Tutorial de Active Directory – Parte 2

Introdução

Prezados leitores, esta é a segunda 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 do Windows, 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.

Conceito de Diretório e Exemplos

No Módulo 1 do Manual de Estudos Para o Exame 70-271 (http://www.juliobattisti.com.br/cursos/70271), fiz um histórico dos modelos de redes e aplicações desde a época do Mainframe (que continua mais vivo do que nunca), passando pelo modelo Cliente/Servidor tradicional, até chegar ao modelo Web, baseado no desenvolvimento de aplicações em 3 ou mais camadas.

Cada fase deixou suas características "impressas" na rede da empresa, no conjunto de aplicações que é utilizado para manter a empresa funcionando. O que ocorre na prática, é que hoje, na empresa, existem, ao mesmo tempo, aplicações rodando no Mainframe, aplicações Cliente/Servidor tradicionais e aplicações baseadas no modelo Web.

A Figura a seguir ilustra bem este "mix" de aplicações, onde um usuário a partir da sua estação de trabalho, acessa aplicações em diferentes ambientes, para poder realizar o seu trabalho diário:

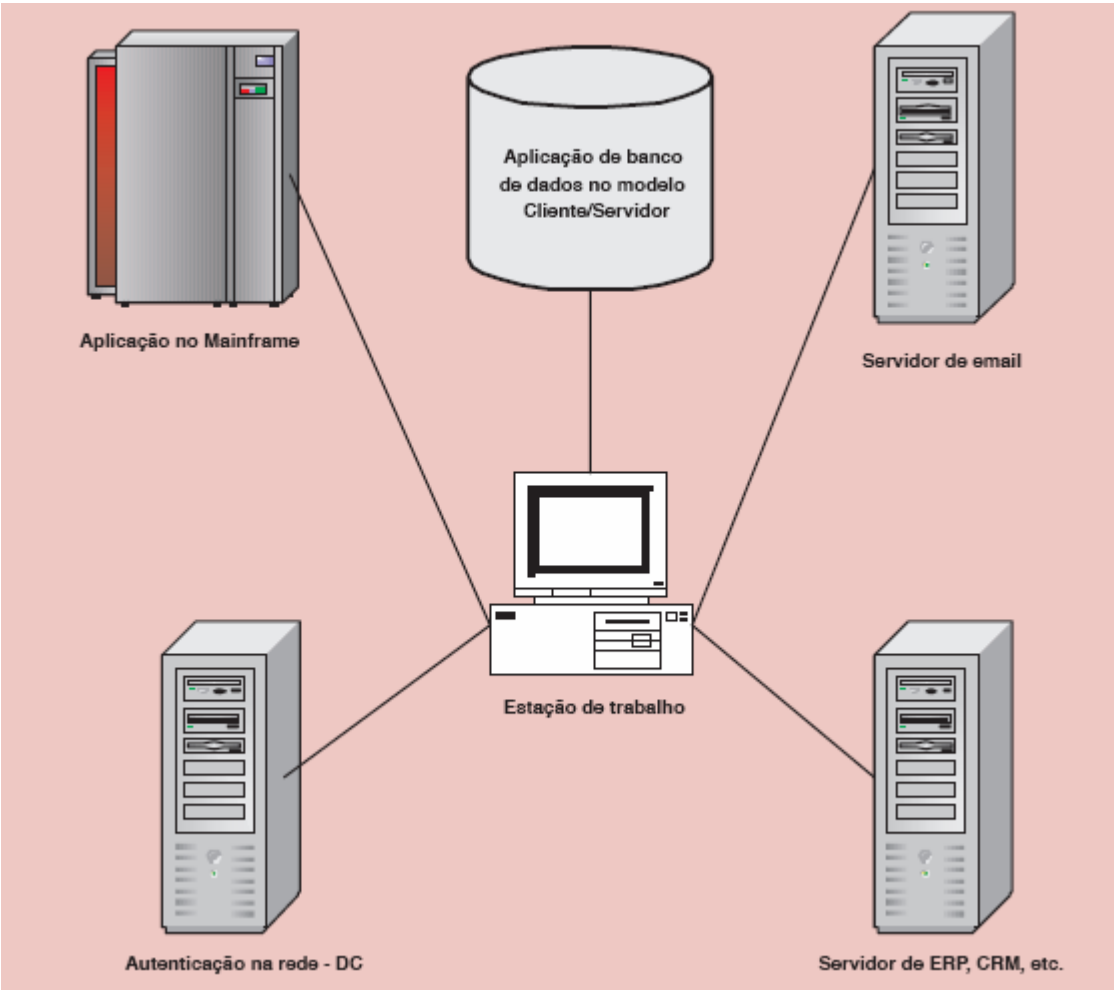

Figura - Aplicações em diferentes ambientes e baseadas em diferentes modelos.

Você pode pensar que dificilmente isso aconteceria na prática. É justamente o contrário. Esta é a situação na qual encontram-se a maioria das empresas, ou seja: Uma variedade de aplicações não integradas, em diferentes plataformas e modelos. Falando de uma maneira mais simples, uma verdadeira "salada-de-fruta", ou de outras formas: salada de aplições e modelos.

No exemplo descrito na Figura, o usuário, para realizar o seu trabalho diário, tem que acessar aplicações e serviços em diferentes plataformas e modelos:

- **No Mainframe:** Alguns sistemas da empresa (muitas vezes a maioria dos sistemas) ainda estão no Mainframe, com acesso através de aplicativos Emuladores de Terminal, instalados na estação de trabalho do usuário. Estes aplicativos mantém a interface a caractere, típica da época do Mainframe. A tão famosa telinha preta com letras verdes. Por exemplo, pode ser que o sistema de RH da sua empresa (controle de férias, curriculum, treinamentos, etc) ainda esteja no Mainframe.

- **Em aplicações cliente/servidor de 2 camadas:** A medida que houve uma migração do Mainframe em direção ao cliente/servidor, muitas aplicações do Mainframe foram substituídas por aplicações Cliente/Servidor tradicionais. Por exemplo, podemos ter uma situação onde o sistema de vendas foi migrado do Mainframe para uma aplicação cliente/servidor de duas camadas. Os dados estão em um ou mais servidores da rede e a aplicação cliente é instalada na estação de trabalho do usuário.

- **Sistema de email e Intranet da empresa:** É praticamente impossível que a sua empresa não tenha um sistema de email instalado. Com isso você utiliza mais um aplicativo (o cliente de email), para acessar o seu correio eletrônico. Você também utiliza o navegador para acessar a Intranet da empresa. Se a sua empresa já evolui bastante no uso da Tecnologia da Informação, é provável que você use o navegador para acessar o Portal Corporativo da empresa.

- Além desta variedade de aplicações você também precisa acesso aos recursos básicos da rede, tais como pastas e impressoras compartilhadas. Para ter acesso a estes recursos você deve estar identificado na rede, para que o servidor onde estão os recursos a serem acessados, possa liberar o acesso, dependendo de você ter ou não as permissões adequadas. Ou seja, o seu nome de usuário na rede e a respectiva senha, devem estar cadastrados em uma base de dados. Logo você descobrirá que base é esta.

Bem apresentado a provável ambiente atual no qual encontra-se a rede da sua empresa, vou salientar um dos principais problemas deste ambiente, problema este que está diretamente relacionado ao conceito de Diretório e também com o Active Directory.

Senhas demais, por favor alguém me ajude!

No cenário descrito anteriormente, onde o usuário tem que acessar sistemas em diferentes ambientes, é necessário um logon e senha para cada ambiente. Por exemplo, no sistema de grande porte o logon pode ser a matrícula do funcionário e uma senha por ele escolhida. Na rede o logon é a primeira parte do seu email, por exemplo jsilva e uma senha por ele escolhida. No sistema de email mais uma senha. Em cada aplicação Cliente/Servidor mais uma senha e assim por diante.

Para piorar um pouco a situação, a senha do Mainframe expira, por exemplo, a cada 30 dias e ele não pode repetir as últimas cinco senhas. A da rede expira a cada 60 dias e ele não pode repetir as últimas treze senhas. A do email expira a cada 45 dias e ele não pode repetir as últimas 10. A do sistema xyz expira a cada 40 dias e ele não pode repetir as últimas 6. Meu Deus, você deve estar pensando, a estas alturas o nosso usuário já deve estar “maluco”.

Na verdade maluco ele não está, mas acaba fazendo algo pior do que estivesse maluco: Ou seleciona senhas que facilmente são descobertas ou anota as senhas e guarda o papel na gaveta. A culpa é do usuário? Obviamente que não, mas sim de um ambiente onde existem múltiplas aplicações, com uma senha diferente para cada uma.

Mas espere aí um pouco. O que tem a ver este monte de senhas com o conceito de Diretório. Tem muito a ver. Observe que em cada ambiente existe um banco de dados para cadastro do nome do usuário, senha e outras informações, como por exemplo seção, matrícula e assim por diante. **Este banco de dados com informações sobre os usuários da rede é um exemplo típico de Diretório**.

Então no Mainframe, onde existe um cadastro de usuários, senhas e perfil de acesso de cada usuário, existe um Diretório. Na rede, onde existe um cadastro de usuários, senha, nome, seção, matrícula, etc, temos mais um diretório. No sistema de e-mail, onde está cadastrado o e-mail do usuário, senha, grupos, etc, temos um terceiro diretório e assim por diante. Observe que para cada diretório (o que implica cadastro em um determinado sistema), o usuário tem uma senha.

> **Então um diretório nada mais é do que um cadastro, ou melhor ainda, um banco de dados com informações sobre usuários, senhas e outros elementos necessários ao funcionamento de um sistema, quer seja um conjunto de aplicações no Mainframe, um grupo de servidores da rede local, o sistema de email ou outro sistema qualquer.**

Saindo do mundo da computação, uma lista telefônica com o cadastro do nome do usuário, telefone e endereço, é um exemplo típico de diretório. O termo Diretório não é muito conhecido para nós, no idioma Português. Talvez um termo mais adequado fosse Cadastro, Banco de dados do sistema ou algo parecido. Mas o termo já é consagrado no idioma Inglês e acabou sendo adotado também no idioma Português (não sei se oficialmente, mas na prática, pelos profissionais de TI).

O Active Directory, introduzido inicialmente com o Windows 2000 Server e agora presente no Windows Server 2003 é também um exemplo típico de diretório. No Active Directory ficam gravadas informações sobre contas de usuários, senhas, grupos de usuários, membros de cada grupo, contas de computadores, informações sobre o Domínio, Relações de confiança, Unidades organizacionais, enfim, todas as informações necessárias ao funcionamento de uma rede baseada no Windows Server 2003.

Nota: No decorrer desta série de tutoriais você aprenderá em detalhes sobre os diversos elementos do Active Directory, tais como Unidades organizacionais, sites, relações de confiança e assim por diante.

Um diretório único para todas as aplicações

Porém o projeto do Active Directory é bem mais ambicioso do que simplesmente ser mais um diretório para conter informações dos elementos de uma rede baseada no Windows Server 2003. Ele foi projetado para tornar-se, com o tempo, o único diretório necessário na rede da empresa.

Mas como seria esta migração da situação atual, caótica, com múltiplos diretórios e senhas, para uma situação mais gerenciável, com um único diretório e senha: O TÃO SONHADO LOGON ÚNICO??

A proposta da Microsoft é que aos poucos as aplicações sejam integradas com o Active Directory. O que seria uma aplicação Integrada com o Active Directory? Seria uma aplicação que, ao invés de ter o seu próprio cadastro de usuários, senhas e grupos (seu próprio diretório), fosse capaz de acessar as contas e grupos do Active Directory e atribuir permissões de acesso diretamente as contas e grupos do Active Directory. Por exemplo, vamos supor que você utilize o Exchange 2000 como servidor de e-mail. Este é um exemplo de aplicação que já é integrada com o Active Directory. Ao instalar o Exchange 2000, este é capaz de acessar a

base de usuários do Active Directory e você pode criar contas de e-mail para os usuários já cadastrados no Active Directory, bem como para os futuros usuários que venham a ser cadastrados. Com isso quando o usuário faz o logon na rede, ele também está sendo autenticado com o Exchange e poderá ter acesso a sua caixa de correio sem ter que fornecer um login e senha novamente.

Chegará o dia do logon único quando todas as aplicações forem ou diretamente integradas com o Active Directory, o forem capazes de acessar a base de usuários do Active Directory e atribuir permissões de acesso aos usuários e grupos do Active Directory. Esta abordagem de um diretório único tem inúmeras vantagens. A mais saliente é o logon único, o que implica em uma única senha. Outra vantagem é o fato de que atualizações feitas no diretório já são refletidas, automaticamente, em todas as aplicações, uma vez que o diretório é único.

Quando o diretório não é único, as alterações devem ser feitas em todos os diretórios, senão ficarão desatualizadas. Vamos voltar um pouco ao ambiente de múltiplos diretórios. Vamos supor que um usuário foi transferido de setor e o seu número de telefone foi atualizado no diretório do Mainframe. Se este número não for também atualizado (e isto tem que ser feito pelo administrador de cada sistema) em todos os demais diretórios, corre-se o risco de alguém pesquisar um dos diretórios que não foi atualizado e obter o número de telefone antigo. Agora considere essa situação em uma empresa grande, onde estão em uso 5 ou mais diretórios diferentes e multiplique isso por 4 ou 5 mil funcionários, você terá uma idéia do problema que é manter sempre atualizados os diversos diretórios em uso na empresa.

Por isso que a proposta do diretório único é interessante e muito bem vinda. É claro que não se faz a migração de um ambiente baseado em vários diretórios para um ambiente de diretório único, da noite para o dia. É um trabalho longo, que envolve um inventário das aplicações em uso. Uma análise do que é prioritário, do que pode ser integrado e do que deverá ser reescrito e assim por diante. Mas é um trabalho que vale a pena, sob risco de chegar-se a um ambiente caótico, com inúmeros de diretórios, ambiente este praticamente impossível de gerenciar ou gerenciável a um custo muito elevado.

Conclusão

Nesta parte do tutorial fiz apenas uma apresentação detalhada do conceito de Diretório. Este conceito é a base sobre a qual irei trabalhar, para apresentar todos os elementos que compõem o Active Director. Mas este já é assunto para as próximas partes deste tutorial.

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