasta que o usuário tentou acessar.

Isso mostra que a conta de usuário e sua identidade na rede, tudo que ele fizer ou tentar fazer estará sendo monitorado pelo administrador.

7.Conclusão

O Active directory trás uma nova visão de como os usuários possam acessar os recursos disponíveis na rede, tendo uma base de usuários única, o que facilita muito o usuário que terá só uma conta para acessar todas as máquinas da rede. O AD e um serviço de diretórios que é um serviço de redes, o qual identifica todos os recursos de rede, o qual identifica todos os recursos disponíveis em uma rede mantendo informações sobre estes dispositivos (conta de usuários, grupos, computadores, recursos, políticas de segurança, etc.) em um banco de dados e torna estes recursos disponíveis para usuários e aplicações. Enfim achei um recurso muito interessante que dá ao administrador controle total sobre sua rede.

8. Referências

- Tadeu Carmona ,Roberto A Hexsel “Universidade Redes”.
- Julio Basttiti “Certificação Microsoft- Guia de estudos para o MCSE 70-290”.
- http://www.juliobattisti.com.br/fabiano/artigos/activedirectory.asp ,acessado em 16 de abril de 2007.
- http://www.itcentral.com.br/, acessado em 21 de abril de2007.