Tutorial de Active Directory – Parte 3

Introdução

Prezados leitores, esta é a terceira 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.

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.

Entendendo o conceito de Diretórios e Workgroups

Introdução

Nesta parte do tutorial mostrarei as diferenças entre uma rede baseada no modelo de Workgroup e uma rede baseada no modelo de diretórios.

Você entenderá porque uma rede baseada no conceito de Workgroup (Grupo de trabalho) somente é indicada para redes muito pequenas, entre cinco e dez computadores, no máximo. E porque para redes maiores seria praticamente impossível administrar um modelo de redes baseado em Grupos de Trabalho ao invés de domínios.

Domínios e Grupos de Trabalho (Workgroups)

Um rede baseada no Windows Server 2003 ou no Windows 2000 Server pode ser criada utilizando-se dois conceitos/modelos de implementação diferentes, dependendo da maneira com que os Servidores Windows Server 2003 (ou Windows 2000 Server) são configurados. Os servidores podem ser configurados para fazerem parte de um Domínio ou de um Grupo de Trabalho, mais comumente chamado de Workgroup (termo que utilizarei de agora em diante).

Entendendo o funcionamento de uma rede baseada no modelo de Workgroups

Em uma rede baseada no modelo de Workgroups cada servidor é independente do outro. Em outras palavras, os servidores do Workgroup não compartilham uma lista de usuários, grupos e outras informações. Cada servidor tem a sua própria lista de usuários e grupos, conforme indicado no diagrama da Figura a seguir:

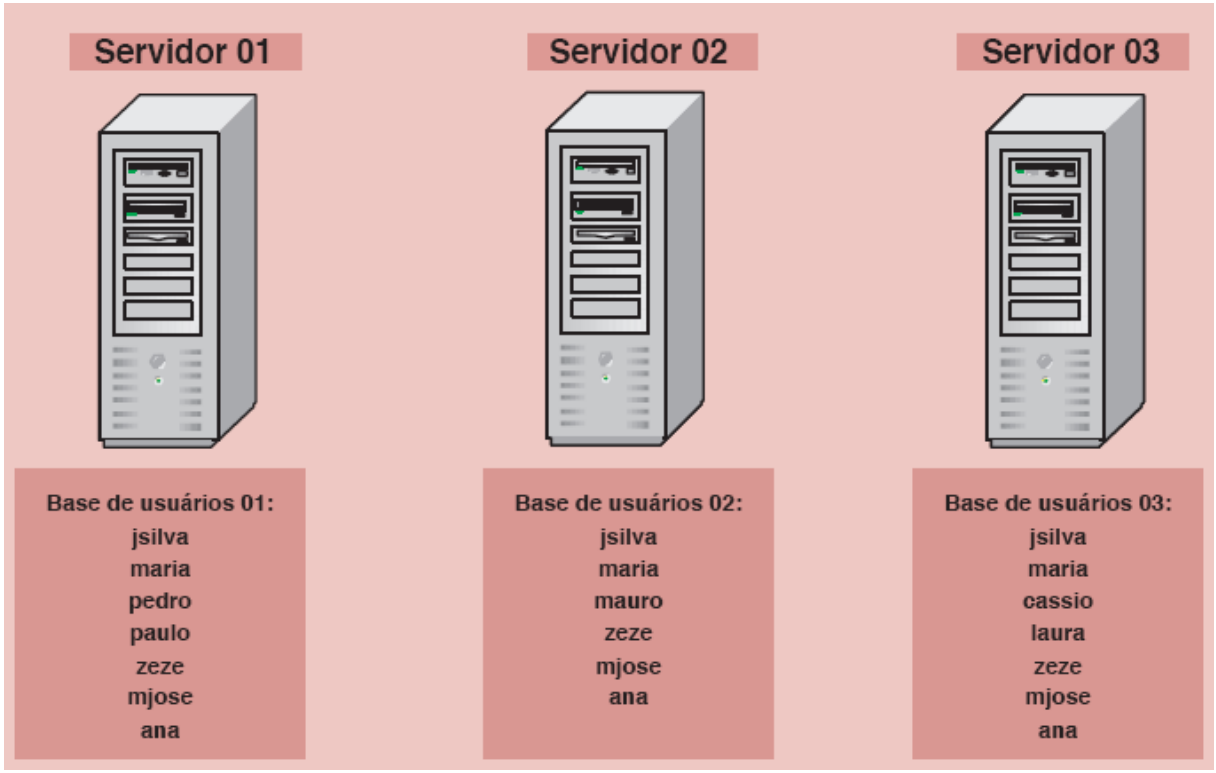

Figura - Uma rede baseada no conceito de Workgroup.

O diagrama demonstra uma rede baseada no modelo de Workgroup. Na rede de exemplo temos três servidores, onde cada servidor tem a sua própria base de usuários, senhas e grupos. Conforme pode ser visto no diagrama, as bases não estão sincronizadas, existem contas de usuários que foram criadas em um servidor mas não foram criadas nos demais. Por exemplo, a conta paulo somente existe no Servidor 01, a conta mauro só existe no Servidor 02 e a conta cassia só existe no servidor 03.

Agora imagine o usuário **paulo**, que está utilizando a sua estação de trabalho. Ele tenta acessar um recurso (por exemplo uma pasta compartilhada) no **Servidor 01**. Uma janela de logon é exibida. Ele fornece o seu nome de usuário e senha e o acesso é liberado (desde que ele tenha as devidas permissões).

Agora este mesmo usuário – **paulo**, tenta acessar um recurso no **Servidor 02**. Novamente uma tela de logon é exibida e ele fornece o seu nome de usuáro e senha. O acesso é negado, com uma mensagem de usuário inválido. E o usuário paulo fica sem entender o que está acontecendo. Orá, isso acontece porque o usuário paulo somente está cadastrado no Servidor 01; para o Servidor 02 e para o Servidor 03 é como se o usuáro paulo não existisse (usuário inválido). Para que o usuário paulo possa acessar recursos dos servidores 02 e 03, o Administrador deveria criar uma conta chamada “paulo” também nestes dois servidores.

Mas a “confusão” pode ser maior ainda. Imagine que o usuário paulo foi cadastrado pelo administrador com a conta paulo e senha: **abc123de**. Muito bem, o administrador fez o cadastro do usuário paulo nos três servidores: Servidor 01, Servidor 02 e Servidor 03. Agora, cerca de 30 dias depois, o usuário paulo resolveu alterar a sua senha. Vamos supor que ele estava conectado ao Servidor 01, quando fez a alteração da sua senha para: **xyz123kj**. Agora o usuário paulo está na situação indicada a seguir:

Servidor	Usuário	Senha
Servidor 01	paulo	xyz123kj
Servidor 02	paulo	abc123de
Servidor 03	paulo	abc123de

Na concepção do usuário paulo, a partir de agora vale a sua nova senha, independentemente do servidor que ele esteja acessando. Pois para o usuário interessa o recurso que ele está acessando. Para o usuário não interessa se o recurso está no servidor 01, 02 ou outro servidor qualquer. Agora vamos ver o que acontece com o usuário paulo.

O usuário paulo, que está utilizando a sua estação de trabalho. Ele tenta acessar um recurso (por exemplo uma pasta compartilhada) no Servidor 01. Uma janela de logon é exibida. Ele fornece o seu nome de usuário e a nova senha e o acesso é liberado (desde que ele tenha as devidas permissões). Como ele fez a troca de senha, enquanto estava conectado ao Servidor 01, a nova senha está valendo no servidor 01

Agora este mesmo usuário – paulo, tenta acessar um recurso no Servidor 02. Novamente uma tela de logon é exibida e ele fornece o seu nome de usuáro e a nova senha e a surpresa: O acesso é negado, com uma mensagem de falha na autenticação. Aí o usuário fica pensando: mas como é possível, eu recém troquei a senha (o usuário não sabe que, no modelo de Workgroup, não existe uma sincronização entre as informações dos servidores). **Ele trocou a senha no Servidor 01. Para os demais servidores continua valendo a senha antiga**. A única maneira de ele conseguir alterar a senha é fazendo o logon com a senha antiga e alterando para a nova senha, em todos os servidores da rede. Agora imagine o problema em uma rede de grandes proporções, com dezenas de servidores e milhares de funcionários. Fica fácil concluir que o modelo de Workgroup ficaria insustentável, impossível de ser implementado na prática, para redes de média a grande porte. Eu somente recomendaria modelo de Workgroup para redes pequenas, com um único servidor e com um número de, no máximo, 10 usuários.

O funcionamento de uma rede baseada no conceito de Diretório – Domínio

Agora vou apresentar o modelo de rede baseado em um diretório. Vamos iniciar considerando o diagrama da Figura a seguir:

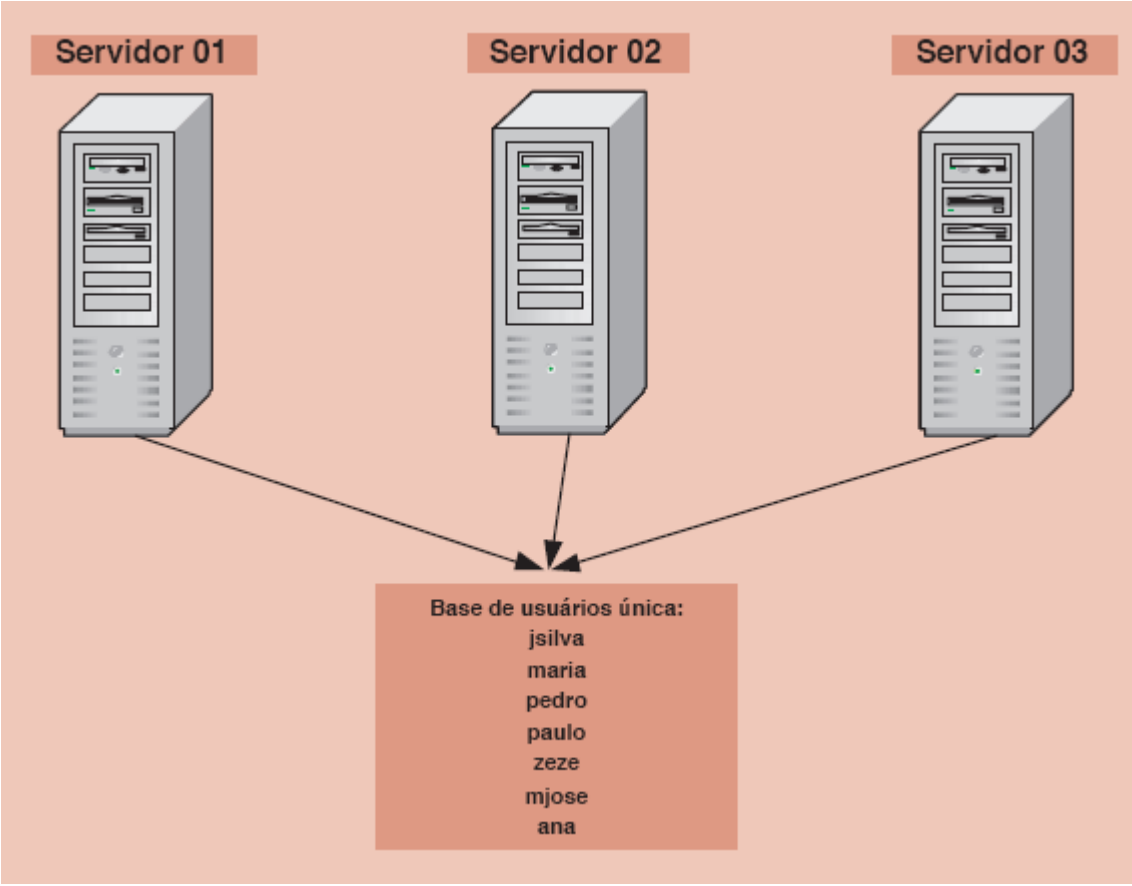

Figura - Uma rede baseada no conceito de Diretório - Domínio.

No modelo baseado em diretório, nos temos uma base de usuários única, ou seja, todos os servidores da rede compartilham a mesma base de usuários. O que acontece, na prática, não é que existe uma única base, armazenada em um determinado servidor, e todos os demais servidores acessam esta base. Não, não é isso. O que ocorre na prática, é que todos os servidores contém uma cópia da base de informações do diretório. Alterações efetuadas em um dos servidores são repassadas para os demais servidores da rede, para que todos fiquem com uma cópia idêntica da base de dados do diretório. Esta sincronização entre os servidores do domínio é conhecida como Replicação do Active Directory.

É importante salientar que o que é replicado, entre os servidores, são as informações do Active Directory, tais como a lista de contas de usuários e respectivas senhas, lista de grupos de usuários e seus membros, políticas de segurança e demais informações do domínio. O conteúdo dos servidores, tais como arquivos, pastas e impressoras compartilhadas, configurações de serviços, tais como SQL Server, IIS, Exchange Server, etc. não são compartilhadas.

O que caracteriza uma rede baseada em diretório é o fato de todos os servidores terem acesso a mesma base de dados do Active Directory, ou seja, todos compartilham o mesmo diretório, as mesmas informações sobre usuários, grupos, servidores e recursos. No próximo tópico será apresentado o conceito de domínio, floresta, relação de confiança, etc. Estes são outros elementos relacionados com o diretório e que permitem a criação de redes de grande extensão

geográfica, como por exemplo redes de uma grande empresa com escritórios no mundo inteiro (Microsoft).

No modelo baseado em diretório, a vida do Administrador fica bem mais fácil. Vamos supor que o usuário paulo queira acessar um recurso em um dos servidores da rede. Sem problemas, qualquer servidor tem uma cópia da base de dados do diretório. Com isso a conta do usuário paulo estará disponível em qualquer servidor que faça parte do domínio. Com isso ele poderá acessar recursos em qualquer um destes servidores. Há, mas se o usuário paulo alterar a sua senha. Isso será feito na cópia do banco de dados do diretório de um dos servidores. Correto? Correto, porém em pouco tempo esta alteração será replicada para todos os demais servidores e a senha do usuário paulo estará sincronizada em todos os servidores.

O modelo baseado em diretórios (e no conceito de domínios, florestas, etc) é bem mais fácil para administrar e permite a implementação de redes de grandes proporções, tanto geográficas quanto em números de usuários. Na empresa onde eu trabalho, temos uma rede baseada no Active Directory. A rede se estende por todos os estados do território nacional e tem cerca de 22.000 usuários. Uma rede e tanto. Seria literalmente impossível manter uma rede destas proporções sem utilizar o modelo baseado em diretórios.

Domínios, Árvores de domínios e Unidades Organizacionais – Conceitos

Agora que você já conhece bem a diferença entre um modelo de rede baseada em Workgroup e outro de rede baseada em diretórios, é hora de avançar um pouco mais e nós aproximar da terminologia do Active Directory. Neste item vou apresentar o conceito de diretório. Não um conceito formal, como o apresentado na Parte 2 deste Tutorial, mas sim o conceito de diretório que é utilizado em redes baseadas no Active Directory e no Windows Server 2003 (ou Windows 2000 Server).

No Windows Server 2003 (e também no Windows 2000 Server), o conjunto de servidores, estações de trabalho, bem como as informações do diretório é que formam uma unidade conhecida como Domínio. Todos os servidores que contém uma cópia da base de dados do Active Directory, fazem parte do domínio. As estações de trabalho podem ser configuradas para fazer parte do domínio. No caso de estações de trabalho com o NT Workstation 4.0, Windows 2000 Professional ou Windows XP Professional, cada estação de trabalho que faz parte do domínio, tem uma conta de computador criada no domínio. A conta de computador tem o mesmo nome do computador. Por exemplo, a estação de trabalho **micro-cont-001**, tem uma conta de computador, na base de dados do Active Directory, com o nome de **micro-cont-001**.

Um domínio pode também ser definido com um limite administrativo e de segurança. Ele é um limite administrativo, pois as contas de Administrador do domínio tem permissões de acesso em todos os recursos do domínio, mas não em recursos de outros domínios.

Ele é um limite de segurança porque cada domínio tem definições de políticas de segurança que se aplicam as contas de usuários e demais recursos dentro de domínio e não a outros domínios. Ou seja, diferentes domínios podem ter diferentes políticas e configurações de segurança. Por exemplo, no domínio A, posso ter uma política de segurança que define um tamanho mínimo de senha como 8 caracteres. Esta política será válida para todas as contas de usuário do domínio A. Um segundo domínio B, pode ter uma política de segurança diferente, a qual define um tamanho mínimo de senha de 12 caracteres. Esta política será válida para todas as contas de usuários do domínio B.

Um Domínio é simplesmente um agrupamento lógico de contas e recursos, os quais compartilham políticas de segurança. As informações sobre os diversos elementos do domínio (contas de usuários, contas de computador, grupos de usuários, políticas de segurança, etc), estão contidas no banco de dados do Active Directory.

PARA NÃO ESQUECER: Não existe domínio sem o Active Directory. Um domínio é criado quando o Active Directory é instalado no primeiro servidor. Ao instalar o Active Directory, o servidor torna-se um DC – Domain Controller. O DC contém uma cópia da base de dados do Active Directory. Na base de dados do Active Directory ficam, dentre outras, informações tais como: Contas e senhas de todos os usuários, grupos de usuários e membros de cada grupos, contas de computador e assim por diante. Um domínio pode ter vários DCs. Qualquer alteração feita nas informações do Active Directory, em qualquer um dos DCs será replicada, automaticamente, para todos os demais DCs do domínio. O resultado prático é que todos os DCs possuem uma cópia idêntica do AD.

Em um domínio baseado no Active Directory e no Windows Server 2003 é possível ter dois tipos de servidores Windows Server 2003:

- Controladores de Domínio (DC – Domain Controlers)
- Servidores Membro (Member Servers).

A criação de contas de usuários, grupos de usuários e outros elementos do Active Directory, bem como alterações nas contas de usuários, nas políticas de segurança e em outros elementos do Active Directory, podem ser feitas em qualquer um dos Controladores de Domínio. Uma alteração feita em um DC será automaticamente repassada (o termo técnico é "replicada") para os demais DCs do Domínio. Por isso se você cria uma conta para o usuário jsilva e cadastra uma senha para este usuário, essa conta passa a ser válida em todo o domínio, sendo que o usuário jsilva pode receber permissões para acessar recursos e serviços em qualquer servidor do Domínio, seja em um Controlador de Domínio ou em um Member Server.

Por isso que o Domínio transmite a idéia de um agrupamento lógico de Contas de Usuários e Grupos, bem como de políticas de segurança, uma vez que todo o Domínio compartilha a mesma lista de Usuários, Grupos e políticas de segurança. A criação de domínios facilita enormemente a administração de uma rede baseada no Windows Server 2003, sendo altamente recomendada para qualquer rede de maior porte seja criada com base em um ou mais domínios (dependendo do porte da rede).

Nos Servidores Membros podem ser criadas contas de usuários e grupos, as quais somente serão válidas no Servidor Membro onde foram criadas. Embora isso seja tecnicamente possível, essa é uma prática não recomendada, uma vez que isso dificulta enormemente a administração de um Domínio. Você pode atribuir permissões para os Recursos de um Servidor Membro, à contas de Usuários e Grupos do domínio, sem a necessidade de criar esses usuários ou grupos localmente. Por exemplo, um usuário jsilva, que pertence ao domínio, pode receber permissões de acesso em uma pasta compartilhada de um Servidor Membro. Com isso você pode concluir que um Servidor Membro, é um servidor que embora não mantenha uma cópia da lista de usuários e grupos do Active Directory, este tem acesso a essa lista. Com isso podem ser atribuídas permissões nos recursos do Servidor Membro (tais como pastas compartilhadas, impressoras, etc) para as contas e grupos do Domínio.

Os DCs também são responsáveis por fazer a autenticação dos usuários na rede. Por exemplo, vamos supor que o usuário jsilva trabalha em uma estação de trabalho com o Windows XP Professional instalado. Esta estação foi configurada para fazer parte do domínio. Quando o usuário jsilva liga a estação de trabalho e o Windows é inicializado, é apresentada a tela de logon para que ele forneça o seu nome de usuário e senha. O Windows precisa verificar se o nome de usuário e senha estão corretos. A Windows tenta localizar um DC na rede. É no DC que a verificação é feita, comparando as informações digitadas pelo usuário, com as informações da base de dados do Active Directory. Se as informações estão OK o logon é liberado, o usuário é autenticado e a área de trabalho do Windows é exibida. A partir deste momento, toda vez que o usuário tentar acessar um recurso do domínio, será apresentada a sua autenticação, com base nas informações de logon apresentadas, para provar a identidade do usuário para a rede. Isso evita que o usuário tenha que entrar com o seu logon e senha

cada vez que for acessar um recurso em um servidor diferente (que é justamente o que acontece no modelo baseado em Workgroup, conforme descrito anteriormente).

Como os Servidores Membro não possuem uma cópia da lista de usuários e grupos, estes não efetuam a autenticação dos clientes e também não armazenam informações sobre as políticas de segurança para o Domínio – as quais também são conhecidas por GPO – Group Polices Objects.

NÃO ESQUEÇA: Estações de trabalho com o Windows XP Home, não podem ser configuradas para fazer parte de um domínio baseado no Active Directory. Estações de trabalho com o Windows 95/98/Me podem ser configuradas para fazer parte de um domínio. Para que estações com o Windows 95/98/Me possam ter acesso a maioria dos recursos do Active Directory, é preciso instalar o Active Directory Client, nestas estações de trabalho. Uma estação de trabalho com o NT Workstation 4.0 também pode ser configurada para fazer parte de um domínio baseado no Active Directory e no Windows Server 2003 ou Windows 2000 Server.

Quando os servidores Windows Server 2003 são configurados para trabalhar com um Workgroup, não existe o conceito de domínio e nem de Controlador de Domínio. Cada servidor mantém uma lista separada para contas de usuários, grupos e políticas de segurança, conforme descrito anteriormente. Com isso se um usuário precisa acessar recursos em três servidores, por exemplo, será necessário criar uma conta para esse usuário nos três servidores diferentes. Um Workgroup somente é recomendado para redes extremamente pequenas, normalmente com um único servidor Windows Server 2003 e não mais do que 10 estações clientes, conforme descrito anteriormente.

Conclusão

Nesta parte do tutorial apresentei dois conceitos de fundamental importância para entender o Active Directory: Modelo de Rede Baseada em Workgroups e Modelo de Rede Baseada em Domínios. Pelo que foi descrito, foi possível concluir que as redes baseadas em Workgroup só devem ser utilizadas para redes extremamente pequenas, normalmente com um único servidor Windows Server 2003 e não mais do que 10 estações clientes. Já para redes maiores, o único modelo viável é o modelo baseado em Domínios.

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:

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