Tutorial de Active Directory – Parte 5

Introdução

Prezados leitores, esta é a quinta 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.

Conhecendo os principais Objetos de um domínio

Nas partes anteriores desta série de tutoriais sobre o Active Directory apresentei os conceitos básicos sobre diretórios, domínios, unidades organizacionais e árvores de diretórios. A partir desta parte passarei a descrever os objetos que fazem parte do Active Directory. Na seqüência falarei sobre os serviços que dão suporte ao Active Directory, tais como os serviços de replicação e o conceito de relações de confiança entre diretórios.

Contas de usuários

Todo usuário que precisa ter acesso aos recursos dos computadores do domínio (pastas compartilhadas, impressoras compartilhadas, etc) deve ser cadastrado no Active Directory. Cadastrar o usuário, significa criar uma conta de usuário e uma senha. Ao cadastrar um usuário, outras informações tais como seção, nome completo, endereço, telefone, etc, podem ser cadastradas.

Uma conta de usuário é um objeto do Active Directory, o qual contém diversas informações sobre o usuário, conforme descrito anteriormente. É importante salientar que a conta somente precisa ser criada uma vez, em um dos Controladores de domínio (DCs). Uma vez criada, a conta será replicada para todos os demais DCs do domínio.

Você também pode criar contas nos servidores membros e nas estações de trabalho com Windows 2000 Professional ou Windows XP Professional. As contas criadas nestes computadores são ditas contas locais, ou seja, somente existem no computador onde foram criadas. Vamos imaginar que você está trabalhando em uma estação de trabalho com o Windows XP Professional instalado. Esta estação foi configurada para fazer parte do domínio abc.com.br. Como a estação de trabalho faz parte do domínio, você terá acesso a lista de usuários e grupos do domínio. Com isso você poderá, por exemplo, atribuir permissão de acesso para um usuário do domínio (ou um grupo de usuários do domínio) em uma pasta compartilhada, na sua estação de trabalho. Nesta mesma estação você também poderá criar contas de usuários e grupos locais, os quais ficam gravados na base de usuários local, a qual só existe no computador onde ela é criada. Cada computador terá a sua própria base local de usuários e grupos, além de ter acesso a lista de usuários e grupos do domínio (caso a estação de trabalho esteja configurada para fazer parte de um domínio). Estes usuários e grupos (criados localmente), somente podem receber permissões de acesso para os recursos do computador onde foram criados. Você não conseguirá atribuir permissão de acesso em uma pasta compartilhada no servidor, para um usuário local da sua estação de trabalho, pois as contas e grupos locais, criados no seu computador, não são “visíveis” nos demais computadores e servidores da rede.

Embora seja tecnicamente possível a criação de usuários e grupos locais, nos Servidores Membros e nas estações de trabalho, esta prática não é recomendada. Quando você trabalha em um domínio, o ideal é que contas de usuários e grupos sejam criadas somente no domínio, isto é, nos DCs.

Importante: O Administrador pode utilizar o recurso de GPOs – Group Polices Objects para impedir que os usuários possam criar contas de usuários e grupos locais, em suas estações de trabalho. O assunto GPOs é abordado, em detalhes, no Capítulo 18 do seguinte Livro, de minha autoria: Windows Server 2003 – Curso Completo, 1568 páginas. Maiores detalhes sobre o livro, acesse o seguinte endereço: http://www.juliobattisti.com.br/loja/vendalivro.asp?CODIGO=WIN3K

Algumas recomendações e observações sobre contas de usuários:

- Todo usuário que acessa a rede deve ter a sua própria conta. Não é recomendado que dois ou mais usuários compartilhem a mesma conta e a respectiva senha. A conta é a identidade do usuário para a rede. Por exemplo, quando o usuário jsilva faz o logon no domínio, a sua conta é a sua identidade para o sistema. Todas as ações realizadas pelo usuário estão associadas a sua conta. O Windows Server 2003 tem um sistema de auditoria de segurança, no qual o Administrador pode configurar quais ações devem ser registradas no Log de auditoria. Por exemplo, o administrador pode definir que toda tentativa de alterar um determinado arquivo seja registrada no log de auditoria. Se o usuário jsilva tentar alterar o referido arquivo, ficará registrado no logo de auditoria que o usuário jsilva, no dia tal, hora tal, tentou alterar o arquivo tal. Se dois ou mais usuários estão compartilhando a mesma conta, fica difícil identificar qual o usuário que estava logado no momento em que uma determinada ação foi executada. Para o sistema é o jsilva. Agora quem dos diversos usuários que utilizam a conta jsilva é que estava logado e tentou alterar o referido arquivo? Fica difícil saber, para não dizer impossível. Por isso a recomendação para que cada usuário seja cadastrado e tenha a sua própria conta e senha.

- Com base nas contas de usuários e grupos, o administrador pode habilitar ou negar permissões de acesso aos recursos da rede. Por exemplo, o administrador pode restringir o acesso a pastas e arquivos compartilhados na rede, definindo quais usuários podem ter acesso e qual o nível de acesso de cada usuário – leitura, leitura e alteração, exclusão e assim por diante. Mais um bom motivo para que cada usuário tenha a sua própria conta e senha.

Padrão para nomeação de contas:

Outro detalhe que você deve observar, é a utilização de um padrão para o nome das contas de usuários. Você deve estabelecer um padrão para a criação de nomes, pois não podem existir dois usuários com o mesmo nome de logon dentro do mesmo Domínio. Por exemplo se existir no mesmo Domínio, dois “José da Silva” e os dois resolverem utilizar como logon “jsilva”, somente o primeiro conseguirá, o segundo terá que se conformar em escolher um outro nome de logon. Para isso é importante que seja definido um padrão para a nomeação de contas. No caso de nomes iguais deve ser definido uma maneira de diferenciá-los. Por exemplo poderíamos usar como padrão a primeira letra do nome e o último sobrenome. No caso de nomes iguais, acrescenta-se números. No nosso exemplo o primeiro José da Silva cadastrado ficaria como jsilva, já o segundo a ser cadastrado ficaria como jsilva1. Caso no futuro tivéssemos mais um José da Silva dentro da mesma Unidade Organizacional, este seria o jsilva2 e assim por diante.

Quando for criar nomes de logon para os usuários, leve em consideração os seguintes detalhes:

- Nomes de Usuários do Domínio devem ser únicos dentro do Domínio.
- Podem ter no máximo 20 caracteres.
- Os seguintes caracteres não podem ser utilizados: “ / \ : ; [ ] | = , + * ? < >

Sempre que você for cadastrar um usuário também deve ser cadastrada uma senha para o usuário. O administrador pode especificar um número mínimo de caracteres aceito para a senha. O número máximo de caracteres da senha é 128.

IMPORTANTE: Para as senhas, o Windows Server 2003 distingue letras maiúsculas de minúsculas. Por exemplo a senha “Abc123” é diferente da senha “abc123”.

Contas de Computador

Estações de trabalho que rodam o Windows NT Workstation 4.0, Windows 2000 Professional ou Windows XP Professional e que fazem parte do domínio, devem ter uma conta de computador no Active Directory. Servidores, quer sejam Member Servers ou DCs, rodando Windows NT Server 4.0, Windows 2000 Server ou Windows Server 2003, também tem contas de computador no Active Directory.

A conta de computador pode ser criada antes do computador ser adicionado ao domínio ou no momento em que o computador é configurado para fazer parte do domínio. A conta do computador deve ter o mesmo nome do computador na rede. Por exemplo, um computador com o nome de **microxp01**, terá uma conta no Active Directory, com o nome: **microxp01**.

Não Esqueça: Computadores rodando Windows 95/98/Me, mesmo tendo acesso a lista de usuários e grupos do domínio, não terão contas de computador criadas no Active Directory.

Grupos de usuários

Um grupo de usuários é uma coleção de contas de usuários. Por exemplo, podemos criar um grupo chamado Contabilidade, do qual farão parte todos os usuários do departamento de Contabilidade (todas as contas de usuários dos funcionários do departamento de Contabilidade).

A principal função dos grupos de usuários é facilitar a administração e a atribuição de permissões para acesso a recursos, tais como: pastas compartilhadas, impressoras remotas, serviços diversos, etc.

Ao invés de dar permissões individualmente, para cada um dos usuários que necessitam acessar um determinado recurso, você cria um grupo, inclui os usuários no grupo e atribui permissões para o grupo. Para que um usuário tenha permissão ao recurso, basta incluir o usuário no grupo, pois todos os usuários de um determinado grupo, herdam as permissões do grupo.

Quando um usuário troca de seção, por exemplo, basta trocar o usuário de grupo. Vamos supor que o usuário jsilva trabalha na seção de contabilidade e pertence ao grupo Contabilidade. Com isso ele tem acesso a todos os recursos para os quais o grupo Contabilidade tem acesso. Ao ser transferido para a seção de Marketing, basta retirar o usuário jsilva do grupo Contabilidade e adicioná-lo ao grupo Marketing. Com isso o jsilva deixa de ter as permissões atribuídas ao grupo Contabilidade e passa a ter as mesmas permissões que tem o grupo Marketing. Este exemplo simples já consegue demonstrar o quanto a utilização de grupos pode facilitar a administração de atribuição de permissões.

Vamos analisar mais um exemplo. Suponha que exista um sistema chamado SEAT, para o qual somente um número restrito de usuários deve ter acesso, sendo que são usuários de diferentes seções. A maneira mais simples de definir as permissões de acesso ao sistema SEAT é criar um grupo chamado SEAT (ou outro nome qualquer que você escolha para o grupo, tais como Usuários do SEAT, ou Acesso ao SEAT, etc.) e dar permissões para esse grupo. Assim cada usuário que precisar acessar o sistema SEAT, deve ser incluído no grupo SEAT. Quando o usuário não deve mais ter acesso ao sistema SEAT, basta removê-lo do grupo SEAT. Simples, fácil e muito prático.

Na Figura a seguir apresento uma ilustração para o conceito de Grupo de usuários. O Grupo Contabilidade possui direito para um recurso compartilhado, o qual pode ser acessado através da rede. Todos os usuários que pertencem ao grupo contabilidade, também possuem permissão para acessar o recurso compartilhado, com os mesmos níveis de acesso do grupo Contabilidade, uma vez que os usuários de um grupo, herdam as permissões do grupo.

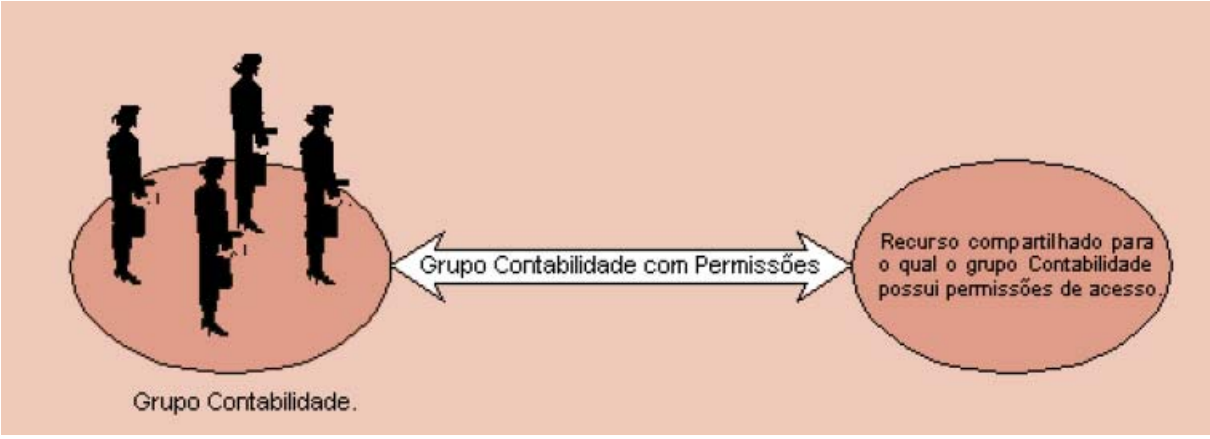

Figura - O Usuário herda as permissões do grupo.

Quando estiver trabalhando com grupos de usuários, considere os fatos a seguir:

- Grupos são uma coleção de contas de usuários.
- Os membros de um grupo, herdam as permissões atribuídas ao grupo.
- Os usuários podem ser membros de vários grupos
- Grupos podem ser membros de outros grupos.
- Contas de computadores podem ser membros de um grupo (novidade do Windows Server 2003).

Agora vou falar sobre os tipos de grupos existentes no Windows Server 2003. Os grupos são classificados de acordo com diferentes critérios, tais como: tipo, escopo e visibilidade.

Podemos ter dois tipos de grupos no Windows Server 2003 : Grupos de segurança (Security Groups) e Grupos de distribuição (Distribution Groups).

Classificação dos grupos quanto ao tipo

- **Grupos de segurança:** Normalmente utilizados para atribuir permissões de acesso aos recursos da rede. Por exemplo, ao criar um grupo Contabilidade, o qual conterá todas as contas dos funcionários do departamento de contabilidade, o grupo será utilizado para atribuir permissões de acesso a uma pasta compartilhada. Devo criar este grupo como sendo do tipo Grupo de segurança. Um grupo de segurança também pode ser utilizado como um grupo de distribuição, embora essa não seja uma situação muito comum. Esses grupos, assim como as contas de usuários são armazenados no Banco de dados do Active Directory.

- **Grupos de distribuição**: São utilizados para funções não relacionadas com segurança (atribuição de permissões) . Normalmente são utilizados em conjunto com servidores de e-mail, tais como o Exchange Server 2000 ou o Exchange Server 2003, para o envio de e-mail para um grupo de usuários. Uma das utilizações típicas para um Grupo de distribuição é o envio de mensagens de e-mail para um grupo de usuários de uma só vez. Somente programas que foram programados para trabalhar com o Active Directory, poderão utilizar Grupos de distribuição (como é o caso do Exchange 2000 Server citado anteriormente). Provavelmente as novas versões dos principais sistemas de correio eletrônico estarão habilitadas para trabalhar com o Active Directory. Não é possível utilizar grupos de distribuição para funções relacionadas com segurança.

Importante: É possível converter um grupo do tipo Segurança para distribuição e vice-versa. Para tal é preciso que o domínio esteja, pelo menos, no modo Windows 2000 Nativo. Para domínios que ainda estejam no modo Windows 2000 Mixed, esta conversão não será possível.

Nas próximas partes deste tutorial falarei sobre Modos de um Domínio e Modos de uma Árvore de Domínios.

Classificação dos grupos quanto ao Escopo

Quando criamos um grupo de usuários, devemos selecionar um tipo (descrito anteriormente) e um escopo. O Escopo permite que o grupo seja utilizado de diferentes maneiras para a atribuição de permissões. O escopo de um grupo, determina em que partes do domínio ou de uma floresta de domínios, o grupo é visível, ou seja, pode ser utilizado para receber permissões de acesso aos recursos da rede.

Existem três escopos para grupos de usuários, conforme descrito a seguir: Universal, Global e Local do domínio. Vamos apresentar as diversas características e usos de cada tipo de grupo.

Grupos universais (Universal group):

Como o próprio nome sugere são grupos que podem ser utilizados em qualquer parte de um domínio ou de uma árvore de domínios e podem conter como membros, grupos e usuários de quaisquer domínios. Em resumo:

- **Pode conter:** Contas de usuários, outros grupos universais, e grupos globais de qualquer domínio.
- **Pode ser membro de**: Grupos locais do domínio ou grupos universais de qualquer domínio.
- **Pode receber permissões:** para recursos localizados em qualquer domínio.

Conforme detalharei nas próximas partes deste tutorial, um domínio baseado no Active Directory pode estar em diferentes modos (Windows 2000 Nativo, Misto ou Windows Server 2003). Para cada modo existem diferentes possibilidades em relação aos grupos Universais:

- Quando o nível de funcionalidade do Domínio está configurado como Windows 2000 Nativo ou Windows Server 2003, os seguintes elementos podem ser incluídos como membros de um grupo universal: Usuários, grupos Globais e grupos Universais de qualquer domínio da floresta.

- Quando o nível de funcionalidade do Domínio está configurado como Windows 2000 Misto, não é possível criar grupos Universais.

- Quando o nível de funcionalidade do Domínio está configurado como Windows 2000 Nativo ou Windows Server 2003, um grupo Universal pode ser colocado como membro de um outro grupo Universal e permissões podem ser atribuídas em qualquer domínio.

- Um grupo pode ser convertido de Universal para Global ou de Universal para Local do domínio. Nos dois casos esta conversão somente pode ser feita se o grupo Universal não tiver como um de seus membros, outro grupo Universal.

Quando devemos utilizar grupos universais:

- Quando você deseja consolidar diversos grupos globais. Você pode fazer isso criando um grupo Universal e adicionando os diversos grupos globais como membros do grupo Universal.

- **Importante**: Os grupos Universais devem ser muito bem planejados. Não devem ser feitas alterações freqüentes nos membros de um grupo Universal, uma vez que este tipo de ação causa um volume elevado de replicação no Active Directory. Mais adiante quando for apresentado o conceito de Catálogo Global e de replicação no Active Directory, você verá o quão justificada é esta recomendação.

Grupo global:

Um grupo Global é "global" quanto aos locais onde ele pode receber permissões de acesso, ou seja, um grupo Global pode receber permissões de acesso em recursos (pastas compartilhadas, impressoras, etc) de qualquer domínio. Em resumo, considere as afirmações a seguir:

- **Pode conter:** Contas de usuários e grupos globais do mesmo domínio, ou seja, somente pode conter membros do domínio no qual o grupo global é criado.
- **Pode ser membro de**: Grupos universais e Grupos locais do domínio, de qualquer domínio e de grupos globais do mesmo domínio.
- **Pode receber permissões:** para recursos localizados em qualquer domínio.

Conforme detalharei nas próximas partes deste tutorial, um domínio baseado no Active Directory pode estar em diferentes modos (Windows 2000 Nativo, Misto ou Windows Server 2003). Para cada modo existem diferentes possibilidades em relação aos grupos Globais:

- Quando o nível de funcionalidade do Domínio está configurado como Windows 2000 Nativo ou Windows Server 2003, os seguintes elementos podem ser incluídos como membros de um grupo Global: contas de usuários e grupos globais do mesmo domínio. Por exemplo, se você cria um grupo global chamado WebUsers, no domínio abc.com.br, este grupo poderá conter como membros, grupos globais do domínio abc.com.br e usuários do domínio abc.com.br

- Quando o nível de funcionalidade do Domínio está configurado como Windows 2000 Misto, somente contas de usuários do próprio domínio é que podem ser membros de um grupo Global. Por exemplo, se você cria um grupo global chamado WebUsers, no domínio abc.com.br e este domínio está no modo Misto, então somente contas de usuários do domínio abc.com.br é que poderão ser membros do grupo WebUsers.

- Um grupo pode ser convertido de Global para Universal, desde que o grupo Global não seja membro de nenhum outro grupo Global..

Quando devemos utilizar grupos globais:

Os grupos Globais devem ser utilizados para o gerenciamento dos objetos que sofrem alterações constantemente, quase que diariamente, tais como contas de usuários e de computadores. As alterações feitas em um grupo Global são replicadas somente dentro do domínio onde foi criado o grupo Global e não através de toda a árvore de domínios. Com isso o volume de replicação é reduzido, o que permite a utilização de grupos Globais para a administração de objetos que mudam freqüentemente.

Grupos locais do domínio (Domain local group):

São grupos que somente podem receber permissões para os recursos do domínio onde foram criados, porém podem ter como membros, grupos e usuários de outros domínios. Em resumo:

- Pode conter membros de qualquer domínio.
- Somente pode receber permissões para o domínio no qual o grupo foi criado.
- **Pode conter**: Contas de usuários, grupos universais e grupos globais de qualquer domínio. Outros grupos Locais do próprio domínio.
- **Pode ser membro de**: Grupos locais do próprio domínio.

Conforme detalharei nas próximas partes deste tutorial, um domínio baseado no Active Directory pode estar em diferentes modos (Windows 2000 Nativo, Misto ou Windows Server 2003). Para cada modo existem diferentes possibilidades em relação aos grupos Globais:

- Quando o nível de funcionalidade do Domínio está configurado como Windows 2000 Nativo ou Windows Server 2003, os seguintes elementos podem ser incluídos como membros de um grupo Local: contas de usuários, grupos universais e grupos globais de qualquer domínio. Outros grupos locais do próprio domínio.
- Um grupo pode ser convertido de Local para Universal, desde que o grupo não tenha como seu membro um outro grupo Local.

Quando devemos utilizar grupos Locais:

Os grupos Locais são utilizados para atribuir permissões de acesso aos recursos da rede. Conforme discutirei nas próximas partes deste tutorial, a Microsoft recomenda uma estratégia baseada nos seguintes passos:

- Criar as contas de usuários.
- Adicionar as contas de usuários a grupos Globais (confere com o que foi dito anteriormente, onde falei que os grupos Globais são utilizados para gerenciar os objetos do dia-a-dia, tais como contas de usuários).
- Adicione os grupos globais ou Universais (se for o caso) como membros dos grupos Locais.
- Atribua permissões de acesso para os grupos Locais.

Conclusão

Nesta parte do tutorial apresentei alguns dos principais objetos que fazem parte do Active Directory: Contas de usuários, grupos de usuários e contas de computador. Você também aprendeu detalhes sobre os tipos e escopos de grupos disponíveis e quais as limitações para os escopos de grupos, dependendo do nível de funcionalidade que está configurado no domínio.

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