

Windows® 2000 Server

Sistema operacional para servidor

Considerações sobre o design e a implantação do Active Directory®

Documento técnico

Resumo

O Windows® 2000 Server oferece diversos recursos e tecnologias que devem ser seriamente analisados ao se projetar e implantar o Windows 2000 como infra-estrutura e elemento funcional de uma organização. Este documento analisa o design do espaço de nome de DNS, o design do espaço de nome do Active Directory, o planejamento da segurança e as considerações das Diretivas de grupo.

© 1999 Microsoft Corporation. Todos os direitos reservados.

As informações contidas neste documento representam a visão atual da Microsoft Corporation com relação às questões discutidas até a data da publicação. Como a Microsoft deve responder a condições mutáveis de mercado, este documento não deve ser interpretado como um compromisso da parte da Microsoft e a Microsoft não pode garantir a exatidão das informações apresentadas após a data da publicação.

Este documento técnico tem propósitos unicamente informativos. A MICROSOFT NÃO DÁ GARANTIAS EXPRESSAS OU IMPLÍCITAS NESTE DOCUMENTO.

Microsoft, BackOffice, a logomarca BackOffice, MS-DOS, Outlook, Windows e Windows NT são marcas registradas ou comerciais da Microsoft Corporation nos Estados Unidos e/ou em outros países.

Os nomes de outros produtos ou de empresas mencionados neste documento são marcas comerciais de seus respectivos proprietários.

Microsoft Corporation • One Microsoft Way • Redmond, WA 98052-6399 • EUA
1098

Revisão técnica por Francisco Baddini – Seminar Group Microsoft Brasil

PREFÁCIO	4
<u>COMPONENTES DO ACTIVE DIRECTORY</u>	5
<u>Domínios</u>	5
<u>Unidades organizacionais</u>	6
<u>Domínio em oposição à UO</u>	8
<u>Considerações sobre o design da UO</u>	9
<u>ÁRVORES E FLORESTAS</u>	10
<u>Árvores</u>	10
<u>Florestas</u>	12
<u>Revisão</u>	14
<u>ESPAÇO DE NOME E HIERARQUIA DE UO</u>	14
<u>Design do espaço de nome de DNS</u>	14
<u>Vantagens e desvantagens dos dois modelos</u>	17
<u>Requisitos de DNS</u>	18
<u>Recomendações de DNS</u>	18
<u>Zonas e domínios de DNS adicionais</u>	19
<u>Revisão</u>	20
<u>INTRODUÇÃO AOS DIVERSOS MÉTODOS DE DESIGN E SUAS IMPLICAÇÕES</u>	20
<u>Domínio raiz</u>	21
<u>Geográfico</u>	21
<u>Político</u>	26
<u>Geo-político</u>	29
<u>Político-geográfico</u>	31
<u>Funcional</u>	34
<u>A SITUAÇÃO SE COMPLICA: CONSIDERAÇÕES PARA SITES</u>	35
<u>Local do controlador de domínio</u>	36
<u>Determinando onde colocar os controladores de domínio e catálogos globais</u>	36
<u>Fronteiras dos sites</u>	37
<u>Replicação de site</u>	37
<u>Links de site</u>	41
<u>Pontes de link de site</u>	43
<u>Criação da topologia</u>	45
<u>Localizando os serviços</u>	46
<u>Campos de ação do site</u>	47
<u>Revisão</u>	49
<u>SEGURANÇA</u>	49
<u>Funções do servidor</u>	50
<u>Diretivas de segurança do Active Directory</u>	52
<u>Direitos e permissões</u>	52
<u>Herança</u>	53
<u>Controle de acesso</u>	53
<u>Administração delegada</u>	55
<u>Infra-estrutura da chave pública</u>	58
<u>Propriedades de segurança</u>	59
<u>Componentes de segurança da chave pública</u>	60
<u>Criptografia e chaves públicas</u>	61
<u>Certificados</u>	62
<u>Serviços de certificado</u>	62
<u>IPSec</u>	65
<u>Kerberos</u>	70
<u>Planejamento de Kerberos</u>	76
<u>Revisão</u>	76
<u>GRUPOS</u>	76
<u>Estruturas de segurança</u>	77
<u>Utilização de grupos</u>	77
<u>Revisão</u>	82

Prefácio

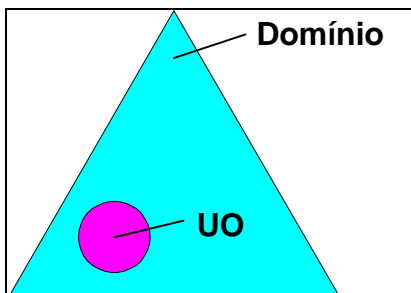
Há diversas formas de se analisar o design e a implantação do Windows 2000 e do Active Directory. Nesta minuta, vamos tentar instigar a imaginação do engenheiro de sistemas e de outros que precisam analisar o campo de ação e o planejamento do design e da implantação. Como tal, este documento não vai abordar situações que envolvam o uso do Windows 2000 e do Active Directory. Em vez disso, este documento vai tentar apresentar informações essenciais a serem usadas ao se considerar o design e implantação do Windows 2000.

O documento está organizado por tópicos, e o fluxo lógico usado ao se elaborar as seções de tópicos é:

- Active Directory e componentes relacionados: Uma análise das florestas, domínios e unidades organizacionais. Analisaremos a finalidade, definição e uso desses elementos.
- Design do espaço de nome de DNS: Uma análise do design do espaço de nome de DNS único e de espaços para nome de DNS separados. As vantagens e desvantagens de cada design e algumas recomendações básicas sobre como cada um deles pode ajudar a organização.
- Design do espaço de nome do Active Directory: Uma análise de cinco modelos diferentes de designs de espaço de nome, as características de cada um e como cada um se encaixa na estrutura de uma organização.
- Sites: Uma análise de como os sites funcionam, sua finalidade e como afetam o design do espaço de nome e a estrutura dos domínios do Windows 2000.
- Segurança: Um exame dos fundamentos da segurança e de como ela afeta o design do ambiente do Windows 2000.
- Grupos: Uma análise sobre a introdução de novos tipos de grupos, o planejamento de como esses grupos são usados e por que se deve analisar com tanto cuidado o seu uso.

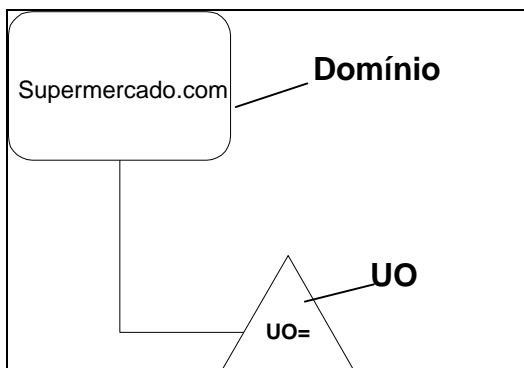
Neste documento: Utilização de figuras

As figuras usadas freqüentemente neste documento representam domínios do Windows 2000 e unidades organizacionais (UOs). Os símbolos preferidos usados para ilustrar esses componentes são geralmente um triângulo para um domínio e um círculo para uma UO.



n Figura 1

Essas representações são usadas quando a análise concentra-se exclusivamente em árvores e florestas. Infelizmente, não é possível empregar esses símbolos em designs de árvores complexas. Portanto, na maioria das figuras que representam estruturas de árvores, retângulos arredondados são usados para representar domínios e triângulos são usados para representar UOs.



n Figura 2

O uso destes símbolos deve ser evidente quando exibidos no contexto das análises.

Componentes do Active Directory

Há diversos componentes do Active Directory que devem ser bem compreendidos para que possam ser usados corretamente. Os domínios e unidades organizacionais são os elementos básicos do Active Directory e vão definir tanto a estrutura como a funcionalidade. A maneira em que os domínios são organizados em árvores e florestas também vai determinar o tom das diretivas administrativas e da interoperabilidade entre as diversas áreas de uma organização.

Esta seção apresenta esses componentes do ponto de vista da sua arquitetura. As suas finalidades e utilização serão analisados posteriormente neste documento.

Domínios

Os domínios representam uma partição lógica do Active Directory que serve tanto para a segurança quanto para a replicação de diretórios. Os domínios estão diretamente relacionados ao espaço de nome de DNS e são, de fato, endereçados através do DNS.

Todos os objetos da rede existem dentro de um domínio, e cada domínio contém um conjunto completo dos seus objetos dentro do Naming Context (NC, contexto de denominação) do domínio. Teoricamente, um diretório de domínio pode conter até dez milhões de objetos.

Os domínios fornecem um limite para a segurança e um campo de ação para a replicação do NC do domínio. Nenhuma das diretivas e configurações de segurança, como direitos administrativos, diretivas de segurança e Access Control Lists (ACLs, listas de controle de acesso), passa de um domínio para outro. O administrador do domínio tem direitos absolutos para definir diretivas somente dentro desse domínio.

O uso específico dos domínios deriva-se da sua função. Geralmente, os domínios são criados para fornecer um campo de ação para autoridade administrativa ou para reter as informações replicadas como parte do NC do domínio. Para exemplificar essa última situação, geralmente os domínios são confinados a limites geográficos para garantir a otimização da rede.

Sempre que possível, deve-se evitar a criação de domínios para refletir grupos de divisões. Às vezes, pode ser necessário estabelecer domínios por motivos políticos, mas isso fará

parte de uma estratégia maior.

Exceto durante a migração e consolidação, nunca se deve criar domínios para servirem como host de recursos. Estes eram conhecidos como domínios de recursos no Windows NT 4.0 e não são mais necessários nem desejáveis no ambiente do Windows 2000.

Ter muitos domínios aumenta de forma significativa os custos administrativos indiretos relacionados ao gerenciamento do Active Directory. Como regra básica de design, deve-se sempre iniciar com um número mínimo de domínios e só acrescentar outros domínios visando atender a critérios específicos.

Unidades organizacionais

As unidades organizacionais (UOs) do Active Directory são um conceito completamente novo para os administradores do Windows NT. Apesar disso, as UOs são uma inovação bem-vinda e garantem uma enorme flexibilidade. Espera-se que as UOs desempenhem um papel importante na consolidação do domínio de recursos durante as migrações do Windows NT 4.0 para o Windows 2000.

Delegação da administração

As UOs permitem a delegação granular das tarefas administrativas. Isso possibilita o emprego inteligente do controle administrativo em diversos níveis, permitindo que os usuários, computadores e outros objetos sejam reunidos em uma UO e que a administração dessa UO seja delegada ao administrador adequado.

Campo de ação das diretivas

As Diretivas de grupo podem ser aplicadas em sites, domínios e unidades organizacionais e filtradas com base na associação ao grupo. Desses, as UOs são provavelmente o recipiente mais funcional que pode aceitar diretivas.

Embora a partição para objetos das diretivas de grupo seja, na verdade, o domínio, as UOs também podem ser consideradas como partições para diretivas. Dependendo da finalidade da UO criada, o emprego das diretivas pode refletir regras comerciais, mandatos políticos técnicos ou automação de tarefas.

Por exemplo, podem ser criadas UOs separadas para funcionários de horário integral e funcionários contratados. Pode-se criar uma diretiva específica para cada classe de funcionários e aplicá-la a UOs individuais.

Considerações sobre a UO

As estruturas da UO devem ser benéficas e significativas. Como a estrutura de diretórios é exposta aos usuários, deve-se evitar UOs arbitrárias. Em outras palavras, não crie uma estrutura só pela estrutura.

Lembre-se também de que a estrutura da UO de um domínio é independente de qualquer outro domínio. Portanto, cada domínio pode implementar a sua própria hierarquia de UO. Isso é uma faca de dois gumes. Se houver vários domínios ponto a ponto com finalidade semelhante, é provável que esses domínios exijam a mesma estrutura básica de UO, como

a criada para a empresa Supermercado.

Embora não exista nenhuma restrição inerente à profundidade das UOs em um domínio, existem algumas diretrizes gerais.

- Estruturas de UO pouco profundas funcionam melhor do que estruturas profundas.
- Não devem existir mais de dez níveis de UOs.
- O emprego das diretivas será prejudicado com estruturas de UO profundas.

Ao considerar estruturas de UO, deve-se analisar também que o proprietário de uma UO tem total autoridade sobre ela e pode restringir o emprego da diretiva a partir de um recipiente pai. Ao estabelecer a estrutura básica da UO, deve-se pensar em quem vai administrar a UO e em quem vai poder exibi-la.

Estruturas das UOs

As UOs do Active Directory atendem a duas finalidades básicas:

- 1) Como partições para delegação administrativa.
- 2) Como recipientes para o emprego de diretivas.

A criação de unidades organizacionais por qualquer outro motivo deve ser bem justificado. Isso significa que as unidades organizacionais não devem ser criadas simplesmente para refletir o aninhamento da estrutura da empresa. Por quê? Porque as UOs não são passivas por natureza. Elas são analisadas quanto às diretivas e permissões, sobrecarregando assim o processador. Quanto mais profunda for a estrutura da UO, maior será a queda de desempenho. Como o Active Directory não permite originalmente a criação de recipientes, é tentador usar UOs com essa finalidade e, em alguns casos, esse uso pode realmente ser apropriado.

Há muitas possibilidades para a criação de UOs que não violam a regra de finalidade:

- Para refletir a estrutura organizacional, como um departamento. Na maioria dos casos, os departamentos são na verdade o nível básico da delegação administrativa.
- Função comercial: Conforme descrito no modelo de diretório Funcional. Frequentemente, a disposição por função comercial será executada pelos grupos e, portanto, você pode justificar as UOs criadas dessa forma.
- Baseadas em objeto: UOs que representam grupos de objetos semelhantes, como usuários, computadores, impressoras, roteadores, etc. Novamente, dependendo da sua estrutura de diretório básica, isso pode não ser apropriado, pois o nível inferior de delegação e atribuição de diretivas pode ser a UO da divisão.
- Baseadas em projeto: UOs temporárias para organizar dados relacionados a projetos, pessoal, etc. As UOs fornecem um excelente mecanismo para reunir objetos para administração e diretivas. Os projetos geralmente têm exigências especiais que precisam ser atendidas através de procedimentos administrativos e diretivas específicas.
- Baseadas em necessidade administrativa: Às vezes, pode ser necessário basear as UOs na necessidade administrativa. Contudo, essas necessidades devem ser bem

justificadas, pois as UOs são expostas aos usuários.

Domínio em oposição à UO

A questão de se usar domínios ou unidades organizacionais nem sempre é simples. Vamos tentar apresentar algumas regras e esclarecimentos aqui.

Motivos para se criar domínios:

Segurança: A exigência de se manter diretivas de segurança separadas será geralmente um fator decisivo na criação de domínios. Essa exigência pode ocorrer quando existirem unidades comerciais autônomas com uma estrutura de TI distribuída. Com menos frequência, ambientes de alta segurança vão exigir que os envelopes de segurança sejam distintos, como no caso de empresas petrolíferas e farmacêuticas.

Replicação: Outra justificativa comum e geralmente válida para um ambiente de vários domínios é a possibilidade de se controlar o campo de ação da replicação com base na região geográfica. Embora os sites forneçam um mecanismo para tornar a replicação eficiente, as condições da rede podem evitar a replicação de dados desnecessários através de links de baixa velocidade da rede.

Migração: Em uma infra-estrutura madura do Windows NT, será necessário estabelecer inicialmente um mapeamento de um para um entre os domínios do Windows NT e do Windows 2000. Os detalhes da migração vão ser analisados em profundidade mais adiante neste documento.

Motivos para não se criar domínios:

Para refletir a estrutura organizacional: Se possível, evite criar domínios baseados em divisões, departamentos ou grupos. Um bom design deve resistir às reorganizações da empresa sem precisar da reestruturação da hierarquia dos domínios.

Para refletir a função comercial (também chamada de diretiva): A reorganização comercial é bastante freqüente nas empresas atuais. Os domínios baseados em grupos políticos oferecem pouca vantagem funcional.

Quando se deve criar unidades organizacionais:

Para controlar a administração: As UOs agem como partições para delegação administrativa. Um uso freqüente das UOs é o de fornecer campo de ação para administração de recursos.

Para substituir os domínios de recursos do Windows NT 4.0: Na maioria dos casos, os domínios de recursos do Windows NT 4.0 podem ser substituídos, um por um, pelas UOs. Quando estiver concluída a migração de um domínio de recursos para o Windows 2000, é fácil transformá-lo em uma UO.

Para criar um campo de ação para diretivas administrativas: As partições de diretivas e de delegação administrativa são geralmente sinônimas, mas devem ser definidas na etapa inicial do processo de planejamento. O método mais fácil de se empregar diretivas é através de UOs, mas pode ser confuso criar uma UO especificamente para uma diretiva. Por exemplo: "UO = Usuários de terminais do Windows" não seria uma boa opção para uma UO.

Para refletir a estrutura organizacional: Na medida em que elas oferecem suporte à administração, as UOs devem fornecer alguns detalhes sobre a estrutura organizacional da empresa.

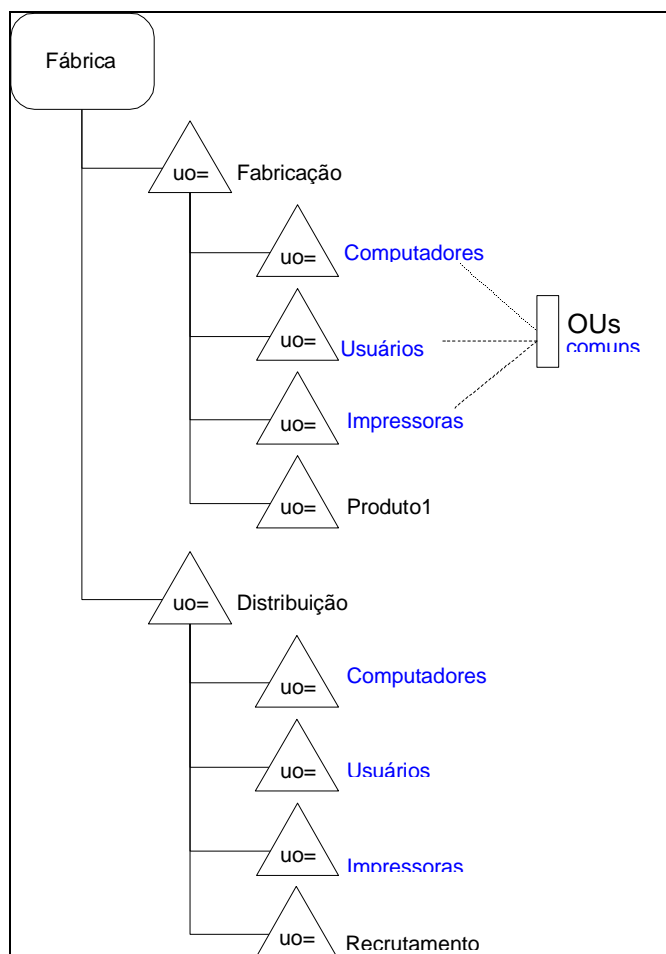
Quando não se deve criar unidades organizacionais:

Para refletir grupos políticos: Caso seja necessário refletir grupos políticos, faça-o usando grupos. Uma UO denominada “VPs do nordeste e amigos” não é um uso adequado.

Para criar uma estrutura arbitrária: As UOs devem ser usadas como grupos e não devem ser criadas como espaços reservados ou em benefício da estrutura somente. Por exemplo: Seria questionável a criação de uma UO denominada “Unidades comerciais” contendo UOs filho denominadas para cada unidade comercial, exceto se tiverem sido aplicadas diretivas e delegação administrativa à UO denominada “Unidades comerciais”.

Considerações sobre o design da UO

Ao se projetar hierarquias de diretório potenciais, deve-se identificar os elementos que são comuns a mais de uma unidade comercial, divisão ou unidade administrativa e estabelecer algumas convenções para a estrutura das UOs a fim de garantir alguma consistência.



n Figura 3

É bastante adequado fornecer uma estrutura base para as unidades organizacionais ou desativar completamente a possibilidade de se criar unidades organizacionais.

No exemplo acima, tanto a Fabricação como a Distribuição têm exigências em comum, uma delas é um local para administrar e gerenciar os seus usuários, computadores e impressoras. Como tal, uma convenção para UOs comuns foi implementada, fazendo com que três UOs (Computadores, Usuários, Impressoras) fossem criadas sob cada UO da divisão básica. Ao se estabelecer alguma estrutura preliminar, são fornecidas aos usuários visualizações consistentes e obtém-se um nível de consistência administrativa.

Embora não haja uma limitação inerente ao número de UOs aninhadas, estruturas profundas de UOs prejudicam o desempenho. Se mais de dez níveis de UOs forem exigidos, você deve considerar a implementação de outra estrutura.

Árvores e florestas

O Active Directory usa *árvores* e *florestas* que fornecem formações e links lógicos que vão definir como e até que ponto os domínios vão se comunicar. Assim como os domínios e as unidades organizacionais, esses componentes fornecem uma funcionalidade específica e são criados para atender a exigências específicas.

Árvores

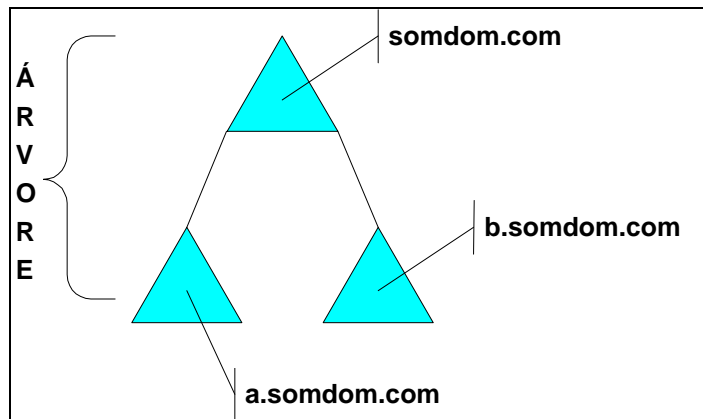
Uma árvore é uma reunião hierárquica de domínios organizados em um espaço de nome contíguo.

(Uma árvore também pode consistir em um único domínio do Windows 2000. Contudo, você pode criar um espaço de nome contíguo maior, unindo diversos domínios em uma estrutura hierárquica.)

Os domínios em uma árvore são unidos de forma transparente através de relações de confiança transitiva Kerberos bidirecional. Uma confiança transitiva Kerberos significa simplesmente que, se o Domínio A confia no Domínio B, e o Domínio B confia no Domínio C, então o Domínio A confia no Domínio C. Portanto, um domínio que pertence a uma árvore estabelece imediatamente relações de confiança com cada domínio da árvore. Essas relações de confiança disponibilizam todos os objetos de todos os domínios da árvore a todos os outros domínios da árvore.

Todos os domínios de uma única árvore têm um espaço de nome comum e uma estrutura de denominação hierárquica. Segundo os padrões de DNS, o nome de um domínio filho é o nome relativo desse domínio filho com o nome do domínio pai anexado.

Todos os domínios de uma única árvore têm um *esquema* comum, que contém definições formais de todos os tipos de objetos que podem ser armazenados em uma implantação do Active Directory. Além disso, todos os domínios de uma única árvore têm um *catálogo global* comum, que é o depósito central das informações sobre os objetos de uma árvore ou floresta.



n Figura 4

Não há um limite específico para a profundidade de uma árvore, mas, como os domínios, as árvores têm processamentos relacionados, e estruturas profundas vão prejudicar o desempenho.

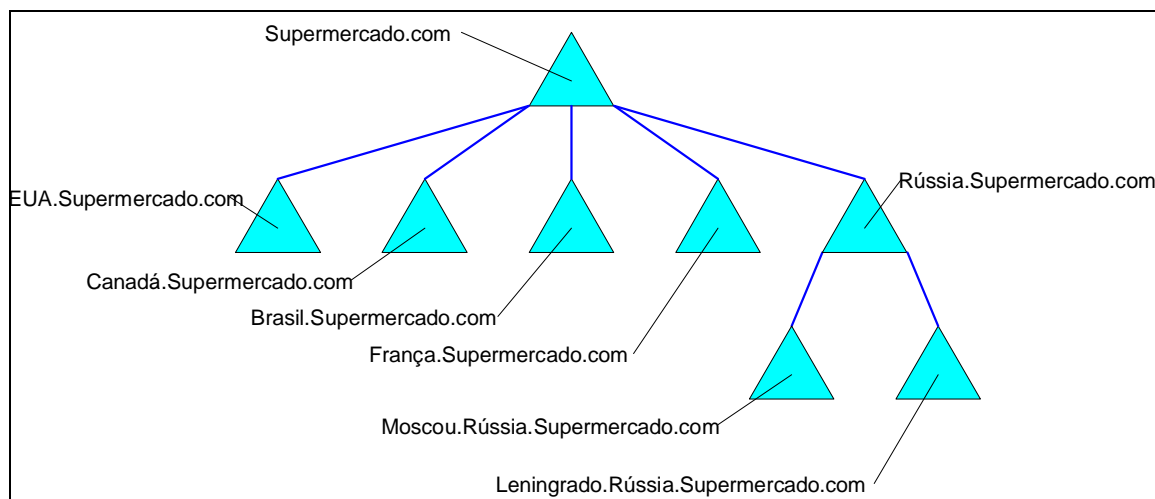
Utilização de árvores

As árvores definem a estrutura mais evidente do Active Directory e dizem respeito à utilização do domínio. Do ponto de vista do design cronológico, a estrutura da árvore não deve preceder as definições do domínio. Os domínios devem ser definidos de acordo com as regras relacionadas à utilização dos domínios. Os domínios devem então ser organizados em uma estrutura de árvore de forma lógica. Por exemplo, digamos que a Supermercado tenha definido os seguintes domínios:

- EUA
- Canadá
- Brasil
- França
- Rússia
- Moscou
- Leningrado

Os domínios foram criados para reduzir o impacto na rede provocado pela replicação de NC do domínio e, no caso de Moscou e Leningrado, surgiram da ausência de serviços de suporte de rede. Esses domínios podem se tornar UOs caso sejam criados serviços de rede estáveis.

A estrutura de árvore resultante geraria a árvore a seguir.

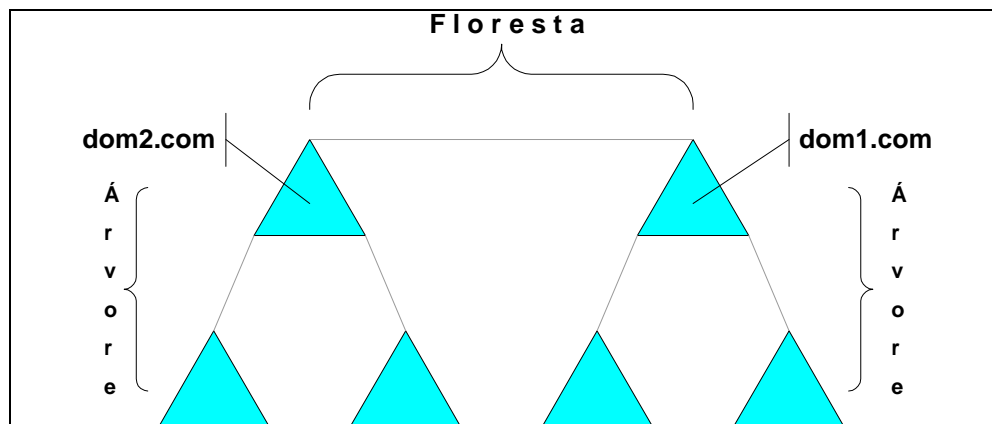


n Figura 5

No caso anteriormente ilustrado, os domínios foram organizados em uma árvore onde os domínios de primeiro nível baseiam-se no país e os domínios de segundo nível baseiam-se na cidade. Contudo, os domínios em si foram criados independentemente da estrutura de árvore resultante.

Florestas

Uma *floresta* é um agrupamento de uma ou mais árvores que vão participar de um sistema de comunicação comum.

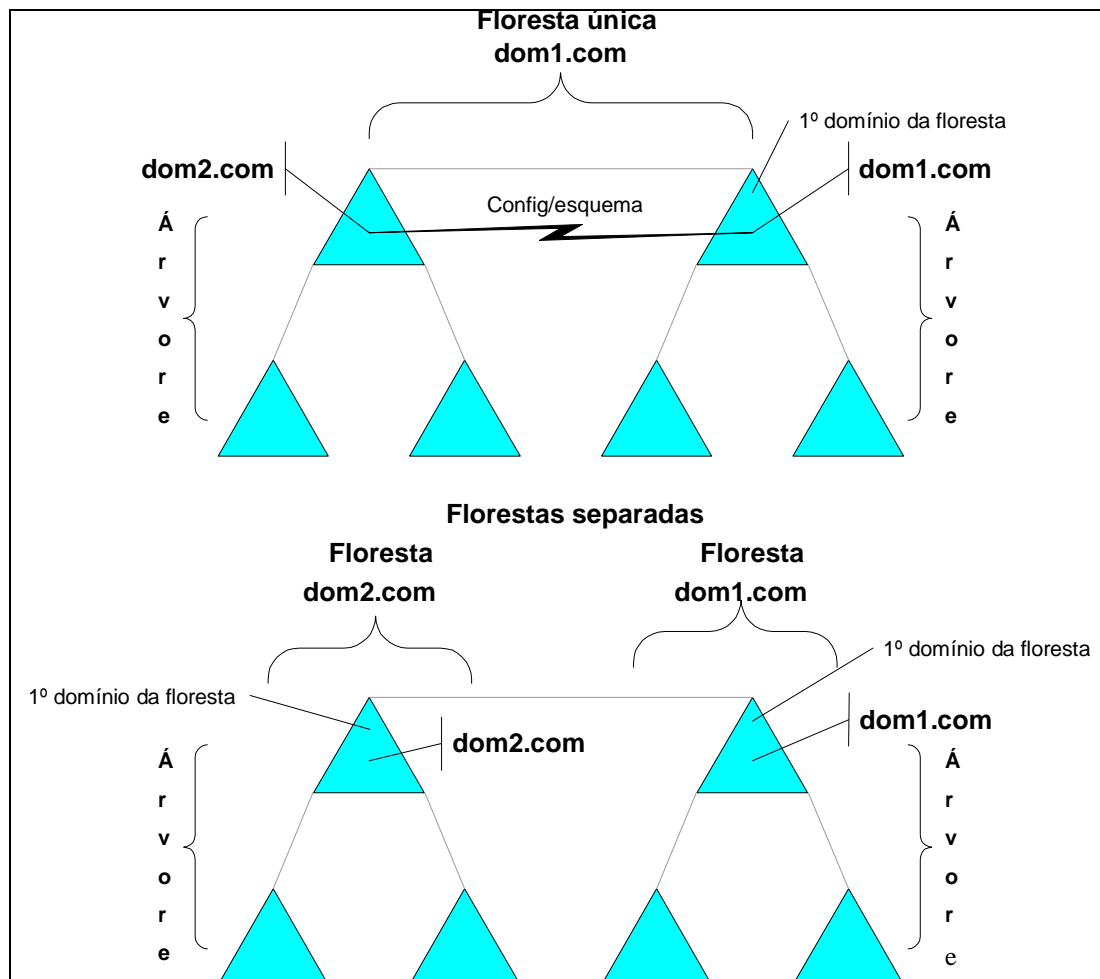


n Figura 6

Uma floresta fornece os limites para muitas das funções do Active Directory, como segurança, convenções, confianças e catálogo global.

Em uma floresta, há um único esquema replicado que é controlado através de um servidor de esquema mestre no domínio raiz.

As relações de confiança Kerberos nunca são transitivas entre florestas, o que as torna adequadas a disposições de parcerias, onde a confiança real também está limitada.



n Figura 7

A distinção entre uma floresta única e florestas separadas refere-se aos objetos de conexão que replicam os NCs de configuração e de esquema, e o catálogo global. Na figura anterior, as mesmas árvores existem nos dois casos, mas implantar **dom2.com** em uma floresta separada fez com que essa árvore fosse completamente dissociada de **dom1.com**. Ainda pode existir uma relação de confiança Kerberos entre as duas florestas, mas não será mais possível se compartilhar o catálogo global e os NCs de configuração e de esquema. O efeito final de se separar as árvores dessa forma é a existência de dois sistemas de comunicação separados.

Utilização de florestas

Uma floresta pode surgir da necessidade de se manter esquemas separados, como é o caso de uma unidade comercial que mantém um aplicativo não confiável. Florestas distintas também vão surgir para estabelecer uma separação entre os recursos internos e os

externos do DNS.

Funcionalmente, criar uma única floresta ou organizar as árvores em florestas separadas é uma decisão fácil de ser tomada durante a instalação do Active Directory. No entanto, essa não é uma decisão a ser tomada despreocupadamente, pois o impacto é grande e duradouro. As florestas não podem ser mescladas nesse momento e atualmente não há suporte para a replicação entre florestas.

Os aspectos funcionais desse tipo de estrutura podem não ser o que se esperava originalmente. Só se deve usar mais de uma árvore em uma única floresta em caso de necessidade. Por exemplo, se Supermercado.com for o nome do domínio estratégico e Loja.com for uma estrutura antiga para a qual há suporte ou uma unidade comercial autônoma, então duas árvores de nível superior seriam adequadas.

Em outros casos, haverá a migração ou inclusão das árvores secundárias de uma floresta em uma árvore homogênea. Árvores adicionais não oferecem nenhum benefício exclusivo em relação à estrutura de árvore única.

Revisão

Os componentes analisados nesta seção foram domínios, unidades organizacionais (UOs), árvores e florestas. Os domínios são partições do Active Directory que são usadas principalmente para oferecer um campo de ação para autoridade administrativa e limitar o campo de ação da replicação. As UOs são partições administrativas do Active Directory que permitem a delegação granular de tarefas administrativas e são ativas por natureza. As árvores são grupos de domínios que formam um espaço de nome contíguo, e as florestas são um ou mais conjuntos de árvores que têm o mesmo esquema e catálogo global.

É importante entender bem os componentes do Active Directory, pois eles são os elementos básicos do Active Directory. Entender o significado e os usos desses componentes é a chave para se criar uma estrutura de diretórios bem projetada.

Espaço de nome e hierarquia de UO

Esta seção aborda as técnicas e a metodologia da criação e ordenação de componentes da Directory Information Tree (DIT, árvore de informações de diretório). Diversas decisões precisam ser tomadas com relação à estrutura real da árvore do Active Directory. Essas decisões vão se basear em uma combinação de diversos fatores, como a estrutura organizacional, a estrutura administrativa e a diversidade geográfica. Esta seção vai proporcionar uma boa compreensão do melhor uso do design de espaço de nome.

Design do espaço de nome de DNS

Hoje em dia, as redes têm duas funções: atender às necessidades de comunicação interna e atender aos pedidos provenientes da Internet. O DNS, é claro, tem um papel essencial na determinação de como esses dois ambientes se relacionam. Há duas escolhas para a infraestrutura básica de DNS que vão afetar o design do espaço de nome.

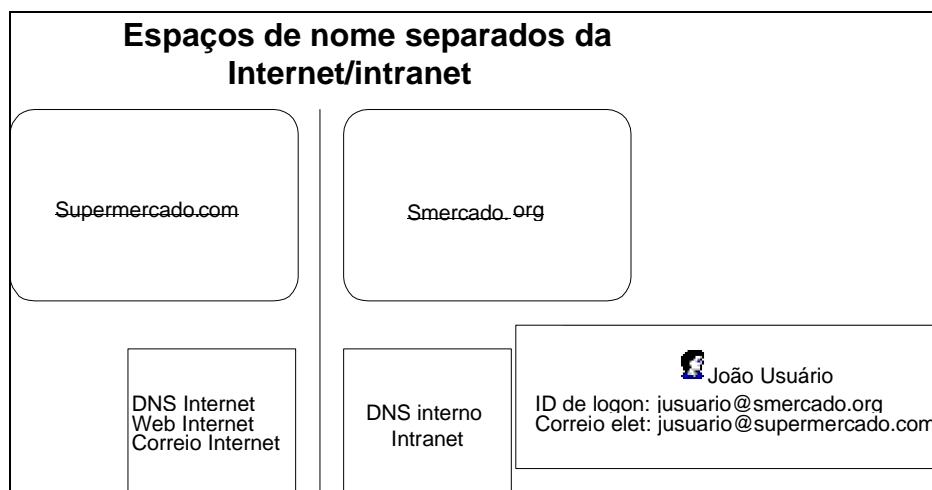
Uma das primeiras decisões a ser feita com relação ao design do espaço de nome é a determinação do papel do DNS e de como o DNS será organizado. Um único espaço de

nome de DNS vai atender aos serviços internos e da Internet ou esses espaços para nome devem ser separados?

Modelo 1: Espaços separados para nome de DNS interno e da Internet

O Active Directory introduz a integração do DNS e do diretório corporativo. As vantagens desse tipo de integração são muitas, mas questões complexas devem ser abordadas no princípio do processo de planejamento. Entre essas decisões, é importante decidir se deve-se fazer uma distinção entre o espaço de nome de raiz interna e o de raiz externa. Em infra-estruturas maduras de DNS, provavelmente essa escolha será determinada pelo ambiente antigo de DNS, mas, se for adequado fazer uma modificação no sistema de DNS, essa é a hora de se fazê-lo.

A decisão de se manter espaços separados para nome interno e externo de DNS baseia-se na lógica convencional, mas as implicações são ampliadas no ambiente do Windows 2000. O espaço de nome usado internamente afeta diretamente os usuários finais, pois faz parte do nome de logon. Consulte os exemplos ilustrados na figura a seguir. Ao se usar espaços para nomes separados, João Usuário deve aprender a distinção entre o seu nome de logon (jusuuario@smercado.org) e o seu endereço de correio eletrônico da Internet (jusuuario@supermercado.com). Usando um único espaço de nome, João Usuário só precisa aprender e usar um único espaço de endereço: @supermercado.com.



n Figura 8: Domínios separados da Internet e interno

É claro que a praticidade para o usuário não é a única nem necessariamente a mais importante consideração a ser feita. A segurança e a administração também são afetadas por essa decisão. Nesse caso, manter uma separação entre os espaços para nome internos e da Internet garante mais segurança e simplifica a administração.

Os espaços para nome separados publicam dispositivos da Internet em um nome de domínio completamente diferente dos dispositivos internos. Nessa configuração, só os serviços internos que são especificamente exigidos são publicados na Internet. A configuração desse tipo de disposição é bastante fácil, pois o gerenciamento e os dispositivos em si são mantidos separadamente.

Há alguns métodos conhecidos de se fazer essa configuração para não comprometer os registros internos.

- Como tanto os nomes de domínio de Internet como os da intranet devem ser registrados com o Internic, as entradas SOA das duas zonas devem poder ser acessadas a partir da Internet. Como tal, a primeira etapa será criar duas zonas primárias no servidor de DNS da Internet: uma para o sistema de domínio da Internet e outra para a intranet.
 - a) No servidor de DNS baseado na Internet, uma zona primária é criada para Supermercado.com (o domínio da Internet)
 - b) No servidor de DNS baseado na Internet, uma zona primária é criada para smercado.org (o domínio da intranet).

As medidas de segurança determinam que os serviços internos não podem ser publicados na Internet. Para atender a essa exigência, o sistema de DNS da intranet também deve ser host da zona de DNS da intranet, como zona primária. Nesse momento, um sistema de DNS não sabe da existência do outro sistema de DNS e eles vão responder aos pedidos do nome de domínio da intranet. São necessários mais dois pontos adicionais de configuração para garantir que a zona da intranet receba todos os pedidos adequados e também seja protegida contra exposição na Internet.

1. No sistema de DNS da Internet, atribua o controle da zona da intranet ao servidor de DNS interno, criando um registro do tipo NS que aponte para o servidor interno.
2. No servidor de DNS da intranet, crie uma zona primária para smercado.org. Esse será o local que vai ser, de fato, o host dos registros dos serviços internos.

Além disso, defina o servidor de DNS da Internet como roteador do sistema de DNS da intranet, a fim de que o servidor de DNS da intranet não tente solucionar as consultas externas diretamente na Internet, mas, em vez disso, passe os pedidos através dos servidores de DNS da Internet.

Um único espaço de nome requer que os servidores proxy, firewalls e clientes sejam configurados para fazer a distinção entre recursos internos e externos. Naturalmente, isso é garantido ao se manter uma separação dos espaços para nome. É mais fácil garantir a segurança com espaços para nome separados, pois, como padrão, nenhum nome de recurso interno jamais seria publicado na Internet.

Modelo 2: Espaço único para nome de domínio raiz

A implantação de um único domínio de DNS vai atender a consultas de nome na Internet e internas. Nesse caso, uma única zona vai se expandir pelos sistemas de DNS da Internet e da intranet, gerando um único espaço de nome para a organização.

Questões prementes surgem relacionadas ao uso de um único domínio de DNS, como, por exemplo, como impedir a publicação de registros internos de DNS na Internet?

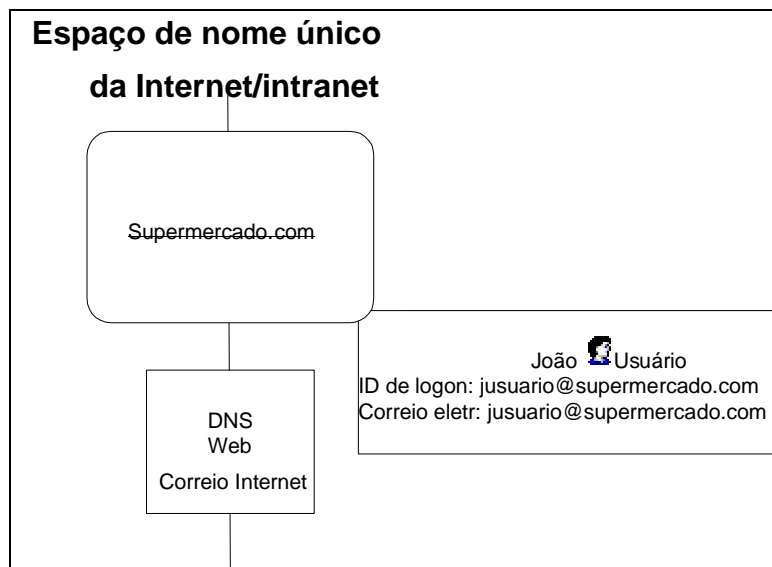


Figura 9: Espaço único para nome de DNS

Ainda existe a necessidade de se proteger os registros internos e, portanto, deve-se usar um método de separação de recursos. São usados novamente servidores de DNS separados para atender aos serviços internos e da Internet. Nesse caso, a zona primária do nome de domínio será criada no servidor de DNS da Internet e no da intranet. Nesse momento, nenhum dos servidores de DNS tem conhecimento do outro. Isso atende aos critérios de segurança desejados para se separar os próprios registros.

O servidor de DNS da intranet nunca deve ser exposto aos pedidos da Internet ou à recursão, mas ainda deve poder atender a resoluções de nome para as quais não tem autoridade. Para fazer isso, o servidor de DNS da intranet deve ser configurado para usar o servidor de DNS como roteador.

Nesse caso, os registros serão gerenciados como se as zonas existissem para dois domínios separados. Os registros da Internet são publicados no sistema da Internet, e os registros internos são publicados no sistema da intranet. Os dois nunca vão se encontrar. A configuração resultante estabelece, de forma eficiente, duas zonas separadas. Embora tenham o mesmo nome de domínio, nenhum dos dois servidores sabe da existência do outro.

Vantagens e desvantagens dos dois modelos

Modelo 1:

Manter uma separação entre o domínio interno e o domínio da Internet tem algumas vantagens características.

- Existe uma distinção clara entre os recursos da Internet e da intranet do ponto de vista do gerenciamento e do usuário final.
- A estrutura é mais fácil de ser gerenciada porque o espaço de nome distinto pode ser mantido separadamente.
- Também é mais fácil fazer a configuração do navegador do cliente, pois as listas de exceção não precisam ser mantidas para se fazer a distinção entre os recursos da

Internet e da intranet.

- A configuração do cliente proxy é facilitada pelo mesmo motivo. É preferível evitar o uso de um servidor proxy para recursos internos. Para realizar essa configuração, uma lista de exceções deve ser fornecida para permitir que o cliente faça a distinção entre os dois ambientes.

A desvantagem dessa configuração é:

- O nome de logon do usuário é diferente do nome de correio eletrônico. Se os usuários trabalham com um espaço de nome homogêneo, passar a usar espaços para nomes separados pode ser uma experiência traumatizante. Lembre-se de que, embora nenhum contexto complexo esteja associado aos usuários, eles ainda assim estão expostos ao contexto de DNS (jusuario@somdom.com) que será diferente do endereço de correio eletrônico da Internet.

Modelo 2:

O principal ponto dessa disposição é que os usuários têm uma visão da Internet e da intranet. É de responsabilidade do administrador fazer uma distinção back-end entre as duas redes.

A administração e o gerenciamento são um pouco mais complicados nesse caso, pois, embora os sistemas sejam tecnicamente distintos, deve-se especificar que recursos existem em que zona primária. Isso pode levar a questões de segurança devido à postagem de recursos internos inadvertidamente no sistema de DNS da Internet.

Requisitos de DNS

O Microsoft DNS não é absolutamente necessário para o Active Directory, mas para usar um sistema de DNS de outro fabricante, ele deve oferecer suporte a determinados requisitos.

- O Service Location Resource Record (SRV RR, registro de recursos de local de serviço), RFC 2052
- O protocolo Dynamic Update, RFC 2136

Se não houver infra-estrutura de DNS, a escolha lógica é implementar o Microsoft DNS. Contudo, esse caso é raro, momento em que deve-se fazer a determinação da adequação do sistema antigo de DNS.

Além dos requisitos funcionais básicos de atender ao suporte de atualização dinâmica e de SRV, uma outra consideração deve ser feita: A zona antiga se enquadra na zona de DNS que se deseja usar no Windows 2000?

Recomendações de DNS

Além disso, lembre-se de que, mesmo que o sistema antigo atenda aos requisitos, você ainda precisa considerar que atualizações dinâmicas vão ser replicadas entre as suas

zonas. Essa não é uma consideração de pouca importância. O DNS dinâmico pode gerar milhares de entradas existentes em um banco de dados de DNS. Até mesmo as transferências de zona incrementais, o banco de dados de arquivo texto sem formatação mantido por software de DNS convencional está sujeito a danos e assume uma grande parte da carga de replicação.

Contudo, o Microsoft DNS permite a integração do banco de dados diretamente com o Active Directory que resulta em um mecanismo de replicação mais eficiente para registros de DNS.

Se o sistema de DNS antigo não atender aos requisitos necessários para o Active Directory, existem três escolhas:

1. Atualizar o(s) servidor(es) existente(s) para atender aos requisitos.
2. Fazer a migração do(s) servidor(es) para o Microsoft DNS.
3. Selecionar um novo nome (nomes de domínio separados) e atribuir a zona interna ao Microsoft DNS.

Considerando-se tudo isso, a implantação do Active Directory é uma boa oportunidade de se fazer a migração para o Microsoft DNS, se possível. O Microsoft DNS está bastante maduro nesse momento e oferece um excelente suporte a padrões e desempenho.

Zonas e domínios de DNS adicionais

Até agora, abordamos somente a raiz dos domínios de DNS e do Active Directory. A maioria das situações vai exigir a existência de vários outros domínios e zonas para atender a subdomínios e zonas secundárias.

Subdomínios

Além do(s) domínio(s) de DNS raiz, cada domínio filho do Windows 2000 vai, na maioria das situações, ser classificado como um subdomínio e ter um espaço de nome de DNS associado. Há diversas opções disponíveis para a criação de serviços de DNS para domínios filho.

O procedimento recomendado para a criação de serviços de DNS para um domínio filho é primeiro criar o subdomínio na raiz interna e atribuir esse subdomínio a um servidor de DNS ativo dentro do domínio filho:

- Criar um subdomínio de DNS para o filho a partir do domínio raiz (p. ex.: Filho.raiz.com).
- Criar uma zona de DNS primário para o filho dentro do seu próprio domínio (p. ex.: Filho.raiz.com).
- A partir da raiz, atribuir o subdomínio ao servidor de DNS filho.

Há outras opções disponíveis que podem ser usadas em situações que não são tão favoráveis. Não é necessário, por exemplo, criar o DNS em um domínio filho. O domínio filho pode ser criado como um subdomínio no pai ou a raiz para atender ao filho. Nesse caso, os serviços de DNS podem ser criados em filho.raiz.com que seria então o host de zonas secundárias para o pai ou a raiz.

Zonas secundárias

Provavelmente, não existirão zonas de DNS secundárias na maioria dos casos. Uma zona secundária é uma cópia de leitura somente da zona primária usada para distribuir serviços de DNS para solucionar dúvidas. Contudo, no Windows 2000, uma zona secundária também pode ser de gravação se o DNS estiver integrado ao Active Directory. As zonas secundárias que podem ser gravadas fornecem um elemento chave em um ambiente de DNS do Windows 2000 com atualização dinâmica.

Como padrão, todos os clientes de DHCP do Windows 2000 vão solicitar que o DHCP atualize automaticamente o DNS. Caso haja zonas secundárias que não estejam integradas ao Active Directory, as modificações de atualização só podem ser gravadas no servidor de DNS que age como o SOA da zona (primária). O impacto disso pode ser significativo. Dado um grande número de clientes ou um ambiente distribuído, os registros de DNS na zona primária e o tráfego de rede associado podem ter um impacto profundo tanto no desempenho do servidor como no da rede. Por esse motivo, recomenda-se que todos os controladores de domínio que contêm DNS estejam integrados ao Active Directory.

Revisão

Projetar o espaço de nome de DNS é uma parte integrante do design da estrutura do Active Directory da sua empresa. Nesta seção, analisamos as vantagens e desvantagens de se ter espaços para nome separados em oposição a um único espaço de nome. Em resumo, os espaços para nome separados são mais flexíveis, mas requerem um ajuste significativo pelos usuários finais. O design do espaço de nome único é mais intuitivo para os usuários, mas é também mais difícil de ser administrado. Esta seção também abordou os requisitos e recomendações de DNS. Lembre-se de que o seu sistema de DNS deve oferecer suporte a registros SRV RR e atualizações dinâmicas. O Microsoft DNS é o sistema escolhido, pois ele atende a esses requisitos e também permite a integração do banco de dados diretamente com o Active Directory, gerando um mecanismo de replicação mais eficiente para os registros de DNS.

Introdução aos diversos métodos de design e suas implicações

O rápido crescimento da tecnologia durante a última década provocou o deslocamento em massa dos sistemas baseados em host para sistemas distribuídos. Essa mudança também gerou um grande aumento dos custos de TI associados à implantação e gerenciamento desses sistemas. Infelizmente, os orçamentos de TI também têm sido sobrecarregados com reimplementações de infra-estrutura distribuída após um ciclo de vida relativamente curto. Um bom design de sistema distribuído deve durar muitos anos e deve passar por inovações tecnológicas como resultado de atualizações ao software de suporte.

É mais fácil falar do que fazer. Um projeto mal feito pode trazer graves conseqüências posteriormente geradas por reorganizações corporativas ou estruturas que não pode ser dimensionadas ou que são difíceis demais de serem gerenciadas.

O Active Directory não exige necessariamente um planejamento antes da implantação, mas retornos

valiosos vão ocorrer como resultado de uma estrutura ampliável para redes distribuídas. A primeira etapa do planejamento é a definição do método básico que pode ser usado para definir o design do espaço de nome.

Existem três tipos básicos de designs de espaço de nome: Geográfico, Político e Funcional. Além desses princípios básicos, combinações simples podem ser incluídas para gerar atributos exclusivos ao design do espaço de nome. Quase todas as organizações vão se enquadrar em um desses princípios de design.

Domínio raiz

Independentemente da base da estrutura de diretório, o componente mais importante é o domínio raiz. Embora seja difícil alterar qualquer nível da estrutura do domínio, modificar o espaço de nome raiz é bastante desagradável. Esse tópico foi parcialmente abordado na seção sobre DNS que forneceu os métodos e motivos para a criação de um domínio de nível superior.

Além dessas considerações, existem atributos específicos do domínio raiz. O domínio raiz (nível superior) é o primeiro domínio a ser instalado na floresta. Esse domínio não pode ser renomeado nem removido. O domínio raiz também vai fornecer duas funções Flexible Single Master Operations (FSMO, operações de mestre único flexível) principais a toda a floresta.

A importância do domínio raiz sugere que, pelo menos, a sua natureza deve ser permanente. Tendo isso em mente, o nome do domínio raiz deve ter um significado para o nível superior da organização, como, por exemplo, o nome da empresa. Esse diretório está correlacionado ao nome de DNS raiz que será usado para os serviços internos.

Em geral, o domínio raiz estará ativo, o que significa que será usado como qualquer outro domínio e que será host de UOs, usuários, recursos e outros objetos. Ou então, o domínio raiz pode ser estático por natureza e existir simplesmente como um espaço reservado na floresta para outros domínios filho. Convém usar domínios de espaço reservado quando a organização já tiver implantado um espaço de nome filho a ser usado nas comunicações internas. Por exemplo, se a empresa Supermercado estivesse usando dentro.Supermercado.com como zona de intranet antes da implantação do Windows 2000, seria adequado criar um domínio raiz para Supermercado.com como espaço reservado.

Outra situação onde convém usar um domínio raiz como espaço reservado é quando uma empresa deseja manter uma única floresta, mas, por questões de segurança, os usuários e os recursos das divisões não podem ser misturados no mesmo domínio. Normalmente, essa situação levaria a uma floresta com duas árvores. Contudo, um domínio raiz de espaço reservado pode ser usado como uma pai estéril das duas árvores de divisão.

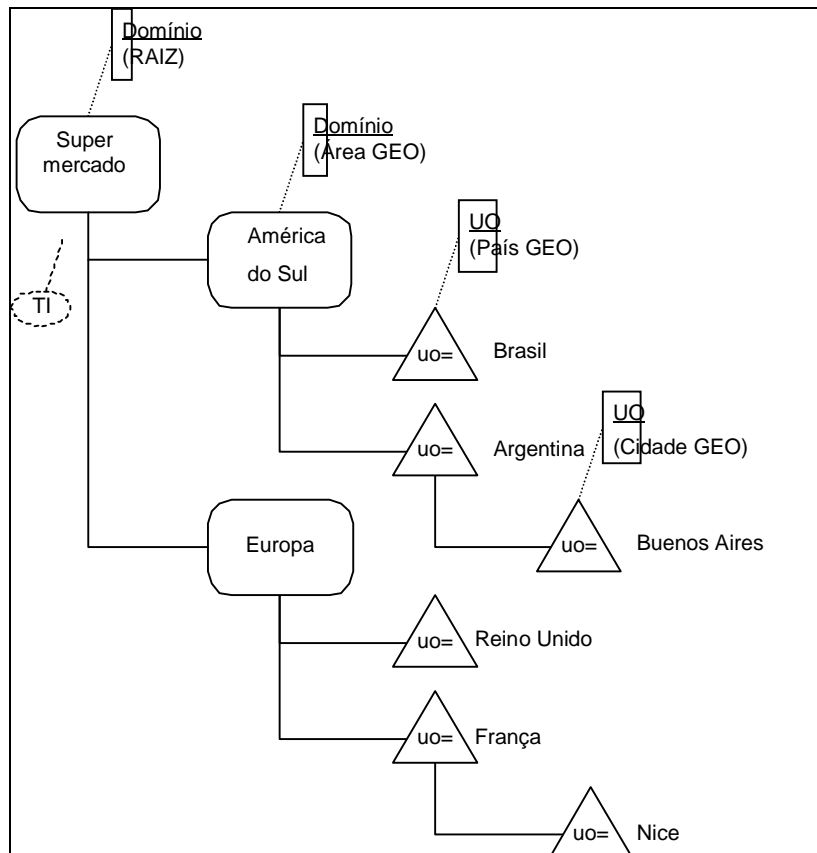
Geográfico

Uma estrutura que é definida por locais físicos é conhecida como grupo Geográfico. Esse é um fundamento conhecido do design do espaço de nome por ser imune a reestruturações organizacionais.

Usar a geografia como base para se estruturar o diretório funciona muito bem logo abaixo

do nível da raiz do diretório, onde as modificações feitas na estrutura do diretório exercem o maior impacto operacional.

O diagrama a seguir representa a estrutura de diretório baseada na geografia de uma empresa denominada Supermercado.



n Figura 10: Geográfico

A figura 10 ilustra uma hierarquia geográfica típica implementada na Supermercado. Os domínios de primeiro nível baseiam-se em divisões continentais, e a estrutura secundária baseia-se no nível do país. Um aspecto característico dessa estrutura é a sua capacidade de se adaptar a reorganizações corporativas. Exceto em caso de guerra civil ou deslocamentos de placas tectônicas, as fronteiras não estão sujeitas à alteração, o que garante uma estabilidade inerente a esse design.

Para se implantar com êxito um modelo geográfico, é imprescindível a existência de um TI centralizado. Salvo se a própria estrutura organizacional se basear em um grupo Geográfico (o que tornaria o modelo político), uma única entidade deve ter autoridade sobre todos os recursos das divisões. Na maioria das grandes organizações, isso é raro.

Esse modelo oferece suporte a:

- Organizações extremamente distribuídas.
- TI centralizado.

As opções de definição dos grupos geográficos reais para a estrutura de diretório variam,

mas são, em grande maioria, motivadas pela necessidade de se dividir a replicação com base nas condições da rede. No exemplo anterior, o uso de dois domínios de primeiro nível oferece um bom mapeamento dos componentes primários da rede que também são obviamente baseados na geografia. Usar domínios dessa forma preserva uma parcela da largura de banda, que é provavelmente um link transatlântico de alto custo. Nas grandes organizações, isso pode representar uma quantidade significativa de tráfego de rede.

Embora esse assunto possa ser uma questão semântica, não se deve criar domínios nesse modelo para criar partições de segurança. As partições de segurança sempre se baseiam em exigências políticas e não geográficas. O fato de que as leis internacionais possam exigir domínios distintos entre fronteiras internacionais é, na verdade, uma consideração política e não geográfica.

Como será descrito na seção de variantes, os domínios podem ser mais ou menos profundos, dependendo do tamanho da empresa e das condições da rede.

PRÓS

- A estrutura de árvore é imune à reorganização corporativa.
- A árvore aceita expansões. Outras divisões ou grupos geográficos podem ser facilmente acrescentados.
- Essa estrutura está bastante adequada à distribuição de operações de suporte e TI. Os limites de segurança permitem unir o campo de ação dessas operações.
- Essa estrutura se adapta muito bem às características positivas e negativas da rede.

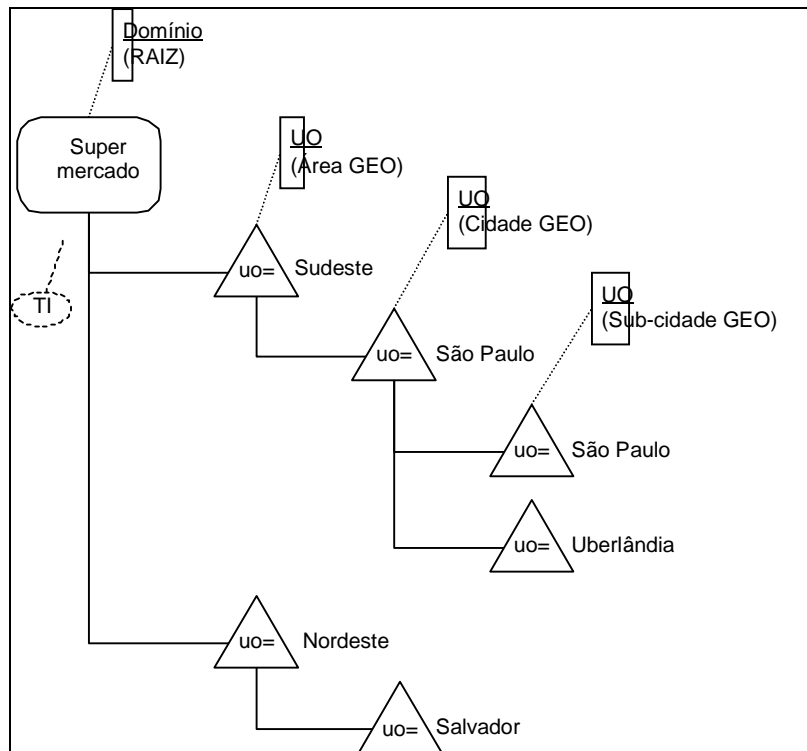
CONTRAS

- A estrutura organizacional não é levada em consideração, o que em geral prejudica o uso da navegação intuitiva.
- Os limites de divisões podem ser transpostos, o que dificulta a desconexão, implantação e gerenciamento.
- Essa estrutura não permite a mudança para um TI descentralizado baseado em departamentos. As entidades que não fazem parte das divisões devem ser gerenciadas de forma centralizada ou participativa.

VARIANTES

Há várias variantes diferentes do modelo geográfico básico. Elas podem se basear em unidades geográficas ou no número de níveis do domínio.

É claro que o nível da estrutura do domínio pode ser aumentado ou diminuído. Ao se lidar com uma distribuição geográfica menor, os domínios de primeiro nível podem ser eliminados e substituídos por unidades organizacionais (UOs). Por exemplo, se as operações da Supermercado se baseassem somente no Brasil, com locais que fossem bem conectados, acabaríamos tendo uma estrutura de diretório parecida com a que se segue.



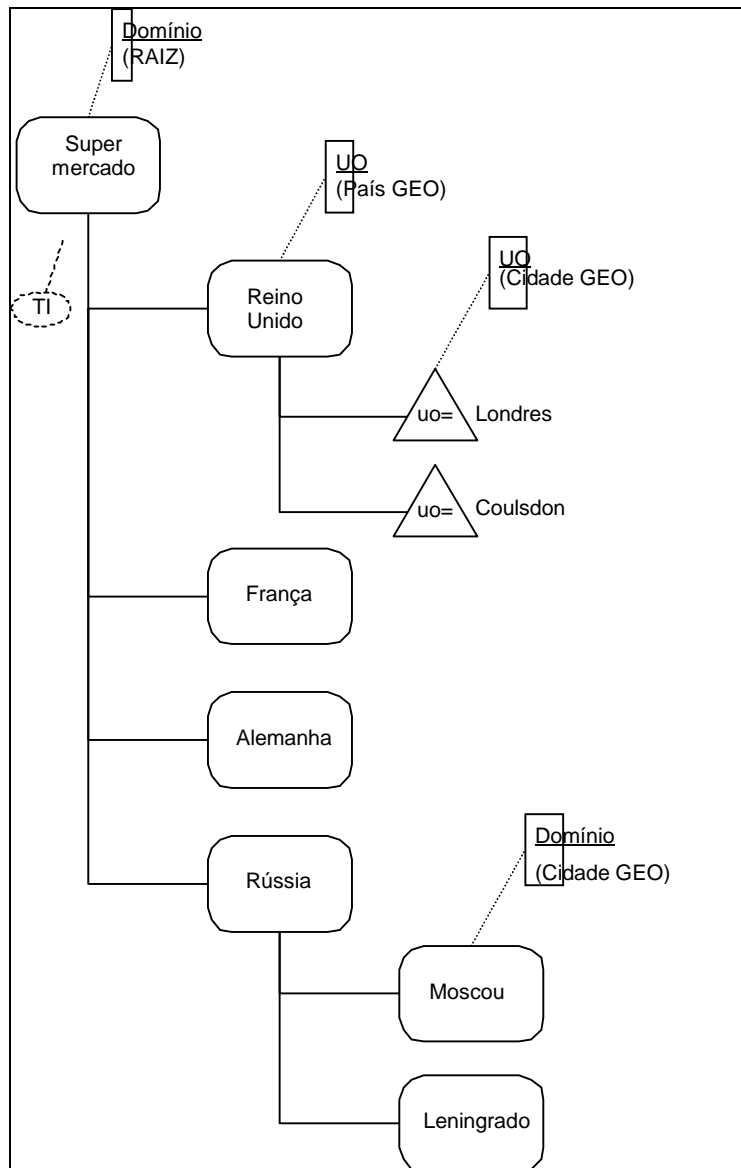
n Figura 11: Geográfico

Na figura 11, eliminamos por completo o domínio de primeiro nível, porque as duas áreas principais (Sudeste e Nordeste), para as nossas finalidades, têm boa conectividade através de WAN. Caso a largura de banda fosse um problema, essas áreas teriam sido criadas como domínios, o que iria:

1. Isolar a réplica completa do Naming Context (NC) do domínio.
2. Ativar a replicação entre os domínios para usar a compactação, reduzindo ainda mais o uso da rede.

As UOs foram criadas para representar áreas geográficas significativas. Em uma organização de pequeno porte, também eliminaríamos as UOs baseadas em áreas e especificaríamos simplesmente as cidades. Mesmo no exemplo anterior, a estrutura de unidade organizacional baseada em país na verdade não oferece nenhuma vantagem a não ser a da própria estrutura.

Nas organizações globais, pode ser necessário criar mais domínios ou níveis mais profundos de domínios. Nesse caso, vamos supor que a Supermercado tenha muitos escritórios em diversos países europeus. As conexões por rede entre esses países baseiam-se em ISDN de discagem por demanda. Todas as conexões de rede da Rússia baseiam-se em ISDN. Somos então forçados a usar a estrutura que se segue.



n Figura 12: Geográfico com vários domínios

O exemplo da figura 12 mostra os seguintes preceitos:

1. Os países individuais da Europa ocidental têm redes sólidas dentro das fronteiras de seus países, permitindo a comunicação e replicação de diversos mestres, sem que hajam custos adicionais de linha.
2. A comunicação e replicação entre os países é limitada e controlada, reduzindo os custos de comunicação relacionados aos links ISDN de discagem por demanda.
3. O transporte entre os escritórios da Supermercado na Rússia não é confiável, o que exige a criação de outro nível de domínio baseado nas cidades. Quando as condições da rede melhorarem, esses domínios podem ser transformados em UOs. No momento, a existência de domínios separados permite que a replicação entre os domínios aconteça através de transporte SMTP baseado em mensagens.

O uso de domínios para dividir a replicação só deve ser usado junto com os recursos fornecidos pelos sites. Resumindo, os sites permitem o amplo controle da forma em que a replicação ocorre, enquanto os domínios determinam o campo de ação real da replicação. Esse tópico será abordado nas seções que se seguem.

Conclusão

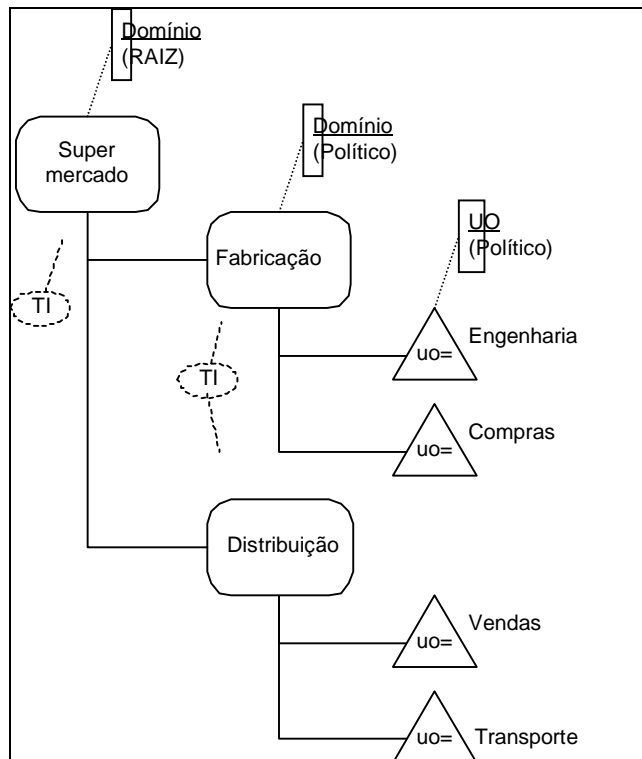
Basear a estrutura do Active Directory em grupos geográficos fornece o tipo mais estável de design, pois as reorganizações corporativas não afetam a estrutura do domínio.

A criação de domínios deve se basear na necessidade de se minimizar o tráfego de replicação através do campo de ação e da replicação compactada, bem como a capacidade de se fazer a replicação através de SMTP.

Político

Até recentemente, era bastante comum se basear uma estrutura de TI em fronteiras políticas. A estrutura política/organizacional se adapta bem ao próprio modelo comercial, é fácil de se projetar e evita questões relacionadas à transposição de grupos de divisões. O motivo que levou ao desuso desse modelo é a tendência relativamente nova de se fazer freqüentes reorganizações corporativas. A reestruturação dos domínios de primeiro nível em um diretório é um processo bastante difícil e longo.

É bastante simples se organizar os domínios e UOs segundo o modelo político, onde os domínios representam divisões administrativas e as UOs representam estruturas e recursos departamentais.



n Figura 13: Estrutura de diretório política

Basear o domínio de primeiro nível em considerações políticas, como a estrutura organizacional, gera uma estrutura de diretório que reflete melhor o modelo comercial. Uma base política funciona bem em um ambiente de TI distribuído, onde as funções de TI estão intimamente relacionadas aos grupos de divisões.

Nesse modelo, há suporte para os seguintes atributos:

- TI centralizado, descentralizado ou distribuído
- Rede de boa conexão
- Grupos de divisões fortes

Nesse modelo, os domínios atendem a duas exigências:

- São necessárias diretivas de segurança separadas para as divisões.
- É necessária uma separação administrativa distinta devido ao TI político ou descentralizado.

Os domínios desse modelo nunca são estabelecidos visando à criação de um campo de ação para a replicação porque a geografia não é a base da estrutura.

PRÓS

- O espaço de nome interno está alinhado com a estrutura organizacional da empresa, o que reduz as exigências e confusão no treinamento do usuário final.
- O design do espaço de nome interno de DNS é mais fácil de se planejar e implementar.

- Os grupos de divisões são evitados, e as fronteiras não são transpostas. Isso aumenta a probabilidade de êxito na conexão e implantação.
- A árvore permite expansão em divisão ou geografia.

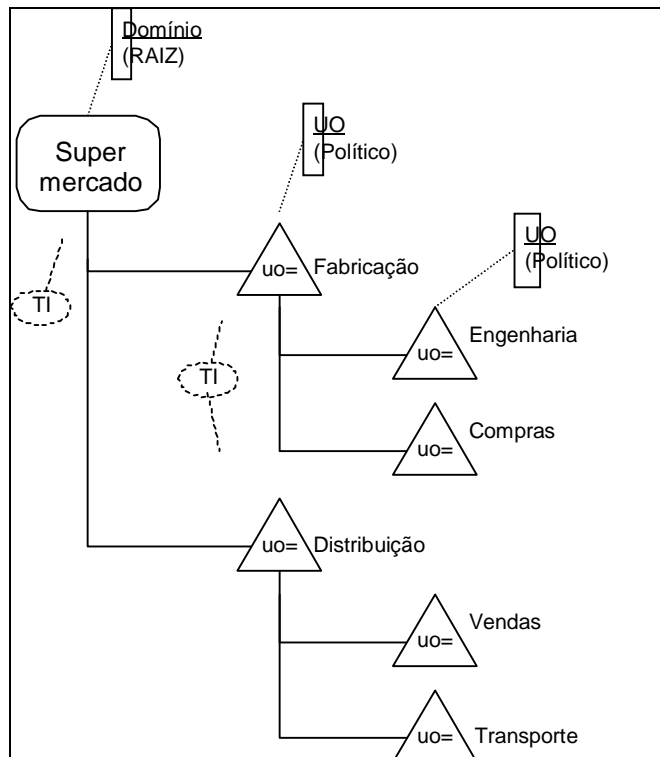
CONTRAS

- A estrutura do domínio não usa de forma eficiente a rede na criação de um campo de ação para a replicação. Os dois domínios vão provavelmente existir nos mesmos locais.
- A reorganização das unidades comerciais levaria a uma iniciativa predominante de TI.

VARIANTES

Assim como o modelo geográfico, as variantes desse design dizem respeito principalmente ao número e disposição dos domínios. Diferentemente do modelo geográfico, a criação de domínios será determinada pelas exigências de segurança e administração e não pela necessidade de se controlar a replicação ou melhorar o desempenho da rede.

Em um ambiente de TI centralizado, a variante óbvia é remover todos os domínios de primeiro nível, exceto um, substituindo-os por UOs.



n Figura 14: Estrutura de diretório política

É possível substituir os domínios de primeiro nível por UOs porque há um departamento de TI controlador que pode manter a raiz e a delegar a administração conforme necessário aos departamentos de TI da unidade comercial. Também é possível implementar essa variante

em um ambiente de TI distribuído desde que os departamentos de TI não sejam autônomos.

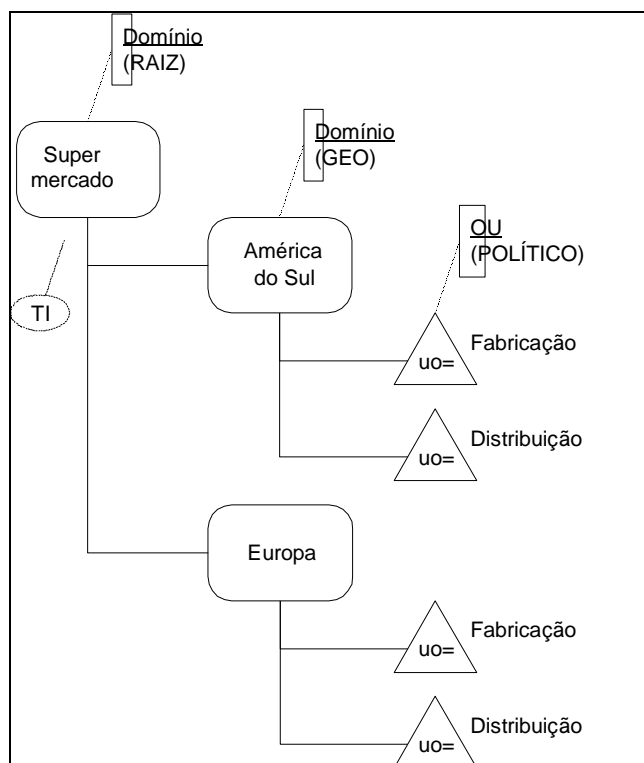
Essa opção remove a desvantagem relacionada à rede e à replicação duplicada e fornece um modelo administrativo eficiente.

Uma vantagem real de se eliminar os domínios de segundo nível é a manutenção de um único espaço de nome para a organização. Se a simplicidade de implantação e de administração for um objetivo, deve-se criar um domínio único e fazer com que ele reflita a empresa.

A justificativa de se criar uma estrutura de domínio profunda nesse modelo é rara, mas pode existir em sociedades de controle e outras organizações distribuídas onde existem empresas operacionais autônomas dentro das unidades comerciais. Contudo, os custos administrativos indiretos desse tipo de modelo são altos e devem ser evitados, se possível.

Geo-político

O modelo de diretório geo-político é talvez o mais funcional. Como o próprio nome sugere, o modelo geo-político mistura aspectos dos modelos geográfico e político nos diversos níveis do diretório. Os níveis específicos em que cada um vai ser aplicado variam, mas pelo menos o primeiro nível sempre se baseia na geografia e os níveis subsequentes se baseiam em fatores políticos.



n Figura 15: Geo-político

A estrutura geo-política oferece os melhores atributos dos dois modelos analisados anteriormente. A capacidade de adaptação é obtida nos níveis mais altos do diretório ao se

basear a estrutura na geografia, enquanto a estrutura organizacional é refletida nos níveis inferiores, garantindo a facilidade de uso e de delegação da administração.

A justificativa desse tipo de estrutura é relativamente simples. O maior impacto potencial para uma organização está no domínio de primeiro nível. Por exemplo, considerando a estrutura descrita na base política, uma mistura forçada entre os domínios de primeiro nível (fabricação e distribuição) afetaria todos os aspectos da infra-estrutura, pois todos os objetos estão contidos nesse dois domínios ou atendem a eles. Contudo, na situação descrita na estrutura geo-política, só os domínios de segundo nível ou UOs podem ser afetados por uma reorganização. Nesse momento, então, o impacto limita-se somente aos domínios diretamente modificados e a seus filhos.

O objetivo dessa regra não é eliminar, mas sim minimizar o risco da exposição a reorganizações. Existe uma compensação evidente entre a estabilidade da árvore e a consideração de realidades políticas para obter vantagens.

Nesse modelo, há suporte para os seguintes atributos:

- TI centralizado ou distribuído
- Organização extremamente distribuída
- Grupos de divisões fortes

O modelo do domínio pode se basear nos dois modelos (Geográfico ou Político). Como sempre, é melhor reduzir ao mínimo o número de domínios.

Use domínios para distinguir áreas geográficas quando há necessidade de se minimizar o tráfego de replicação através de links de WAN ou se for exigida uma separação de segurança entre os países, etc.

Use domínios abaixo do nível geográfico para representar a estrutura organizacional somente se a empresa for organizada de forma que os diversos grupos de divisões se baseiem em regiões geográficas específicas e se esses domínios precisarem de separação protegida e distinta entre si.

PRÓS

- A estrutura de árvore de diretório minimiza o impacto das reorganizações.
- A árvore permite expansão. Outras divisões ou grupos geográficos ou políticos podem ser facilmente acrescentados.
- Essa estrutura se adequa bem à distribuição das operações de suporte e de TI. Os limites de segurança permitem unir o campo de ação dessas operações.
- Provavelmente, essa estrutura se adapta muito bem às características positivas e negativas da rede.

CONTRAS

- Não oferece suporte fácil à mudança para um TI descentralizado devido à necessidade de gerenciar entidades geográficas separadas.
- A administração departamental pode estar espalhada em diversos domínios,

aumentando os custos administrativos indiretos. Observe que, se a administração se basear em fatores políticos, as mesmas entidades administrativas podem se expandir pelos dois domínios.

- Isso pode exigir um pouco de administração participativa dentro dos domínios geográficos.

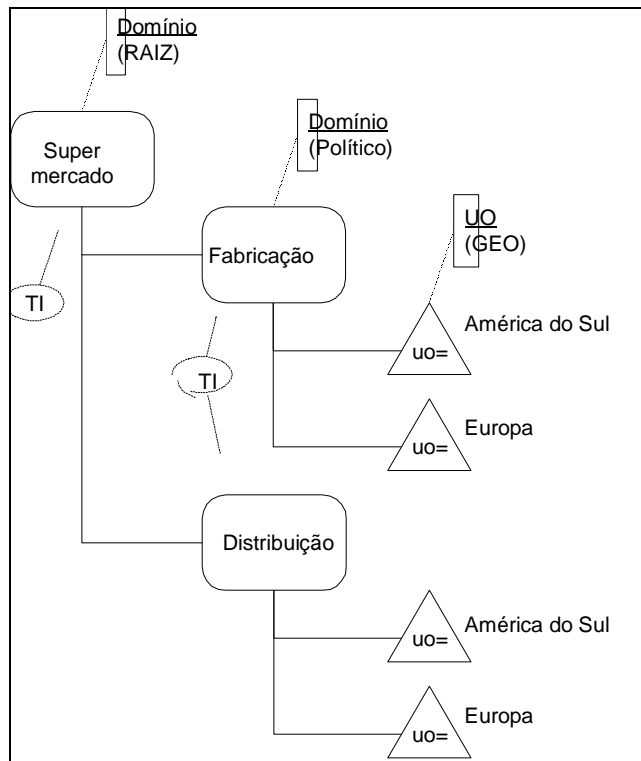
VARIANTES

Na verdade, não há variantes desse modelo além da profundidade dos domínios em relação às UOs. Mesmo nesse caso, substituir domínios de primeiro nível por UOs geraria OUs geográficas que, na maioria dos casos, não trariam nenhuma vantagem, gerando uma estrutura puramente política.

Político-geográfico

Também é possível aplicar a estrutura geográfica abaixo da estrutura organizacional em um diretório. O modelo político-geográfico lida primeiro com a estrutura organizacional e depois aplica a estrutura baseada em considerações geográficas.

Existem algumas justificativas para se aplicar essa estrutura específica ao diretório. Grandes empresas multinacionais vão freqüentemente escolher esse modelo porque a capacidade de fornecer uma separação entre as unidades comerciais primárias e dentro dessas unidades comerciais é responsável pela distribuição geográfica. Geralmente, as grandes empresas mantêm unidades comerciais que são por si só grandes empresas. Essas subempresas, por sua vez, são multinacionais e provavelmente vão exigir domínios para criar o campo de ação do NC do domínio.



n Figura 16: Político-geográfico

Caso seja necessário delegar administração ou aplicar diretivas com base em unidades suborganizacionais (UOs geográficas), essa estrutura seria apropriada. Contudo, se esse não for o caso, o nível que representa as unidades geográficas seria arbitrário e, portanto, desperdiçado. As separações geográficas dentro desse modelo baseiam-se exatamente nisso. Se essas separações fossem parte da estrutura organizacional da empresa, seriam na verdade baseadas em considerações políticas e não geográficas.

Nesse modelo, há suporte para os seguintes atributos:

- Oferece suporte a todos os ambientes de TI
- Unidades comerciais distribuídas fisicamente
- Grupos políticos fortes

Típicos da rede que representam, os domínios podem ser justificados por facilitar as exigências de segurança (entre divisões) ou limitar a replicação para acomodar as limitações da rede física. Em geral, o uso desse modelo específico vai misturar os dois, gerando domínios de vários níveis. Um único domínio raiz também pode ser usado, garantido por UOs políticas e geográficas.

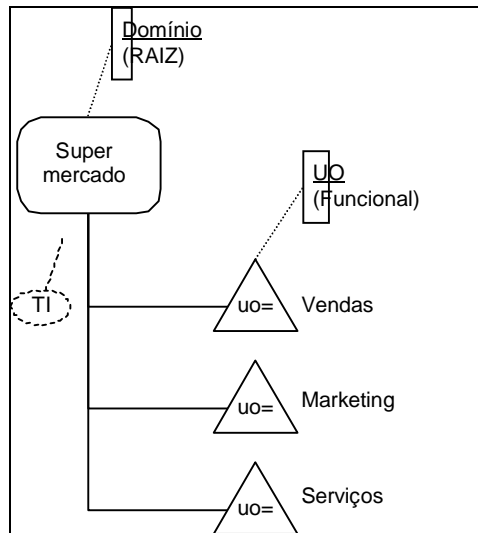
PRÓS

- Oferece suporte à organização comercial no primeiro nível.
- Oferece suporte à distribuição de TI em todos os níveis.
- Fornece excelente segurança entre unidades comerciais enquanto permite a delegação administrativa ou campo de ação de replicação com base no local físico.

Funcional

O modelo funcional considera, independentemente de todas as outras considerações, que o objetivo mais importante das comunicações internas é facilitar a participação. Um modelo funcional considera somente as funções comerciais de uma organização, sem levar em conta as considerações políticas ou geográficas.

Esse modelo pode funcionar bem em pequenas organizações, com um TI centralizado. Só é necessário um nível de domínio nesse modelo porque a segurança entre as unidades não é uma consideração. O tema do modelo funcional é o de comunicações participativas considerando somente os objetivos comerciais. Isso requer uma regra rígida no nível executivo sênior, pois não há suporte para grupos de divisões.



n Figura 18: Funcional

O modelo funcional está completamente imune à reorganização corporativa, pois desconsidera por completo todos os atributos exceto as operações comerciais funcionais. Portanto, algo menos que um realinhamento completo do negócio essencial pode ser absorvido pela estrutura. Uma empresa de consultoria relativamente pequena seria uma boa candidata a esse tipo de modelo.

Não pode haver mais de um nível de domínio dentro do modelo funcional, pois não há base para essa criação. Isso limita o campo de ação desse modelo a pequenas organizações ou empresas com distribuição geográfica limitada.

PRÓS

- Fornece uma plataforma para comunicação participativa devido ao agrupamento de funções semelhantes em UOs.
- É intuitivo para os usuários.

CONTRAS

- Podem ser necessárias UOs de segundo ou terceiro nível para o gerenciamento de recursos da rede.

Revisão

Esta seção apresentou diversos designs diferentes de espaço de nome baseados em modelos diferentes.

- Político
- Geográfico
- Geo-político
- Político-geográfico
- Funcional

Embora cada design tenha as suas próprias características positivas e negativas inerentes, deve-se ter em mente que o design do espaço de nome do Active Directory pode se basear na estrutura organizacional e em regras comerciais e, como tal, pode ser adaptado a vários modelos diferentes.

A situação se complica: considerações para sites

Um *site* é uma ou mais sub-redes IP bem conectadas. Como regra básica, um site pode ser considerado como áreas conectadas usando-se tecnologias de LAN. Os sites só consistem em objetos de servidor e de configuração que são usados para replicação.

Infelizmente, não há uma regra geral para determinar o campo de ação correto dos sites, mas, através da compreensão de como o Active Directory usa as informações dos sites, é possível se tomar uma decisão bem fundamentada sobre como implementá-los da melhor forma. O Active Directory usa sites das quatro formas que se seguem:

- Quando um cliente solicita uma conexão com um controlador de domínio (p. ex.: para logon), o site permite que o cliente se conecte a um controlador de domínio dentro do mesmo site, sempre que possível. Isso reduz a latência e preserva a largura de banda da rede.
- Os sites definem a topologia da replicação para os controladores de domínio que fazem parte desses sites. O Knowledge Consistency Checker (KCC, verificador de consistência do conhecimento) também usa as informações contidas nesse site para adicionar automaticamente outros servidores à topologia da replicação.
- As mensagens de replicação entre controladores de domínio em um site são compactadas e, portanto, usam menos ciclos de CPU nos controladores de domínio. As mensagens de replicação entre controladores de domínio de sites diferentes são compactadas e, portanto, usam menos largura de banda da rede.
- A replicação entre controladores de domínio de um site é acionada pela chegada de atualizações, reduzindo a latência da replicação dentro de um site. A replicação entre controladores de domínio de sites diferentes é executada com base em um cronograma, preservando a largura de banda. A compactação nesses casos pode chegar a 10 para 1.

Os sites não são vinculados de forma alguma ao espaço de nome do Active Directory. O nome de um

objeto de diretório não reflete o site ou sites onde o objeto está armazenado. Um site pode conter controladores de domínio de diversos domínios, e podem existir controladores de domínio de um domínio em diversos sites. (Os sites do Exchange Directory Service são vinculados ao espaço de nome.)

Local do controlador de domínio

Quando um usuário efetua logon, a estação de trabalho vai tentar localizar um controlador de domínio no seu site local. Quando não há controladores de domínio disponíveis no site, a estação de trabalho vai usar outro controlador de domínio da rede.

A proximidade dos controladores de domínio aos clientes da rede terá um impacto evidente durante a autenticação.

Determinando onde colocar os controladores de domínio e catálogos globais

Ao se planejar a colocação de controladores de domínios, leve em consideração ter pelo menos um controlador de domínio por site. A teoria por trás dessa abordagem baseia-se em um modelo de “99% de consulta e 1% de atualização”. Isso significa que 99% do tráfego da rede do Active Directory estará relacionado a consultas à medida que usuários, administradores e aplicativos solicitam informações sobre outros objetos na rede e se autenticam. Atualizações ao diretório, que geram o tráfego de replicação de diretório, vão ocorrer com bem menos frequência.

Ao se colocar um controlador de domínio em cada site, todos os usuários terão um computador local que pode atender a pedidos de consulta sem exigir um tráfego de link de baixa velocidade. Você pode configurar controladores de domínio em sites menores para receber atualizações de diretório somente em horários fora do expediente a fim de otimizar o fluxo do tráfego.

Vamos analisar as seguintes diretrizes para a colocação de controladores de domínio na sua empresa:

- Um controlador de domínio deve poder responder aos pedidos dos clientes de forma oportuna.
- O melhor desempenho de consulta acontece quando você coloca um controlador de domínio (em um site pequeno) com um servidor de catálogo global, permitindo que esse servidor atenda a consultas sobre objetos em todos os domínios da sua rede.

Os servidores de catálogo global são controladores de domínio que também armazenam informações usadas frequentemente de outros domínios. Essa função pode parecer trivial, mas todos os usuários que efetuam logon são processados por um servidor de catálogo global para associação no grupo universal. As seguintes diretrizes devem ser analisadas para a colocação de servidores de catálogo global na sua empresa:

- Um servidor de catálogo global deve poder armazenar todos os objetos de todos os outros domínios da floresta.
- Um servidor de catálogo global deve poder responder às consultas dos clientes e aos pedidos de autenticação de forma oportuna.

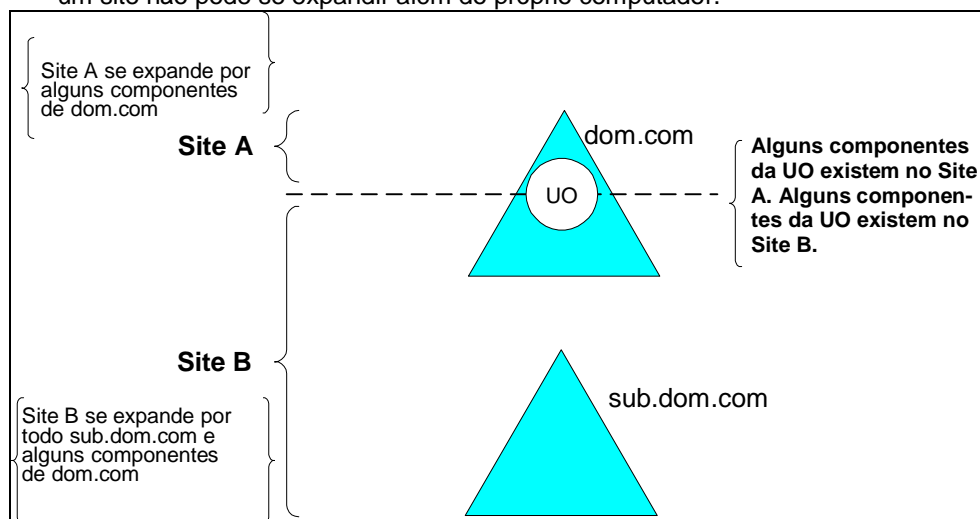
A disponibilidade é a chave da colocação tanto dos controladores de domínio quanto dos servidores de catálogo global. Enquanto um servidor de catálogo global pode estar

localizado em um nível superior da empresa, atendendo a diversos sites, pelo menos um controlador de domínio deve ser colocado em cada local de site. O número de servidores de catálogo global também vai afetar a quantidade de informações replicadas em todo o diretório.

Fronteiras dos sites

Dois conceitos importantes relacionados a sites são:

- Um site pode se expandir por mais de um domínio. Como um site é simplesmente um grupo de objetos que existem em locais físicos, a distribuição lógica dos objetos pode incluir os domínios inteiros ou parciais existentes na definição do site.
- Diversos sites também podem se expandir por domínios e até mesmo unidades organizacionais. Isso é especialmente interessante ao se considerar como as diretivas de grupo vão afetar os objetos dentro de um determinado domínio. A boa notícia é que um site não pode se expandir além do próprio computador.



n Figura 19

Na figura anterior, o Site A é definido de forma a conter somente quase metade dos componentes do domínio dom.com. Contudo, o Site B contém todos os componentes de sub.dom.com, além de alguns objetos do domínio dom.com. Uma observação interessante é que alguns objetos da UO também são divididos entre os sites.

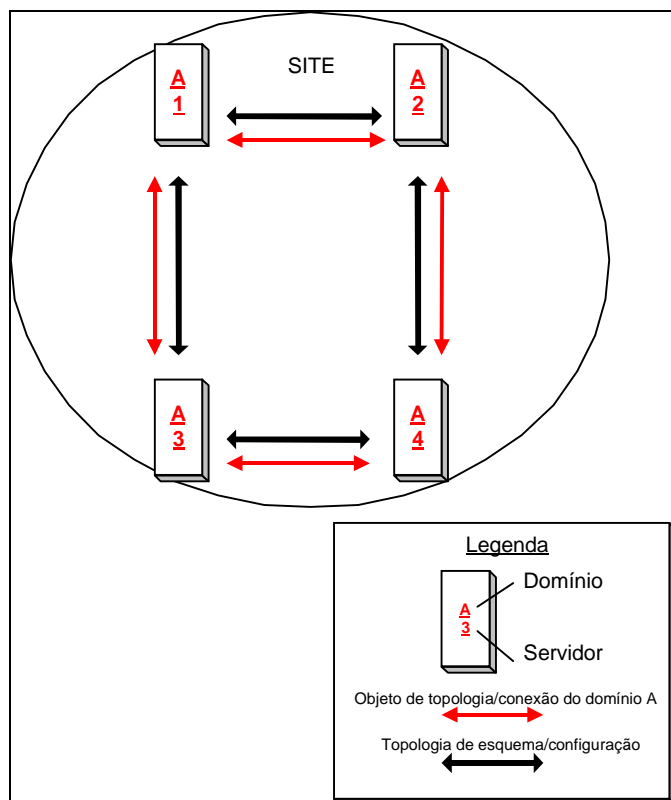
Replicação de site

Para entender bem a replicação dentro de um site, deve-se também entender as partes do diretório que são replicadas. Três itens são replicados em um site:

- Naming Context (NC, contexto de denominação) do domínio
- NC de configuração
- NC de esquema

Os contextos de denominação de configuração e de esquema têm a mesma topologia de replicação em um site, enquanto o contexto de denominação de domínio tem uma topologia separada para cada domínio em um site.

Isso pode parecer confuso, mas na verdade é bastante simples. Cada servidor que se junta a um site se insere automaticamente nas topologias de replicação de configuração/esquema e de domínio. Ao lidar com servidores do mesmo domínio, as topologias de replicação são idênticas.

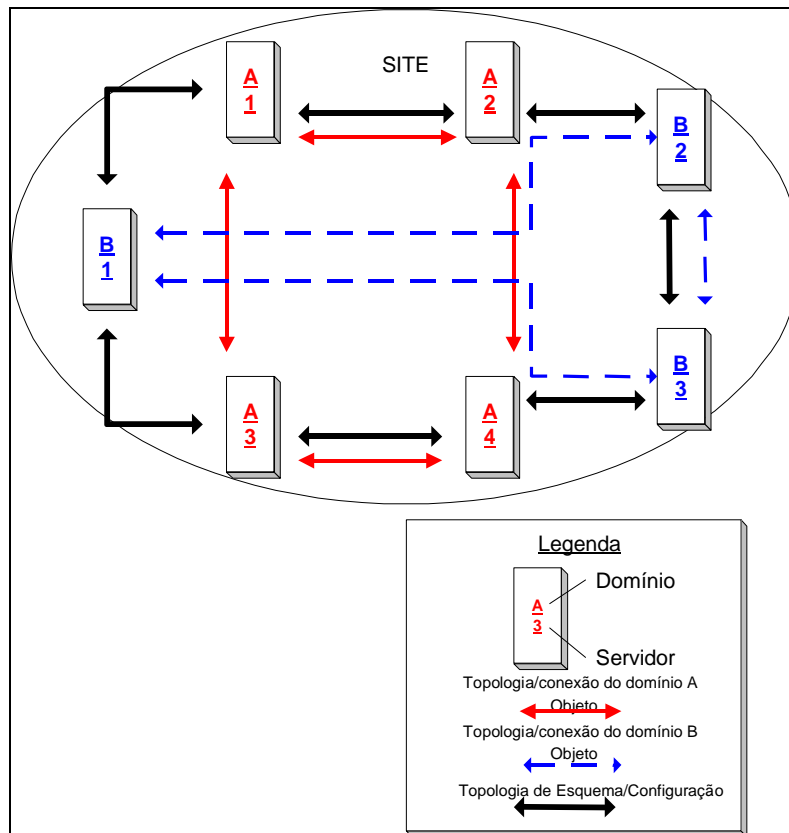


n Figura 20: Replicação de site – domínio único

À medida que cada controlador de domínio é adicionado ao site, a topologia vai se alterar para acomodar o novo membro do site.

Os controladores de domínio separados também vão se inserir nas topologias de replicação, só que de duas formas separadas. A inserção na topologia de configuração/esquema vai ocorrer de forma normal. O servidor também vai se inserir na topologia de contexto de denominação do domínio do site.

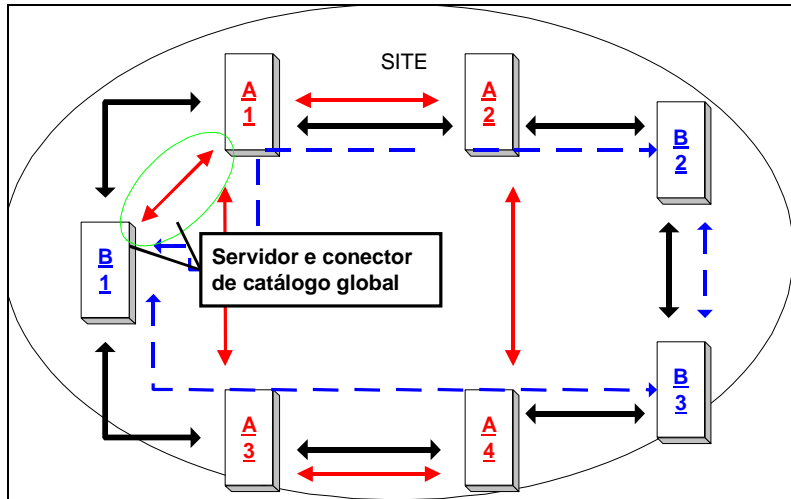
A figura que se segue ilustra um site com dois domínios: A e B. Observe que, à medida que os controladores de domínio são acrescentados à topologia do site, duas topologias distintas são formadas: uma para o contexto de denominação de configuração/esquema e outra para o de domínio.



n Figura 21: Replicação de site – vários domínios

A topologia de configuração/esquema (comum em uma floresta) é replicada em rodízio, independentemente da associação ao domínio, enquanto cada domínio mantém uma topologia distinta.

Surge a dúvida de como um domínio sabe o contexto de denominação de domínio do outro domínio. Isso é feito pelos controladores de domínio que servem como servidores de catálogo global – um catálogo global de cada domínio, replicando com um controlador de outro domínio. Só um conector de replicação de contexto de denominação de domínio é necessário já que o configuração/esquema replicam globalmente.



n Figura 22: Replicação de catálogo global

Nesse caso, o domínio B introduziu um catálogo global no site. Além das suas tarefas de replicação normais, o catálogo global (B1) criou um objeto de conexão com o controlador de domínio A1 do domínio A. O catálogo global vai fornecer uma réplica parcial do NC do Domínio A que será incluída no catálogo global.

À medida que são criados sites adicionais, eles vão constantemente ajustar a topologia de replicação para acomodar novos controladores de domínio. A replicação entre sites é feita usando-se conectores de site, o que é analisado na próxima seção.

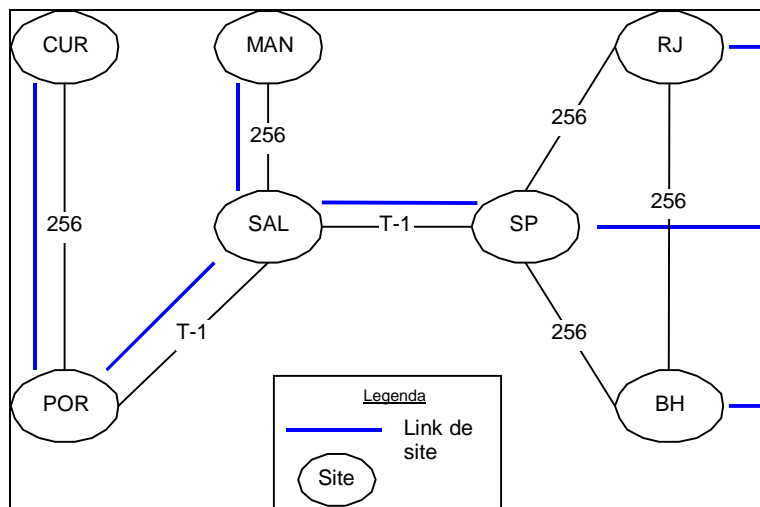
O processo de replicação dentro do site é totalmente automático e sempre usa DS-RPC (Remote Procedure Call) para transmitir alterações de diretório. Ainda assim, é útil ter uma boa compreensão da replicação dentro do site caso seja necessário fazer ajustes manuais à topologia.

Replicação entre sites

Os sites não afetam as informações que serão replicadas, mas apenas a forma como essas informações são replicadas. Geralmente, a replicação entre sites é realizada usando-se DS-RPC em um conector lógico definido por um *link de site*. Opcionalmente, a replicação entre sites pode usar mensagens SMTP desde que esses sites não estejam no mesmo domínio.

Para que a replicação do Active Directory ocorra, os caminhos de replicação entre os sites precisam estar vinculados manualmente, definindo links de site. Um link de site define uma conexão lógica entre dois ou mais sites. Uma vez definidos, os objetos de conexão são configurados automaticamente.

Os links de site pode representar um grupo de conexões semelhantes de rede ou um único link de WAN. Um link de site pode conter vários sites.



n Figura 23: Links de site, sites e rede

No exemplo anterior, os sites SP, BH e RJ estão conectados através de uma rede de links de WAN de 256k. Todos foram incluídos em um único link de site, o que significa que a comunicação entre esses três sites é feita ponto a ponto. Os demais sites foram todos conectados, seguindo o mapeamento da rede e usando links de site separados para cada conexão.

Links de site

Um objeto *link de site* representa um conjunto de sites que podem se comunicar a um custo uniforme através do transporte entre sites. Para transporte IP, um link de site típico conecta apenas dois sites e corresponde a um link de WAN real. Um link de site IP conectando mais de dois sites pode corresponder a um backbone ATM conectando mais de dois clusters de prédios em um campus grande ou diversos escritórios em uma grande área metropolitana conectada através de linhas alugadas e roteadores IP.

Você cria um objeto de link de site para um determinado transporte entre sites (geralmente transporte IP) especificando:

- Um custo para o caminho
- Dois ou mais sites
- O agendamento

O agendamento determina os períodos durante os quais o link está disponível. Isso pode ser útil para se conectar sites que usam conexões de alto custo, como conexões dial-up.

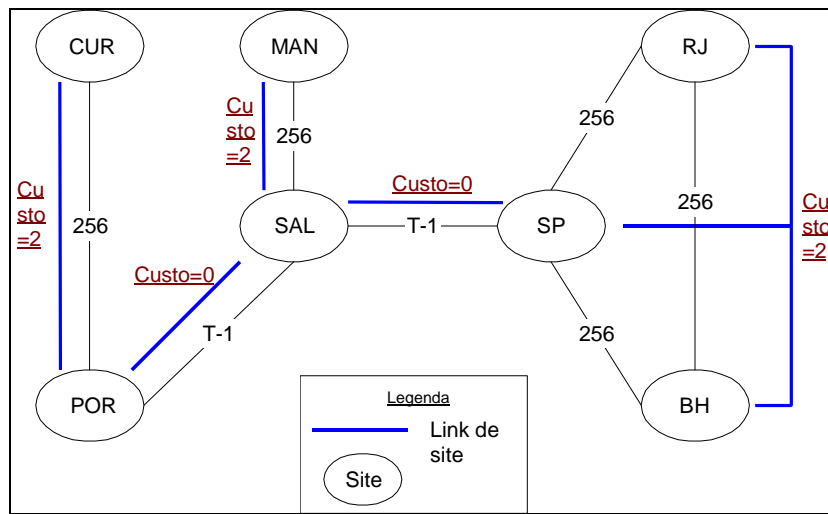
Um site pode ser conectado a outros sites através de um número qualquer de objetos de links de site. Cada site de um diretório de vários sites deve ser conectado por pelo menos um link de site. Caso contrário, ele não pode replicar com controladores de domínio de nenhum outro site e, portanto, o diretório está desconectado. Sendo assim, você deve configurar pelo menos um link de site em um diretório de vários sites.

Custo

Os links de site têm custos numéricos associados, que afetam o roteamento das

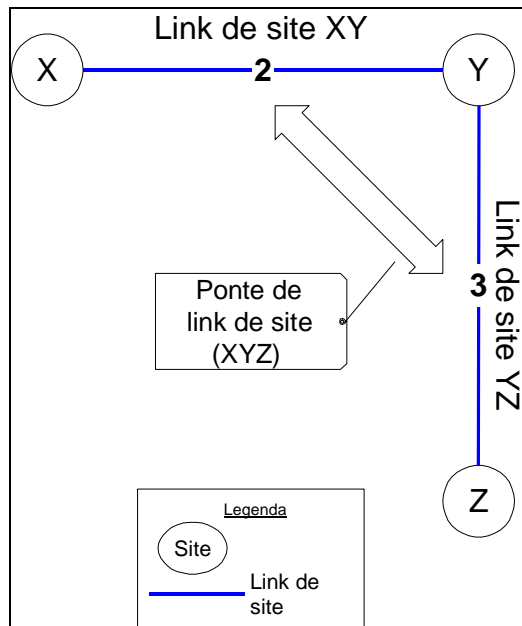
mensagens entre os sites. Os custos são atribuídos automaticamente, mas podem ser alterados manualmente para refletir os atributos dos caminhos percorridos da rede. Normalmente, os custos dos links de site serão associados a velocidades de link de WAN. Números de custo mais altos representam caminhos de mensagem mais onerosos.

Por exemplo, se você criar um objeto de link de site SP-RJ-BH que conecta três sites (São Paulo, Rio de Janeiro e Belo Horizonte) ao custo de 20, você está dizendo que uma mensagem de replicação pode ser enviada entre todos os pares de sites (SP para RJ, SP para BH, RJ para SP, RJ para BH, BH para SP, BH para RJ) ao custo de 20.



n Figura 24: Links de site

Os custos dos links de site têm um impacto no roteamento das mensagens entre os sites. Por exemplo, na figura 16 a seguir, uma mensagem enviada do site POR para BH tomaria a rota menos onerosa, nesse caso POR-SAL-SP-BH cujo custo é dois, embora o site BH esteja bem próximo.

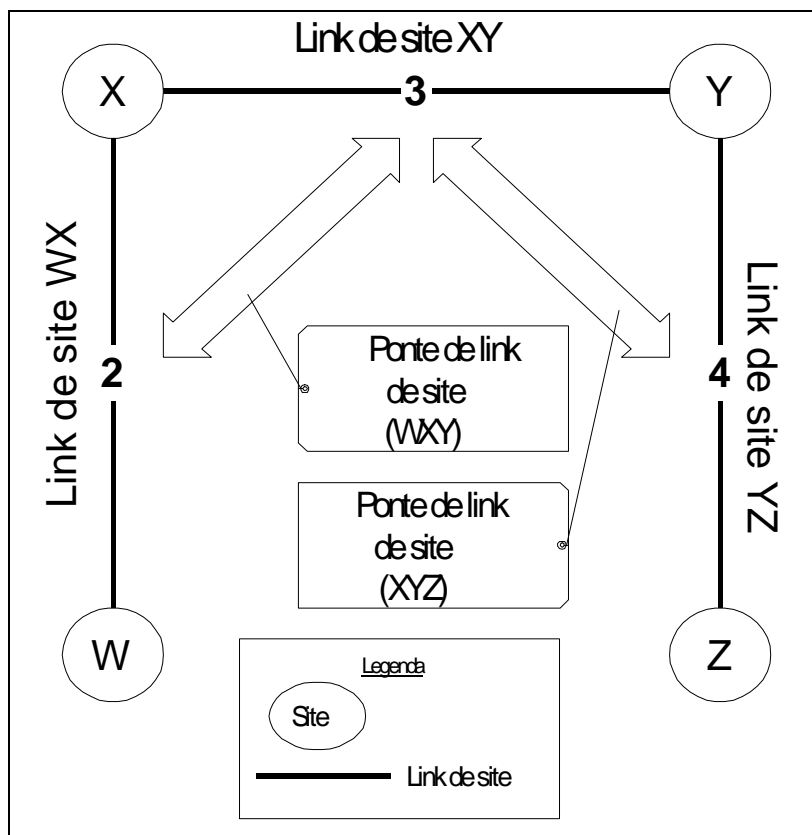


n Figura 26: Ponte de link de site

Cada link de site de uma ponte deve ter um site em comum com outro link de site da ponte. Caso contrário, a ponte não pode calcular o custo dos sites no link L para os sites de outros links da ponte.

As pontes de link de site separadas, até para o mesmo transporte, são independentes. Acrescente os seguintes objetos ao exemplo anterior:

- O link de site WX conecta os sites W e X através de IP a um custo de 2
- A ponte de link de site WXY conecta WX e XY.



n Figura 27: Várias pontes de link de site

A existência dessa ponte adicional significa que uma mensagem IP pode ser enviada de W para Y a um custo de $2+3 = 5$. Mas *não* significa que uma mensagem IP pode ser enviada do site W para o site Z a um custo de $2+3+4 = 9$. Em quase todos os casos, você vai usar uma única ponte de link de site como modelo da rede IP inteira.

Qualquer rede que possa ser descrita através da combinação de links de site e pontes de link de site, também pode ser descrita somente pelos links de site. Ao usar pontes de link de site, a sua descrição da rede torna-se menor e mais fácil de ser mantida, pois você não precisa de um link de site para descrever cada caminho possível entre os pares de sites.

Criação da topologia

Dependendo do nível de controle necessário, as topologias dos sites podem ser inteiramente configuradas, de forma totalmente automática ou totalmente manual.

Se você tiver feito um trabalho adequado ao apreçar os links dos sites, pode simplesmente criar pontes entre todos os sites a partir das configurações de NTDS no nível do site e permitir que o KCC determine a melhor rota para o roteamento das mensagens.

Por outro lado, você pode controlar completamente o processo, desativando a geração de KCC e criando manualmente todas as pontes de link de site. Nesse caso, contudo, o administrador é totalmente responsável pela criação e manutenção de pontes de link de site, o que, em grandes organizações, pode ser uma tarefa monumental.

Pode-se usar também uma mistura de configurações automáticas e manuais. Esse procedimento permite que um administrador influencie a replicação sem ter que configurar toda a topologia manualmente. Esse método permite que o KCC gere automaticamente todas as pontes de link de site que podem então ser modificadas manualmente, conforme necessário.

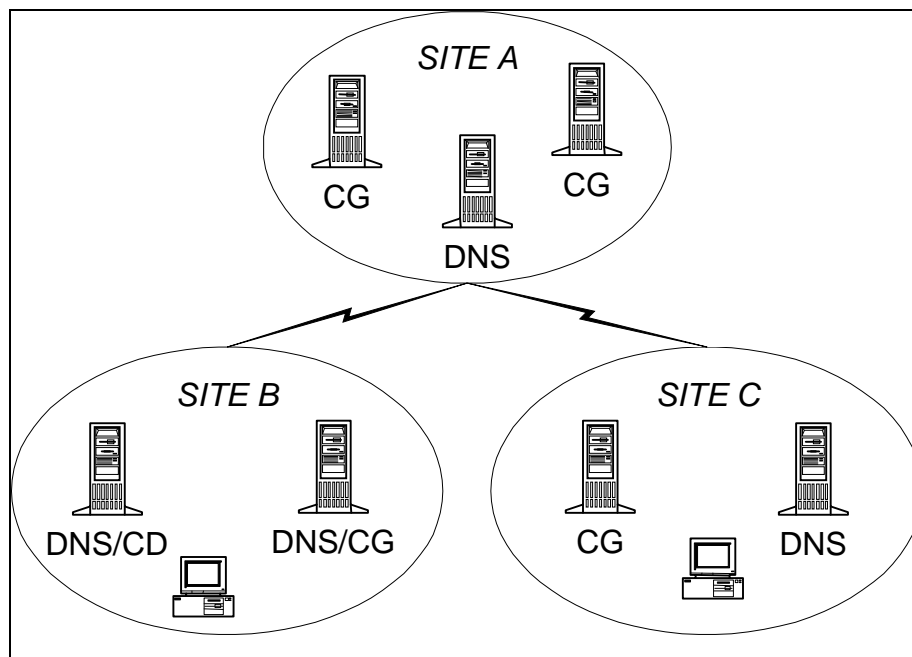
Localizando os serviços

O servidor de catálogo global armazena uma réplica parcial de leitura somente contendo as informações frequentemente acessadas de cada domínio da floresta. Ele também armazena uma réplica de leitura/gravação contendo essas informações do seu próprio domínio. Ainda mais importante, cada objeto que é autenticado no Active Directory deve referenciar o servidor de catálogo global. Isso significa que todos os usuários que efetuarem logon e todos os computadores que forem inicializados devem ser referenciados no catálogo global quanto à associação em grupos universais.

Isso não significa necessariamente que todos os controladores de domínio devem ser identificados como um catálogo global. Embora seja verdade que o catálogo global desempenha um importante papel no processo de autenticação, também é verdade que uma quantidade bem menor de tráfego e processamento da rede está associado com o catálogo global do que a um controlador de domínio. Isso significa que menos catálogos globais podem atender a mais clientes. Na verdade, é o controlador de domínio de autenticação (e não o cliente) que entra em contato com o catálogo global para associação do grupo universal.

Como regra, cada site deve ter pelo menos um servidor de catálogo global. Contudo, se diversos sites estiverem bem conectados através de links de rede confiáveis, os servidores de catálogo global podem atender a mais de um site.

Conforme analisado anteriormente, é absolutamente possível misturar as funções e colocação dos servidores para atingir o resultado desejado de fornecer serviços confiáveis e disponíveis específicos a cada site.



n Figura 28

Site A: Está configurado com dois servidores de catálogo global e um único servidor de DNS. O site A permite excelente disponibilidade do catálogo global. Caso o servidor de DNS não esteja disponível, um servidor de DNS no site B ou no site C pode ser usado.

Site B: Mantém dois servidores que fornecem serviços de DNS. Um dos controladores de domínio também age como um servidor de catálogo global do site. Novamente, os servidores de catálogo global estão disponíveis em outros sites, se o catálogo global local não estiver disponível.

Site C: Contém um único catálogo global e um único controlador de domínio. Caso um deles não esteja disponível, os clientes podem usar os serviços do site A.

Um caso considerado menos favorável seria o uso de um único servidor fornecendo serviços de catálogo global e de DNS. Caso esse servidor não esteja disponível, todos os serviços precisariam ser fornecidos além das fronteiras do site.

De qualquer forma, é essencial que um servidor de DNS e um servidor de catálogo global estejam disponíveis aos clientes de um site. Se um servidor de catálogo global não estiver disponível, o cliente não poderá efetuar login na rede e muitos serviços não vão estar disponíveis.

Campos de ação do site

Os tamanhos reais dos sites vão variar bastante dependendo de:

- O tamanho da organização
- O número de clientes e a sua distribuição física
- A quantidade de dados a serem replicados

Em grandes organizações com centenas de locais, talvez não seja viável criar um site para

cada segmento da rede ou do campus. Nesses casos, será necessário criar para os sites campos de ação com o maior tamanho possível para reduzir o volume necessário de administração e gerenciamento. Os sites desse exemplo podem se expandir por diversos locais físicos conectados através de links de WAN (T-1) confiáveis e rápidos.

Os sites podem ser usados para aumentar o desempenho de logon dos clientes. Se os logons dos clientes estiverem demorando muito devido ao grande número de clientes em um site ou à autenticação de clientes através de links de baixa velocidade, a solução pode ser reduzir o tamanho de um site ou acrescentar outro site.

Determinar o campo de ação dos sites nem sempre é um procedimento simples. Os sites são apenas um grupo definido de sub-redes IP que estão bem conectadas. Contudo, como você vai definir tanto as próprias sub-redes IP quanto as sub-redes que serão incluídas em um site, provavelmente as opções serão muitas.

Em organizações de pequeno porte, as definições dos sites devem ser fáceis e se basear na conectividade de velocidade da LAN. Em situações simples, definir a topologia de replicação também é simples e pode até ser executada pelo KCC.

Nas grandes organizações com diversos locais, definir as fronteiras dos sites será mais difícil devido às diferentes condições de largura de banda dos links da rede, além de se tentar minimizar os custos administrativos indiretos associados à configuração e gerenciamento das conexões entre sites.

Em uma situação onde existem diversos sites, você também vai querer ter uma boa idéia da aparência da topologia de replicação entre sites. A replicação do diretório ocorre dentro de um site e entre sites.

O Active Directory já tem alguns recursos internos que ajudam a reduzir o tráfego da replicação:

- Replicação diferencial: O Active Directory só replica alterações para um objeto e não o objeto em si. Por exemplo, se um número de telefone de um usuário for modificado, somente o número de telefone é replicado, em vez de todas as informações do usuário.
- Replicação agendada: A replicação dentro de um site e entre sites pode ser agendada e configurada. Portanto, a replicação pode ser agendada para os horários de menor uso da rede.
- Compactação: A replicação de RPC entre sites vai usar a compactação. (Isso só se aplica entre domínios diferentes.)
- Campo de ação da replicação: O volume de informações replicadas entre os domínios é menor do que o volume de informações replicadas dentro de um domínio.
- Topologias configuráveis: A ordem em que os servidores e sites replicam pode ser completamente configurada, assim como os horários dessa replicação, permitindo que a replicação (entre sites) seja agendada e que a replicação dentro de um site seja gerenciada.

Em várias situações, as fronteiras dos sites serão baseadas nas fronteiras dos links de rede de 10 megabits ou mais. Isso não significa que as fronteiras dos sites não possam se expandir por links de velocidade mais baixa. O número de variáveis, como largura de banda, topologia da rede, latência da rede e tráfego de cliente e de replicação, impedem a criação de uma expansão máxima para os sites da rede. Como a própria topologia do site é

replicada e como os sites são, na sua maioria, inter-relacionados, deve-se planejar bem a topologia do site e criar esse plano com base em estimativas de tráfego futuro e não atual.

Revisão

Nesta seção, analisamos os sites e a replicação. Especificamente, definimos os sites, links de site e pontes de link de site, e analisamos a replicação entre sites e dentro de um site. Além de entender essas definições, é necessário entender como o Active Directory usa as informações do site. Dessa forma, você pode decidir qual é a melhor forma de implementar sites na sua empresa.

Um site é uma ou mais sub-redes IP bem conectadas. Os links de site fornecem links entre sites e permitem estimar preços e agendar. As pontes de link de site fornecem links transitivos entre os links de site. A replicação é o processo pelo qual as informações do Active Directory são transmitidas através da empresa. Definir um site como um conjunto de sub-redes permite que se configure rápida e facilmente a topologia de acesso e de replicação do Active Directory a fim de aproveitar as vantagens da rede física.

Segurança

Implementar a segurança, quer seja em uma empresa, em um domínio ou em um único computador, significa encontrar um equilíbrio entre forças fundamentalmente opostas — fazer com que as informações estejam facilmente disponíveis ao maior número de usuários e proteger as informações críticas contra acesso não autorizado.

Encontrar o equilíbrio adequado requer um planejamento cuidadoso:

- Avalie o risco e determine o nível adequado de segurança da sua organização.
- Identifique as informações importantes.
- Defina as diretivas de segurança que usam os seus critérios de gerenciamento de risco e proteja as informações identificadas.
- Determine a melhor forma de implementar as diretivas dentro da organização existente.
- Certifique-se de que as exigências de gerenciamento e tecnologia foram atendidas.
- Forneça a todos os usuários acesso eficiente aos recursos adequados, de acordo com as suas necessidades.

O Windows 2000 oferece extraordinários recursos de segurança que devem garantir a flexibilidade necessária para se atender às mais difíceis exigências de segurança. Ao se planejar a segurança do Active Directory, os fundamentos da sua solução de segurança devem se basear em:

- Autenticação
- Diretivas de segurança
- Controle de acesso (direitos e permissões)
- Auditoria
- Privacidade e integridade dos dados

A estrutura de segurança do Windows 2000 foi projetada para atender às mais rígidas exigências de segurança. Contudo, o software em si pode facilmente se tornar ineficiente sem um planejamento e avaliação cuidadosos, diretrizes de segurança eficientes e treinamento do usuário.

Funções do servidor

As considerações de segurança também sofrem a influência da função que um determinado servidor desempenha em uma organização (como um controlador de domínio, servidor da Web, servidor de arquivos ou servidor de bancos de dados).

As implementações de segurança devem ser aplicadas de forma adequada. Isso pode ser facilitado pela definição das funções de um determinado servidor. A seguir estão as funções básicas que podem ser desempenhadas por um servidor:

- Controlador de domínio
- Servidor de arquivos
- Servidor de aplicativos
- Servidor de bancos de dados
- Autoridade certificadora
- Servidor da Web
- Firewall
- Servidor de serviço de acesso remoto e roteamento

Controlador de domínio

Os controladores de domínio gerenciam todos os aspectos das interações dos domínios dos usuários. O Active Directory está localizado em cada controlador de domínio e armazena as credenciais de segurança de todas as contas de domínio, assim como as diretivas e configurações de segurança baseadas em domínios. Devido à confidencialidade das informações armazenadas e devido à sua função crítica na empresa, os servidores que agem como controladores de domínio devem estar associados a medidas de segurança rígidas.

Servidor de arquivos

Os servidores de arquivo armazenam arquivos para acesso por grupos e usuários. O principal objetivo dos servidores de arquivo é garantir a integridade dos arquivos e a disponibilidade dos arquivos aos grupos e usuários adequados.

Definir o nível de segurança que deve ser associado aos servidores de arquivos está diretamente relacionado aos dados que estão sendo armazenados. Os proprietários dos dados ou as diretivas departamentais vão em geral determinar as medidas e normas que devem ser aplicadas ao armazenamento dos dados.

Servidor de aplicativos e de bancos de dados

Os servidores de aplicativos e de bancos de dados executam programas para uso na rede por diversos grupos e usuários. O principal objetivo da segurança para servidores de aplicativos é garantir a disponibilidade dos programas aos grupos e usuários adequados, a integridade do programa ou programas e a integridade dos dados do Registro.

Deve-se atribuir direitos e permissões adequados aos grupos que acessam o servidor. Geralmente, eles serão especificados pela(s) pessoa(s) que administra(m) o aplicativo em

questão.

Em geral, os grupos não precisam modificar os dados dos servidores de aplicativos, e a permissão de Leitura deve ser suficiente na maioria dos casos. Contudo, se os usuários puderem modificar os arquivos de configuração específicos aos programas durante a sessão, eles vão precisar de permissão de Gravação para esses arquivos.

Autoridade certificadora

Ao usar um software para criar uma autoridade certificadora, como o Microsoft Certificate Server, você pode designar um servidor para funcionar como uma autoridade certificadora na sua organização, emitindo certificados digitais para a identificação e autenticação de usuários, assinatura por código ou objetivos personalizados.

Os servidores de certificados serão freqüentemente o alvo pretendido da segurança de nível mais elevado disponível na empresa, pois comprometer a autoridade certificadora pode danificar todos os outros aspectos da segurança de dados.

Servidor da Web

Um software de servidor da Web, como o Microsoft Internet Information Services (IIS), permite que um computador que esteja executando o Windows 2000 Server possa ser host dos dados para acesso à intranet e à extranet e acesso geral à Internet.

A segurança para servidores da Web é aplicada junto com o determinado dado que está sendo servido. No mínimo, um servidor da Web também é um servidor de aplicativos, mas, às vezes, os servidores da Web também oferecem acesso a redes internas e da Internet.

Firewall

Um firewall (como o Microsoft Proxy Server) age como um gateway protegido entre um site (rede interna) e redes externas (intranets, extranets ou a Internet), restringindo a direção e os tipos de pedidos. Os firewalls mais eficientes agem como proxies para serviços específicos. Ou seja, um programa no firewall serve como intermediário entre o site e os serviços que existem para oferecer suporte às operações na rede externa (como navegação na Web). Os programas proxy foram projetados para serem usados com determinados protocolos de comunicação e podem aplicar restrições complexas aos dados. Os firewalls também podem ocultar da rede externa os endereços internos da rede e recusar conexões com determinados endereços externos da rede.

Servidor de acesso remoto e roteamento

Um servidor de acesso remoto fornece acesso remoto aos recursos da empresa. O Routing and Remote Access Service (RRAS, serviço de acesso remoto e roteamento) do Windows 2000 oferece suporte às seguintes funções do servidor:

- Servidor dial-in
- Servidor Virtual Private Network (VPN, rede particular virtual)
- Servidor de roteamento

Um único servidor pode executar todas essas funções, ou determinadas funções podem ser distribuídas entre servidores.

Diretivas de segurança do Active Directory

As diretivas de segurança podem ser aplicadas aos sites, domínios e UOs (nessa ordem). Como é o caso de toda a segurança do Active Directory, a herança é aplicada, como padrão; os direitos aplicados a um domínio também são aplicados às UOs filho desse domínio.

O campo de ação das diretivas de segurança está diretamente relacionado ao espaço de nome do Active Directory — a hierarquia de árvore estruturada de sites, domínios, UOs e usuários/computadores. Em vários casos, isso vai gerar uma única diretiva de segurança ampla que vai existir para um site ou domínio. Cada uma das UOs filho (ou domínios filho) vai ter diretivas de segurança que são um subconjunto das diretivas aplicadas ao pai, com diretivas adicionais atribuídas que são específicas à sua finalidade organizacional ou funcional.

Uma diretiva de segurança está contida em um objeto Diretivas de grupo (ou Group Policy Object). Você pode aplicar diretivas de segurança, atribuindo um objeto Diretivas de grupo a cada domínio e UO. Só um objeto Diretivas de grupo pode ser atribuído por domínio ou UO em um determinado momento.

Direitos e permissões

O acesso aos recursos e/ou objetos é controlado através de permissões e direitos de acesso. Os direitos se aplicam a contas de grupos e de usuários (e aos processos que agem em nome de grupos e de usuários) e autorizam o grupo ou usuário a realizar determinadas operações, como fazer backup de arquivos e diretórios, efetuar logon interativamente ou desligar um computador. Os direitos definem as capacidades no nível do domínio ou no nível do local e podem ser melhor administrados por grupo; um usuário que efetua logon como membro de um grupo herda os direitos associados ao grupo.

As permissões são atributos de segurança dos objetos. Os objetos incluem objetos do sistema de arquivos NTFS (arquivos, pastas ou volumes), objetos do sistema (como processos) e objetos locais ou do Active Directory (como objetos de usuário, grupo ou impressora).

As permissões especificam que usuários ou grupos podem acessar o objeto, bem como que ações eles podem executar nele. Os tipos de permissões que podem ser concedidas variam com o objeto em questão. Os objetos do sistema de arquivos contêm atributos de permissão, como Leitura, Gravação e Execução de uma pasta, enquanto uma fila de impressão tem permissões associadas à concessão da possibilidade de impressão e gerenciamento da impressora e da fila de trabalhos. As permissões atribuídas a um objeto permanecem com o objeto, mesmo que ele seja movido para outro recipiente ou domínio do Active Directory.

Os direitos são aplicados independentemente dos outros objetos, o que significa que um direito pode às vezes sobrepor a uma permissão. Por exemplo, um usuário que é membro do grupo Operadores de backup tem o direito de executar operações de backup em todos os servidores de um domínio. Como esse direito requer a capacidade de ler todos os arquivos desses servidores, o usuário terá acesso aos dados que de outra forma lhe seria

negado através das permissões do objeto. O direito, nesse caso, o direito de executar um backup, prevalece sobre todas as permissões de arquivo e de diretório.

As permissões são acumulativas; uma permissão de nível superior inclui todas as permissões de níveis inferiores, com exceção da permissão Sem acesso, que se sobrepõe às outras. Por exemplo, se o usuário A for membro de dois grupos com permissões a um determinado arquivo, sendo que o Grupo 1 tem permissão de Leitura e o Grupo 2 tem permissão de Alteração, os direitos em vigor para o usuário A nesse arquivo são de Alteração. Contudo, se o usuário A for adicionado ao Grupo 3 assinalado com a permissão Sem acesso, o usuário A não teria acesso ao arquivo, independentemente das permissões concedidas por outros membros do grupo.

O Windows 2000 Server usa um conjunto de permissões padrão para os diretórios e arquivos do NTFS. As permissões padrão podem ser combinações de permissões individuais específicas. As permissões individuais são:

- Controle total
- Modificação
- Leitura e Execução
- Listagem de conteúdo de pasta (para pastas somente)
- Leitura
- Gravação

Herança

Como padrão, cada objeto filho herda as permissões de seu pai. A herança transmite as permissões atribuídas a um objeto e suas propriedades a todos os filhos do objeto. A herança pode ser limitada em qualquer objeto do recipiente.

Ao aplicar a herança à atribuição de direitos e permissões, você pode distribuir em toda a gerência da empresa a administração das contas, diretivas e recursos. O componente administrativo das diretivas de segurança pode equivaler de forma eficiente a um organograma — uma árvore de administradores com um campo de autoridade sucessivamente limitado.

Como padrão, um objeto herda as permissões de seu pai quando ele é criado. Isso facilita a criação e administração de hierarquias lógicas. Contudo, as permissões atribuídas ou modificadas no próprio objeto vão sempre prevalecer em relação às permissões herdadas. Por exemplo, se você acrescentar um arquivo a uma pasta que permite ao grupo de TI a permissão de Alteração e ao grupo de Finanças permissão de Leitura, essas mesmas permissões se aplicam ao arquivo. Você pode alterar as permissões dos arquivos, selecionando e modificando as permissões do grupo de Finanças para Sem acesso. Ao desativar a opção de herdar permissões do pai, as permissões de arquivo não serão afetadas por nenhuma alteração subsequente às permissões atribuídas à pasta pai.

Controle de acesso

O acesso aos recursos e/ou objetos é controlado através de permissões e direitos de acesso. O controle de acesso pode ser aplicado a qualquer objeto do Active Directory. Os

direitos e permissões atribuídos no nível do domínio são distribuídos em todo o domínio pelo Active Directory.

Direitos e permissões

Os direitos se aplicam às contas de grupo e de usuário (e aos processos que agem em nome de grupos e de usuários) e autorizam o grupo ou usuário a realizar determinadas operações, como fazer backup de arquivos e diretórios, efetuar logon interativamente ou desligar um computador. Os direitos definem capacidades no nível do domínio ou no nível local e são melhor administrados por grupos: um usuário que efetua logon como membro de um grupo herda os direitos associados ao grupo.

Os direitos são aplicados independentemente dos outros objetos, o que significa que um direito pode às vezes sobrepor a uma permissão. Por exemplo, um usuário que é membro do grupo Operadores de backup tem o direito de executar operações de backup em todos os servidores de um domínio. Como esse direito requer a capacidade de ler todos os arquivos desses servidores, o usuário terá acesso aos dados que de outra forma lhe seria negado através das permissões do objeto. O direito, nesse caso, o direito de executar um backup, prevalece sobre todas as permissões de arquivo e de diretório.

As permissões são atributos de segurança dos objetos. Os objetos incluem objetos do sistema de arquivos NTFS (arquivos, pastas ou volumes), objetos do sistema e objetos locais ou do Active Directory (como objetos de usuário, grupo ou impressora).

As permissões especificam que usuários ou grupos podem acessar o objeto, bem como que ações eles podem executar nele. Os tipos de permissões que podem ser concedidas variam com o objeto em questão. Os objetos do sistema de arquivos contêm atributos de permissão, como Leitura, Gravação e Execução de uma pasta, enquanto uma fila de impressão tem permissões associadas à concessão da possibilidade de impressão e gerenciamento da impressora e da fila de trabalhos. As permissões atribuídas a um objeto permanecem com o objeto, mesmo que ele seja movido para outro recipiente ou domínio do Active Directory.

Você pode atribuir permissões aos objetos como um todo ou a qualquer atributo desse objeto. Isso permite se aplicar um controle de acesso granular dentro do Active Directory. Isso também pode gerar um esquema administrativo complexo demais que é impossível de se administrar. Ao se planejar o controle de acesso, certifique-se de que os direitos são aplicados de uma forma lógica.

As permissões atribuídas permitem ou rejeitam determinadas ações para um determinado objeto ou suas propriedades. Para os recipientes (como UOs), essas permissões podem ser aplicadas a objetos filho. Isso garante uma gama de opções para se exercer o controle de acesso. É possível controlar não só quem vê um objeto, mas também quem pode ver determinadas propriedades de objeto. As permissões para uma única propriedade representam o nível mais alto de granulosidade que se pode definir.

O Active Directory fornece grande flexibilidade na forma como as permissões são aplicadas. As permissões atribuídas a um recipiente (domínio/UO) podem ser aplicadas a:

- O objeto atual

- O objeto e todos os seus objetos filho
- Somente aos seus objetos filho
- Somente a determinados objetos filho

Herança

As permissões são acumulativas; uma permissão de nível superior inclui todas as permissões de níveis inferiores, com exceção da permissão Sem acesso, que se sobrepõe às outras. Por exemplo, se o usuário A for membro de dois grupos com permissões a um determinado arquivo, sendo que o Grupo 1 tem permissão de Leitura e o Grupo 2 tem permissão de Alteração, os direitos em vigor para o usuário A nesse arquivo são de Alteração. Contudo, se o usuário A for adicionado ao Grupo 3 assinalado com a permissão Sem acesso, o usuário A não teria acesso ao arquivo, independentemente das permissões concedidas por outros membros do grupo.

Como padrão, cada objeto filho herda as permissões de seu pai. A herança transmite as permissões atribuídas a um objeto e suas propriedades a todos os filhos do objeto. A herança pode ser limitada em qualquer objeto do recipiente.

Ao aplicar a herança à atribuição de direitos e permissões, você pode distribuir (em toda a gerência da empresa) a administração das contas, diretivas e recursos.

Como padrão, um objeto herda as permissões de seu pai quando ele é criado. Isso facilita a criação e administração de hierarquias lógicas. Contudo, as permissões atribuídas ou modificadas no próprio objeto vão sempre prevalecer em relação às permissões herdadas. Por exemplo, se você acrescentar um arquivo a uma pasta que permite ao grupo de TI a permissão de Alteração e ao grupo de Finanças permissão de Leitura, essas mesmas permissões se aplicam ao arquivo. Você pode alterar as permissões dos arquivos, selecionando e modificando as permissões do grupo de Finanças para Sem acesso. Ao desativar a opção de herdar permissões da pai, as permissões de arquivo não serão afetadas por nenhuma alteração subsequente às permissões atribuídas à pasta pai.

Administração delegada

A capacidade de delegar administração é um dos recursos chave do Active Directory e tem sido aguardado com ansiedade pelos administradores. A administração delegada permite que se forneça controle administrativo limitado a partes e tarefas do Active Directory. Isso elimina a necessidade de que vários administradores tenham autoridade completa sobre um domínio ou site inteiro. Um gerente que tenha os direitos adequados pode, por sua vez, delegar a administração de um subconjunto de contas e recursos. A forma mais fácil de se usar a delegação é espelhar as responsabilidades administrativas da organização nas diretivas de segurança. Por exemplo, ao se especificar o departamento de contabilidade como um recipiente, é possível atribuir direitos do gerente do departamento relacionados à criação e gerenciamento dos recursos, grupos e usuários de contabilidade.

A delegação pode se aplicar a um recipiente individual ou a uma árvore de recipientes. Os direitos atribuídos são válidos somente para o recipiente ou recipientes designados e permitem que o usuário de confiança:

- Atribua propriedades para um determinado recipiente.

- Crie e exclua determinados tipos de objetos filho do recipiente.
- Atribua propriedades específicas a determinados tipos de objetos filho do recipiente.

As opções para delegação de acesso podem ser assustadoras devido ao enorme número de opções disponíveis.

O administrador pode:

- Delegar o controle de todo o recipiente ou 14 tipos diferentes de objetos que podem ser delegados. Dentro desse recipiente de objetos selecionados que podem ser delegados, existem:
 - a) 16 tipos de permissões gerais.
 - b) 54 permissões de propriedades individuais.
 - c) 88 permissões individuais associadas às permissões de criação e exclusão de sub-objetos.

Existem, portanto, 158 opções de permissões individuais, o que gera milhares de combinações. Embora seja uma boa idéia conhecer os tipos disponíveis de permissões que podem ser delegadas, convém manter as permissões em um nível alto o suficiente para que sejam gerenciáveis.

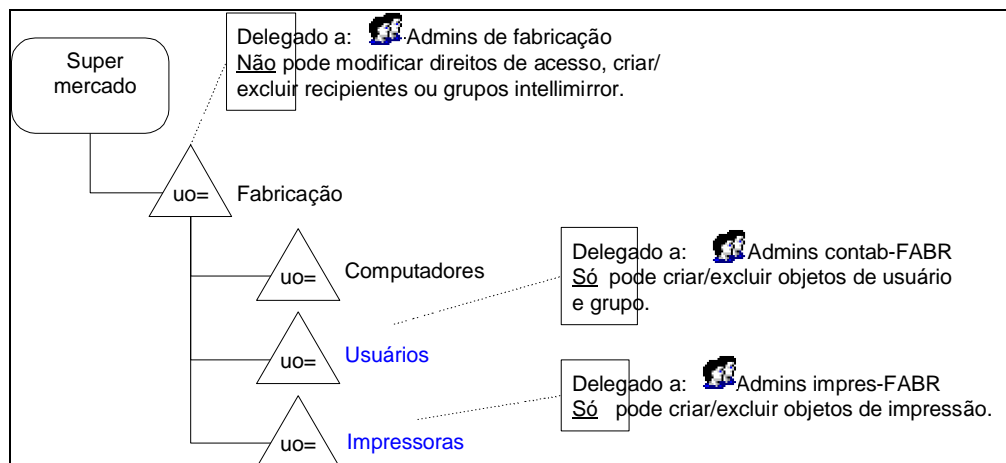
- Delegar recipientes inteiros quando:
 - a) O campo de ação da administração para o grupo delegado envolverá todos os objetos do recipiente.
 - b) Ao se passar a autoridade para uma sub-árvore de um ambiente de TI descentralizado.

Esse tipo de delegação é adequado à delegação de UO departamental.

- Delegar objetos do recipiente parcial quando:
 - c) Ao se atribuir autoridade administrativa baseada em tarefas, como ao se criar administrações de impressora ou de usuário, etc.

A delegação do recipiente parcial adequa-se bem à administração baseada em tarefas.

A figura a seguir ilustra a delegação básica para as duas finalidades. O grupo de administradores de fabricação foi delegado na UO de fabricação e forneceu acesso completo, exceto o reservado aos administradores do nível da raiz. As UOs de usuários e de impressoras só receberam o controle dos seus respectivos objetos (usuários e impressoras).



n Figura 29: Delegação simples

Observe que a entidade administrativa para a UO recebeu acesso completo, exceto as permissões reservadas pelos administradores da empresa, enquanto os administradores baseados em tarefas (usuários e impressoras) receberam explicitamente somente as permissões necessárias para realizar as tarefas designadas. Salvo que se esteja completamente confortável com os impactos da delegação de permissão, convém trabalhar com alguns conceitos básicos durante o planejamento:

- 1) Qualquer permissão que tenha um impacto adverso em unidades adjacentes ou recipientes superiores na hierarquia devem estar restritos à autoridade administrativa superior.
- 2) Nunca se deve delegar autoridade completa a um recipiente (ou seja, permissões de modificação e controle de acesso), exceto se não houver nenhuma autoridade administrativa superior.
- 3) Ao se delegar tarefas, só se deve delegar os objetos e permissões do recipiente necessários à execução do trabalho.

A forma em que as permissões são delegadas também vai variar dependendo do modelo de TI administrativo usado:

Tipo de TI	Método recomendado de delegação de UO
Centralizado	A delegação sempre se baseia em tarefas.
Descentralizado	Todas as permissões são delegadas.
TI distribuído	A delegação de permissões e a criação de recipientes é restrita.

Impacto no design do diretório

A capacidade de realizar delegações administrativas lógicas com base em recipientes é suficiente para justificar um impacto na estrutura da UO para justificar recipientes que podem ser delegados. Contudo, deve-se ter cuidado para não se basear uma estrutura de diretório somente na necessidade administrativa.

Do ponto de vista de se priorizar considerações de design, o peso colocado na facilidade da administração será ajustado depois que determinados objetivos forem alcançados.

É claro que a estrutura do diretório deve poder ser administrada, e até esse momento a administração prevalece. Contudo, assim que esse objetivo for alcançado, a administração deve assumir um papel secundário em relação aos outros objetivos de design, como segurança, otimização da rede, capacidade de adaptação e escalabilidade.

Infra-estrutura da chave pública

As redes não são mais sistemas fechados onde a simples presença do usuário na rede serve como prova de identidade. As redes empresariais podem consistir em intranets, sites da Internet e extranets, e todos esses podem se estender além da rede local.

Há diversos motivos de preocupação quanto ao acesso aos dados. Muitas transações comerciais são realizadas através da rede. E muitos funcionários podem não ser permanentes. Ou a empresa pode trabalhar com parceiros em projetos de abrangência e duração limitados, com funcionários sobre os quais nada se sabe.

Em outras palavras, verificar a identidade de um usuário tornou-se uma tarefa difícil nos últimos anos, enquanto as relações comerciais (entre as empresas e entre as empresas e seus funcionários) tornaram-se mais transitórias. Uma infra-estrutura de chave pública pode fornecer mecanismos para solucionar esses problemas, apresentando certificados de confiança que podem verificar a autenticidade.

Dependendo das necessidades da empresa, uma infra-estrutura de chave pública pode incluir:

- Uma diretiva abrangente determinando como os certificados e chaves devem ser usados.
- Os certificados podem ser usados por programas clientes somente nas intranets por todos os funcionários ou por funcionários específicos. Eles podem ser usados para contas associadas a empresas de parceiros nas extranets ou para contas de acesso limitado na Internet. E os certificados podem ser usados para procedimentos de logon com smartcards.
- Diretivas de gerenciamento de confiança para cada autoridade certificadora (AC).
- A empresa pode precisar de uma AC para emitir certificados para autenticação de contas padrão ou para segurança de correio eletrônico. Nesse caso, convém escolher uma AC de confiança para essa finalidade. Contudo, se a organização tiver várias funções de certificado, como assinatura por código, autenticação, correio eletrônico e acesso à extranet/Internet, deve-se considerar a atribuição de uma AC de confiança a cada função.
- Regras de emissão e de validação para cada AC.
- As regras de emissão e de validação especificam para quem e em que condições uma AC pode emitir um certificado. Uma única AC que está emitindo certificados para autenticação ou uso de correio eletrônico pode emitir certificados para todos os funcionários ou para funcionários específicos. Diversas ACs emitiriam certificados somente para usuários que possam ser validados de acordo com a base funcional da AC, como um membro do grupo de desenvolvimento para uma AC de assinatura por código.
- Disponibilidade das ACs em uma cadeia de certificados de AC.
- Quando um certificado de AC é validado por outra AC, os certificados para as duas ACs devem estar disponíveis para o cliente. Quando as cadeias de AC se tornam muito longas, pode ser difícil garantir a disponibilidade dos certificados de todas as ACs. A infra-estrutura da chave pública deve lidar com essas possíveis situações.

- Diretivas de revocação de certificados.
- Devem ser criadas diretivas para revocação de um certificado que não se aplica mais ou que foi mal usado. Por exemplo, convém revogar um certificado que foi emitido para um funcionário que não está mais na organização.
- Diretivas de renovação de certificados.
- Na expiração, em vez de exigir um novo certificado, convém renovar o certificado já existente. As diretivas devem abordar quando, como e se isso pode ocorrer.

O Microsoft Windows 2000 introduz uma Public Key Infrastructure (PKI, infra-estrutura de chave pública) abrangente na plataforma do Windows. Isso maximiza e amplia os serviços de criptografia de Public Key (PK, chave pública) do Windows, introduzidos durante os últimos anos, fornecendo um conjunto integrado de serviços e ferramentas administrativas para a criação, implantação e gerenciamento de aplicativos baseados em chaves públicas. Isso permite que os desenvolvedores de aplicativos aproveitem os mecanismos de segurança secreta compartilhada do Windows 2000 Server ou o mecanismo de segurança baseado em chaves públicas, conforme adequado. Ao mesmo tempo, as empresas têm a vantagem de poder gerenciar o ambiente e os aplicativos com base em ferramentas consistentes e mecanismos de diretivas.

Propriedades de segurança

As propriedades de segurança descrevem os atributos fornecidos através dos protocolos de chave pública e de segurança IP. Esses atributos incluem itens como autenticação, integridade dos dados e confidencialidade.

O Windows 2000 inclui um sistema de gerenciamento de chaves totalmente funcional que é realizado pelo Microsoft Certificate Server. Os certificados do Windows 2000 se integram ao Active Directory para permitir a publicação e processamento automáticos dos pedidos de certificado.

A segurança PKI e IP protege os dados particulares em um ambiente público. Os administradores e usuários do sistema precisam que os seus dados estejam protegidos contra interceptação, modificação ou acesso por indivíduos não autorizados, e os certificados garantem essa segurança.

Autenticação: Determina a identidade real do outro host. Sem uma autenticação forte, qualquer dado e o host que envia o dado são suspeitos. É possível selecionar o método de autenticação que será usado na comunicação.

Integridade: Protege os dados contra modificação não autorizada em trânsito, garantindo que os dados recebidos estejam exatamente como eram quando foram enviados. É possível selecionar que algoritmo será usado para os serviços de integridade.

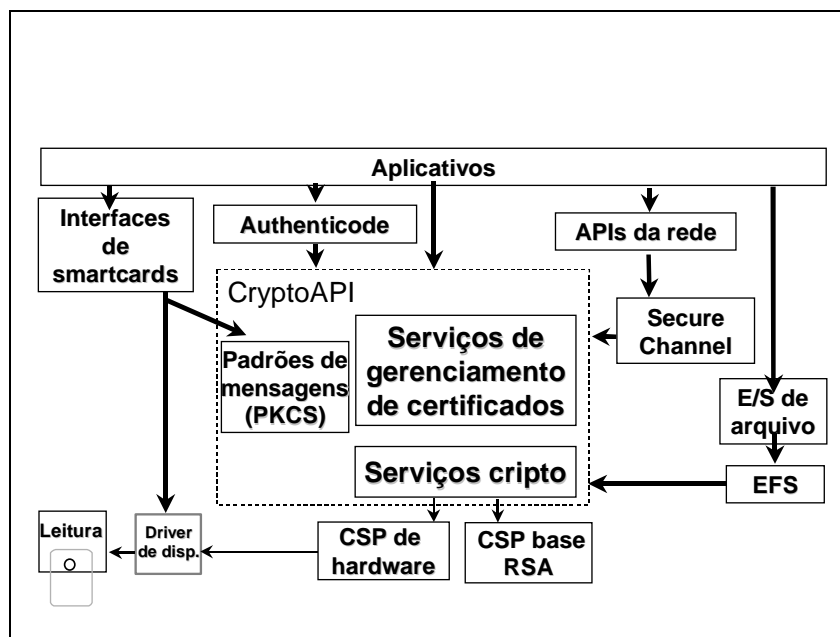
Confidencialidade: Garante que os dados só sejam mostrados aos recipientes desejados, ao criptografar os dados antes da transmissão. Essa propriedade pode ser configurada para atender a restrições de exportação, que colocam limites nos tamanhos das chaves.

Anti-reprodução ou prevenção contra reprodução: Garante que cada pacote IP seja diferente. Isso protege contra ataques durante os quais uma tentativa é feita de se interceptar uma mensagem a ser usada posteriormente para recursos de acesso inválido.

Impossibilidade de repúdio: Protege os dados contra a desautorização pela fonte. Em outras palavras, um remetente não pode negar que ele era a fonte dos dados gerando uma fonte de dados duvidosa.

Componentes de segurança da chave pública

O suporte para a criação, implantação e gerenciamento de aplicativos baseados em chaves públicas é fornecido uniformemente nas estações de trabalho e servidores de aplicativos do Windows NT e 2000, assim como nas estações de trabalho do Windows 95 e 98. A figura mostrada a seguir fornece uma visão geral desses serviços de aplicativos. O Microsoft CryptoAPI é a base desses serviços. Ele fornece uma interface padrão para a funcionalidade criptográfica fornecida por Cryptographic Service Providers (CSPs, provedores de serviço de criptografia) instaláveis. Esses CSPs podem ser baseados em software ou aproveitar os dispositivos de hardware de criptografia e oferecem suporte a diversos algoritmos e chaves. Conforme indicado na figura, um possível CSP baseado em hardware oferece suporte a smartcards.



n Figura 30

Um conjunto de serviços de certificados está colocado em camadas nos serviços de criptografia. Esses serviços oferecem suporte aos certificados padrão X.509v3, garantindo um armazenamento persistente, serviços de enumeração e suporte de decodificação. Por fim, existem os serviços que lidam com formatos de mensagens de padrão industrial.

Outros serviços aproveitam as vantagens do CryptoAPI para fornecer funcionalidade adicional aos desenvolvedores de aplicativos. O Secure Channel (schannel) oferece suporte à autenticação e criptografia usando protocolos TLS e SSL de padrão industrial. Eles podem ser acessados usando-se a interface WinInet da Microsoft para uso com o protocolo HTTP (HTTPS) e usado com outros protocolos através da interface SSPI. O

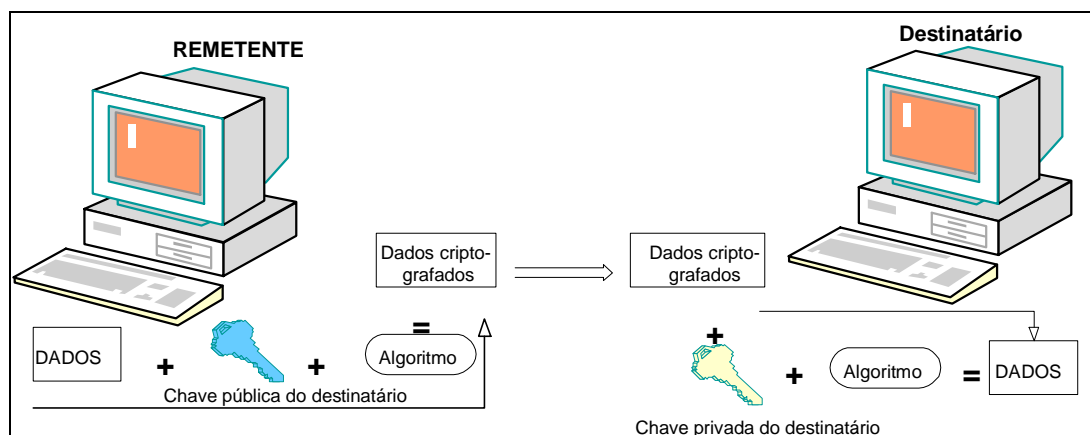
Authenticode oferece suporte à assinatura e verificação de objetos. Isso tem sido usado principalmente para determinar a origem e integridade dos componentes descarregados da Internet, embora possa ser usado em outros ambientes. Por fim, há suporte para interfaces de smartcards de finalidade geral. Essas têm sido usadas para integrar smartcards de criptografia em um aplicativo independentemente da forma e são a base do suporte de logon da smartcard integrado ao Windows 2000.

Criptografia e chaves públicas

A criptografia é a ciência da proteção dos dados. Os algoritmos de criptografia combinam matematicamente dados sem formatação de entrada e uma chave de criptografia a fim de gerar dados criptografados denominados texto cifrado.

Na criptografia tradicional de chave secreta, as chaves de criptografia e descryptografia são idênticas e, portanto, têm os mesmos dados confidenciais. Os indivíduos que desejam se comunicar através da criptografia de chave secreta devem trocar em segurança as suas chaves de criptografia e descryptografia para que possam trocar dados criptografados.

Em oposição, a propriedade fundamental da criptografia de chave pública é que as chaves de criptografia e descryptografia são diferentes. A criptografia que usa uma chave de criptografia pública é uma função de “mão única”; o texto sem formatação se transforma em texto cifrado facilmente, mas a chave de criptografia é irrelevante ao processo de descryptografia. Uma chave de descryptografia diferente (relacionada, mas não idêntica à chave de criptografia) é necessária para transformar o texto cifrado de volta em texto sem formatação. Portanto, para a criptografia de chave pública, cada usuário tem um par de chaves que consistem em uma chave pública e uma chave privada. Ao disponibilizar a chave pública, é possível que outros enviem dados criptografados para o proprietário da chave que só podem ser descryptografados com a chave privada. Da mesma forma, um usuário pode transformar dados usando a chave privada de forma que outros usuários possam verificar que ela se originou com o proprietário da chave privada. Essa última capacidade é a base das assinaturas digitais analisadas em seguida.



n Figura 31

A figura anterior ilustra o fluxo de dados usando a criptografia de chave pública. Se o

remetente nesse caso desejasse enviar dados ao computador destinatário usando uma chave secreta, por exemplo, tanto o remetente quanto o destinatário gerariam metade da chave secreta. O remetente obteria a chave pública do destinatário para criptografar metade da chave secreta e a enviaria ao destinatário. O remetente e o destinatário juntariam as metades da chave secreta para gerar a chave secreta compartilhada a ser usada na criptografia dos dados a serem enviados. Essa negociação de chave secreta e o uso da chave secreta para criptografar dados garantem autenticidade, integridade e confidencialidade.

Certificados

Os certificados garantem um mecanismo para obter confiança na relação entre uma chave pública e a entidade que detém a chave privada correspondente. Um certificado é um determinado tipo de declaração assinada digitalmente; o assunto do certificado é uma determinada chave pública de assunto e o certificado é assinado pelo seu emissor (que detém outro par de chaves particulares de públicas).



n Figura 32

Geralmente, os certificados também contêm outras informações relacionadas à chave pública de assunto, como informações de identidade sobre a entidade que tem acesso à chave privada correspondente. Portanto, ao emitir um certificado, o emissor está atestando a validade da junção entre a chave pública de assunto e as informações de identificação do assunto.

Serviços de certificado

O Microsoft Certificate Server, incluído no Windows 2000, fornece serviços personalizáveis para emissão e gerenciamento de certificados para aplicativos que usam a criptografia de

chave pública. O Certificate Server tem uma função central no gerenciamento desse sistema a fim de fornecer uma comunicação segura na Internet, nas intranets corporativas e em outras redes não protegidas. O Microsoft Certificate Server pode ser personalizado para atender às exigências de aplicativos de diferentes organizações.

A função dos serviços de certificado é criar uma autoridade certificadora (AC) com a finalidade de receber um pedido de certificado no formato PKCS #10, verificar as informações do pedido e emitir um certificado X.509 correspondente no formato PKCS #7. O módulo de diretivas do Certificate Server usa a autenticação de pedidos de certificado da rede para emitir certificados para usuários de contas de domínio do Windows 2000. O módulo de diretivas pode ser personalizado para atender às necessidades da organização emissora. O Certificate Server gera certificados em um formato X.509 padrão.

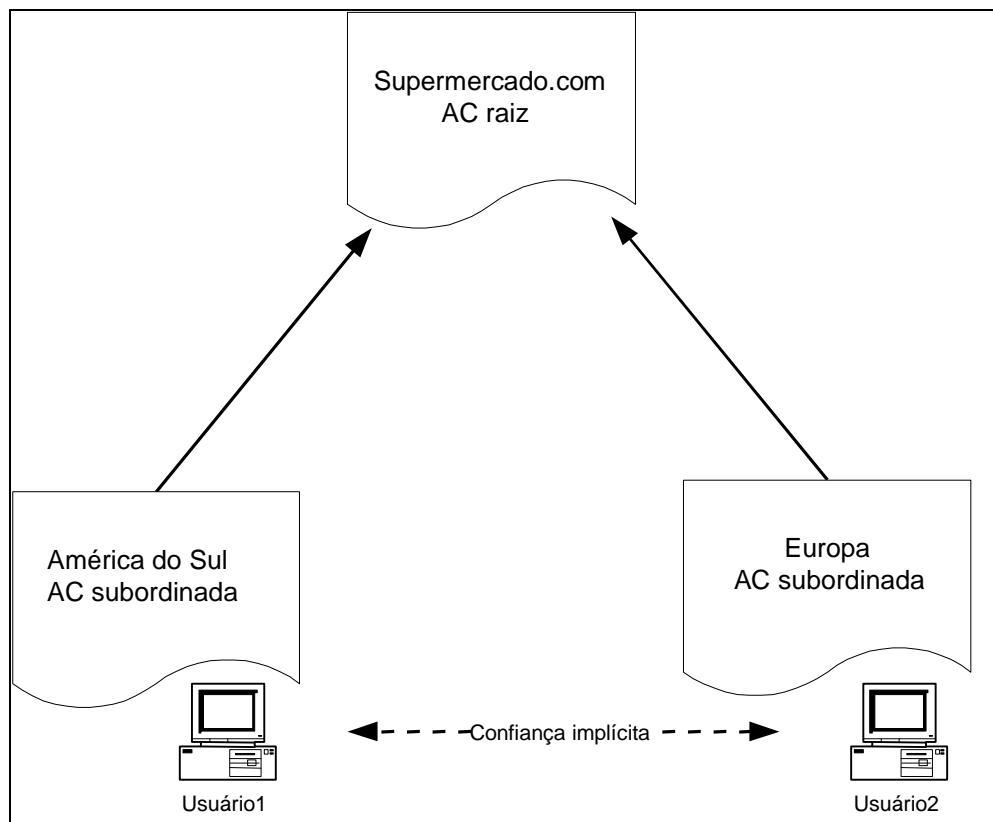
O Certificate Server recebe pedidos de novos certificados através de transportes como RPC, HTTP ou correio eletrônico. Ele verifica cada pedido em relação às diretivas personalizadas ou específicas ao site, define as propriedades opcionais do certificado a ser emitido e emite o certificado. Ele também permite que os administradores acrescentem elementos a uma Certificate Revocation List (CRL, lista de revogação de certificados) e publiquem freqüentemente uma CRL assinada. Para solicitar um certificado, um usuário pode usar o snap-in do Gerenciador de certificados ou o Internet Explorer. Um Cryptographic Service Provider (CSP, provedor de serviços criptográficos) localizado no computador gera um par de chaves pública e privada para o usuário. A chave pública do usuário é enviada com as informações necessárias de identificação para a AC. Se as informações de identificação do usuário atenderem aos critérios da AC para concessão de um pedido, a AC gera o certificado, que é recuperado pelo aplicativo do cliente (Gerenciador de certificados ou Internet Explorer) e armazenado localmente.

Os serviços de certificado oferecem suporte a Secure/Multipurpose Internet Mail Extensions (S/MIME, extensões de correio eletrônico da Internet de várias finalidades/seguras), pagamento seguro, como Secure Electronic Extensions (SET, extensões eletrônicas seguras) e assinaturas digitais. A sua organização pode preferir emitir todos os certificados a partir de uma única AC ou usar diversas ACs que estão conectadas em uma *hierarquia* de ACs.

Planejando autoridades certificadoras

Uma autoridade certificadora (AC) é simplesmente uma entidade ou serviço que emite certificados. Uma AC age como abonador da vinculação entre a chave pública e as informações de identificação contidas nos certificados que emite. ACs diferentes podem ser vinculadas para formar uma confiança hierárquica de autoridades conhecida como hierarquia de ACs.

Uma implementação comum no Windows 2000 é a criação de uma hierarquia de certificados da empresa para distribuir a administração e a carga. Isso não tem nenhuma relação com a hierarquia de domínios, embora as confianças de ACs geralmente coincidam com as confianças Kerberos. Uma hierarquia de autoridades certificadoras estabelece uma confiança transitiva de certificados emitidos.



n Figura 33

Por exemplo, como a América do Sul e a Europa confiam na AC raiz Supermercado, elas também vão confiar mutuamente nos seus certificados.

Dentro de grandes organizações que são compostas de diversas unidades pequenas, é comum a necessidade de cada unidade gerenciar os seus próprios recursos na intranet corporativa. Cada unidade deve implementar as diretivas segundo as quais os solicitantes obtêm aprovação para acessar os recursos da intranet.

Você pode dar a essas unidades a capacidade de estabelecer diretivas e emitir certificados por si próprias, permitindo que elas instalem serviços de certificado e criem a sua própria autoridade certificadora (AC). Você deve monitorar cuidadosamente a proliferação de diversas ACs dentro de uma intranet para que a autoridade não seja mal empregada.

Nas empresas grandes, podem existir várias camadas de ACs e, portanto, a hierarquia pode ser implantada em todas as unidades da organização pai. O uso de uma hierarquia de ACs dá às organizações grandes a flexibilidade necessária para o gerenciamento de diretivas e a concessão de certificados em todo o sistema de certificação composto de diversas autoridades certificadoras e gerenciado a partir de um único ponto central.

IPSec

O Microsoft Windows 2000 Server inclui uma implementação da Internet Protocol Security (IPSec, segurança do protocolo da Internet), baseada nos padrões IETF para IPSec. A implementação da segurança IP no Windows 2000 foi criada para proteger as

comunicações ponta-a-ponta entre hosts. Supõe-se que o que está entre eles, o meio usado para a transmissão de dados, não é seguro.

Os dados do aplicativo do host que está iniciando a comunicação são criptografados de forma transparente antes de serem enviados através da rede. No host de destino, os dados são descriptografados de forma transparente antes de serem passados para o aplicativo receptor. Criptografar todo o tráfego da rede IP garante que qualquer comunicação que use o TCP/IP esteja protegida contra escutas. Como os dados são transmitidos e criptografados no nível do protocolo IP, não são necessários pacotes de segurança distintos para cada protocolo do stack TCP/IP.

Geralmente, um nível alto de segurança aumenta a administração. O Windows 2000 fornece uma interface administrativa, o IP Security Policy Management, para gerenciar de forma centralizada as diretivas, equilibrando facilidade de uso e segurança. As diretivas de IPSec podem ser facilmente configuradas para atender às exigências de segurança de um usuário, grupo, aplicativo, domínio, site ou empresa global. As diretivas se baseiam em metodologias críticas de filtragem de IP, deixando que você permita ou bloqueie as comunicações em um nível alto (sub-redes inteiras) ou em um nível granular (protocolos específicos em portas específicas), conforme julgado necessário.

O IPSec pode fornecer um nível alto de proteção devido à sua implementação no nível de transporte IP (camada 3 da rede). A segurança da camada 3 fornece proteção para todos os protocolos de camadas superiores e IP do conjunto de protocolos TCP/IP (TCP, UDP, ICMP, Raw [protocolo 255] e até mesmo protocolos personalizados). Aplicativos que usam TCP/IP transmitem os dados para a camada do protocolo IP, onde os dados são protegidos pela IPSec.

Os mecanismos de segurança que funcionam acima da camada 3, por exemplo o Secure Sockets Layer (SSL, camada de soquetes de seguros), só protegem aplicativos que usam o SSL, como navegadores da Web. Os mecanismos de segurança que funcionam abaixo da camada 3, por exemplo criptografia da camada de link, não são portáteis para comunicação pela Internet ou intranet encaminhada.

Ao funcionar na camada 3, a IPSec é transparente para usuários e aplicativos. Você não precisa de pacotes de segurança distintos para cada protocolo do conjunto TCP/IP. Assim que as diretivas estiverem configuradas, os usuários não vão precisar agir para proteger os dados.

Diretivas da segurança IP

O recurso IPSec é implantado através das diretivas do Windows 2000. Diversas diretivas de segurança podem existir para um determinado domínio, mas os componentes das diretivas são constantes.

Diretivas de negociação: As diretivas de negociação determinam os serviços de segurança usados durante uma comunicação. Você pode escolher entre serviços que incluem confidencialidade (ESP) ou que não fornecem confidencialidade (AH), ou o algoritmo de segurança IP pode ser especificado. Também é possível se definir diversos métodos de segurança para cada diretiva de negociação. Se o primeiro método não for aceito para a associação de segurança, o serviço ISAKMP/Oakley vai prosseguir na lista

até encontrar um método que possa ser usado para estabelecer a associação.

Diretivas de segurança: Cada configuração dos atributos da segurança IP é chamada de diretiva de segurança. As diretivas de segurança são compostas de diretivas de negociação e filtros IP associados. As diretivas de segurança são associadas às diretivas do controlador de domínio. Uma diretiva de segurança IP pode ser atribuída às Diretivas de domínio padrão, Diretivas locais padrão ou diretivas de domínio personalizadas criadas por você. Um computador que efetua logon no domínio vai aproveitar automaticamente as propriedades das diretivas de domínio padrão e locais padrão, incluindo as diretivas de segurança IP atribuídas a essas diretivas de domínio.

Filtros IP: Os filtros IP determinam ações diferentes a serem tomadas com base no local de destino de um pacote de IP, no protocolo IP que está sendo usado (por exemplo, TCP ou UDP) e nas portas relacionadas que são usadas pelo protocolo. O próprio filtro é usado como um padrão para correspondência de pacotes IP. Cada pacote IP é verificado em relação ao filtro IP e, se houver uma correspondência, as propriedades das diretivas de segurança associadas são usadas para enviar a comunicação.

Opções de segurança IP

Parte das diretivas de negociação de IPSec determina a função a ser desempenhada por um computador durante a comunicação. Três modos básicos de funcionamento podem ser atribuídos a um computador:

- **Respondedor:** Um respondedor vai se comunicar através de IPSec, quando solicitado. Isso pode resultar do fato de um respondedor iniciar uma sessão de comunicação com um computador que esteja funcionando no modo de iniciador ou de bloqueio ou de ser solicitado por um iniciador.
- **Iniciador:** Como padrão, um iniciador vai se comunicar através de IPSec. Se o computador de destino não oferecer suporte a comunicações seguras, um iniciador vai responder e se comunicar sem proteção.
- **Bloqueio:** Um computador no modo de bloqueio só vai se comunicar através de IPSec.

As diretivas básicas podem ser aprimoradas com filtros para fornecer aplicação granular das diretivas. Por exemplo, os computadores de um determinado departamento podem ter diversas diretivas de negociação dependendo do endereço IP do computador com o qual está estabelecendo uma comunicação.

Os usuários experientes podem decidir que algoritmo HMAC será usado para garantir a integridade. HMAC-MD5 e HMAC-SHA fornecem o mesmo nível de proteção, com a diferença sendo o tamanho da chave usada para proteger as informações: MD5 usa uma chave de 128 bits e SHA, uma chave de 160 bits. Chaves mais compridas oferecem mais segurança.

Os usuários experientes também podem decidir que algoritmo será usado em serviços de confidencialidade. A confidencialidade é garantida usando-se o Digital Encryption Standard (DES, padrão de criptografia digital). 40DES é oferecido para garantir a compatibilidade com normas de exportação, que limitam o tamanho das chaves. 3DES, também chamado de DES triplo, oferece o tamanho padrão de chave de 56 bits ao passar três vezes pelo processo de criptografia. Em cada passagem, ele usa uma nova chave exclusiva, gerando

a criptografia tripla das informações. Cipher Block Chaining (CBC, encadeamento de bloco cifrado) com DES (DES-CBC) também fornece um tamanho de chave de 56 bits e evita reprodução adicional.

Protocolos de segurança

Os protocolos de segurança oferecem serviços de proteção de dados e identidade (endereçamento). Os usuários experientes podem selecionar o protocolo que será usado em uma comunicação:

Authentication Header (AH, cabeçalho de autenticação) fornece proteção de identidade, com serviços de autenticação, integridade e anti-reprodução. Proteção de identidade significa que somente as informações de endereçamento são criptografadas e não os dados. Contudo, já que a integridade é fornecida, os dados não podem ser modificados, embora possam ser lidos (AH não oferece confidencialidade). O Authentication Header (AH) do IP pode não oferece a impossibilidade de repúdio se usado com determinados algoritmos de autenticação.

Encapsulated Security Protocol (ESP, protocolo de segurança encapsulado) ESP é um mecanismo para fornecer integridade e confidencialidade aos datagramas IP. Também pode fornecer autenticação, dependendo do algoritmo e do modo de algoritmo que são usados. O ESP não fornece a impossibilidade de repúdio e proteção contra análise do tráfego. O Authentication Header (AH) do IP pode fornecer não repúdio se usado com determinados algoritmos de autenticação.

O Authentication Header do IP pode ser usado junto com o ESP para fornecer autenticação.

Planejando as diretivas de PKI e IPSec

O gerenciamento e a administração de IPSec estão integrados à interface de gerenciamento base do Active Directory.

Nos domínios do Windows 2000, a autenticação pode ser obtida através do protocolo Kerberos predefinido. Portanto, as infra-estruturas dos certificados não precisam ser implantadas para proteger clientes, servidores de arquivos ou UOs de segurança (um grupo de computadores em uma unidade organizacional [UO] do Active Directory com a finalidade de segurança).

Em situações de acesso remoto/VPN/roteador a roteador, os certificados de chave pública devem ser usados para autenticação (ou chaves pré-compartilhadas, no caso de roteador a roteador).

Em geral, as comunicações pela Intranet requerem níveis inferiores de segurança do que as comunicações de rede pública: sem confidencialidade; sem encapsulamento; permissão de comunicações não seguras. Isso vai acelerar a taxa de transferência das comunicações, permitindo ainda algum nível de segurança: integridade e autenticação.

As comunicações IPSec podem ser acionadas, aceitas ou impostas entre qualquer conjunto de computadores ou individualmente. Se os dados forem muito confidenciais, é fácil forçar um computador a aceitar somente comunicações de IPSec.

Em geral, já que o encapsulamento é adequado a níveis altos de segurança, as regras de IPSec que especificam o encapsulamento também devem ter um alto nível de segurança nas diretivas de negociação. Os dados vão estar trafegando, na verdade, em uma rede pública e, portanto, a confidencialidade (ESP) é em geral garantida. Como os pacotes são encapsulados, o que protege o cabeçalho inicial, não é necessário se associar ESP a AH para obter proteção de endereçamento (cabeçalho).

Definindo níveis de segurança

A implementação de IPSec requer um equilíbrio entre tornar as informações facilmente disponíveis para o maior número de usuários e proteger informações críticas contra modificação e interpretação não autorizadas. As estruturas de segurança IP e do Windows 2000 devem ser analisadas durante o planejamento:

- Avalie os níveis de risco para determinar o nível adequado de segurança necessário.
- Determine as informações que devem ser criptografadas e o que deve ser protegido contra modificação.
- Defina diretivas de acordo com critérios de risco e proteja as informações categorizadas.

As considerações sobre diretivas também são influenciadas pela função dos computadores aos quais elas se aplicam: será usada uma segurança diferente para controladores de domínio, servidores da Web, servidores de acesso remoto, servidores de arquivos, servidores de bancos de dados, clientes da intranet e clientes remotos. A IPSec pode se tornar ineficiente rapidamente se não houver o planejamento e avaliação cuidadosos das diretrizes de segurança e o design e atribuição adequados das diretivas.

Antes de criar as diretivas de IPSec, você deve definir:

- o que deve ser protegido
- como protegê-lo
- onde protegê-lo
- quem vai gerenciar as diretivas
- se as exigências de exportação são uma questão a ser considerada

Os níveis de segurança a seguir são recomendados como diretrizes na implementação da estrutura geral de segurança do Windows 2000. Para maior clareza, os níveis de segurança de IPSec corresponderão a essa lista.

- Segurança mínima
- Segurança padrão
- Segurança alta

Níveis mínimos de segurança: Como padrão, a IPSec não é ativada. Se o plano de segurança não exigir nenhuma proteção em determinadas situações, nenhuma ação administrativa é necessária.

Níveis padrão de segurança: Não há uma definição exata dos níveis padrão de segurança. Eles podem variar bastante, dependendo das diretivas e da infra-estrutura da organização. A IPSec vai tentar atender a essa exigência ambígua com:

- Diretivas e regras padrão

- Serviços de confidencialidade são fornecidos como uma opção e, portanto, os serviços de proteção estão automaticamente em um nível padrão.
- Como padrão, as configurações ISAKMP, algoritmos de autenticação e de integridade, encapsulamento e nova geração de chaves são definidos no nível padrão.

Em geral, as comunicações pela intranet exigem níveis mais baixos de segurança do que as comunicações pela Internet, WAN ou redes externas: sem confidencialidade; sem encapsulamento; permissão de comunicações não seguras. Isso vai acelerar a taxa de transferência das comunicações pela intranet, permitindo ainda algum nível de segurança: integridade e autenticação.

Níveis altos de segurança: Um nível alto é adequado para situações dial-up remotas, comunicações WAN ou qualquer comunicação entre redes externas. As comunicações de redes particulares não devem ser excluídas automaticamente; em alguns casos uma segurança alta pode ser garantida para a intranet.

Novamente, não há uma definição exata pelos mesmos motivos, e a IPSec atende a esses critérios com:

- Serviços de confidencialidade para criptografar dados
- Sigilo perfeito de roteamento, duração configurável das chaves, limites Quick Mode, grupos Diffie-Hellman configuráveis e algoritmos extremamente resistentes (3DES e SHA).
- Encapsulamento para qualquer tipo de conexão de rede.
- A capacidade de associar ESP a AH para fornecer o nível mais alto de proteção: integridade de pacote e privacidade de dados.

Lembre-se de que nem todos os ataques vêm de fora das redes corporativas. Se for exigida uma segurança extremamente alta para uma intranet, encapsulamento deve ser usado, além das diretivas de negociação de alta segurança.

Quando os dados são extremamente confidenciais, não deve ser ativada a comunicação não protegida com um host que não reconhece IPSec, mesmo que o host esteja na mesma rede, pois isso não garante que os dados estejam protegidos.

Em geral, como o encapsulamento é adequado a níveis altos de segurança, as regras de IPSec que especificam o encapsulamento também devem ter um alto nível de segurança nas diretivas de negociação. Os dados estarão trafegando, na verdade, pela Internet e, portanto, os serviços de confidencialidade (ESP) estão geralmente garantidos.

Kerberos

Nesse release do Windows 2000, a versão 5 do Kerberos é o principal protocolo de segurança. O Kerberos verifica tanto a identidade do usuário como a integridade dos dados da sessão.

Os serviços Kerberos estão instalados em cada controlador de domínio, e um cliente Kerberos é instalado em cada estação de trabalho e servidor do Windows 2000. A autenticação Kerberos inicial do usuário garante ao usuário um único logon aos recursos da empresa.

Além de melhorar a segurança, o Kerberos permite:

- Relações de confiança transitiva para autenticação entre domínios
- As credenciais de autenticação emitidas por um serviço Kerberos são aceitas por todos os serviços Kerberos dentro da árvore do domínio. Além disso, as credenciais emitidas por um serviço Kerberos em uma floresta de árvores de domínio são aceitas por todos os serviços Kerberos da floresta.
- Autenticação mútua de cliente e servidor
- Tanto o cliente como o servidor são autenticados em uma sessão Kerberos.
- Processos eficientes de autenticação
- O Windows 2000 Server pode verificar as credenciais do cliente sem consultar o serviço Kerberos no controlador de domínio.
- A implementação do Kerberos no Windows 2000 é compatível com qualquer outra implementação da versão 5 do Kerberos que seja compatível com IETF RFCs 1510 e 1964. Os clientes e servidores do Windows 2000 podem autenticar e, portanto, se comunicar com várias outras plataformas que implementam o pacote de autenticação Kerberos.

Autenticação delegada para transações cliente/servidor de várias camadas

Em algumas arquiteturas de aplicativos, uma transação de cliente precisa transitar em diversos servidores. Nesse caso, o servidor atual pode autenticar para o servidor solicitado em nome do cliente.

Termos do Kerberos

Authentication Server, Ticket Granting Ticket Server, Key Distribution Center:

A documentação do Kerberos (RFC 1510) se refere a um Authentication Server (AS, servidor de autenticação), um Ticket-Granting Server (TGS, servidor de concessão de tickets) e um Key Distribution Center (KDC, centro de distribuição de chaves).

O KDC é um serviço de rede que fornece tickets e chaves temporárias de sessão. O KDC atende aos pedidos de ticket inicial e de ticket de concessão de tickets. A parte de ticket inicial é, às vezes, conhecida como AS. A parte de ticket de concessão de tickets é, às vezes, conhecida como TGS. Portanto, o KDC é tanto AS como TGS, conforme RFC 1510.

Privileged Attribute Certificate (PAC, certificado de atributos privilegiados):

O PAC é uma estrutura que contém a SID do usuário e as GIDs universais, globais e locais aos quais pertence.

Ticket, ticket de concessão de tickets:

Em uma troca Kerberos básica, o cliente envia primeiro um pedido para o AS para solicitar um ticket de concessão de tickets que será usado para solicitar um ticket do TGS para o servidor de destino.

Um ticket é um registro que ajuda o cliente a se autenticar para um servidor. Ele contém a identidade do cliente, o PAC, uma chave de sessão, uma marca de data e hora e outras

informações, tudo isso criptografado através da chave secreta do servidor. Portanto, só o servidor que conhece essa chave secreta pode decodificar o ticket. O ticket é obtido de um KDC e passado ao servidor de destino para autenticação.

Normalmente, um Ticket-Granting Ticket (TGT, ticket de concessão de tickets) é obtido durante o início de uma sessão de logon (em uma troca de AS). O TGT inclui informações do PAC para o usuário e será usado para obter credenciais para outros servidores (p. ex.: servidores de arquivos) sem necessitar do uso adicional da chave secreta do cliente. O TGT é criptografado na chave secreta do KDC e não pode ser descriptografado pelo cliente para evitar que ele altere as informações de associação a grupos contidas no PAC.

Kerberos e o tempo

Devido à natureza sensível ao tempo do protocolo Kerberos, é vantajoso sincronizar os relógios do sistema. Tanto os clientes como os controladores de domínio vão sincronizar automaticamente o tempo usando o SNTP (Secure Network Time Protocol, protocolo de tempo de rede segura).

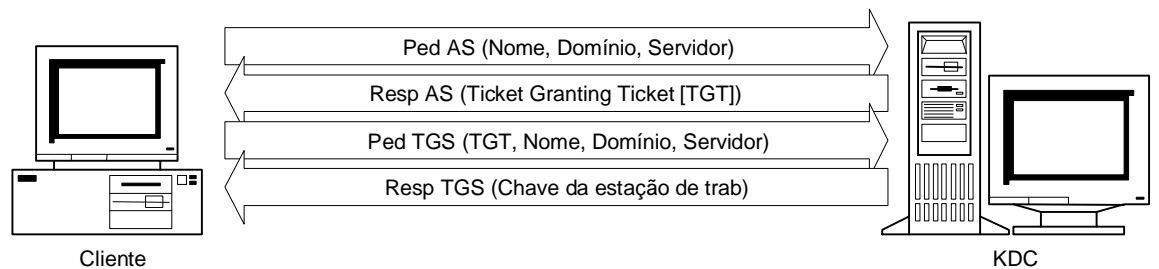
Um cliente do Windows 2000 vai obter o tempo do sistema de um controlador de domínio durante o logon e as renovações subseqüentes de ticket. Os controladores de domínio também sincronizam o tempo de forma hierárquica dentro do Active Directory. A raiz da estrutura do SNTP será, como padrão, o mestre de denominação do domínio da floresta. O Windows 2000 vai incluir uma interface de usuário para configuração de parâmetros SNTP e mestres de tempo adicionais.

Autenticação Kerberos: logon de domínio

O KDC pode ser executado em todos os controladores de domínio do Windows 2000 e consiste em um AS (Authorization Service, serviço de autorização) e um TGS (Ticket Granting Service, serviço de concessão de tickets). Esses dois serviços agem juntos para fornecer TGT (Ticket Granting Tickets, tickets de concessão de tickets) e tickets de sessão para autenticação.

Quando um cliente efetua logon inicialmente no domínio do Windows 2000, duas etapas básicas vão estar envolvidas.

- O cliente vai solicitar e receber um ticket de concessão de tickets a partir do KDC.
- O cliente vai submeter esse TGT ao KDC e receber subseqüentemente um ticket de sessão para autenticação para o LSA local.



n Figura 34

Todos os controladores de domínio do Windows 2000 são executados como KDCs Kerberos. Antes de efetuar logon, o sistema cliente vai primeiro localizar um controlador de domínio antes de prosseguir. Como a estação de trabalho faz parte de um domínio, isso geralmente ocorre quando o canal seguro é criado e um controlador de domínio já é conhecido.

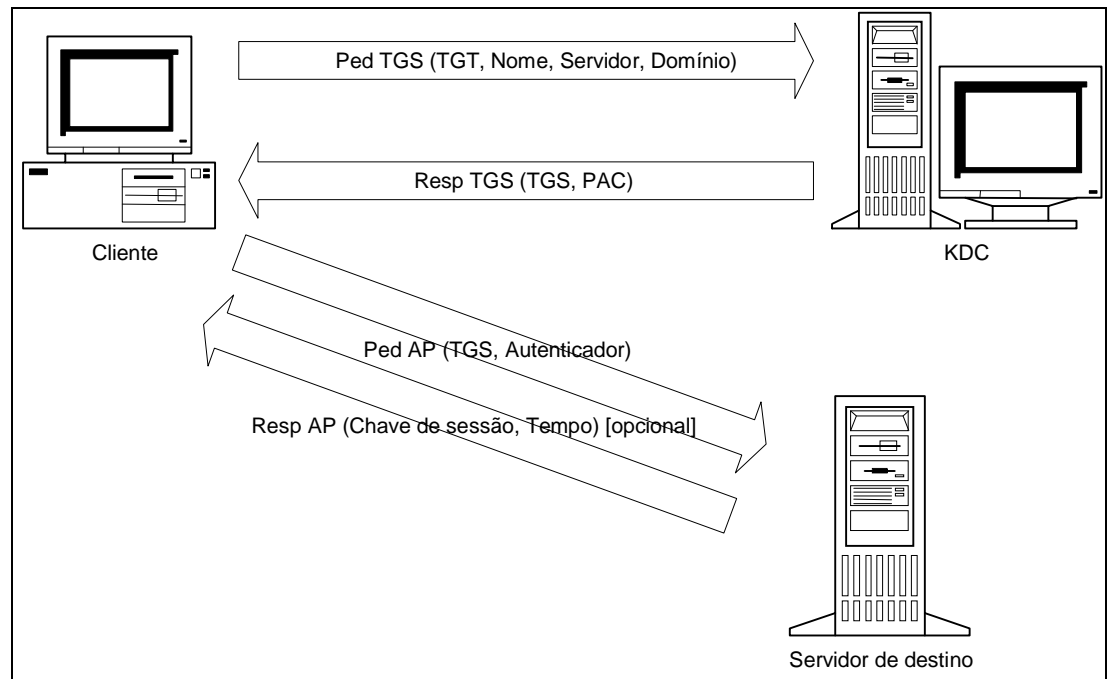
As trocas de AS e TGS com o KDC são enviadas através da porta 88 UDP. As trocas entre o cliente e o servidor de destino dependem do protocolo ponto a ponto usado por esses componentes.

- O cliente envia um pedido de AS inicial ao KDC, fornecendo o nome do usuário e o do domínio. Esse é um pedido de autenticação e um TGT.
- O KDC gera uma resposta de AS contendo um TGT criptografado com a chave secreta do KDC e uma chave de sessão para trocas de TGS criptografadas na chave secreta do cliente. O PAC está contido na parte de dados de autorização do TGT. O KDC criptografa o TGT com a sua própria chave privada para evitar que o cliente altere as informações de associação ao grupo.
Essa resposta é enviada de volta para o cliente.
- Para autenticar um usuário que efetua logon em um sistema local, o TGT obtido na troca de AS é usado na troca de TGS para obter credenciais para um sistema local. Isso significa que o usuário que está efetuando logon precisa ter direitos para trabalhar no sistema local.
O cliente gera e envia um pedido de TGS contendo o nome principal do cliente (= nome do usuário) e o ambiente, o TGT (a partir da troca de AS) para identificar o cliente e o nome da estação de trabalho local como servidor de destino. Ele também inclui um autenticador. Dessa forma, o usuário está solicitando acesso à máquina local.
- O KDC gera e envia uma resposta de TGS contendo um ticket para a estação de trabalho criptografada na chave privada do cliente e outras informações (p. ex.: uma marca de data e hora) criptografadas usando-se a chave da sessão do TGT. Também está incluído na parte de dados de autorização do ticket o PAC copiado pelo KDC a partir do TGT original. A partir das informações incluídas no PAC, o LSA do lado do cliente vai criar um token de acesso para o usuário.

Autenticação Kerberos: acesso aos recursos

Para que um cliente possa acessar um recurso em um servidor de destino, o cliente deve

solicitar um ticket válido para o servidor de destino a partir do KDC.



n Figura 35

Pedido de TGS:

Para solicitar o ticket válido para o servidor de destino, o cliente envia um pedido de TGS para o KDC que inclui o TGT obtido durante o logon inicial, o nome do cliente (=usuário) e o nome do servidor de destino.

Resposta de TGS:

O KDC responde com um ticket para o servidor de destino e uma chave de sessão a ser usada entre o cliente e o servidor de destino.

O PAC é incluído nos dados de autenticação desse ticket. Tanto a chave da sessão como o ticket são criptografados.

Pedido de AP:

Depois de obter um ticket válido para o servidor de destino, o cliente envia um Application Request (AP, pedido de aplicativo) ao servidor de destino. O pedido AP contém o ticket do servidor e um autenticador a ser usado entre o cliente e o servidor de destino.

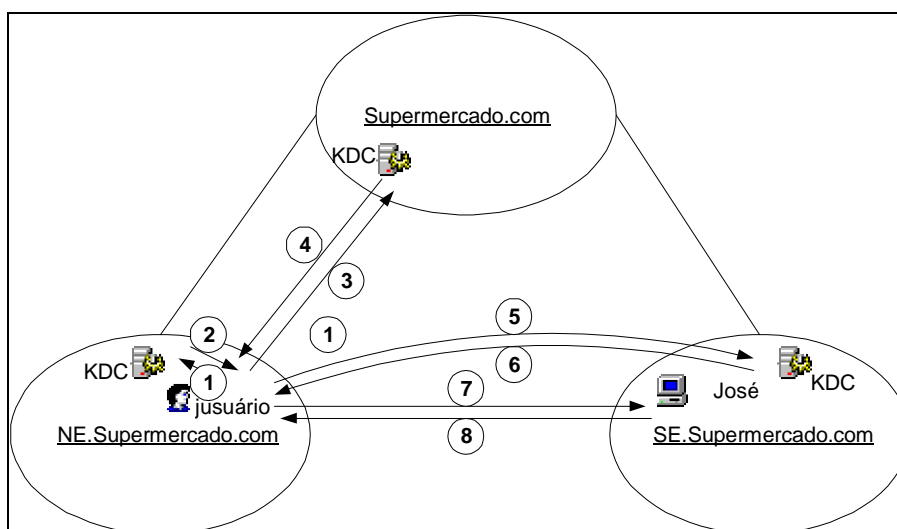
O servidor de destino então descriptografa o ticket e o autenticador, e verifica se essa mensagem não é uma reprodução.

Resposta de AP:

A resposta de AP só contém a hora atual criptografada com a chave da sessão para informar ao cliente que ela foi validada no servidor de destino.

Autenticação Kerberos – entre ambientes

As fronteiras de um ambiente Kerberos são idênticas às de um domínio do Windows 2000. A autenticação entre ambientes pode ser declarada como acesso aos recursos de outros domínios. O processo de acesso entre ambientes é bastante semelhante ao do acesso dentro de um ambiente, exceto que o KDC do cliente vai remeter o cliente para KDCs de outros ambientes, que seguem a confiança explícita estabelecida para o ambiente de destino.



n Figura 36

Por exemplo, jusuário deseja acessar José no ambiente SE (domínio). O processo para se obter esse acesso é:

- 1) jusuário envia TGS_REQ para KDC de NE
- 2) O KDC de NE responde com a chave de sessão para Supermercado
- 3) jusuário envia TGS_REQ para o KDC da Supermercado com informações de destino
- 4) O KDC da Supermercado responde com a chave de sessão para SE.
- 5) jusuário envia TGS_REQ para KDC de SE com informações de destino
- 6) O KDC de SE responde com TGT e dados de autorização para José
- 7) jusuário envia AP_REQ para José com TGT e dados de autorização
- 8) José responde com autenticador (opcional)

*O mesmo ticket de sessão é usado para acessar José

As confianças Kerberos do Windows 2000 são transitivas dentro do campo de ação de uma floresta. Contudo, as confianças não estabelecem necessariamente uma relação direta entre todos os domínios. Em vez disso, os clientes receberão TGTs para ambientes pai que, por sua vez, fornecem um caminho para o destino. No caso ilustrado aqui, uma enorme quantidade de acesso entre NE.Supermercado.com e SE.Supermercado.com pode justificar a criação explícita de uma confiança Kerberos entre dois domínios. Assim que um ticket for obtido para acesso a um recurso, o cliente pode usar esse ticket até a sua expiração (normalmente dez horas).

Interoperabilidade Kerberos

Há duas formas em que o Windows 2000 pode funcionar com KDCs baseados em Kerberos MIT.

1. Primeiro, a estação de trabalho do Windows 2000 pode ser configurada para usar um KDC Unix. Os usuários podem efetuar logon no Windows 2000 usando uma conta definida no KDC Unix. Isso é igual ao suporte de estação de trabalho Unix para logon Kerberos. Qualquer aplicativo do Windows 2000 ou Unix que só requer autenticação baseada em nomes pode usar um KDC Unix como servidor Kerberos.

2. A segunda forma em que o Windows 2000 funciona com Kerberos MIT é através de confiança entre um ambiente Unix e um domínio do Windows 2000. A confiança entre ambientes é a melhor forma de se oferecer suporte aos serviços do Windows 2000 que usam a personificação e controle de acesso.

Contudo, os clientes do Windows 2000 não podem usar um KDC Unix para autenticação no Active Directory. O modelo de segurança distribuída do Windows 2000 depende em mais do que uma lista de SIDs para autorização de dados em tickets Kerberos, e esses protocolos vão bem além dos serviços de autenticação fornecidos pelo servidor Kerberos MIT.

Planejamento de Kerberos

O uso de Kerberos nativo dentro do Windows 2000 requer pouco planejamento além da implementação de extensões de cliente nas máquinas com o Windows 95 e Windows 98. Contudo, caso alguma forma de interoperabilidade de Kerberos seja exigida em ambientes externos, isso deve ser planejado na etapa inicial da implantação. Quanto a isso, deve ser permitida uma integração de PKI com o esquema de autenticação. Além disso, deve-se planejar passar a Porta 88 através de qualquer firewall para realizar a replicação de confiança entre os ambientes.

Revisão

A segurança no Active Directory precisa achar um equilíbrio entre tornar os dados facilmente acessíveis e, ao mesmo tempo, protegê-los. Esta seção analisou os conceitos de segurança do Windows 2000, como controle de acesso e herança. Também explicou os mecanismos de segurança fornecidos com o Windows 2000 e apresentou uma análise de como se deve planejar a infra-estrutura de segurança.

Grupos

O melhor método de se aplicar as diretivas de segurança é através do gerenciamento eficiente de contas. Os grupos de segurança do Windows 2000 representam o terceiro princípio de segurança e são a base da relação entre os usuários e a segurança.

A forma mais eficiente de se administrar a segurança é atribuir direitos e permissões aos grupos de segurança em vez de a usuários ou computadores individuais. Em geral, um usuário ou computador precisa acessar diversos recursos. Se o usuário ou computador for

membro de um grupo com acesso aos recursos, você pode controlar o acesso, acrescentando ou removendo o usuário ou computador do grupo, em vez de alterar as permissões do recurso. Definir permissões para um usuário ou computador individual não altera as permissões concedidas ao usuário ou computador através dos grupos aos quais o usuário pertence.

Basear as diretivas de segurança e o gerenciamento de contas em grupos, em vez de em usuários ou computadores, reduz o custo de propriedade. A administração no nível da conta ou do recurso pode então ser limitada a casos excepcionais.

Estruturas de segurança

Os grupos fornecem um mecanismo eficiente para a criação de estruturas de segurança no Windows 2000, enquanto as estruturas de segurança são uma hierarquia administrativa usada para reduzir o número de itens a serem administrados individualmente.

As estruturas de segurança podem ser usadas para associar usuários a grupos e esses grupos a outros grupos que são gerenciados por agrupamentos administrativos. Por exemplo, um determinado conjunto de usuários pode estar contido dentro de um grupo denominado Usuários do escritório. Esse grupo pode ser usado para atribuir um determinado ambiente de área de trabalho através de diretivas. Outro grupo denominado Todos os usuários pode incluir o grupo Usuários do escritório, além de outros para facilitar a aplicação de definições globais em usuários. O grupo Todos os usuários é pai dessa determinada estrutura de segurança, mas também pode ser gerenciado por outra estrutura de segurança composta de grupos de tipo de administrador.

A finalidade das estruturas de segurança é classificar e agrupar regras de segurança da mesma forma que devem ser administradas.

Utilização de grupos

Os grupos também podem pertencer a outros grupos. Você pode usar isso para criar um intervalo adequado de contextos de grupo para avaliação dos direitos. Por exemplo, pode haver um grupo Produção que engloba responsabilidades de fabricação, empacotamento e envio. Você pode criar os grupos Fabricação, Envio e Produção, atribuir direitos adequados a cada um deles e fazer com que todos eles pertençam ao grupo Produção. Os direitos que você atribui ao grupo Produção são aplicados a todos os seus grupos membros.

Para implementar uma estratégia baseada em grupos:

- Crie grupos de segurança abrangente.
- Atribua direitos aos grupos antes de criar contas de usuários ou computadores.
- Delegue a administração dos grupos ao gerente ou líder de grupo adequado.

O tipo de grupo usado para gerenciar contas e recursos determina parcialmente como as diretivas de segurança vão ser aplicadas. O Windows 2000 Server introduz grupos novos e mais funcionais – cada um tem mais funções diferentes e campo de ação. Há três tipos de grupos de segurança dentro do Active Directory:

Grupos globais: Os grupos globais só contêm usuários do domínio local, mas podem ser

usados em qualquer lugar. Portanto, se membros de um grupo devem estar limitados a um único domínio, mas o acesso aos recursos globais é exigido, use grupos globais.

Grupos locais de domínio: Os grupos locais de domínio também contêm membros de qualquer domínio, mas só podem ser usados no domínio onde são criados. Os grupos locais de domínio são, portanto, bem adequados ao acesso aos recursos do domínio local que requerem associação global.

Grupos universais: Os grupos universais podem conter membros de qualquer domínio e são usados para atribuir direitos de acesso aos recursos.

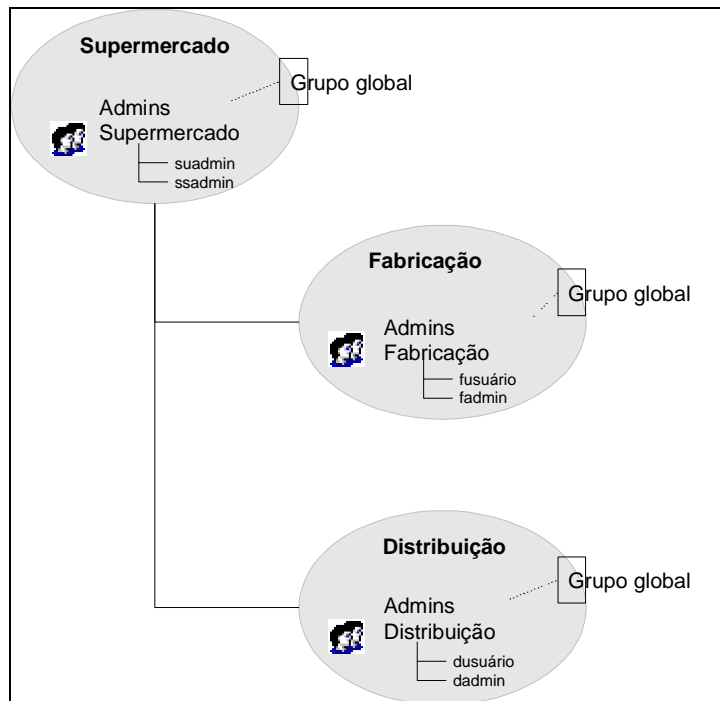
As seções a seguir fornecem distinções entre os tipos de grupos – qualidades e limitações – bem como recomendações de uso.

Grupos globais

Os grupos globais são os membros mais versáteis da família de grupos e têm os seguintes atributos:

- Só podem conter membros do domínio onde foram criados.
- Os membros podem incluir contas de usuários e outros grupos globais do mesmo domínio.
- Podem ser eles mesmos membros de grupos universais e de grupos locais de domínio.

Esses atributos proporcionam um uso claro dos grupos globais. Considerando-se que a associação é limitada, os grupos globais devem ser usados para definir grupos, cuja associação vai estar sempre limitada aos seus próprios domínios.



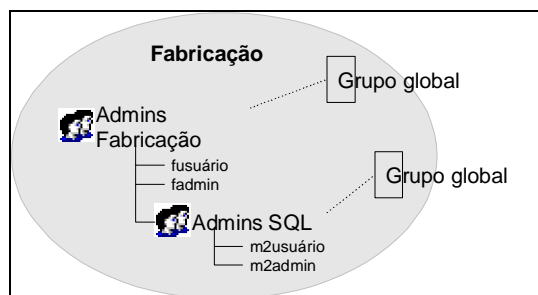
n Figura 37: Associação a grupo global

Por exemplo, esses grupos globais foram criados nos domínios Supermercado, Fabricação e Distribuição com a intenção expressa de só permitir a associação das suas respectivas

contas de domínio.

A associação limitada reduz o número de problemas de segurança que normalmente surgiriam nesse tipo de situação – onde as contas de domínios externos não autorizadas são acrescentadas intencional ou inadvertidamente aos grupos globais.

Os grupos globais são bem adequados à criação de estruturas de segurança dentro de um domínio, pois podem ser aninhados, mas somente dentro do domínio onde foram criados. Ao se incrementar o exemplo anterior, o grupo global “Admins Fabricação” pode conter outros grupos globais do domínio de fabricação, como Admins SQL. Usar grupos globais dessa forma fornece uma base para cada controle de acesso granular e atribuição de permissões.



n Figura 38: Aninhamento de grupos globais

Usar grupos globais dessa forma fornece uma base para cada controle de acesso granular e atribuição de permissão.

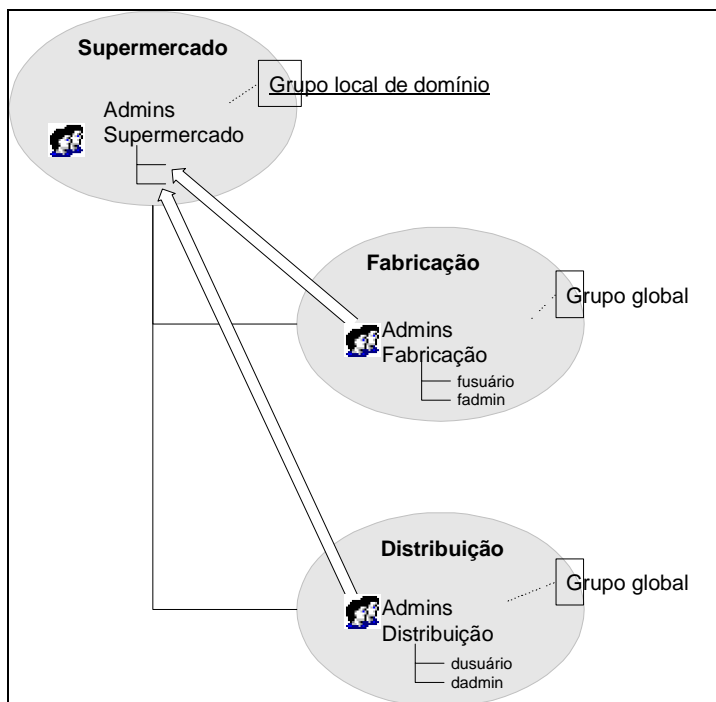
O aspecto global dos grupos globais vem na sua própria utilização. Um grupo global pode ser membro de qualquer outro tipo de grupo de segurança e, portanto, incrementando o conceito das estruturas de segurança. Isso significa que podem ser usados para a atribuição de permissões diretas aos recursos fora do domínio, além de serem incluídos nos grupos universais ou locais de qualquer domínio.

Grupos locais de domínio

Os grupos locais de domínio são a antítese dos grupos globais, pois eles podem conter membros de qualquer outro tipo e de qualquer domínio, mas só podem ser endereçados localmente. Como os grupos globais, os grupos locais de domínio podem conter outros grupos locais de domínio, mas somente do seu próprio domínio.

Esses atributos tornam os grupos locais de domínio bem adequados para limitar o campo de ação da sua utilização, enquanto permitem a associação de qualquer domínio.

Incrementando o conceito de estruturas de segurança apresentado na utilização dos grupos globais, um uso adequado dos grupos locais de domínio seria o de servir como raiz da estrutura de segurança.



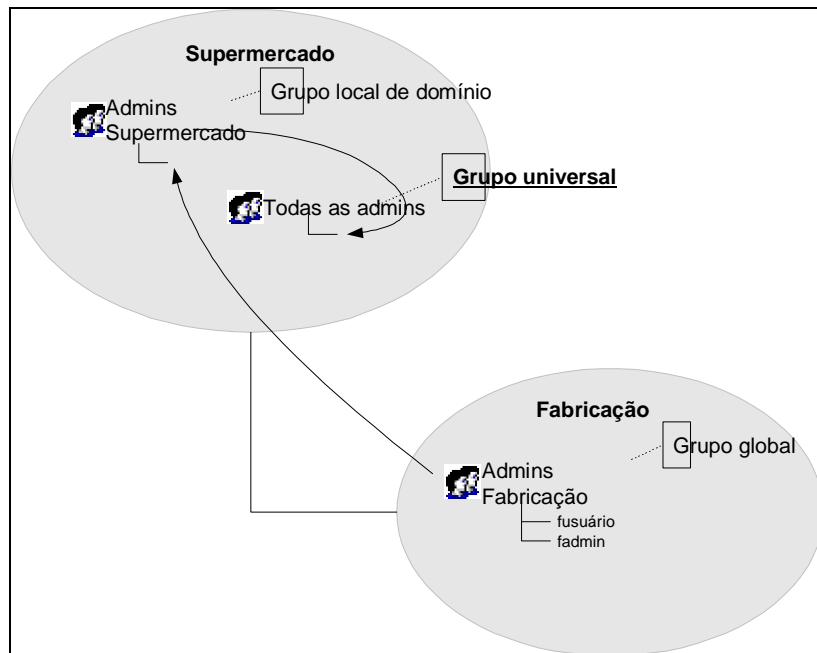
n Figura 39: Utilização dos grupos locais de domínio

Na figura anterior, o grupo “Admins Supermercado” foi criado com a intenção de ter associação global e permissões atribuídas aos recursos dentro do domínio Supermercado. Esse é um grupo agregado de forma eficiente que contém os grupos globais dos domínios filho. O grupo local de domínio “Admins Supermercado” nesse caso só pode ser acessado a partir do domínio Supermercado.

Grupos universais

Os grupos universais são muito semelhantes aos grupos locais de domínio, pois podem conter contas de usuários, grupos universais e grupos globais de qualquer outro domínio. Contudo, os grupos universais também podem ser acessados de qualquer domínio, tornando-os muito flexíveis.

Novamente, para usar os exemplos anteriores, os grupos universais seriam usados para criar a estrutura, mas agora a estrutura pode se basear em qualquer nível, até mesmo dentro do seu próprio domínio.



n Figura 40: Utilização de grupos universais

No exemplo anterior, o grupo universal contém os grupos globais e locais de domínio, mas podem ser acessados de qualquer um dos domínios. Além disso, o grupo universal “Todas as admins” pode estar contido em outro grupo universal em qualquer um dos domínios.

Da mesma forma, os próprios grupos universais podem agir como membros de qualquer outro tipo de grupo, o que fornece um mecanismo para estruturas de grupo muito complexas.

Considerações sobre design

Os grupos de segurança devem ser usados como um fundamento para o gerenciamento de contas do usuário e a segurança distribuída. O planejamento e implementação corretos dos grupos terá uma papel importante na redução do custo total de se administrar um sistema distribuído.

Enquanto o enfoque até agora esteve na utilização dos grupos para ajudar a administração dos recursos, os grupos também fornecem um excelente mecanismo para se administrar os próprios usuários. Agrupar usuários semelhantes em classificações para administração vai permitir que tarefas trabalhosas, como distribuição de software e aplicação de diretivas, sejam feitas de forma mais rápida. Esse aspecto dos grupos vai ser abordado em detalhe mais adiante na seção sobre planejamento das diretivas de grupo.

As informações a seguir são úteis no planejamento de grupos e de diretivas de grupos.

Um controlador de domínio requer conhecimento global das associações de grupo para calcular todos os grupos (direta ou indiretamente) que contém. Com os grupos universais, o controlador de domínio usa o catálogo global para realizar esse cálculo de associação.

Como o controlador de domínio usa o catálogo global para calcular as associações de

grupos universais, o catálogo global deve conter todas as associações de grupos universais. Mas se todos os grupos são grupos universais, as associações de grupos universais vão ser alteradas com bastante frequência, gerando um alto nível de tráfego de replicação do catálogo global. Um escritório de médio porte talvez não seja capaz de sustentar a largura de banda da rede necessária para que o catálogo global fique atualizado.

Quando você efetua logon em um servidor de recursos, um controlador de domínio no domínio de conta calcula o conjunto de todos os grupos aos quais você pertence que podem ser usados para controlar o seu acesso ao servidor de recursos. Esse conjunto inclui todos os grupos universais aos quais você pertence. Geralmente, só uma fração dos grupos aos quais você pertence será usada para controlar o acesso em qualquer servidor de recursos específico.

Local de domínio: Entrando em detalhes, os grupos locais de domínio não são replicados como parte do NC do domínio e, portanto, geram menos sobrecarga de replicação.

<i>Atributo</i>	Global	Local de domínio	Universal
Associação	Limitado	Aberto	Aberto
Pode conter	Usu/Global	Usu,Univ,Global	Usu,Univ,Global
Atribuição de permissões	Aberto	Limitado	Aberto
Aninhamento	Limitado	Limitado	Aberto
Pode ser atualizado	Para universal	Para universal	não
<p>* Associação: O campo de ação da associação (limitado = domínio local de objeto somente; Aberto = objetos de qualquer domínio). Pode conter: Tipos de objetos que podem pertencer a esse grupo. Atribuição de permissões: O campo de ação onde esse domínio pode ser acessado (limitado = só pode ser usado no domínio criado). Aninhamento: A capacidade do grupo de conter o seu próprio tipo de grupo (limitado = dentro do seu próprio domínio somente). Pode ser atualizado: A capacidade de um grupo de ser alterado (atualizado) para outro grupo.</p>			

Restrições de modo misto

Enquanto estiver operando em modo misto, há poucas restrições em relação à funcionalidade dos grupos. Geralmente, essas restrições estão relacionadas a fornecer compatibilidade retroativa ao Windows NT 4.0 e estão associadas ao aninhamento. No modo misto:

- Os grupos universais não existem como um grupo de segurança.
- Os grupos globais só podem conter contas e não podem ser aninhados.
- Os grupos locais de domínio podem conter contas e grupos globais, mas não podem ser aninhados.

Essas restrições não se aplicam mais quando o domínio é convertido para o modo nativo.

Revisão

Compreender as propriedades e implicações dos diversos tipos de grupos do Windows 2000 é essencial ao se planejar a hierarquia e as funções administrativas. Revendo: os grupos são unidades administrativas e podem ser globais, locais de domínio ou universais.

Os grupos globais só podem conter usuários do domínio local, mas podem ser usados em qualquer lugar. Os grupos locais de domínio também podem conter membros de qualquer

domínio, mas só podem ser usados no domínio onde foram criados. Os grupos universais podem conter membros de qualquer domínio e são usados para atribuir direitos de acesso aos recursos.

Como você usa grupos para administrar e implementar as diretivas de segurança da sua organização, é necessário compreender bem os grupos e certificar-se de que eles sejam bem planejados.