FTC – Faculdade de Tecnologia e Ciências

Luan Gabriel Pereira Dotto

Entendendo o Active Directory

Vitória da Conquista – Ba

2011

FTC – Faculdade de Tecnologia e Ciências

Luan Gabriel Pereira Dotto

Entendendo o Active Directory

Monografia apresentada à Faculdade de Tecnologia e Ciências, com o objetivo de obter o título de bacharel em Sistemas de informação.

Vitória da Conquista – Ba

2011

Resumo

O Active Directory é o serviço de diretório presente na família Windows Server. Um Serviço de Diretório é um serviço de rede, o qual identifica todos os recursos disponíveis em uma rede, denominados de objetos (contas de usuários, Usuários, Pasta Compartilhadas, Grupos, Computadores, Impressoras, Contatos).

Estes por sua vez podem ser manipulados pelos administradores de sistema de forma que se adéqüe a realidade de cada empresa, proporcionando um ambiente centralizado, seguro e estável.

Palavras chave: Active Diretory; Windows Server

SUMÁRIO

1. Introdução

1.1. Contextualização

As ferramentas de gerenciamentos e serviços de rede são parte essencial para os administradores de sistemas de grandes empresas, nesta monografia serão apresentados os conceitos dos diversos objetos do Active Directory que é uma destas ferramentas.

Tipos de objetos: Usuários, Pasta Compartilhadas, Grupos, Computadores, Impressoras, Contatos.

Uma conta de usuário é um objeto de Active Directory, o qual contém diversas informações sobre o usuário. Para ter acesso aos recursos dos computadores do domínio, deve ser cadastrado no Active Directory.

Todo computador que faz parte do domínio, seja uma estação de trabalho, servidor membro, deve ter uma conta de computador no Active. Directory.Responsável para facilitar a administração e a atribuição de permissões para acesso a recursos, tais como: pastas compartilhadas, impressoras remotas, serviços diversos etc.

O Active Directory é o serviço de diretórios do Windows Server. Um Serviço de Diretório 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.

Afinal, o que é Diretório? 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 e-mail ou outro sistema qualquer.

Imagine uma empresa onde o usuário, para realizar o seu trabalho diário, tem que acessar aplicações e serviços em diferentes plataformas e modelos: No Mainframe, em aplicações cliente/servidor, sistemas de e-mail, intranet da empresa e além desta variedade de aplicações, você também precisa de acesso aos recursos básicos da rede, tais como pastas e impressoras compartilhadas.

Para piorar um pouco a situação, a senha do Mainframe expira, por exemplo, a cada 30 dias e não pode repetir as últimas 5 senhas. A da rede expira a cada 60 dias e não pode repetir as últimas 13. A do e-mail expira a cada 45 dias e ele não pode repetir as últimas 10. O que tem a ver este monte de senha com o conceito de Diretório? Tem muito a ver. Observe que em cada ambiente existe um banco de dados para cadastro do nome de usuário, senha e outras informações, como por exemplo seção, matrícula e assim por diante. Este banco de dados, com informações sobre usuários da rede, é um exemplo típico de diretório.

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 cadastros de usuários, senhas e grupos (seu próprio diretório), fosse capaz de acessar

as contas e grupos do Active Directory e atribuir as permissões de acesso diretamente às contas e grupos do Active Directory. Por exemplo, vamos supor que você utilize o Exchange 2003 como servidor de e-mail. Este é um exemplo de aplicação que já é integrada com o Active Directory. Ao instalar o Exchange 2003, este é capaz de acessar a base de usuários do Active Directory e você pode criar contas de e-mail para os usuários do Active Directory.

Chegará o dia do logon único, quando todas as aplicações forem ou diretamente integradas com o Active Directory, ou capazes de acessar a base de usuários do Active Directory e atribuir permissões de acesso aos usuários e grupos do Active Directory.

1.2. Motivação

Há grande heterogeneidade das redes de computadores contemporâneas e que há um grande desafio a ser vencido no gerenciamento de identidade entre essas plataformas distintas. A autenticação entre sistemas proprietários e de código aberto já é uma realidade no meio empresarial.

Devido a esse cenário, e as inúmeras mudanças no mundo dinâmico da TI

com foco cada vez maior em interoperabilidade, se faz necessário uma maior explanação e pesquisa sobre a capacidade de tecnologias distintas coexistirem no mesmo ambiente, provendo a autenticação cruzada de forma harmoniosa e mais do que isso, produtiva.

1.3. Objetivo

Este trabalho tem por objetivo a implementação de um ambiente de rede heterogêneo interoperável, no qual será garantido a organização e segurança na rede de trabalho. Através do serviço de diretório que provemos de forma centralizada e segura todo o gerenciamento e autenticação dos usuários corporativos. Existem alguns mecanismos que permitem tal gerenciamento e autenticação em ambientes mistos, em particular o LDAP (Lightweight Directory Access Protocol) merece destaque. Entre as implementações desse protocolo deve-se analisar e descrever o principal foco o Active Directory.

1.4.Objetivo específico

Este ambiente tem como propósito que usuários de estações clientes Windows ou Linux possam ser autenticados usando o protocolo LDAP, tanto no serviço de diretório da Microsoft, o Active Directory , quanto em sua versão livre, o OpenLDAP, de forma que estes possam usufruir das potencialidades de ambas as tecnologias, garantido assim maior segurança e versatilidade no acesso às informações.

1.5. Metodologia

Os procedimentos metodológicos e as técnicas adotadas na implementação da ferramenta foram à coleta de dados, analise do ambiente empresarial, tipos de ferramenta, aplicação e nível de segurança.

Este artigo teve como base para sua criação a implementação da ferramenta na empresa Disbel – Distribuidora de Bebidas Sertaneja LTDA e os benefícios que a mesma promoveu ao meio empresarial.

Antes da implementação do Active Directoty feito uma analise minuciosa de cada setor da empresa e da mesma como um todo (horário de trabalho, arquivos, aplicativos, tempo de indisponibilidade, sistema operacional utilizado, viabilidade do projeto, benefícios, impactos, nomes dos usuários, telefone, endereço, etc.).

Após a coleta dos dados a estrutura foi implementada em um ambiente de testes onde foram analisados se ocorreriam incompatibilidades por parte de alguma ferramenta, possíveis falhas ou inconsistências.

A implementação do Active Directory no ambiente de produção foi feita em um final de semana diminuindo o tempo de indisponibilidade das maquinas para os usuários, após implementação da ferramenta todas as maquinas foram ingressadas no domínio e os dados dos usuários migrados para o seu novo perfil.

Com a conclusão dos processos foram criadas documentações do projeto e ministrado mini treinamento aos usuários.

2. Levantamento Bibliográfico

Para uma melhor compreensão do trabalho apresenta-se neste capítulo os conceitos e ferramentas necessárias para a implementação e desenvolvimento do ambiente de autenticação cruzada proposto.

2.1 Conceitos Fundamentais

2.1.1. Domínio

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.

Um domínio pode também ser definido como um limite administrativo e de segurança. Ele é um limite administrativo, pois as contas de Administrador têm 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 às contas de usuários e demais recursos dentro do domínio e não a outros domínios.

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)

Um Domínio é simplesmente um agrupamento lógico de contas e recursos, os quais compartilham políticas de segurança.

A criação de conta 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 Domínios. Uma alteração feita em um DC será automaticamente repassada (o termo técnico é “replicada”) para os demais Controladores de Domínio. 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.

Nos Servidores Membros podem ser criadas contas de usuários e grupos, as quais somente serão validas 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.

Os DCs compartilham uma lista de usuários, grupos e políticas de segurança e também são responsáveis por fazer a autenticação dos usuários na rede, já os servidores membros não possuem uma cópia da lista de usuário 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 Policies Objects.

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. Como 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 de qualquer um dos Domínios.

A utilização do Active Directory simplifica em muito a administração, pois fornece um local centralizado, através do qual os recursos da rede podem ser administrados.

O Active Directory utiliza o DNS (Domain Name 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 pois este tem papel fundamental ao funcionamento.

Um usuário cadastrado em um Domínio pode receber permissões para acessar recursos de outros Domínios, o Windows Server 2003 cria e mantém relação de confiança entre os diversos Domínios. As relações de confiança são bidirecionais e transitivas.

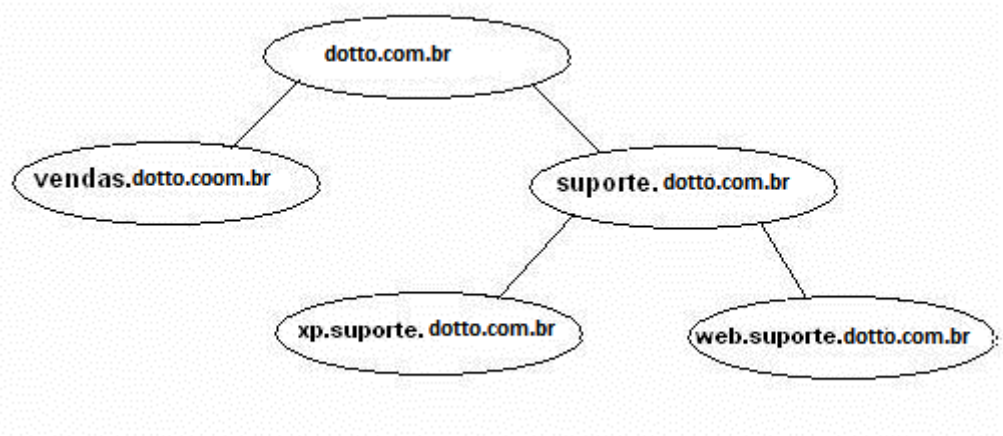
Todo Domínio possui as seguintes características:

. 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

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”.



2.1.2. Unidades Organizacionais

Uma Unidade Organizacional é uma divisão que 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. Com a utilização de unidades organizacionais, é possível restringir os direitos administrativos apenas em nível da Unidade Organizacional sem que, com isso, o usuário tenha poderes sobre todos os demais objetos do Domínio.

Utilize Unidades Organizacionais quando quiser delegar tarefas administrativas sem que, para isso, tenha que dar poderes administrativos em todo o Domínio ou para melhorar alterações na estrutura da sua companhia.

A infra-estrutura das OU´s não deve-se basear na estrutura organizacional da companhia, mas sim na infra-estrutura da política da rede.

2.2. Objetos do Active Directory

O Active Directory e composto por diversos objetos (Usuários, Grupos, Computadores, Impressoras) aos quais tem finalidade de organizar, delegar

segurança, criar hierarquia e facilitar a administração estes por suas vez ainda são divididos em subgrupos que serão descritos mais abaixo

2.2.1 Usuários

Conta de usuário é um objeto utilizado com freqüência no gerenciamento do Active Directory. Ela consiste em todas as informações que definem um usuário, essas informações são classificadas em atributos. Os atributos são números de telefone, email, endereço, nome, entre outros.

Ao criar um usuário, seis atributos são definidos, sendo que dois são configurado pelo administrador, cn e SamAccountName, onde o cn é o nome completo do usuário, e SamAccountName é o nome de logon do usuário e os outros quatros são configurados pelo serviço de diretório, Instance Typ, objectCategory, objectCalss, objectSid. Podemos visualizar e modificar qualquer atributo utilizando a ferramenta Adsiedit.msc presente no CD do SO na pasta Support, instale o pacote de ferramentas, lembrando que este recurso esta disponível para Windows 2000 e Windows Server 2003.

Utilizamos diariamente a ferramenta Active Directory Users and Computers para gerenciamento de usuários, criação, mover, excluir, alterar atributos e localizar.

Cada conta de usuário possível quatro tipos de nomes associados, um nome de logon de usuário, um nome de logon do usuário anterios ao Microsoft Windows 2000, um nome de logon principal do usuário e um nome distinto relativo do LDAP (Lightweight directory Access Protocol).

- **Nome de logon de usuário:** Deve ser exclusivo na floresta na qual a conta de usuário foi criada. É utilizado durante o processo de logon.

Ex: luan

- **Nome de logon anterior ao Windows 2000:** Utilizado para fazer logon em um domínio do Windows onde os computadores que executam sistemas operacionais anteriores ao Windows 2000 usando um nome como o formato Nome do Domínio\Nome do Usuário. Também é possível utilizar este nome para fazer logon em domínios apartir de computadores que executam o Windows 2000 ou o Windows XP, ou Windows Server 2003.
- Ex: DOTTO\luan.
- **Nome de logon principal de usuário:** Consiste do nome de logon do usuário e do sufixo do nome principal do usuário, unidos pelo símbolo de arroba @. O (UPN User Principal Name) deve ser exclusivo na floresta.

Ex:luan@dotto.com.br

- **Nome distinto relativo do LDAP:** Este nome é utilizado para adicionar usuários à rede a partir de um script ou linha de comando. Identifica com exclusividade o objeto em seu recipiente pai.

Ex: CN=luan,CN=users,DC=dotto,DC=.com.br

Pastas Compartilhadas

Objeto de pastas compartilhas consiste na publicação de uma pasta compartilhada na rede. Com a pasta publicada no Active Directory facilita a localização das pasta compartilhadas na rede.

2.2.2. Grupos

Utilizamos grupos para simplificar a administração, permitindo conceder permissões para recursos uma vez por grupo e não por cada conta de usuário.

Um grupo é um conjunto de contas de usuário e de computadores, podemos utilizar os grupos separadamente ou pode colocar um grupo dentro de outro, para simplificar ainda mais a administração.

Existe dois tipos de grupos:

- **Grupos de segurança:** São utilizados para atribuir direitos e permissões de usuário a grupos, onde direitos determinam o que os membros do grupo de segurança pode fazer em um domínio ou floresta, já as permissões determinam quais recursos um membro de um grupo pode acessar na rede.

Grupos de distribuição: Utilizados em aplicações de email, com Microsoft Exchange, para enviar email para conjunto de usuários. Este grupo não tem recursos de segurança, desta forma, não é possível conceder permissão.

Os grupos estão divididos em escopo:

- **Grupo Global:** É um grupo de segurança ou de distribuição que pode conter usuários, grupos e computadores do mesmo domínio que o grupo

global. Podemos utilizar grupos de segurança onde os membros podem acessar recursos de qualquer domínio da floresta.

- **Grupo Universal:** É um grupo de segurança ou de distribuição que pode conter usuários, grupos e computadores de qualquer domínio da floresta. Podemos utilizar grupos de segurança onde os membros podem acessar recursos de qualquer domínio da floresta.
- **Grupo Dominio Local**: É um grupo de segurança ou de distribuição que pode conter grupos universais, grupos globais, outros grupos domínio local de seu próprio domino e contas de qualquer domínio da floresta. Podemos utilizar grupos de segurança domínio local onde os membros podem acessar recursos somente no mesmo domínio em que se encontra o grupo domínio local.
- **Grupo Locais:** É um conjunto de contas de usuários ou grupos de domínio, criados em um servidor membro. Podemos utilizar grupos locais onde os membros podem acessar recursos no computador local.

2.2.3. Computadores

Conta de computador ajuda os administradores a gerenciar a estrutura de rede, quando uma conta de computador é criada, o computador pode usar os processos de autenticação avançados como a autenticação para determinar como a auditoria deve ser aplicada e registrada. Todo computador que executa o Windows NT, Windows 2000, Windows XP ou Windows Server 2003 e ingressa em um domínio, possui uma conta de computador. Não é

possível criar contas para computadores que executam windows 95, Windows 98, Windows Millennium e Windows XP Home Edition.

Quando uma conta de computador é criada podemos escolher duas opções: Atribuir esta conta de computador como um computador pre-Windows 2000: Desta forma uma senha aleatória será atribuída como a senha inicial para a conta de computador. A senha será alterada automaticamente a cada cinco dias entre o computador e o domínio no qual a conta esta localizada. Atribuir esta conta de computador como um computador de domínio de backup: Deve-se utilizar em ambiente misto com um controlador de domínio de Windows Server2003 e o BDC do Windows NT 4.0. Depois da conta pode-se adicionar o BDC ao domínio durante a instalação do Windows NT 4.0

2.2.4. Impressoras

Conta de impressora consiste na publicação de uma impressora compartilhada na rede. Com a impressora publicada no Active Directory facilita a localização das impressoras de rede.

2.2.5. Contatos

O objeto contatos é diferente do objeto usuários onde é possível atribuir permissões, já a conta contatos é somente utilizada para informação, onde geralmente é configurada para armazenar informações de telefone, endereço e email.

3. Conclusão

Conclui-se que o AD não só tem um papel fundamental na infra-estrutura de redes, com o levantamento e a criação de toda a estrutura lógica/física e design da organização, bem como no auxílio à tomada de decisão por parte dos gerentes de TI e administradores na implementação de planos/projetos de redes.

4. Referências

GEYER, C.; KELLERMANN, G. A.; SILVELLO, J. C. Manual OpenLDAP. Disponível em http://www.inf.ufrgs.br/gppd/disc/inf01008/trabalhos/sem01-1/t1/openldap/. Consultado em 10/09/2010.

JUNIOR, C. H. F. G. GERI Gerenciamento de Identidade Monografia (Graduação em Sistemas de Informação) - Faculdade Salesiana Maria Auxiliadora, Macaé, 2009.

MEIRELLES, F. S. 21a Mercado Brasileiro de Informática e Uso nas Empresas. 21a Pesquisa Anual da FGV-EAESP-CIA, São Paulo, maio 2010. Disponível em: <http://www.eaesp.fgvsp.br/subportais/interna/relacionad/GVciaPesqResumoNoticias2010.pdf>. Acesso em: 19 ago. 2009.

MICROSOFT, C. Introdução à infra-estrutura do Active Directory. 1.ed. 2003. 44 p.