

Administração Windows NT

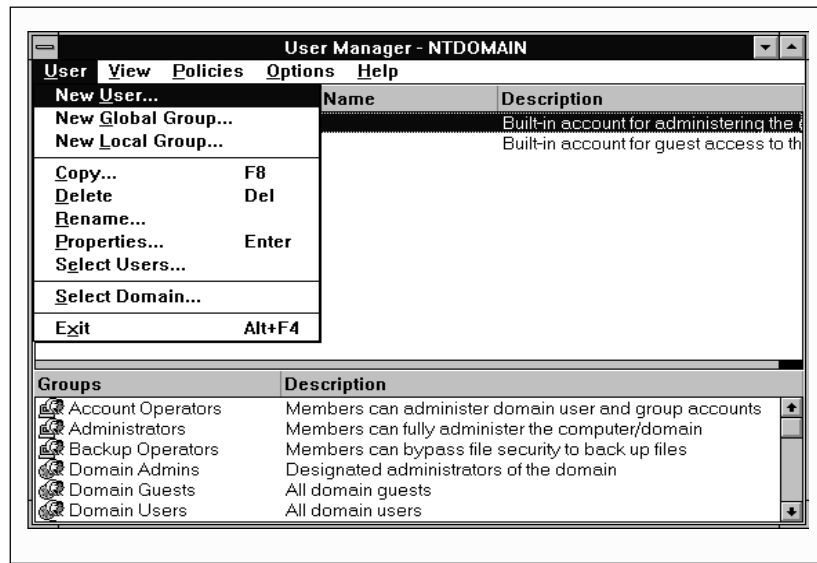


Tópicos

- Gerenciamento de contas de usuários e grupos
- Gerenciamento ambientes de trabalho de usuário
- estratégias de administração
- NTFS Overview - Segurança
- Ferramentas de administração:
 - Administrative wizards;
 - Server Manager;
 - Disk Administrator;
 - Performance Monitor
 - Event Viewer;
 - Windows NT diagnostics;



User manager for Domains

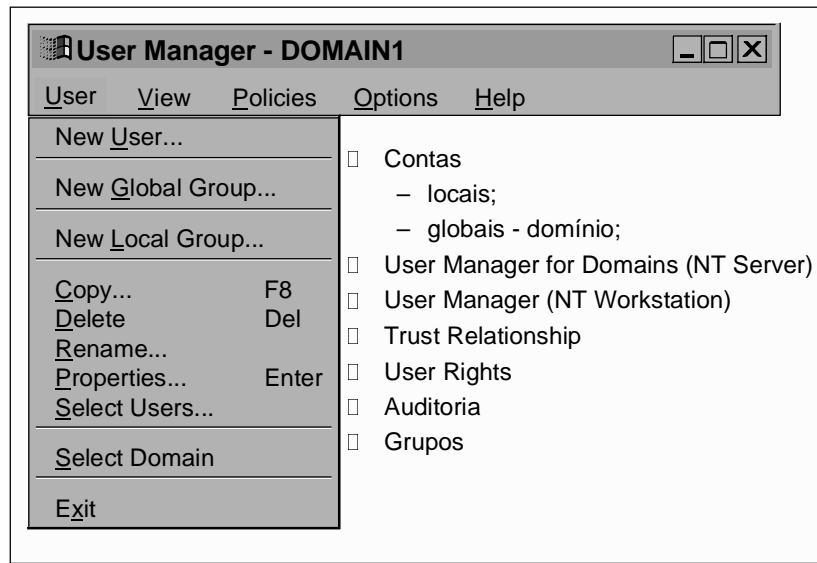


O sistema operacional de um computador determina o tipo de contas que você pode gerenciar, bem como o utilitário que você utiliza para gerenciá-las:

- Em computadores executando o Windows NT Workstation, você gerencia as contas somente daquela estação de trabalho e usa o utilitário Gerenciador de usuários.
- Em computadores executando o Windows NT Server, você gerencia contas no domínio local ou em qualquer estação de trabalho, servidor membro ou outro domínio ao qual você tenha acesso. Para isso, você utiliza o utilitário Gerenciador de usuários para domínios.
- Você instala o Gerenciador de usuários para domínios em um computador executando o Windows NT Workstation ou Windows® 95 usando as Ferramentas Administrativas baseadas no cliente. Com o Gerenciador de usuários para domínios instalado no computador cliente, você pode administrar controladores de domínio e outras estações de trabalho a partir daquele computador.

Usando conexão em baixa velocidade Alguns domínios e computadores poderão se comunicar com o seu computador através de uma conexão com velocidades de transmissão relativamente baixas. Por exemplo, transmissão em baixa velocidade pode ocorrer em um controlador de domínio que esteja conectado ao seu computador utilizando uma conexão do Serviço de Acesso Remoto (RAS, Remote Access Service), uma conexão intercontinental ou uma conexão que esteja saturada com outras tarefas de grande volume que não deverão ser interrompidas por tarefas do Gerenciador de usuários para domínios. Para reduzir atrasos na exibição de contas de usuário, grupos ou computadores, selecione Conexão em baixa velocidade.

User Manager



Planejamento de contas

- ❑ Convenção de usernames;
- ❑ atributos de senha;
- ❑ Grupos a que pertencem;
- ❑ diretório home, profile, scripts;
- ❑ horas que é permitido o logon;
- ❑ estações que é permitido o logon;
- ❑ políticas de contas
- ❑ conta ativa ou não



Cada pessoa que usará regularmente a rede e participará de um domínio deve ter uma conta de usuário em um domínio na rede. A conta de usuário contém informações sobre o usuário, incluindo nome, senha, várias entradas opcionais que determinam quando e como os usuários efetuam logon e como as configurações de sua Área de trabalho são armazenadas.

Propriedades das contas

New User X

Username:
 Full Name :
 Description :
 Password :
 Confirm Password:

☒ User Must Change Password at Next Logon
☐ User Cannot Change Password
☐ Password Never Expires
☐ Account Disabled

Groups

Profile

Hours

Logon To

Account

Dialin

Exercício de criação de contas.

Ao criar uma conta de usuário, você fornece vários fragmentos de informações que determinam como a conta pode ser usada. A tabela a seguir mostra o conteúdo de cada conta de usuário:

Nome do usuário	O nome exclusivo que o usuário digita ao efetuar logon; muitas vezes uma combinação de partes do nome e sobrenome do usuário.
Nome completo	O nome completo do usuário.
Descrição	Qualquer texto que descreve o usuário ou a conta do usuário.
Senha	A senha secreta do usuário.
Horário de logon	O horário em que o usuário pode efetuar logon. Esta configuração afeta tanto a capacidade de efetuar logon na rede como a de acessar os servidores. Uma configuração na diretiva de segurança de contas do domínio determina se os usuários são ou não forçados a efetuar logoff ao expirar seu horário de logon. Para obter maiores informações, consulte “Gerenciando horário de logon” posteriormente neste capítulo.
Estações de trabalho de logon	Os nomes de computador dos computadores com Windows NT a partir dos quais o usuário pode trabalhar. Por padrão, o usuário pode usar qualquer estação de trabalho, mas você pode limitar isso, se quiser.
Data de expiração	Uma data futura em que a conta será automaticamente desativada; é útil para garantir que as contas de funcionários temporários ou de estudantes não sejam mantidas ativas desnecessariamente.
Pasta base	Uma pasta que é privativa ao usuário. Um administrador cria essa pasta e o usuário controla o acesso a ela.

Script de logon Um arquivo em lotes ou um arquivo executável que é executado automaticamente quando o usuário efetua logon.

Perfil O caminho para uma pasta contendo informações que são retidas para criar o ambiente da Área de trabalho do usuário entre logons, tais como grupos de programas, conexões de rede e cores da tela, e configurações que determinam quais aspectos do ambiente o usuário pode alterar. Para obter informações sobre perfis de usuário, consulte o capítulo 3, “Gerenciando ambientes de trabalho do usuário”.

Tipo de conta O tipo de conta é global ou local. A maioria das contas que você cria será contas globais. Para obter informações sobre contas locais, consulte “Adicionando contas de usuário locais” posteriormente neste capítulo. Esta opção está disponível somente em domínios do Windows NT Server.

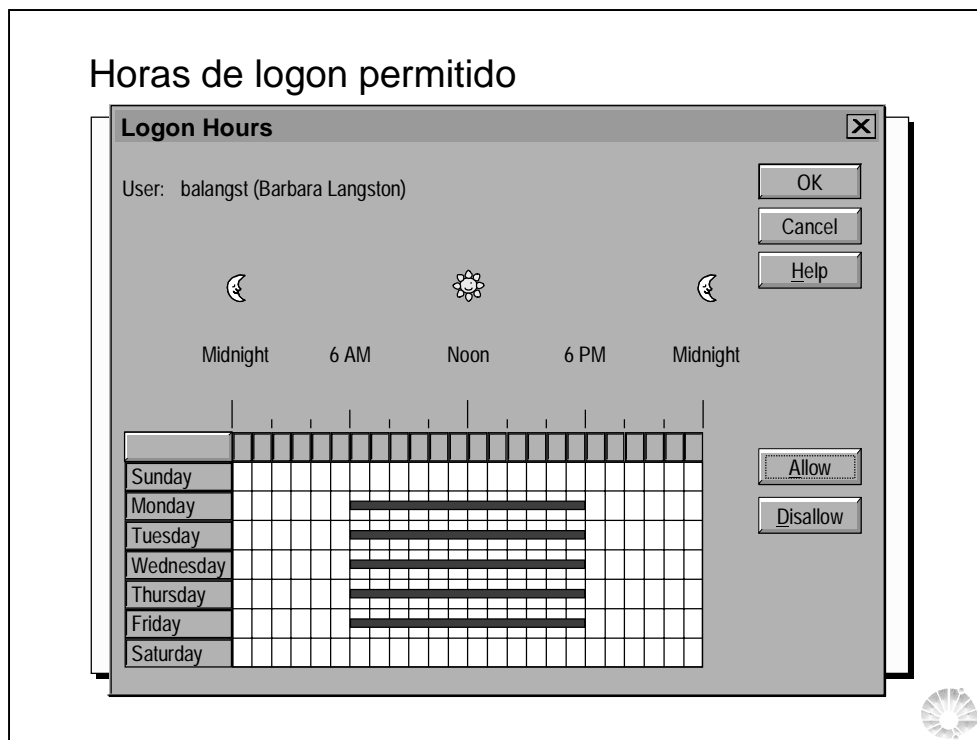
Adicionalmente, várias condições afetam o usuário com respeito à sua senha exclusiva de domínio ou computador local. Essas condições podem ser selecionadas ou apagadas pelo administrador ou operador de contas do controlador de domínio ou pelo administrador de uma estação trabalho ou de um servidor membro contendo as contas de usuário.

<i>Condição da conta</i>	<i>Padrão</i>	<i>Comentários</i>
O usuário deve alterar a senha no próximo logon	Selecionada	Se selecionada, o usuário será forçado a alterar a senha na próxima vez que efetuar logon. A configuração muda para Ativado quando a senha do usuário atingir a duração máxima da senha, conforme definido para o domínio em Diretiva de Contas. Depois de alterada a configuração muda para Desativado. senha, a
O usuário não pode alterar a senha	Desmarcada	Se selecionada, o usuário não pode alterar sua própria senha . Esta restrição é útil para contas aplica a administradores.
A senha nunca expira	Desmarcada	Se selecionada, esta conta de usuário ignora a diretiva d e expiração de senha configurada para o domínio e a senha nunca expira. É usada para contas que representam serviços, como o serviço Duplicadores. Também é útil para contas para as quais você quer que a senha nunca mude, como contas de convidado.
Conta desativada	Desmarcada	Se selecionada, esta conta está desativada e não é possível efetuar logon nela. Não é removida do banco de dados, mas ninguém pode efetuar logon na conta até que você a ativar-la. enquanto você não voltar a

Identificação de segurança (SID)

Uma conta de usuário ou grupo que inclui uma identificação de segurança (SID, Security Identifier), um número exclusivo que identifica a conta. Toda conta na sua rede recebe uma SID exclusiva no momento em que é criada. Processos internos no Windows NT referem-se à SID de uma conta, e não ao nome de usuário ou de grupo da conta. Se você criar uma conta, excluí-la e então criar uma conta com o mesmo nome de usuário, a nova conta não terá os direitos ou permissões anteriormente concedidos à conta antiga pois as contas têm números de SID diferentes.

Horas de logon permitido



Por padrão, os usuários podem se conectar a um servidor 24 horas por dia, 7 dias por semana. Para restringir esse acesso, use a caixa de diálogo Propriedades de usuário.

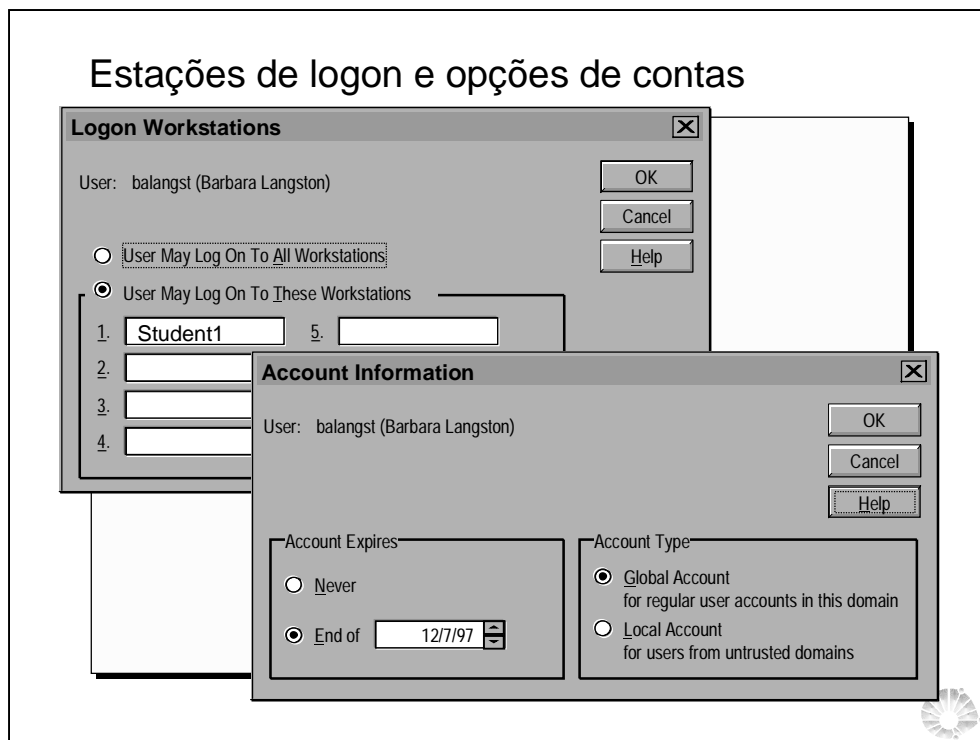
Ao selecionar uma conta de usuário no Gerenciador de usuários para domínios e visualizar as propriedades do usuário, você pode selecionar Horário de logon na caixa de diálogo Propriedades de usuário para alterar as configurações desse usuário. A caixa de diálogo Horário de logon exibe um calendário de uma semana, com o horário de logon exibido em incrementos de uma hora ao longo de sete dias. Uma caixa representa cada hora. Por exemplo, a primeira caixa em cada linha representa a hora desde meia-noite até 0:59h e a última caixa em cada linha representa a hora desde 23:00h até 23:59h.

Observação O horário de logon está no fuso horário do controlador de domínio primário, não na estação de trabalho ou servidor em que o usuário está efetuando logon ou se conectando.

As caixas preenchidas indicam quando o usuário pode se conectar aos servidores do domínio; as caixas vazias indicam quando é proibido ao usuário se conectar.

Quando um usuário está conectado a um servidor e o horário de logon é ultrapassado, o usuário poderá ser desconectado de todas as conexões com o servidor ou poderá permanecer conectado, embora lhe seja negado qualquer nova conexão, dependendo do status de uma opção na caixa de diálogo Diretiva de contas.

Estações de logon e opções de contas



Você pode definir uma data de expiração da conta e especificar o tipo de conta para as contas de usuário selecionadas.

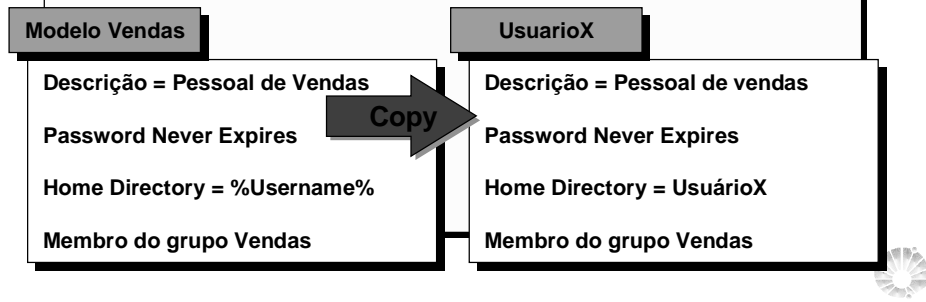
Quando uma conta tem data de expiração, ela é desativada no final daquele dia. (Contas expiradas não são excluídas, somente desativadas). Quando uma conta expira, um usuário conectado permanece conectado, mas não pode estabelecer nenhuma nova conexão de rede e, depois de efetuar logoff, não poderá efetuar logon novamente.

Por padrão, uma nova conta de usuário é uma conta de usuário global.

Uma conta local é uma conta de usuário em um domínio fornecida a um usuário cuja conta normal não está em um domínio confiável. Contas locais fornecem acesso a recursos em um único domínio e os recursos podem ser usados somente através da conexão a um controlador de domínio na rede. (Você pode efetuar logon interativo em uma conta local somente se tiver sido concedido à conta o direito de efetuar logon local).

Criando contas modelos

- ❑ **Maneira rápida para criar muitas contas**
- ❑ **Copia todas as propriedades das contas, exceto:**
 - Username e nome completo
 - Password e confirm password
 - Account disabled
 - Direitos e permissões



Muitas vezes é mais rápido e prático copiar uma conta de usuário existente do que criar uma nova. Através da cópia, você assegura que a participação em grupos e várias outras propriedades são copiadas na nova conta.

Quando uma conta de usuário é copiada, a descrição, participação em grupos, horário de logon, estações de trabalho de logon e informações de conta são copiadas com exatidão.

Para fazer com que o sistema insira automaticamente o nome de usuário da conta no caminho da pasta base, use %USERNAME%. Para obter maiores informações, consulte “Usando %USERNAME% no caminho da pasta base”.

· As caixas do nome de usuário, nome completo e senha da nova conta estão em branco e devem ser preenchidas. As caixas de verificação O usuário não pode alterar a senha e A senha nunca expira são copiadas.

Observação Ao copiar uma conta que é membro do grupo local Administradores, a configuração O usuário não pode alterar a senha não é copiada.

· Em geral, a caixa de verificação O usuário deve alterar a senha no próximo logon está selecionada, independentemente de sua configuração na conta original. Contudo, se a caixa de verificação O usuário não pode alterar a senha for copiada como selecionada, então a caixa de verificação O usuário deve alterar a senha no próximo logon estará desmarcada.

· A Caixa de verificação Conta desativada está sempre desmarcada, independentemente da configuração na conta de usuário original. Você pode criar uma nova conta de usuário, configurá-la conforme necessário, desativá-la e, então, utilizá-la como modelo. Você pode fazer rapidamente inúmeras cópias de uma conta modelo desativada.

O Gerenciador de usuários para domínios não copia direitos e permissões concedidos a uma conta de usuário. Entretanto, recomendamos que eles sejam fornecidos somente a grupos em vez de diretamente concedidos a contas de usuário. Uma vez que a participação em grupos da conta original é copiada para a nova conta de usuário, esta geralmente terá as mesmas capacidade e acesso a recursos que a conta original.

Usando modelo para criar contas

Copy of Sales Template [X]

Username:

Full Name:

Description:

Password:

Confirm Password:

☒ User Must Change Password at Next Logon

☐ User Cannot Change Password

☐ Password Never Expires

☐ Account Disabled

☐ Account Locked Out



Implementando política de contas

- **A política de contas determina como as senhas serão criadas e utilizadas pelos usuários**
- **A política de contas configura:**
 - Password age, length, and uniqueness
 - Account lockout

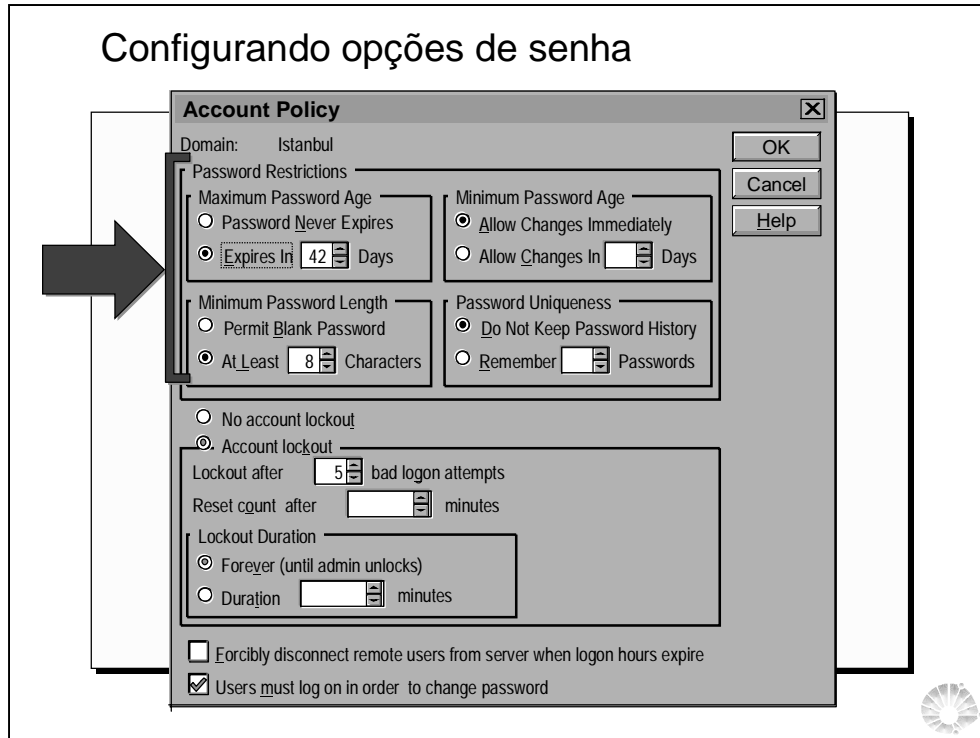


A diretiva de Contas controla como as senhas devem ser utilizadas por todas as contas de usuários de um computador ou domínio e também determina a diretiva de bloqueio de conta.

As restrições de senha incluem limites de expiração de senha, se uma senha pode ser alterada e quando é requerida, se cada nova senha deve ser exclusiva em relação a senhas anteriores e o tamanho que uma senha pode ter.

O recurso de bloqueio de conta permite tornar o Windows NT Server mais seguro contra intrusos que experimentam efetuar logon tentando adivinhar as senhas de contas de usuário existentes. Quando o bloqueio de conta está ativado, uma conta de usuário ficará bloqueada se ocorrer um número de tentativas incorretas de logon durante um intervalo de tempo especificado. Contas bloqueadas não podem efetuar logon. Uma conta bloqueada permanece bloqueada enquanto um administrador não a desbloquear ou enquanto não decorrer um intervalo especificado de tempo. Por padrão, o bloqueio de conta está desativado.

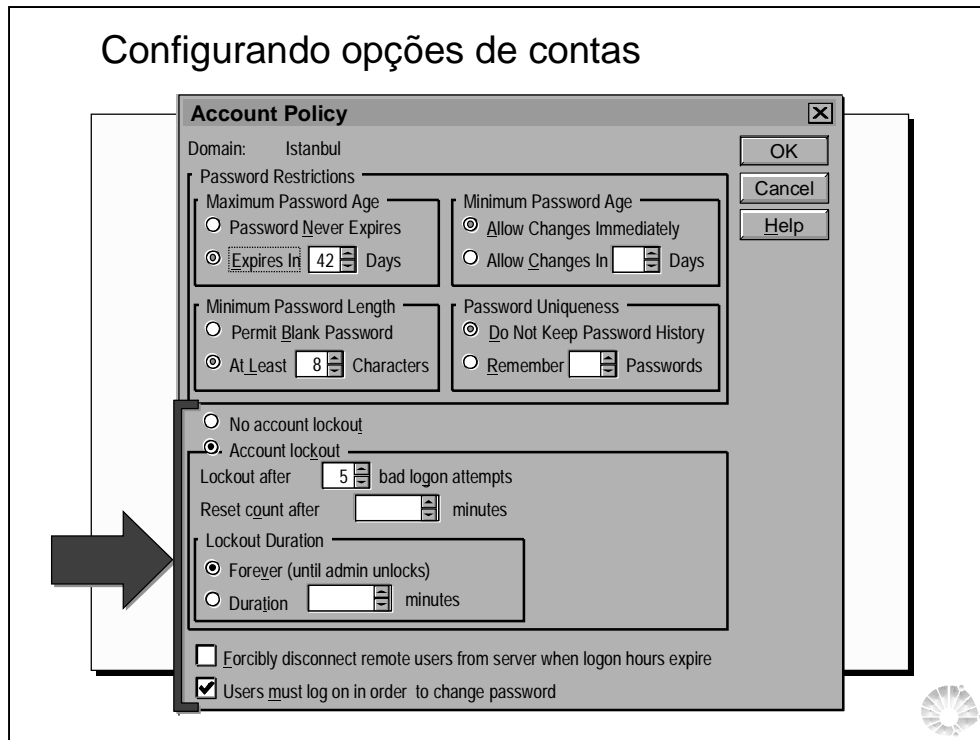
Configurando opções de senha



Há quatro parâmetros para senha que você define na caixa de diálogo Diretiva de contas.

Parâmetro	Descrição
Duração máxima da senha	O período de tempo em que uma senha pode ser utilizada até que o sistema requeira que o usuário a altere.
Duração mínima da senha	O período de tempo em que uma senha deve ser utilizada até que o usuário tenha permissão para alterá-la. Se você selecionar a opção Permitir alterações imediatamente, então em Exclusividade da senha você deverá selecionar a opção Não manter histórico de senhas.
Comprimento mínimo da senha	O menor número de caracteres que uma senha pode conter.
Exclusividade da senha	O número de novas senhas que devem ser utilizadas por uma conta de usuário até que uma antiga senha possa ser reutilizada. Se você inserir aqui um valor de exclusividade (por exemplo, “Lembrar 4 senhas”), então em Duração mínima da senha, você deverá especificar um valor de duração (por exemplo, “Permitir alterações em 7 dias”).

Configurando opções de contas



Se você selecionar Bloqueio de conta, deverá também configurar os parâmetros a seguir.

Parâmetro Significado

Bloquear após O número de tentativas de logon incorretas que fará com que a conta seja bloqueada. O intervalo é de 1 a 999.

Recomeçar a contagem após O número máximo de minutos que podem decorrer entre duas tentativas de logon incorretas. O intervalo é de 1 a 99999. Por exemplo, se Bloquear após for 5 tentativas de logon incorretas e Recomeçar a contagem após for de 30 minutos, então 5 tentativas de logon incorretas, com intervalos de 29 minutos, causariam um bloqueio.

Duração do bloqueio Selecione Até um administrador desbloquear para que as contas desbloqueadas permaneçam bloqueadas até que um administrador as desbloqueie. Selecione Duração e digite um número para que as contas permaneçam bloqueadas durante um número de minutos especificado.

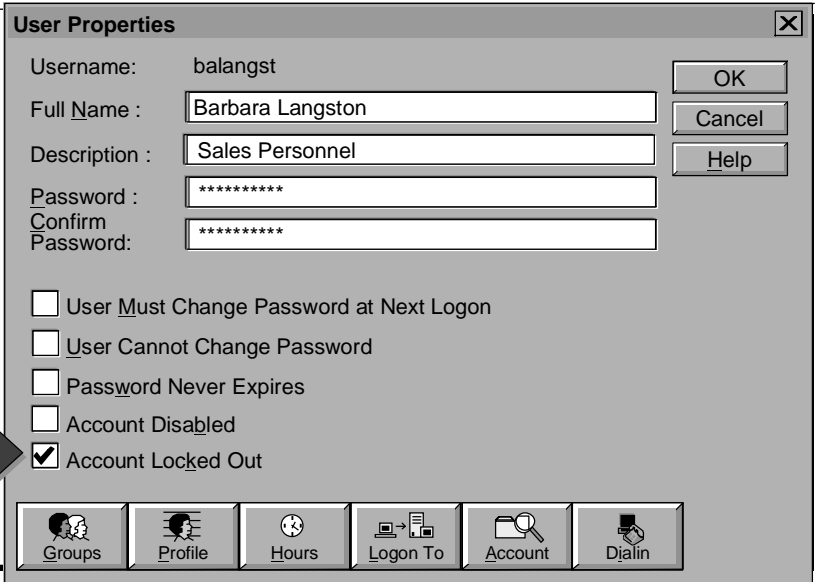
A opção Desconectar os usuários remotos do servidor ao expirar as horas válidas de logon interage com as horas de logon definidas para uma conta de usuário. Se a opção for selecionada, uma conta de usuário que exceda o tempo definido na caixa de diálogo Horário de logon será desconectada de todas as conexões com qualquer servidor do domínio. O usuário receberá uma mensagem de advertência poucos minutos antes da expiração das horas de logon.

Se essa opção estiver desmarcada, o usuário não será desconectado quando o Horário de logon for atingido, mas nenhuma nova conexão será permitida e uma mensagem de advertência será enviada a cada 10 minutos.

Quando a opção Os usuários devem efetuar logon para alterar a senha está selecionada, os usuários não podem alterar suas próprias senhas quando elas expiram ³/₄ eles devem obter ajuda de um administrador. Quando essa opção está desmarcada, os usuários podem alterar suas próprias senhas quando elas expiram, sem ajuda de um administrador.

Alterações feitas na diretiva de contas afetam todos os usuários do computador ou domínio no próximo logon.

Destruvando contas



The image shows a Windows 'User Properties' dialog box for the user 'balangst'. The 'Full Name' is 'Barbara Langston' and the 'Description' is 'Sales Personnel'. The password fields are masked with asterisks. The 'Account Locked Out' checkbox is checked, indicated by a large black arrow pointing to it from the left. Other options like 'User Must Change Password at Next Logon', 'User Cannot Change Password', 'Password Never Expires', and 'Account Disabled' are unchecked. At the bottom, there are tabs for Groups, Profile, Hours, Logon To, Account, and Dialin. The 'Account' tab is currently selected. The dialog has 'OK', 'Cancel', and 'Help' buttons on the right. A loading spinner is visible in the bottom right corner of the overall image frame.

User Properties

Username: balangst

Full Name : Barbara Langston

Description : Sales Personnel

Password : *****

Confirm Password: *****

☐ User Must Change Password at Next Logon

☐ User Cannot Change Password

☐ Password Never Expires

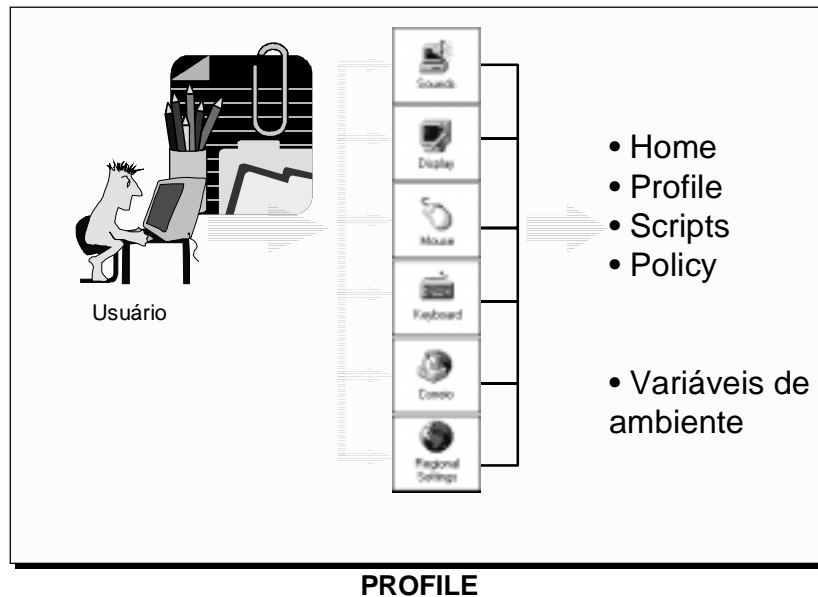
☐ Account Disabled

☒ Account Locked Out

Groups Profile Hours Logon To Account Dialin

OK Cancel Help

Gerenciando ambiente de trabalho de usuário



Os ambientes de trabalho de usuário incluem itens e configurações da Área de trabalho, como cores da tela, configurações do mouse, tamanho e posição da janela, e conexões da rede e impressora.

Você pode utilizar as seguintes ferramentas para gerenciar os ambientes de trabalho de usuário em uma rede do Windows NT Server:

- **Perfis de usuário**

O perfil de usuário contém todas as configurações definidas pelo usuário para o ambiente de trabalho de um computador que esteja executando o Windows NT, incluindo configurações de vídeo e conexões da rede. Todas as configurações específicas do usuário são automaticamente gravadas na pasta Profiles, dentro da pasta raiz do sistema (geralmente C:\winnt\profiles).

- **Editor de diretivas do sistema**

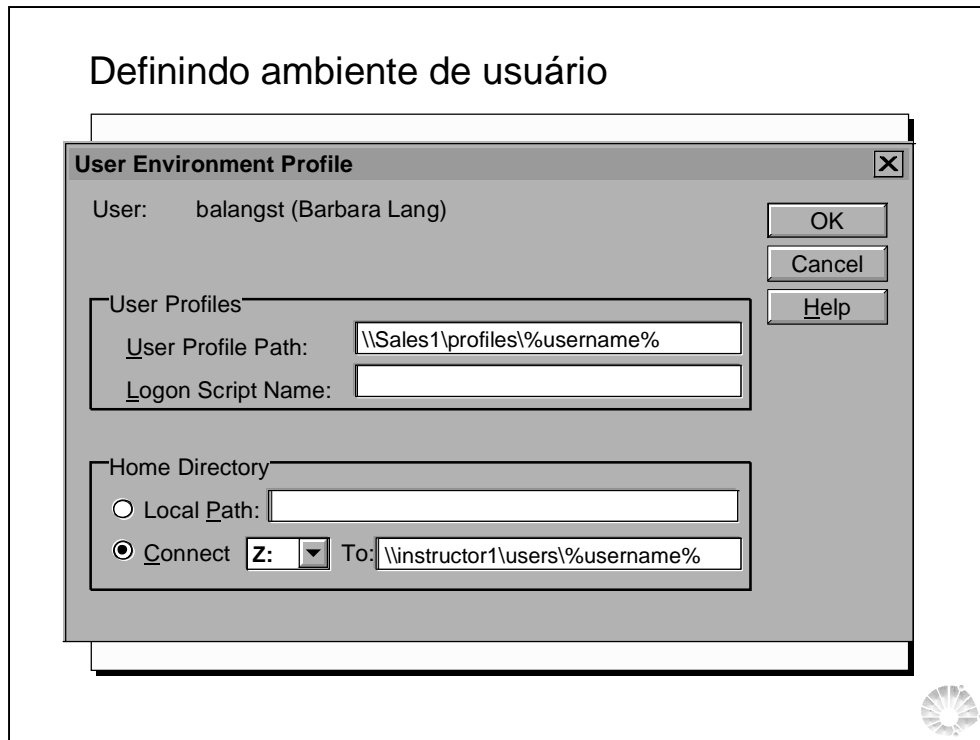
As diretivas do sistema permitem que você controle as configurações definidas pelo usuário no Windows NT e no Windows 95, assim como as configurações do sistema. Você pode utilizar o Editor de diretivas do sistema para modificar as configurações da Área de trabalho e restringir o que os usuários podem fazer a partir das suas Áreas de trabalho.

- **Scripts de logon**

Um script de logon é um arquivo em lote (.bat) ou executável (.exe) que é executado sempre que um usuário efetua logon em qualquer tipo de estação de trabalho na rede. O script pode conter comandos do sistema operacional, como comandos para fazer conexões da rede ou iniciar aplicativos.

- **Variáveis de ambiente**

As variáveis de ambiente especificam o caminho de pesquisa do computador, a pasta para arquivos temporários e outras informações similares.



Especificando uma localização do perfil de usuário

Na caixa de diálogo Perfil de ambiente de usuário, atribua um perfil ambulante ou obrigatório para uma conta de usuário digitando seu caminho completo e o nome da pasta de perfil de usuário na caixa Caminho para o perfil de usuário.

\\servidor\compartilhamento\nome do perfil

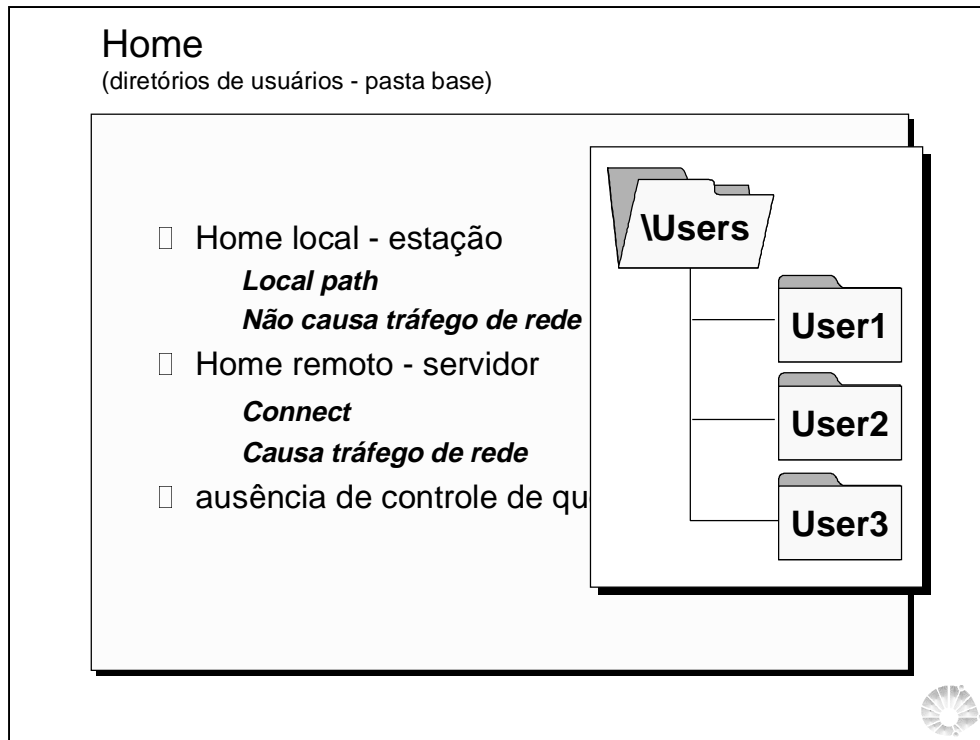
Para obter informações sobre como adicionar uma localização para o perfil de usuário, consulte Gerenciando o ambiente do usuário na Ajuda do Gerenciador de usuários para domínios.

Para obter informações sobre como criar e gerenciar perfis de usuário, consulte o capítulo 3, “Gerenciando ambientes de trabalho do usuário”.

Usando %USERNAME% no caminho da pasta base

Na caixa Pasta base, %USERNAME% pode ser substituído pela última entrada no caminho. Mais tarde, o sistema substitui o nome de usuário da conta do usuário. Esta substituição é útil quando várias contas de usuário são selecionadas.

Por exemplo, você selecionou oito contas de usuário. Na caixa Pasta base, você poderia selecionar Conectar, especificar K como a letra da unidade de disco, selecionar a caixa Para e digitar \\SALES\home\%username%. Quando você escolher OK para salvar o Perfil de Ambiente de Usuário, o nome real do usuário será substituído em cada entrada %USERNAME%.



Uma pasta base contém os arquivos e programas de um usuário; pode ser atribuída a um usuário individual ou ser compartilhada por vários usuários. Por reunirem os arquivos do usuário em um único local, as pastas base facilitam o trabalho de um administrador de efetuar backup de arquivos do usuário e excluir contas do usuário. Você especifica uma pasta base adicionando um caminho de pasta para a conta do usuário. Pastas base devem ser adicionadas a uma pasta compartilhada com um acesso apropriado.

A pasta base é a pasta padrão de um usuário para as caixas de diálogo Abrir arquivo e Salvar como, para o prompt de comando e para todos os aplicativos que não tenham uma pasta de trabalho definida.

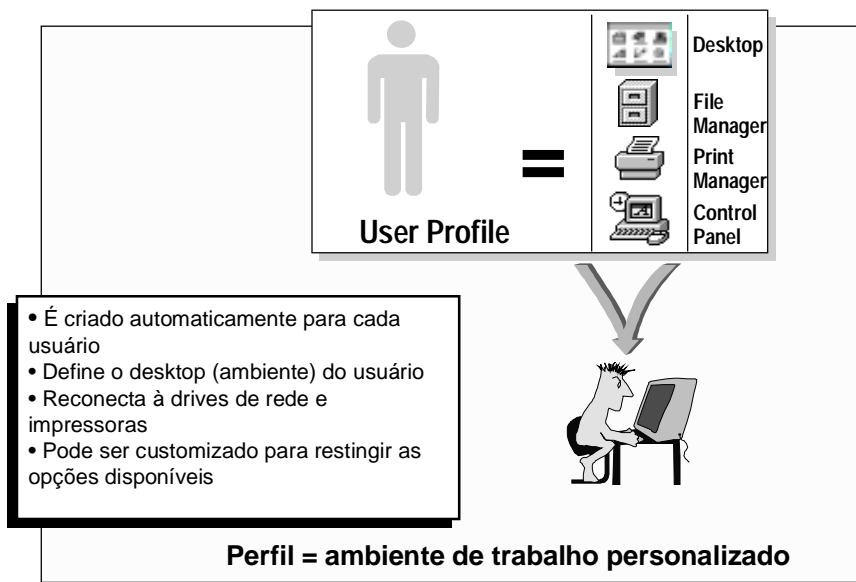
O Gerenciador de usuários para domínios aplica automaticamente as permissões de pasta se ele criar a pasta base. Quando uma conta de usuário está sendo administrada e uma nova pasta base é criada, é concedido a esse usuário Controle total. Quando duas ou mais contas de usuário estão sendo administradas e uma nova pasta base é criada, é concedido Controle Total para Todos.

O Gerenciador de usuários para domínios não aplicará automaticamente as permissões se a pasta já existir. Neste caso, você deverá aplicar as permissões usando o Windows NT Explorer. Se a conta de usuário não especificar uma pasta base, a pasta base padrão para computadores atualizados é \USERS\DEFAULT na unidade de disco local do usuário onde o Windows NT está instalado. Se o Windows NT Workstation ou o Windows NT Server estiver sendo instalado pela primeira vez, a pasta base padrão é a raiz da unidade de disco onde o Windows NT está instalado. (Para alterar a pasta base padrão para uma pasta de rede compartilhada ou para uma outra pasta local na estação de trabalho do usuário, use o Gerenciador de usuários para domínios).

• Quando estiver administrando as contas de usuário de um domínio, você deve atribuir pastas base de rede. O Gerenciador de usuários para domínios cria automaticamente essa pasta base. Se não puder, uma mensagem instrui para que você crie a pasta manualmente.

• Quando estiver administrando contas de usuário de uma estação de trabalho ou de um servidor membro, você deve atribuir pastas base locais. O Gerenciador de usuários para domínios cria automaticamente essa pasta base naquele computador. Se não puder, uma mensagem instrui para que você crie a pasta manualmente.

Entendendo perfis (profiles) de usuários



Em computadores executando o Windows NT Workstation ou o Windows NT Server, os perfis de usuário automaticamente criam e mantêm as configurações da Área de trabalho para cada ambiente de trabalho de usuário no computador local. Um perfil de usuário é criado para cada usuário quando o usuário efetua login em um computador pela primeira vez.

Os perfis de usuário proporcionam vários benefícios aos usuários:

Quando os usuários efetuam login em suas estações de trabalho, recebem as configurações da Área de trabalho como existiam quando efetuaram o logoff.

- Vários usuários podem utilizar o mesmo computador, sendo que cada um deles recebe uma Área de trabalho personalizada quando efetua login.
- Os perfis de usuário podem ser armazenados em um servidor de modo que possam acompanhar os usuários para qualquer computador que execute a plataforma Windows NT versão 4.0 na rede. São denominados perfis de usuário ambulantes.

Como uma ferramenta administrativa, os perfis de usuário proporcionam estas opções:

Você pode criar perfis de usuário personalizados e atribuí-los a usuários para oferecer ambientes de trabalho consistentes que sejam adequados às suas tarefas.

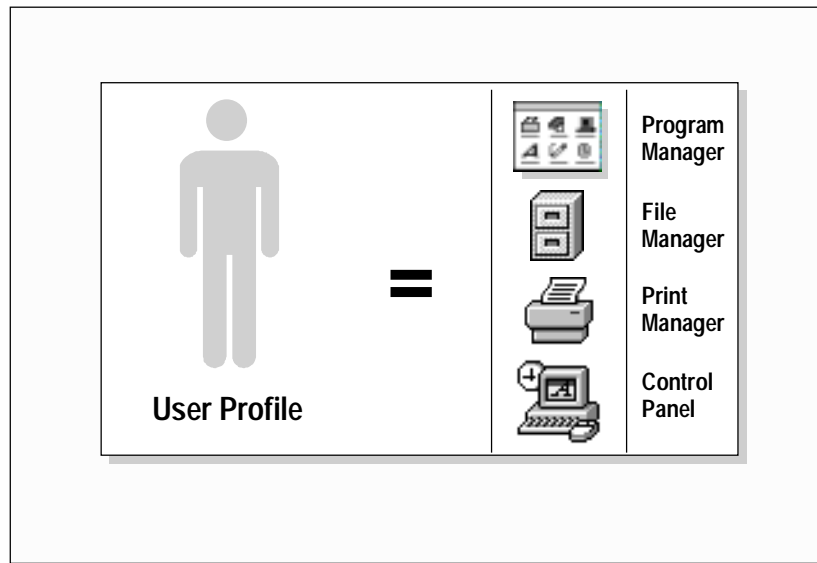
- Você pode especificar configurações de grupo comuns para todos os usuários.
- Você pode atribuir perfis de usuário obrigatórios para impedir que os usuários modifiquem qualquer configuração da Área de trabalho.
- Os perfis de usuário podem ser utilizados em computadores executando o Windows 95, mas devem ser ativados para se tornar disponíveis. Os perfis de usuário não têm efeito em computadores executando MS-DOS, UNIX ou OS/2

Profiles

- **Quando entram em ação ?**
- **Modelos de profiles:**
 - de Usuário;
 - Mandatory;
- **Tipos de profiles - comportamento:**
 - System Default;
 - User Default;
 - Local profile;
 - Roaming (ambulante) profile / Server-based;



Conteúdo do Profile



Um perfil de usuário contém as preferências e opções de configuração de cada usuário: um instantâneo do ambiente da Área de trabalho do usuário.

A tabela abaixo descreve as configurações em um perfil de usuário.

Origem	Parâmetros gravados
<i>Windows NT Explorer</i>	Todas as configurações definidas pelo usuário para o Windows NT Explorer.
<i>Barra de tarefas</i>	Todos os grupos de programas pessoais e suas propriedades, e todas as configurações da Barra de tarefas.
<i>Configurações de impressoras</i>	Conexões de impressoras da rede.
<i>Painel de controle</i>	Todas as configurações definidas pelo usuário feitas no Painel de controle.
<i>Acessórios</i>	Todas as configurações de aplicativos específicas de usuários que afetem o ambiente Windows NT do usuário, incluindo Calculadora, Relógio, Notepad, Paint e HyperTerminal, entre outras.
<i>Aplicativos baseados</i>	Qualquer aplicativo desenvolvido especificamente para o Windows <i>no Windows NT</i> pode ser projetado para que este monitore as configurações de aplicativo para cada usuário. Se esta informação existir, ela é gravada no perfil de usuário.
<i>Indicadores da Ajuda</i>	Todos os indicadores inseridos no sistema de Ajuda do <i>on-line</i> Windows NT.

Estrutura dos perfis (profiles)



Todos os perfis de usuário iniciam com uma cópia do Usuário Padrão, um perfil Default User armazenado em todos os computadores executando o Windows NT Workstation ou o Windows NT Server. A pasta de perfil Default User, as pastas de perfil de usuário de cada usuário e as pastas de perfil All Users estão localizadas na pasta Profiles na raiz do sistema (normalmente C:\Winnt). A pasta Default User e as pastas individuais de perfil de usuário contêm um arquivo NTuser.dat mais uma pasta de vínculos com itens da Área de trabalho.

As pastas de perfis de usuário contêm vínculos para vários itens da Área de trabalho.

Pasta de perfil de usuário Conteúdo

Dados de aplicativos

Dados de aplicativo específicos. Por exemplo, um dicionário personalizado. Os fabricantes de aplicativos decidem quais dados são armazenados na pasta User Profile.

Desktop

Itens da Área de trabalho, incluindo arquivos e atalhos.

Favoritos

Atalhos para itens de programas e localidades favoritas.

Ambiente de rede

Atalhos para itens do Ambiente de rede.

Pessoal

Atalhos para itens de programas.

Ambiente de Impressão

Atalhos para itens da pasta de impressoras.

Recent

Atalhos para os itens utilizados mais recentemente.

SendTo

Atalhos para itens de documentos.

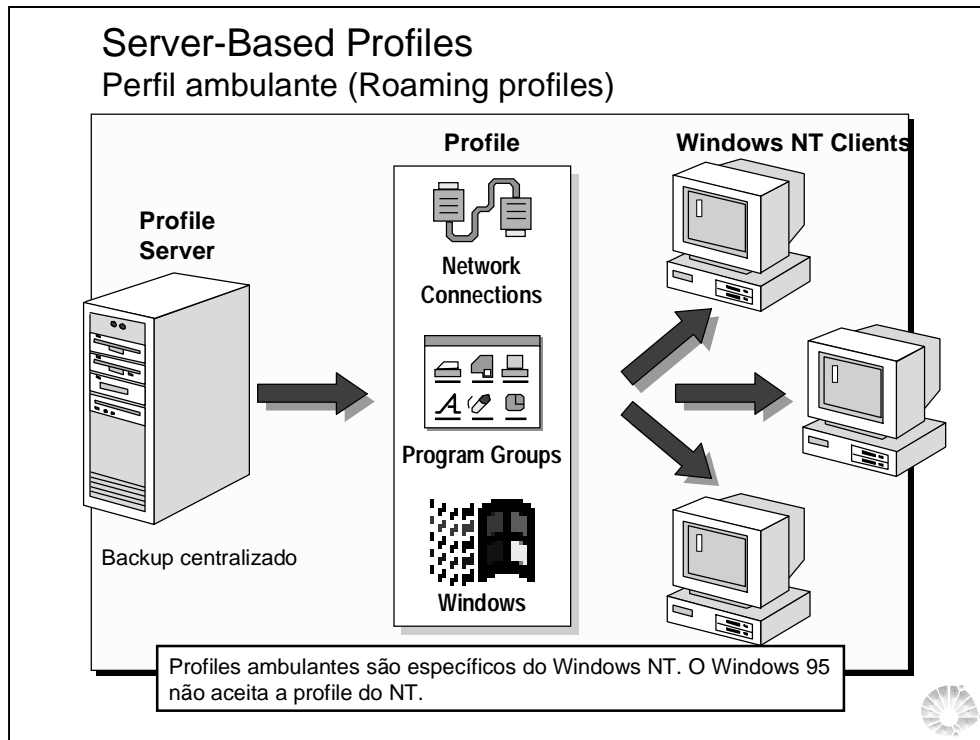
Menu Iniciar

Atalhos para itens de programas.

Modelos

Atalhos para itens de modelos.

Observação As pastas Ambiente de Rede, Ambiente de Impressão, Recent e Modelos são ocultas e, como padrão, não aparecem no Windows NT Explorer. Para visualizar essas pastas e seus conteúdos no Windows Explorer, clique em Opções no menu Exibir e, em seguida, clique em Mostrar todos os arquivos.



Os perfis de usuário ambulantes podem ser implementados de três maneiras:

Adicione um caminho para o perfil de usuário para cada conta de usuário, para criar automaticamente uma pasta de perfil de usuário vazia, nomeada para o usuário na localização do servidor, e para permitir que os usuários criem seus próprios perfis de usuário.

- Adicione um caminho para o perfil de usuário para cada conta de usuário e copie um perfil de usuário pré-configurado para o caminho para o perfil de usuário especificado em cada conta de usuário.

- Adicione um caminho para o perfil de usuário para cada conta de usuário, copie um perfil de usuário pré-configurado para o caminho para o perfil de usuário especificado em cada conta de usuário e, em seguida, renomeie o arquivo NTuser.dat para NTuser.man no caminho para o perfil de usuário especificado em cada conta de usuário. Isso cria um perfil de usuário obrigatório.

No Gerenciador de usuários para domínios, você pode designar uma localização no servidor para perfis de usuário. Se você inserir um caminho para o perfil de usuário em uma conta de usuário do domínio, uma cópia do perfil de usuário local do usuário será gravada, tanto localmente quanto na localização do caminho para o perfil de usuário, quando o usuário efetuar o logoff. Da próxima vez que o usuário efetuar logon, o perfil de usuário na localização do caminho para o perfil de usuário será comparado com a cópia na pasta de perfil de usuário local, e a cópia mais recente do perfil de usuário será aberta. O perfil de usuário local torna-se um perfil de usuário ambulante devido à localização de domínio centralizada. Estará disponível em qualquer lugar em que o usuário efetuar logon, desde que o servidor esteja disponível.

Se o servidor não estiver disponível, a cópia em cache local do perfil de usuário ambulante será utilizada. Se o usuário não efetuou logon no computador anteriormente, um novo perfil de usuário local será criado. Em ambos os casos, se o perfil de usuário armazenado centralmente não estiver disponível por ocasião do logon, ele não será atualizado quando o usuário efetuar logoff. Se o perfil de usuário não for carregado devido a problemas do servidor, ele não será carregado de volta quando o usuário efetuar o logoff. Da próxima vez que o usuário efetuar logon, deverá especificar qual perfil de usuário utilizar a cópia em cache local mais nova do perfil de usuário ou a cópia mais antiga armazenada centralmente.

Para criar um perfil de usuário ambulante pré-configurado, utilize o Gerenciador de usuários para domínios para designar uma localização de servidor para um perfil de usuário e, em seguida, utilize a guia Perfis de usuário da opção Sistema no Painel de controle para copiar um perfil de usuário pré-configurado para o servidor. Da primeira vez que o usuário efetuar o logon, em lugar de obter uma cópia do Perfil Padrão, obterá uma cópia do perfil de usuário pré-configurado a partir do servidor. Daí em diante, o perfil de usuário funciona exatamente como um perfil de usuário ambulante padrão. A cada vez que o usuário efetuar o logoff, o perfil de usuário é gravado localmente e copiado também no servidor.

Observação Para copiar um perfil de usuário, você deve utilizar a guia Perfis de usuário da opção Sistema no Painel de controle. Você não pode utilizar o Windows NT Explorer nem qualquer outra ferramenta de gerenciamento de arquivos.

Um perfil de usuário obrigatório é apenas um perfil de usuário ambulante pré-configurado que o usuário não pode atualizar. Ele ainda pode modificar a Área de trabalho, mas as alterações não são gravadas quando ele efetua o logoff. Da próxima vez que o usuário efetuar logon, o perfil de usuário obrigatório é carregado novamente. Os perfis de usuário tornam-se obrigatórios quando você renomeia o arquivo NTuser.dat no servidor para NTuser.man. Essa extensão torna o perfil de usuário somente leitura.

O mesmo perfil de usuário obrigatório pode ser utilizado pelo número de usuários que for necessário.

Dica Quando for desejável ter controle sobre as escolhas e estilos de trabalho dos usuários, seja por uma questão de segurança ou para compensar as habilidades com computadores dos usuários, o plano do sistema oferece mais opções de controle. Você pode selecionar um subconjunto de configurações para controlar e pode, também, controlar ambas as configurações, de usuário e de computador.

Copiando o perfil para o servidor



Para fornecer um perfil de usuário específico para alguns usuários, copie o perfil de usuário no local adequado executando o Painel de controle, escolhendo Sistema e, em seguida, selecionando a guia Perfis de usuário. Esse local deve coincidir com a entrada Caminho para o perfil de usuário para a conta do usuário no Gerenciador de usuários para domínios.

Na guia Perfis de usuário na caixa de diálogo Propriedades do sistema, todos os perfis de usuário que foram criados no computador são listados na caixa Perfis armazenados neste computador.

Para copiar um perfil de usuário específico, clique em Copiar para e, em seguida, digite o nome da pasta de destino ou procure-o na rede.

Scripts

☐ **O que são logon Scripts ?**

☐ **Quando atuam ?**

☐ **Utilidade**

☐ **Diretório container**

`%systemroot%\system32\Repl\Import\Scripts`

- Configura conexões de impressora e drives de rede para clientes que não sejam Windows NT

- Não configura o desktop (ambiente) do usuário



Você atribui um script de logon em uma conta de usuário ou conta de grupo inserindo um caminho para o arquivo de script de logon no Gerenciador de usuários para domínios. Quando um usuário efetua o logon e um caminho para um script de logon está presente na conta de usuário, o arquivo é localizado e executado no logon.

Na caixa de diálogo Perfil de ambiente de usuário, você pode atribuir scripts de logon a contas de usuário digitando o nome de arquivo (por exemplo, Clerks.bat) na caixa Nome do script de logon. No logon, o servidor que está autenticando-o localiza o script de logon (se algum estiver atribuído) procurando pelo arquivo especificado em seguida ao caminho do script de logon local daquele servidor (geralmente C:\WINNT\System32\Repl\Import\Scripts). Se um caminho relativo for fornecido antes do nome de arquivo (por exemplo, Admins\CristalW.bat), o servidor procurará pelo script de logon nessa subpasta do caminho do script de logon.

A entrada na caixa Nome do script de logon especifica somente o nome de arquivo (e opcionalmente o caminho relativo) e não cria o script de logon real. Você cria um script de logon do nome especificado e o coloca na pasta apropriada do servidor de exportação de duplicação apropriado.

Você pode inserir um script de logon em uma pasta local de um computador de usuário, mas em geral você utiliza essa localização quando está administrando contas de usuário que existem em um único computador e não em um domínio. Nesse caso, você deve inserir o script de logon em seguida ao caminho do script de logon do computador ou em uma subpasta desse caminho do script de logon.

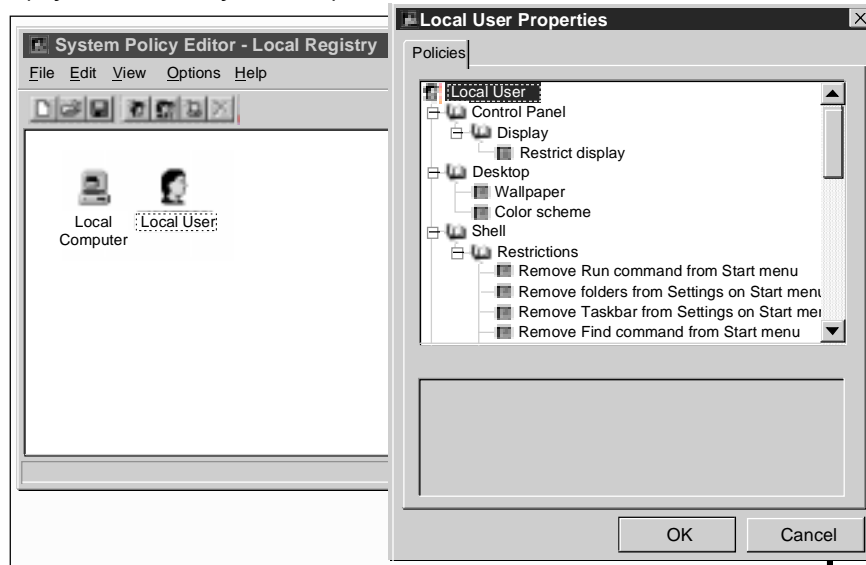
O caminho do script de logon para um computador Windows NT é `raizdosistema\System32\Repl\Import\Scripts`.

System Policy Editor

- ❑ **Políticas de usuário vs. De computador**
- ❑ **Usando políticas para criar estações seguras**
- ❑ **Entendendo as políticas de sistema**



Planos do sistema (System Policy Editor)



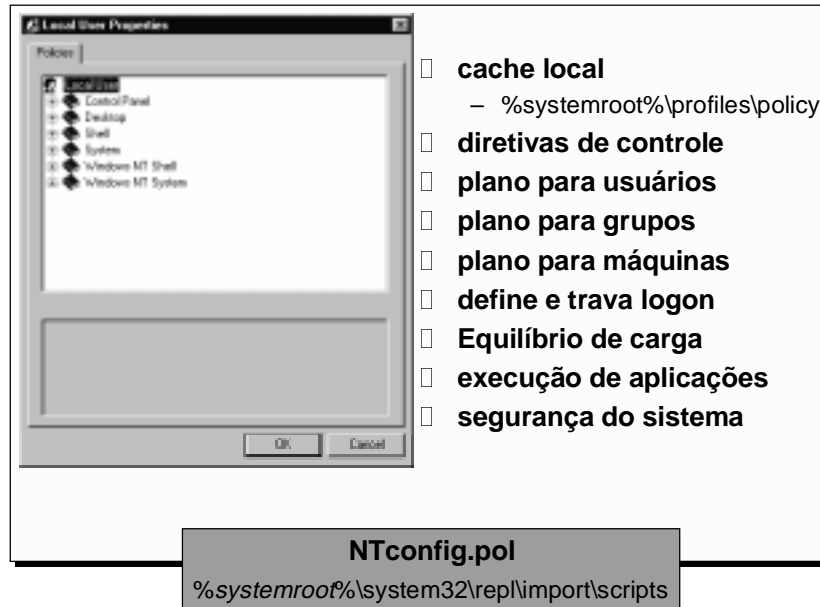
Complemento para a segurança sobre os atos do usuário



Em computadores executando o Windows NT Workstation ou o Windows NT Server, o conteúdo do perfil de usuário é tomado da parte de usuários do Registro do Windows NT. Outra parte do Registro, a do computador local, contém as definições de configuração que podem ser gerenciadas, juntamente com os perfis de usuário, utilizando o Editor de diretivas do sistema. Com essa ferramenta, você cria as diretivas do sistema, para controlar os ambientes de trabalho e ações do usuário e para reforçar a configuração do sistema para todos os computadores executando o Windows NT Workstation e o Windows NT Server.

Com as diretivas do sistema, você pode controlar alguns aspectos de ambientes de trabalho de usuário sem impor as restrições de um perfil de usuário obrigatório. Você pode restringir o que os usuários podem fazer a partir da Área de trabalho; como restringir algumas opções do Pannel de controle, personalizar partes da Área de trabalho ou configurar as definições da rede.

Detalhes sobre a configuração dos planos de sistema



As configurações da Área de trabalho nos perfis de usuário, assim como as configurações de logon e acesso à rede, são armazenadas no banco de dados do Registro do computador. As diretivas do sistema para usuários sobrescrevem as configurações na área do usuário atual do registro, e as diretivas do sistema para computadores sobrescrevem a área da máquina local atual do Registro. Isso permite que você controle as ações do usuário (perfis de usuário) assim como as ações do computador para usuários e grupos. No Editor de diretivas do sistema, você gerencia a Área de trabalho do usuário alterando as configurações de Usuário padrão, e gerencia as configurações de logon e da rede alterando as configurações de Computador padrão.

Utilizando o Editor de diretivas do sistema, você cria um arquivo denominado NTConfig.pol que contém as configurações para usuários (perfis de usuário) e computadores (configurações de logons e de acesso à rede). Para ativar um plano uniforme para todos os computadores da rede executando o Windows NT Server, Windows NT Workstation, você salva esse arquivo na pasta Netlogon na pasta raiz do sistema do controlador do domínio primário: \\nomeservidorPDC\Netlogon.

Quando um usuário efetua o logon em qualquer computador da rede que esteja executando o Windows NT, o sistema operacional procura na pasta Netlogon na pasta raiz do sistema do servidor de logon para verificar se existe um arquivo NTConfig.pol presente. Se o arquivo for encontrado, o conteúdo do arquivo será copiado para o registro do computador local e utilizado para sobrescrever as partes do usuário e máquina local atuais do registro.

As entradas do Editor de diretivas do sistema alteram as configurações do registro do computador local das seguintes maneiras:

- As configurações da Área de trabalho para Usuário Padrão no Editor de diretivas do sistema modificam a chave HKEY_CURRENT_USER no registro, que define o conteúdo do perfil de usuário em efeito para o computador.
- As configurações de logon e acesso à rede para Computador Padrão no Editor de diretivas do sistema modificam a chave HKEY_LOCAL_MACHINE no registro.

Quando um usuário efetua o logon para o domínio, o conteúdo do arquivo NTConfig.pol no servidor é mesclado com o arquivo NTuser.dat encontrado na localização do perfil de usuário para o usuário que está efetuando logon. As configurações do NTuser.dat que não coincidem com as configurações do NTConfig.pol são sobrescritas e, assim, as diretivas do sistema controla as configurações de perfil de usuário para todo o domínio. As configurações de Computador Padrão que não estiverem contidas no perfil de usuário serão adicionadas à seção de máquina local do Registro.

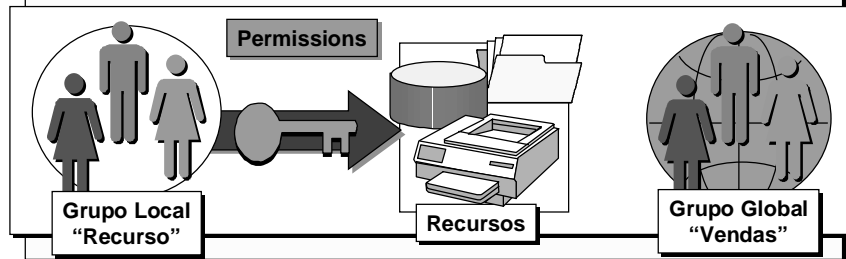
Tópicos

- **Introdução a grupos**
- **Estratégia de grupos**
- **Grupos Globais e Locais**
- **Implementando grupos “*Built-in*”**



Introdução a grupos

- ❑ Grupos são conjuntos de contas de usuários
- ❑ Os membros de um grupo herda as permissões e direitos cedidos ao grupo
- ❑ Grupos locais estão ligados à permissões e direitos para desempenham tarefas no sistema
- ❑ Grupos globais organiza os usuários



Contas de grupo são coleções de contas de usuário. Dar a uma conta de usuário uma participação em um grupo dá a esse usuário todos os direitos e permissões concedidos ao grupo. A participação em grupo proporciona um meio fácil de conceder capacidades comuns a conjuntos de usuários.

Uma vez que a manutenção de permissões de um grupo é mais fácil que a manutenção de permissões para várias contas de usuário, em geral é preferível usar grupos para gerenciar acesso a recursos (como pastas, arquivos ou impressoras):

- Atribua permissões de recurso a um grupo e, então, adicione contas de usuário a esse grupo, conforme desejado.
- Altere as permissões fornecidas a um grupo de usuários, adicione ou remova as permissões atribuídas ao grupo, mas não altere cada conta

Observação Ao atribuir capacidades de usuário, lembre-se de tirar proveito dos grupos internos fornecidos com o Windows NT, que receberam conjuntos de direitos e capacidades. (Por exemplo, membros do grupo Administradores têm capacidades administrativas no domínio e sobre os servidores do domínio).

Tipos de grupos

□ Local Groups

- Implementados localmente, relacionado ao recurso
- Incluem usuários e outros grupos globais de qualquer domínio

□ Global Groups

- Implementado globalmente, relacionado a divisão lógica de usuários
- Incluem somente contas do banco de contas local

□ Special Groups

- São grupos com direitos pré-definidos



Um grupo global contém um número de contas de usuários de um domínio que são agrupadas sob um único nome de conta de grupo. Um grupo global pode conter somente contas de usuário do domínio onde o grupo global foi criado. Uma vez criado um grupo global, ele pode receber permissões e direitos em seu próprio domínio, em estações de trabalho ou em servidores de membros, ou em domínios confiáveis. Entretanto, é melhor conceder direitos e permissões a grupos locais e utilizar o grupo global como um método de adicionar usuários a grupos locais.

Grupos globais podem ser adicionados a grupos locais no mesmo domínio, em domínios que confiam naquele domínio, ou a servidores de membros ou computadores executando o Windows NT Workstation no mesmo domínio ou em um domínio confiável. Grupos globais contêm somente contas de usuário de domínio. Você não pode criar um grupo global em um computador executando o Windows NT Workstation ou em um computador executando o Windows NT Server como servidor membro.

O termo “globais” em “grupos globais” indica que o grupo está disponível para receber direitos e permissões em múltiplos domínios (globais).

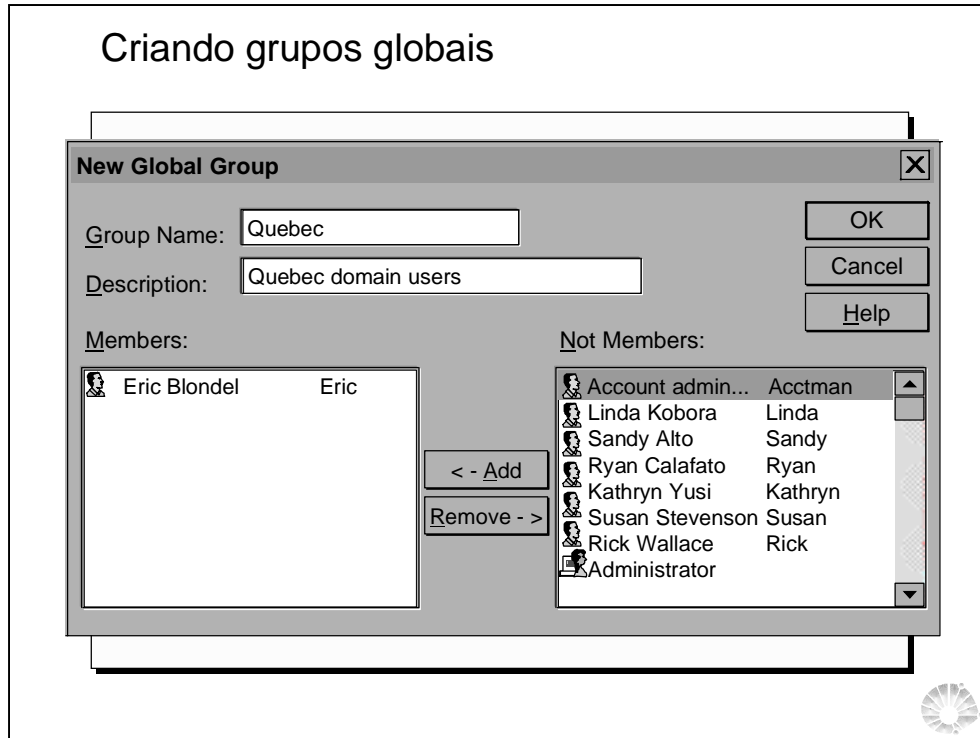
Um grupo local contém contas de usuário e contas de grupo global de um ou mais domínios, agrupados sob um único nome de conta de grupo. Usuários e grupos globais de fora do domínio local podem ser adicionados ao grupo local somente se pertencerem a um domínio confiável. Grupos locais tornam possível atribuir rapidamente direitos e permissões dos recursos de um domínio (isto é, o domínio local) a usuários e grupos daquele domínio e a outros domínios que confiam nele.

Grupos locais também existem em servidores de membros e computadores executando o Windows NT Workstation e podem conter contas de usuário e grupos globais.

O termo “locais” em “grupos locais” indica que o grupo está disponível para receber permissões e direitos somente em um único domínio (local).

Um grupo local não pode conter outros grupos locais.

Criando grupos globais



Para criar e definir grupos adicionais, use o Gerenciador de usuários para domínios:

- Crie novos grupos locais para conceder permissões para recursos.
- Crie novos grupos globais para organizar usuários com base no tipo de trabalho que fazem.

Por exemplo, suponhamos que você tenha uma impressora colorida no seu domínio e queira restringir o acesso a ela:

1. Crie um grupo local que tenha permissão para imprimir na impressora colorida.
2. Crie um grupo global que consiste de usuários que têm permissão para usar a impressora colorida.
3. Adicione o grupo global ao grupo local.
4. Adicione ou remova as pessoas que podem usar a impressora alterando a participação em grupos do grupo global.

Se quiser que os membros desse grupo sejam capazes de usar uma impressora conectada a uma determinada estação de trabalho ou a um determinado servidor de grupos, adicione o grupo global ao grupo local que governa a impressão naquele computador. Da mesma forma, se uma impressora colorida estiver disponível em um domínio confiante, você coloca o grupo global em um grupo local naquele domínio.

Para obter informações sobre como gerenciar permissões de recurso, consulte o capítulo 4, “Gerenciando os recursos compartilhados e a segurança dos recursos”.

Durante a adição de um grupo, você fornecerá um nome de grupo. Ele deve ser exclusivo ao domínio ou ao computador que está sendo administrado. O nome de um grupo global pode conter até 20 caracteres. Também pode conter qualquer caractere em maiúscula ou minúscula, exceto:

" / \ [] : ; | = , + * ? < >

O nome de um grupo local pode conter até 256 caracteres. Também pode conter qualquer caractere em maiúscula ou minúscula, exceto o caractere barra invertida (\).

Criando grupos locais

New Local Group

Group Name: Sales

Description: Sales Personnel

Members:

StefanH

OK

Add Users and Groups

List Names From: CLASSROOM*

Names:

Account Operators

Administrators

Backup Operators

Domain Admins

Domain Guests

Domain Users

Everyone

Guests

Members can administer domain user al

Members can fully administer the compu

Members can bypass file security to bac

Designated administrators for the doma

All domains guests

All domains users

All Users

Users granted quest access to the comp

Add

Show Users

Members...

Search...

Add Names:

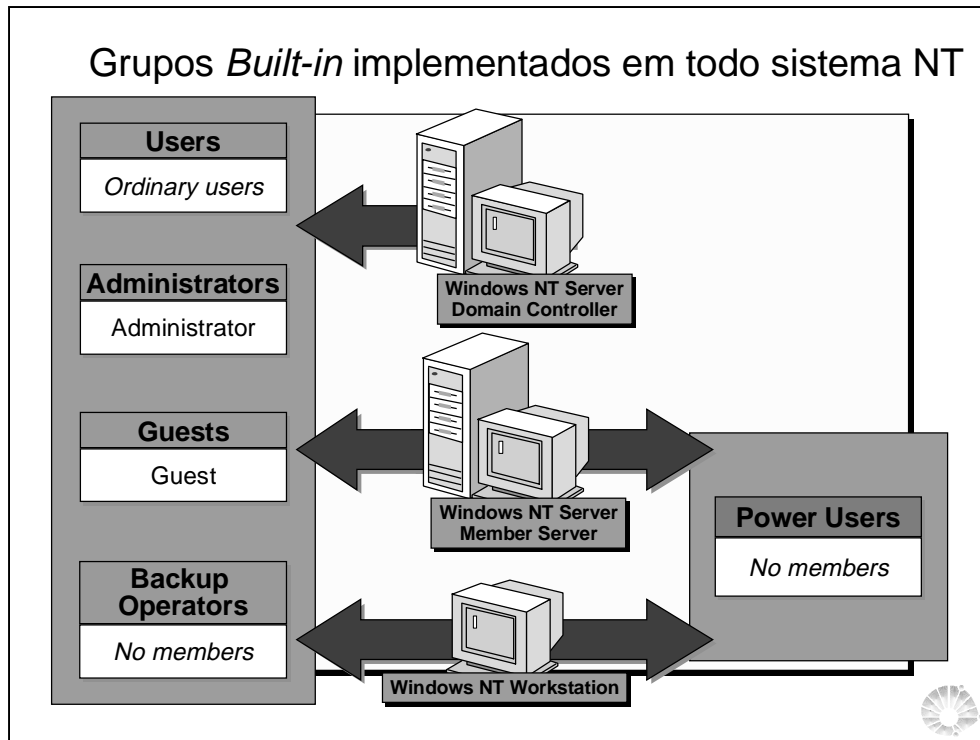
CLASSROOMDomain Users

Type of Access: Read

OK

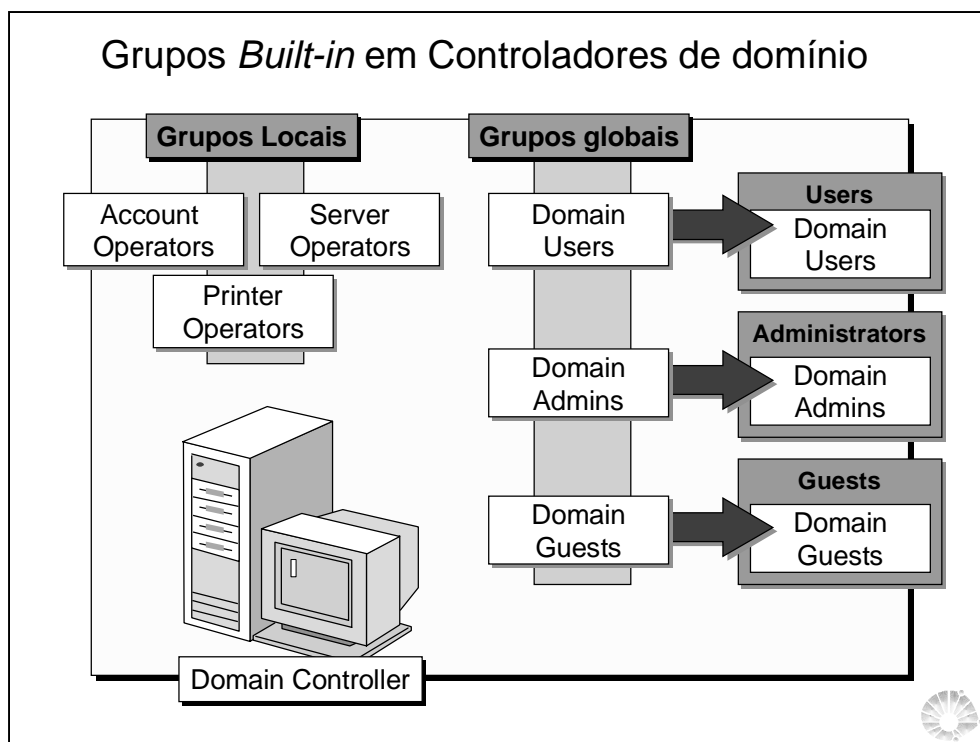
Cancel

Help



Direitos de usuário são regras que determinam as ações que um usuário pode executar em controladores de domínio, estações de trabalho ou servidores membros. Além disso, controlam se um usuário pode efetuar login em um computador diretamente (localmente) ou na rede, adicionar usuários a uma estação de trabalho ou grupo de domínios, excluir usuários, etc. Quando você atribui direitos do usuário, esses direitos se aplicam a todos os controladores de domínio em um domínio (o que os usuários podem fazer em qualquer PDC ou BDC) ou a um computador executando o Windows NT Workstation ou um computador executando o Windows NT Server como um servidor membro (o que os usuários podem fazer naquele computador específico).

Grupos predefinidos (internos) têm conjuntos de direitos de usuário já atribuídos. Os administradores geralmente atribuem os direitos de usuário pela adição de uma conta de usuário a um dos grupos predefinidos ou pela criação de um novo grupo e atribuição de direitos de usuário específicos àquele grupo. Os usuários que são posteriormente adicionados a um grupo ganham automaticamente todos os direitos de usuário atribuídos à conta de grupos. Usuários individuais podem receber direitos de usuário específicos; contudo, a maioria dos administradores prefere controlar ações com base em grupos ao invés de usuários individuais.



Ser um membro de um dos grupos locais internos de um domínio dá a um usuário os direitos e capacidades de executar várias tarefas nos controladores de domínio no domínio. Da mesma forma, ser membro de um grupo local interno em um servidor membro ou estação de trabalho dá ao usuário os direitos e capacidades nesse computador.

Você pode adicionar um usuário a mais de um grupo interno. Por exemplo, um usuário nos grupos Operadores de Impressão e Operadores de Backup tem todos os direitos concedidos a operadores de impressão e todos os direitos concedidos a operadores de backup.

Entretanto, nem todos os grupos locais existem simultaneamente nos controladores de domínio do Windows NT Server e em computadores individuais com Windows NT (computadores com Windows NT Workstation e servidores de membros com o Windows NT Server). A tabela abaixo mostra os grupos locais internos existentes em controladores de domínio e em computadores individuais.

Controladores de domínio

do Windows NT Server

Estações de trabalho e servidores

de membros do Windows NT

Administradores Administradores

Operadores de Backup

Operadores de Backup

Operadores de Servidor

Usuários Avançados

Operadores de Contas

Usuários

Operadores de Impressão

Convidados

Usuários

Duplicadores

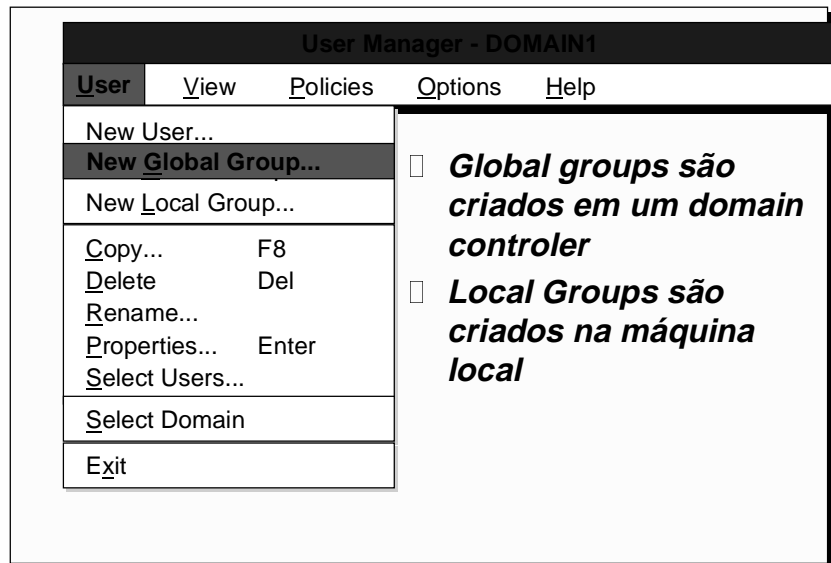
Convidados

Duplicadores

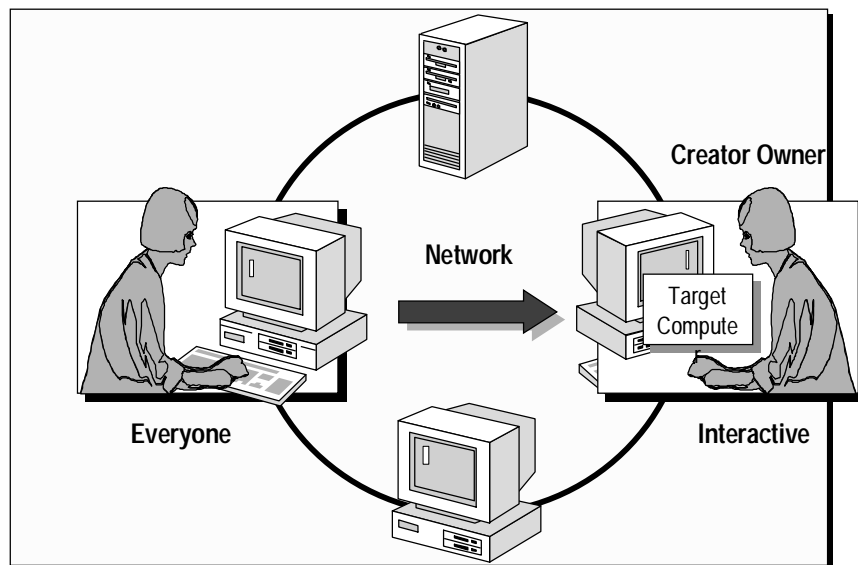
Por padrão, todo novo usuário de domínio (global ou local) é membro do grupo global Usuários do Domínio, que é membro do grupo local interno Usuários. Cada novo usuário da estação de trabalho ou do servidor membro é um membro do grupo local interno Usuários no computador.

Em geral, você desejará adicionar usuários administradores de um domínio ao grupo global Admins. do Domínio, em vez de adicioná-los diretamente ao grupo local Administradores. Ao serem adicionados ao Admins. do Domínio, os usuários também se tornam administradores em estações de trabalho e servidores de membros.

Criando grupos



Grupos especiais

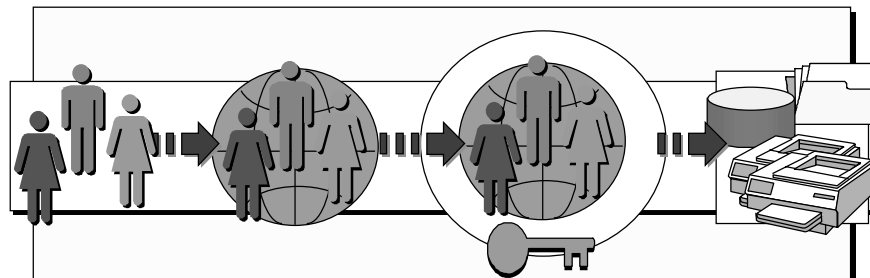


Além dos grupos internos mencionados, grupos são criados pelo sistema e usados para fins especiais. Já que, nesses grupos, a participação em grupos não pode ser alterada, os grupos não estão listados no Gerenciador de usuários para domínios.

Entretanto, quando você administra um computador e o Windows NT apresenta listas de grupos, esses grupos especiais às vezes aparecem na lista. Por exemplo, eles podem aparecer durante a atribuição de permissões a pastas, arquivos, pastas de rede compartilhadas ou impressoras.

Grupo	Refere-se a
Todos	Qualquer pessoa utilizando o computador. Inclui todos os usuários locais e remotos (isto é, os grupos Interativo e Rede combinados). Em um domínio, membros de Todos podem, por padrão, acessar a rede, conectar-se a pastas de rede compartilhadas de um servidor e imprimir em impressoras de um servidor.
Interativo	Qualquer pessoa utilizando o computador localmente.
Rede	Todos os usuários conectados através da rede ao computador.
Sistema	O sistema operacional.
Proprietário	Transferência de permissões a criadores de subpastas, arquivos e trabalhos de impressão.
Criador	Para uma pasta, se permissões forem concedidas ao grupo Proprietário Criador, serão concedidas ao criador de uma subpasta ou arquivo aquelas permissões para a subpasta ou arquivo em questão. Para uma impressora se permissões forem concedidas ao grupo Proprietário Criador, serão concedidas ao criador de um trabalho de impressão aquelas permissões para o trabalho de impressão em questão.

Estratégia de utilização de grupos - AGLP



- ☐ **Organize os usuários logicamente de acordo com as necessidades comuns**
- ☐ **Adicionar Usuarios nos grupos Globais**
- ☐ **Criar grupos locais ligados aos recursos necessários**
- ☐ **Ceder permissões ao grupo local**
- ☐ **Adicionar grupos globais em grupos locais**



Um grupo local é uma única entidade de segurança a quem pode ser concedido o acesso a vários objetos em um único local (um domínio, ou uma estação de trabalho ou servidor membro), em vez de ser necessário editar as permissões sobre todos esses objetos separadamente.

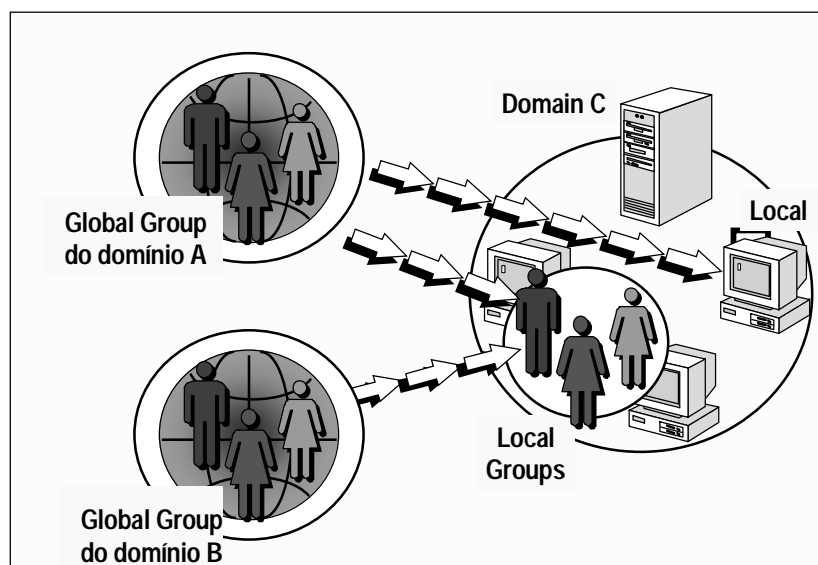
Com grupos globais, você pode agrupar contas de usuário às quais poderiam ser concedidas permissões para usar objetos em vários domínios e estações de trabalho.

Por exemplo, numa configuração de múltiplos domínios, você pode pensar em grupos globais como um meio de adicionar usuários aos grupos locais de domínios confiantes. Para estender os direitos e permissões a recursos em outros domínios, adicione suas contas a um grupo global no domínio e, então, adicione o grupo global a um grupo local em um domínio confiante.

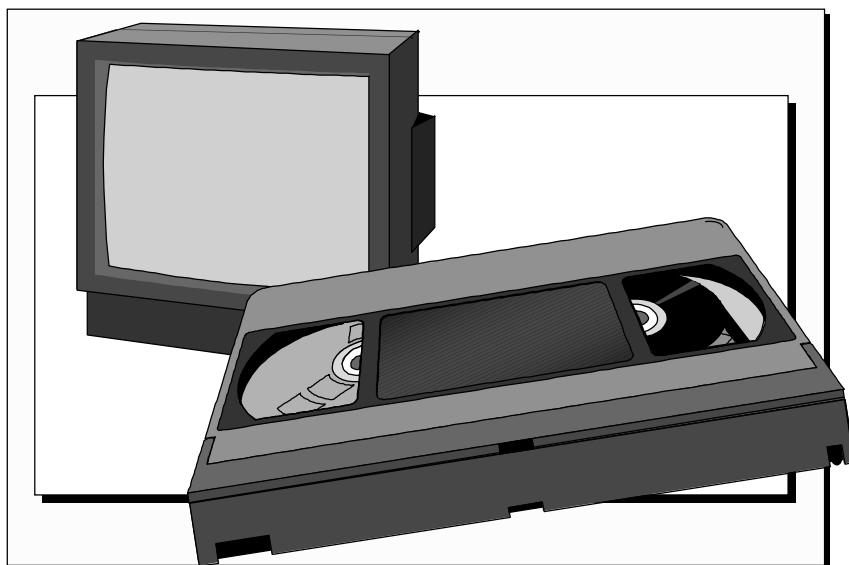
Mesmo para um único domínio, se você tiver em mente que domínios adicionais poderão ser adicionados no futuro, poderá usar os grupos globais adicionados aos grupos locais para conceder todos os direitos e permissões. Mais tarde, se for criado um outro domínio, os direitos e permissões atribuídos aos grupos locais poderão ser estendidos aos usuários de um novo domínio através da criação de uma relação de confiança e da adição dos grupos globais do novo domínio aos grupos locais. Da mesma forma, se o novo domínio confia em seu domínio, seus grupos globais poderão ser adicionados aos novos grupos locais do domínio.

Grupos globais de domínio também podem ser usados para fins administrativos em computadores executando o Windows NT Workstation ou servidores de membros executando Windows NT Servers. Por exemplo, o grupo global Admins. do Domínio é adicionado por padrão ao grupo local interno Administradores em cada estação de trabalho ou servidor membro que se associa ao domínio existente. A participação no grupo local Administradores da estação de trabalho ou do servidor membro torna possível ao administrador da rede gerenciar remotamente o computador através da criação de grupos de programa, instalação de software e solução de problemas do computador.

Grupos no gerenciamento



Video sobre AGLP



File System

- ❑ **Sistemas de arquivos suportados pelo Windows NT**
- ❑ **Gerenciando compressão NTFS**

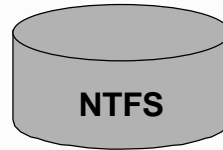
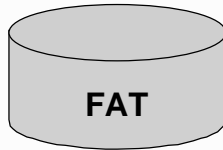


File Systems suportados pelo Windows NT

- ☐ **FAT File System**
- ☐ **NTFS**
- ☐ **NTFS considerações de implementação**
- ☐ **Comparação entre sistema de arquivos**
- ☐ **Convertendo FAT para NTFS**



FAT File System

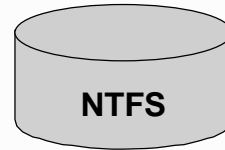
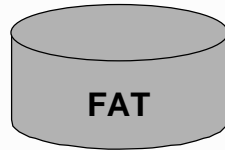


Características

- ☒ Suporta Long File Names
- ☒ Sem segurança local
- ☒ Tamanho máximo da partição: 4 GB



NTFS

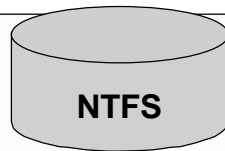


Características

- ☒ suporta Long File Names
- ☒ Suporta segurança local
- ☒ Tamanho da partição:
16 Exabytes (theoretical)
2 Terabytes (actual)



NTFS Implementation Considerations



Considerações de implementação

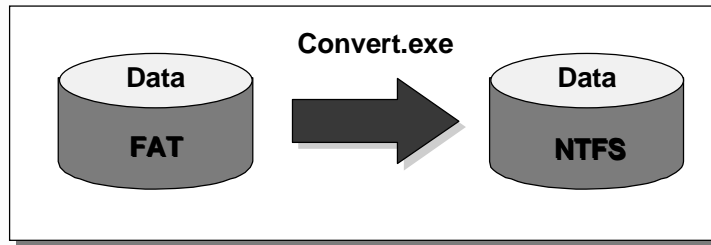
- ☒ Recoverability é desenvolvido para NTFS
- ☒ NTFS implementa segurança para arq. e dirs.
- ☒ Cria um Recycle Bin para cada usuário
- ☒ Não formata floppy discos com NTFS
- ☒ Fragmentação é reduzida



Convertendo uma partição FAT para NTFS

■ Usar o comando Convert.exe

- Conversão não é reversível
- Dados não são perdidos na conversão



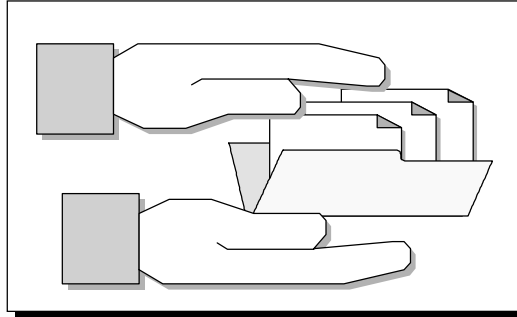
Se você quiser alterar o sistema de arquivos de uma partição existente, deve efetuar backup das informações contidas na partição.

Se o Windows NT não estiver instalado na partição, utilize o comando Format do menu Ferramentas do Administrador de discos para reformatar essa partição com um outro sistema de arquivos. Ou você pode também utilizar o programa de formatação no prompt de comando. Entretanto, reformatar a partição irá também destruir todos os dados existentes.

Se você deseja alterar o sistema de arquivos de uma partição FAT existente para o formato NTFS, pode utilizar o programa de conversão no prompt de comando. A utilização do programa Convert não grava sobre os dados do disco. Esse programa não pode ser utilizado para converter uma partição NTFS para FAT.

Compressão NTFS

- **Arquivos e diretórios podem ser comprimidos**
- **Arquivos comprimidos copiados não mantêm a compressão, os movidos mantêm**

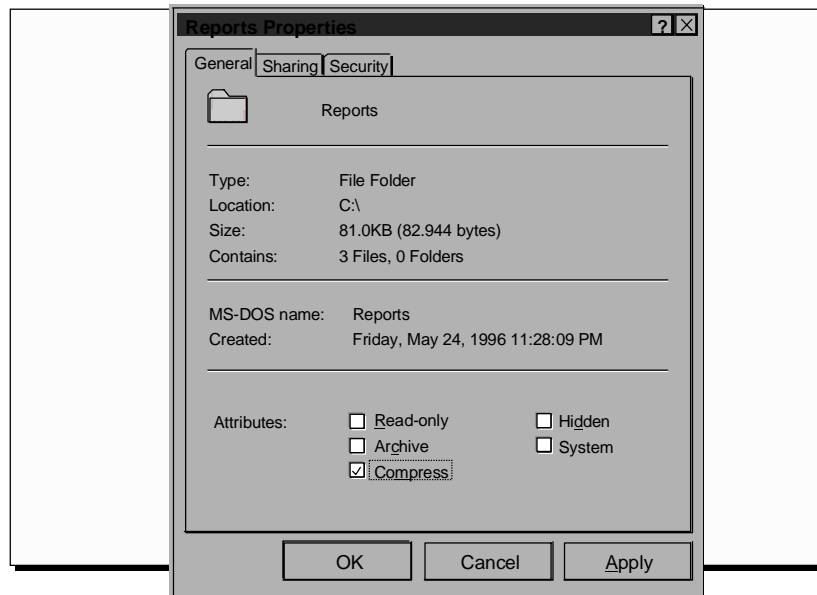


Os arquivos em volumes NTFS (mas não em volumes FAT) podem ser compactados e descompactados por meio do Windows NT Explorer ou do utilitário de linha de comando compact. No Explorer, clique o botão direito do mouse em qualquer pasta ou arquivo e depois em Propriedades para compactar ou descompactar:

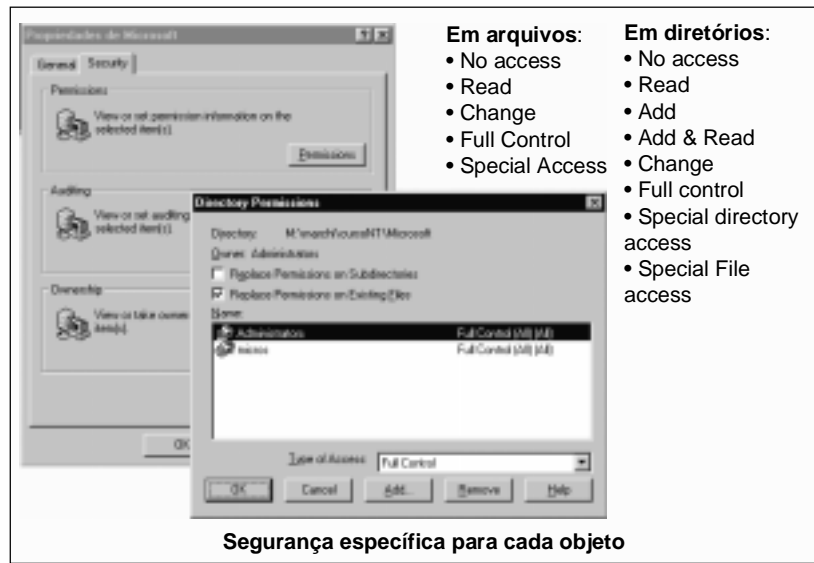
- Você pode compactar todos ou somente um arquivo de uma pasta. A compactação de uma pasta assegura que novos arquivos criados nessa pasta sejam compactados automaticamente. A sua descompactação assegura que novos arquivos criados nessa pasta sejam criados descompactados.
- Quando você copia ou move um arquivo para uma pasta ou subpasta dentro de um volume NTFS (ou de um volume NTFS para outro), o arquivo herda o estado de compactação da pasta de destino.
- Quando você move um arquivo para uma pasta ou subpasta em um volume NTFS, o arquivo retém sua compactação, independentemente da configuração de compactação do arquivo de destino.
- Quando você move um arquivo de um volume NTFS para outro, o arquivo herda a compactação do diretório de destino.
- Quando você compacta ou descompacta uma pasta, o Explorer pergunta se você deseja compactar ou descompactar as subpastas existentes na pasta selecionada. As subpastas existentes nas pastas compactados ou descompactados retêm sua compactação, a menos que você a altere.
- Você pode optar por realçar arquivos e pastas compactados em uma cor diferente clicando em Opções no menu Exibir.
- Outras operações de arquivo podem ser executadas durante a compactação e descompactação.

Para obter informações sobre como compactar e descompactar arquivos, pastas e volumes, consulte Para descompactar um arquivo em um volume NTFS e Compactando um volume NTFS na Ajuda do Windows NT.

Comprimindo e descomprimindo arquivos e diretórios



Segurança no file system



Antes de compartilhar uma pasta em um volume NTFS, defina as permissões individuais para a pasta e seus arquivos e subpastas. Cada permissão especifica o acesso que um grupo ou usuário pode ter a uma pasta ou arquivo.

O Windows NT Server oferece um conjunto de permissões padrão para pastas e arquivos NTFS. As permissões padrão são combinações de tipos específicos de acesso denominados permissões individuais. As permissões individuais e suas abreviações são:

Ler (R)	Gravar (W)	Executar (X)
Excluir (D)	Alterar Permissões (P)	Apropriar-se (O)

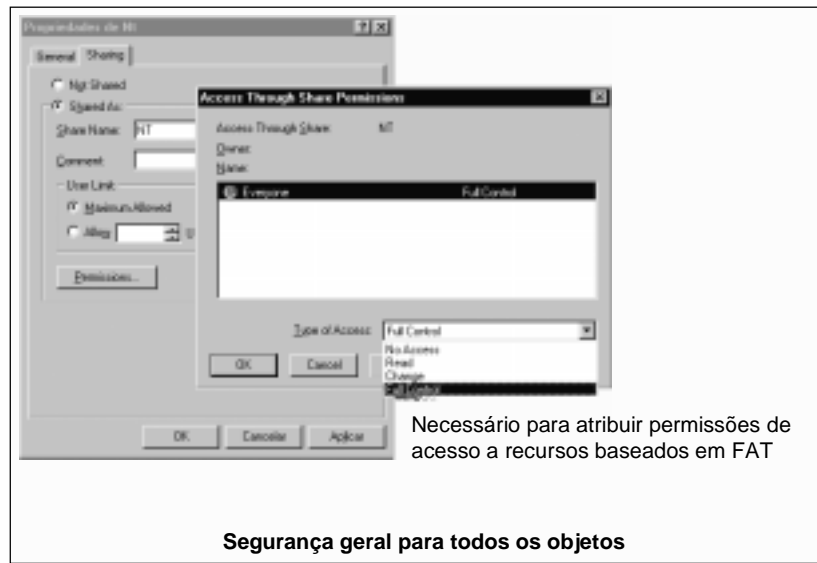
As permissões padrão e seus significados para pastas e arquivos são mostrados nas tabelas a seguir, junto às permissões individuais que representam. Na primeira coluna da primeira tabela (para permissão de pasta), o primeiro conjunto de parênteses, após a permissão padrão, indica as permissões individuais para a própria pasta. O segundo conjunto de parênteses indica as permissões individuais que se aplicam aos novos arquivos subsequentemente criados na pasta.

Quando você configura permissões para pastas e arquivos em um servidor executando o Windows NT Server, você controla o acesso a pastas e arquivos por:

- Grupos locais, grupos globais e usuários individuais no domínio que contém o servidor
- Grupos globais e usuários individuais em domínios em que esse domínio confia
- As entidades especiais Todos, Sistema, Rede, Interativo e Proprietário Criador

Você pode conceder permissões aos grupos locais internos (como Administradores e Usuários de Domínio) e a qualquer grupo que venha a criar no domínio.

Segurança no recurso compartilhado



As permissões definidas em pastas compartilhadas são chamadas de permissões de compartilhamento e elas determinam quem pode utilizar as pastas compartilhadas na rede e de que maneira.

Em volumes NTFS você pode definir permissões em pastas e arquivos e essas permissões serão aplicadas aos usuários que acessam os arquivos no servidor. Quando a pasta NTFS for compartilhada, essas mesmas permissões de arquivos e pastas serão aplicadas aos usuários que acessam as pastas compartilhadas através da rede. Portanto, Permissões Compartilhadas não são críticas para a segurança das pastas NTFS.

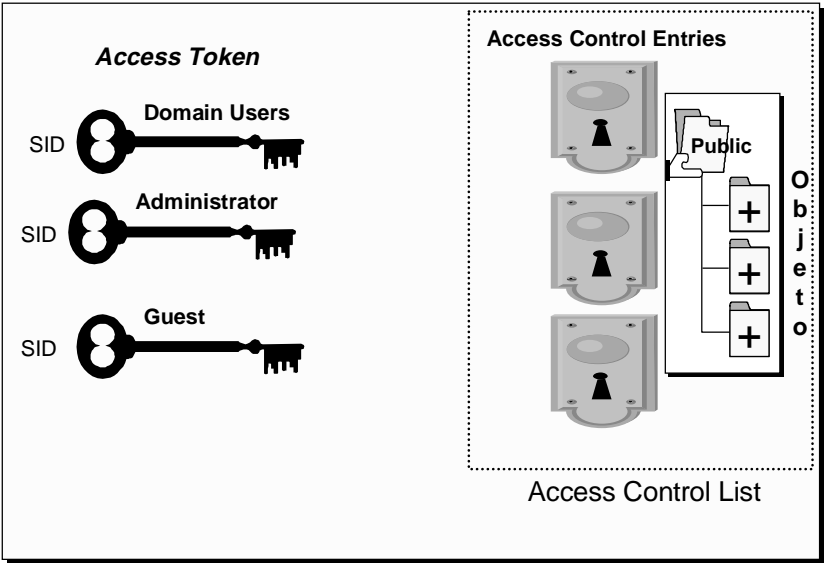
No entanto, as pastas dos volumes FAT não podem ser protegidas contra o acesso dos usuários que trabalham no próprio computador. Elas poderão ser protegidas por permissões somente depois que forem compartilhadas, sendo que as permissões afetarão somente o acesso através da rede. Para volumes FAT, as Permissões Compartilhadas fornecem o único meio de limitar o acesso aos arquivos da rede. Você pode especificar um conjunto de Permissões Compartilhadas numa pasta compartilhada que se aplique a todos os usuário para todos os arquivos e subpastas da pasta compartilhada.

O método para configurar as Permissões Compartilhadas é o mesmo, tanto para os arquivos do tipo NTFS quanto para os arquivos do tipo FAT. Use a guia Compartilhamento na folha de propriedades da pasta para definir permissões na pasta compartilhada. Quando você compartilhar uma pasta, poderá conceder a cada grupo e usuário, um dentre quatro tipos de permissões para a pasta compartilhada e todas as suas subpastas e arquivos: Controle total, Alterar, Ler, ou Sem Acesso.

Para manter eficazmente a segurança das pastas compartilhadas, tenha em mente o seguinte:

- Para trabalhar com permissões de pastas compartilhadas é necessário efetuar login como membro do grupo Administradores ou do grupo Operadores de Servidor.
- As permissões padrão definidas em um compartilhamento recém-criado são Controle total para Todos.
- As permissões definidas através de uma pasta compartilhada serão efetivas somente quando a pasta for acessada através da rede.
- As permissões definidas através de uma pasta compartilhada aplicam-se a todos os arquivos e subpastas na pasta compartilhada.
- As permissões definidas através de uma pasta compartilhada em um volume NTFS funcionam em acréscimo às permissões definidas na própria pasta.

Access Control List



Ferramentas de Administração

(Administrative Tools)



Server Manager

Utilidade

- ☐ **Visualização da Rede (diferencia cada tipo de máquina)**
- ☐ **Administração Remota - propriedades de servidor;**
- ☐ **Adicionar máquinas ao domínio;**
- ☐ **Sincronização de BDCs com PDC;**
- ☐ **Gerenciar recursos compartilhados;**
- ☐ **Explorar serviços;**
- ☐ **Mandar alertas para usuários conectados;**



Quando tiver estabelecido um ou mais domínios, você utilizará os utilitários do Windows NT Server para executar as tarefas de gerenciamento de domínio requeridas:

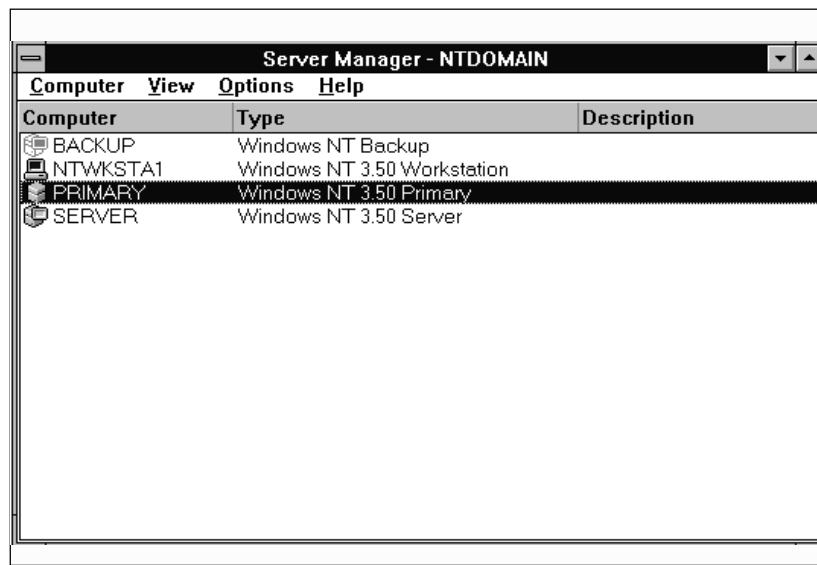
- Promoção e rebaixamento de controladores de domínio
- Sincronização de controladores de domínio reserva com o controlador de domínio primário
- Sincronização de todos os servidores do domínio
- Adição, remoção e renomeação de computadores do domínio
- Gerenciamento da segurança do domínio, inclusive diretiva de contas, diretiva de auditoria e relações de confiança (com múltiplos domínios)

Tópicos

- ❑ Ícones do Server Manager
- ❑ Gerenciando Server Properties e Services
- ❑ Adicionando e removendo computadores no domínio
- ❑ Promovendo e sincronizando Domain Controllers
- ❑ Gerenciando sessão de usuários
- ❑ Gerenciando recursos compartilhados
- ❑ Gerenciando recursos em uso



Ícones do Server Manager



The screenshot shows a window titled "Server Manager - NTDOMAIN" with a menu bar containing "Computer", "View", "Options", and "Help". Below the menu bar is a table with three columns: "Computer", "Type", and "Description". The table lists four computer icons: "BACKUP" (Windows NT Backup), "NTWKSTA1" (Windows NT 3.50 Workstation), "PRIMARY" (Windows NT 3.50 Primary), and "SERVER" (Windows NT 3.50 Server). The "PRIMARY" row is highlighted.

Computer	Type	Description
BACKUP	Windows NT Backup	
NTWKSTA1	Windows NT 3.50 Workstation	
PRIMARY	Windows NT 3.50 Primary	
SERVER	Windows NT 3.50 Server	



Organização do Domínio

- **Primary Domain Controller (PDC)**
 - Apenas um em cada domínio;
 - Contém uma cópia dominante (original) do *domain security database*;
 - Valida logon de todos os usuários do domínio;
- **Backup Domain Controller (BDC)**
 - Valida logon
 - Contém uma cópia replicada periodicamente do *domain security database*;
- **Outros Servidores**
 - Não têm função administrativa no domínio;
 - Existem para servir aplicações, dados, impressoras, etc...
 - Não podem se tornar um PDC/BDC sem reinstalar o Windows NT



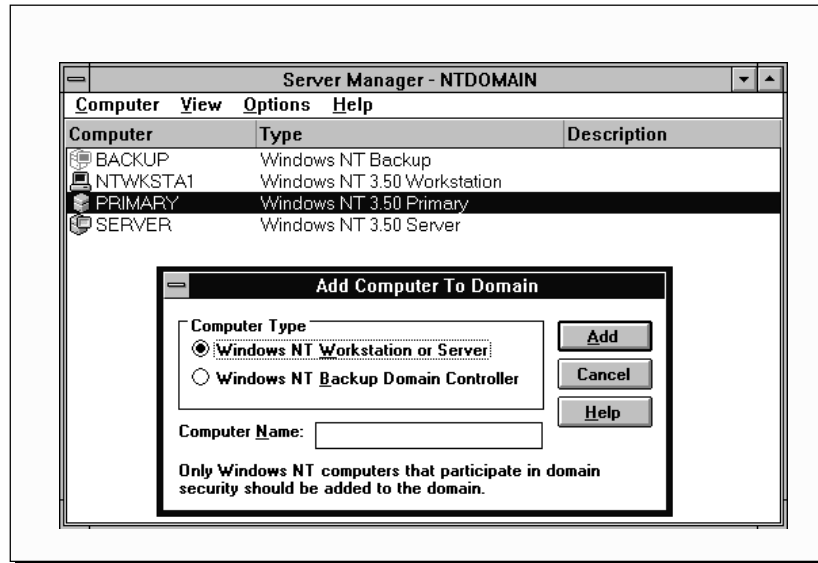
Dentro de um domínio, os controladores de domínio gerenciam todos os aspectos das interações usuário-domínio. Os controladores de domínio são computadores executando o Windows NT Server que compartilham um único banco de dados do diretório para armazenar informações sobre segurança e contas de usuários relativas a um domínio inteiro; eles constituem uma única unidade administrativa. Os controladores de domínio utilizam as informações no banco de dados do diretório para autenticar usuários que efetuam logon em contas do domínio. Existem dois tipos de controladores de domínio:

· O controlador de domínio primário (PDC, Primary Domain Controller) monitora as alterações feitas em contas do domínio. Sempre que um administrador faz uma alteração em uma conta do domínio, a alteração é registrada no banco de dados do diretório no PDC. O PDC é o único servidor do domínio que recebe essas alterações diretamente. Um domínio tem um único PDC.

· Um controlador de domínio reserva (BDC, Backup Domain Controller) mantém uma cópia do banco de dados do diretório. Essa cópia é sincronizada periódica e automaticamente com o PDC. Os BDCs também autenticam logons de usuário e um BDC pode ser promovido para que funcione como PDC. Vários BDCs podem existir em um domínio.

Você cria um domínio quando instala o Windows NT Server em um computador e designar esse computador como o PDC. Pode haver tantos BDCs quantos necessários em um domínio para compartilhar a carga para autenticar logons de rede. Em uma pequena organização, um PDC e um único BDC em um domínio podem ser tudo o que é necessário.

Adicionando e removendo computadores no domínio



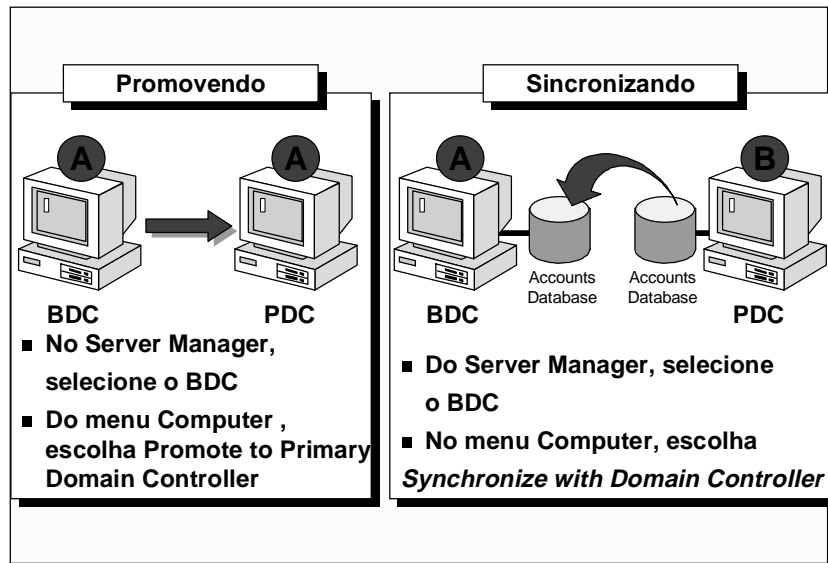
Um domínio é criado instalando-se o Windows NT Server e designando-se o computador como um controlador de domínio. Outros computadores podem então ser adicionados ao domínio.

Para que um computador executando o Windows NT Workstation ou o Windows NT Server possa ser um membro do domínio e participar da segurança do domínio, ele deve ser adicionado ao domínio. Quando um computador é adicionado a um domínio, o Windows NT Server cria uma conta para o computador. Se o computador adicionado for um controlador de domínio reserva, ele solicitará uma cópia do banco de dados do diretório do domínio.

Quando você remove de um domínio um computador executando o Windows NT Workstation ou um computador executando o Windows NT Server, a conta do computador é removida. Para adicionar um computador a um outro domínio, uma nova conta de computador deverá ser criada e, então, o computador poderá se associar àquele domínio.

Observação Para remover um controlador de domínio reserva de um domínio, você deve excluir a conta de computador e reinstalar o Windows NT Server nesse computador, indicando o novo domínio.

Promovendo e sincronizando Domain Controllers



Além do controlador de domínio primário (PDC), você deve ter um ou mais controladores de domínio reserva (BDCs) para cada domínio.

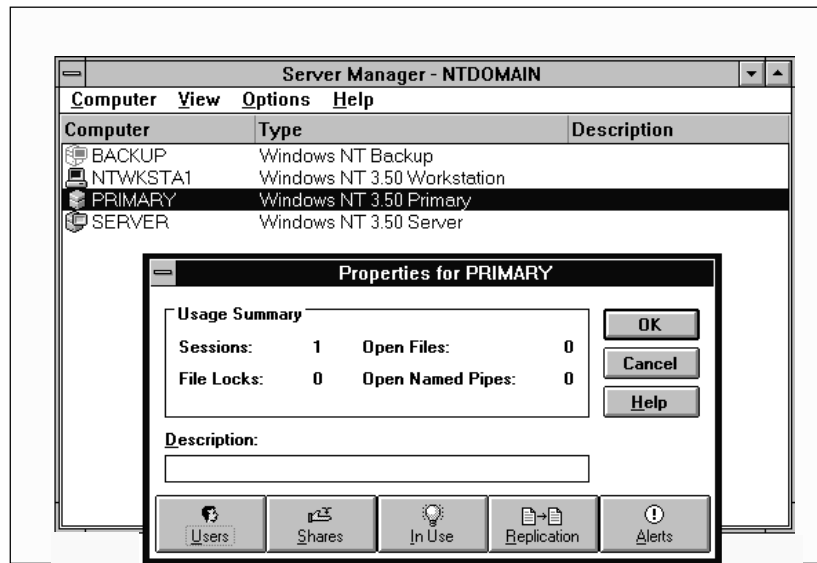
Se o PDC tornar-se indisponível, um BDC pode ser promovido a controlador de domínio primário e o domínio continuará a funcionar. Em tal cenário, as regras a seguir entram em vigor:

- Quando um BCD é promovido a PDC, uma cópia atualizada do banco de dados do diretório do domínio é replicada do antigo PDC para o novo, e o antigo PDC é rebaixado a BDC.
- Se um BDC for promovido a PDC enquanto o PDC existente estiver indisponível (por exemplo, enquanto estiver sendo consertado) e se, mais tarde, o antigo PDC retornar ao serviço, você deverá rebaixar o antigo PDC a BDC. Até que seja rebaixado a BDC, ele não executará o serviço Net Logon, não participará da autenticação de logons de usuário e seu ícone na janela Gerenciador de servidores ficará escurecido.

Observação Em geral, quando um BDC é promovido a PDC, o sistema automaticamente rebaixa o antigo PDC a BDC. Contudo, se o Gerenciador de servidores não conseguir localizar o PDC, ele não será rebaixado e o usuário receberá uma mensagem informando essa condição. O usuário poderá então optar por continuar sem rebaixar o PDC ou aguardar até que o PDC possa ser rebaixado.





Para obter informações sobre como promover e rebaixar controladores de domínio, consulte Promovendo um controlador de domínio reserva a controlador de domínio primário e Rebaixando um controlador de domínio primário a controlador de domínio reserva na Ajuda do Gerenciador de servidores.

Gerenciando Server Properties e Services







Gerenciando Sessão de usuário

User Sessions on PRIMARY

Connected Users	Computer	Opens	Time	Idle	Guest
	NTWKSTA1	0	00:02	00:01	No
	NTWKSTA1	1	00:02	00:01	No
 administrator	SERVER	1	00:02	00:02	No
 student1	NTWKSTA1	1	00:02	00:01	No

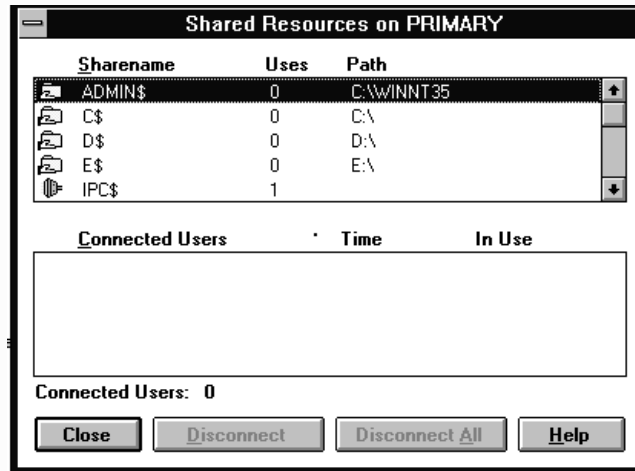
Connected Users: 4

Resource	Opens	Time
 IPC\$	0	00:02
 IPC\$	1	00:02
 ntsvr	1	00:01
 NwDATA	0	00:01

Close **Disconnect** **Disconnect All** **Help**



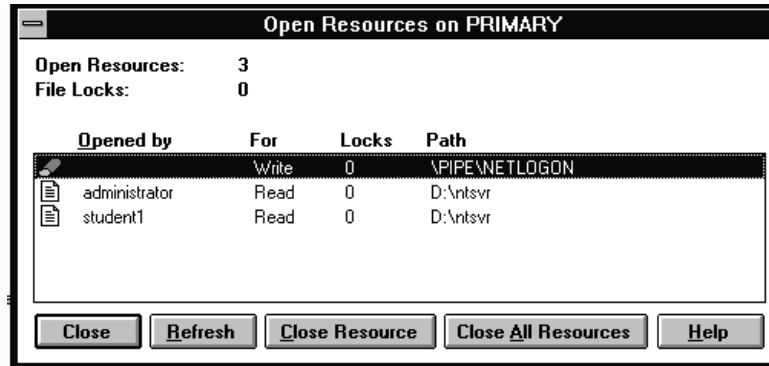
Gerenciando recursos compartilhados



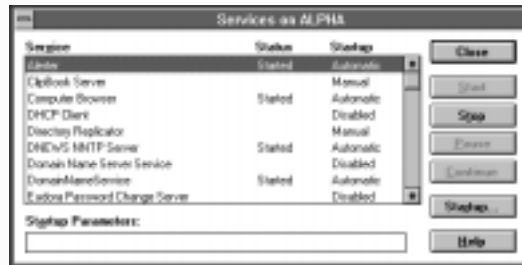
Recursos Administrativos



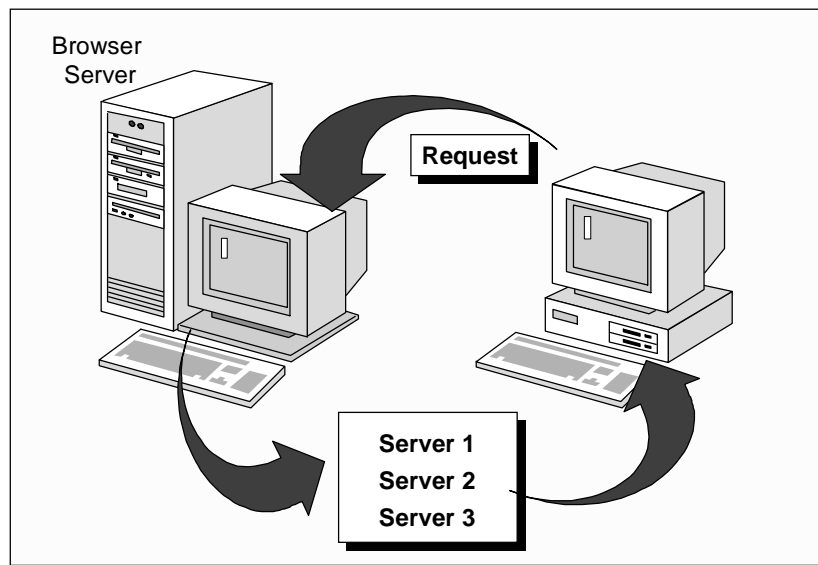
Gerenciando recursos em uso

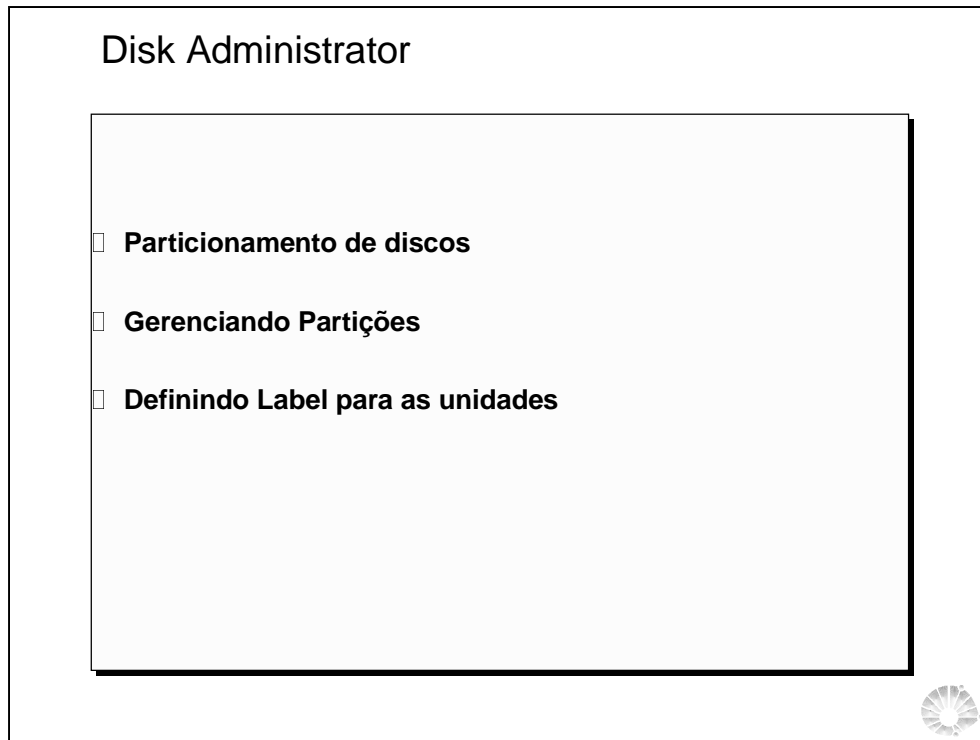


Gerenciando serviços



O Serviço Computer Browser





O Administrador de discos é uma ferramenta gráfica para o gerenciamento de discos. Ele abrange e estende a funcionalidade das ferramentas de gerenciamento de discos baseadas em caracteres, como os aplicativos de caracteres Fdisk o MS-DOS e Microsoft LAN Manager Fault Tolerance.

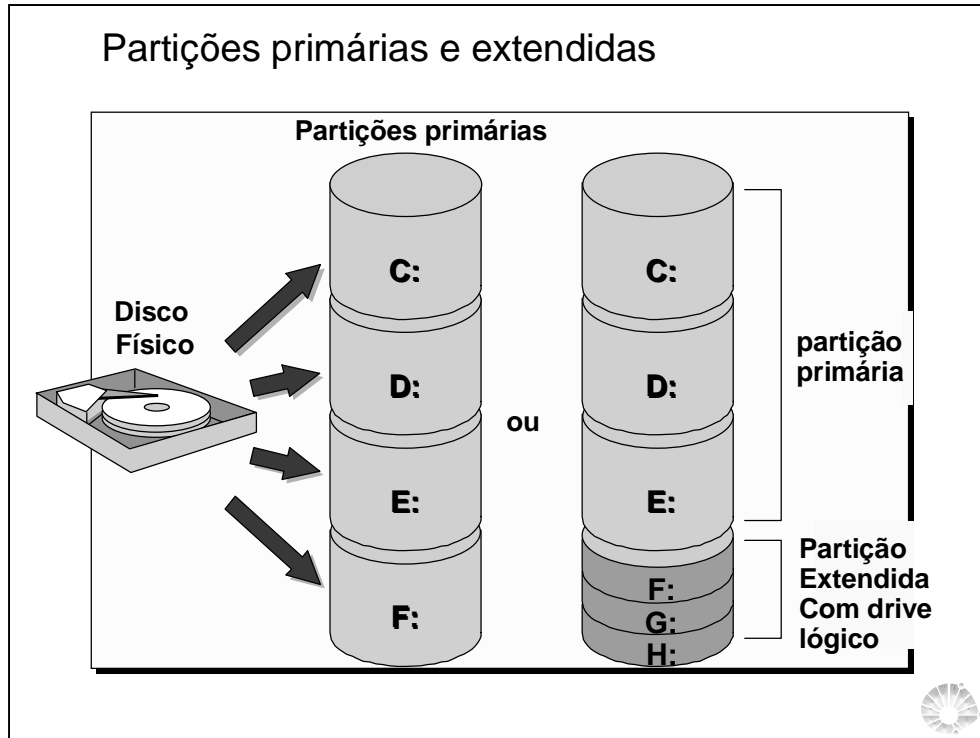
A lista seguinte fornece uma visão geral do que você pode fazer com o Administrador de discos:

- Criar e excluir partições em um disco rígido.
- Criar e excluir unidades de disco lógicas dentro de uma partição estendida.
- Formatar e dar nome a volumes.
- Ler informações de status dos discos, como o tamanho das partições e a quantidade de espaço livre disponível para a criação de partições adicionais.
- Ler informações de status dos volumes do Windows NT, como a atribuição de letra da unidade, nome do volume, tipo de sistema de arquivos, tamanho e espaço disponível.
- Fazer e alterar atribuições de letras de unidades para volumes de disco rígido e dispositivos de CD-ROM.
- Criar e excluir volumes.
- Estender volumes e volumes.
- Criar e excluir faixas de disco com ou sem paridade.
- Regenerar um membro faltante ou com falha de um conjunto de faixas de disco com paridade.
- Estabelecer ou quebrar espelhos de disco.
- Salvar e restaurar configurações de discos.

Observação Você não pode utilizar o Administrador de discos para particionar ainda mais a partição de sistema ou de inicialização porque elas contêm arquivos necessários para operar o Windows NT. O Administrador de discos pode ser utilizado somente para particionar espaço livre em um disco existente ou para particionar novos discos.

A versão do Administrador de discos do Windows NT Server inclui as ferramentas comuns de organização de discos (volumes e faixas de disco) e adiciona as ferramentas de proteção (tolerância a falhas) de dados (espelhos e faixas de disco com paridade). Para obter maiores informações sobre tolerância a falhas, espelhos e faixas de disco com paridade, consulte “Tolerância a falhas”.

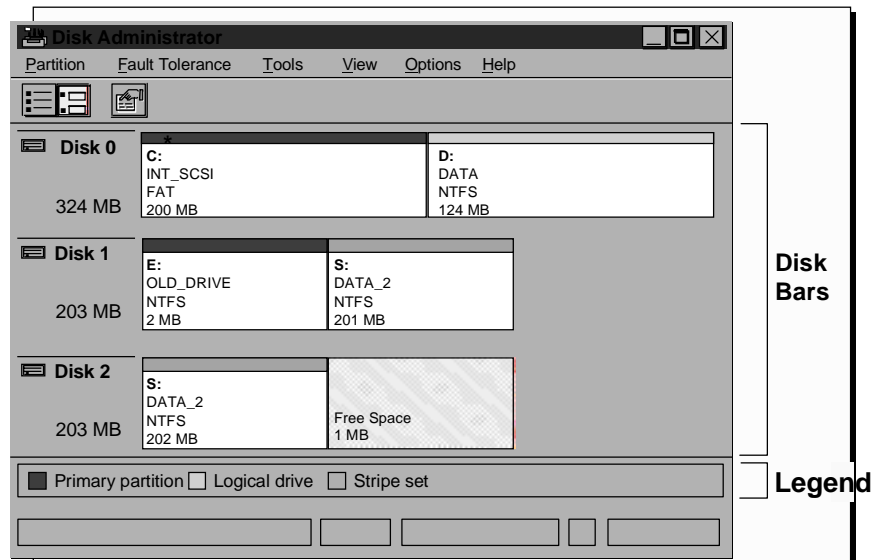
Partições primárias e extendidas



Na criação de partições primárias o sistema atribui espaço a uma partição, começando do início do espaço disponível. Portanto, no começo, não há espaçamento entre as partições. Os espaçamentos ocorrem somente quando, mais tarde, você exclui uma partição. Por exemplo, se você excluir a segunda de três partições e criar uma nova segunda partição menor que a anterior, isto deixará uma folga de espaço livre entre a segunda e terceira partições.

Uma das quatro partições que você pode criar no Windows NT, se o espaço em disco permitir, é a partição estendida. Você pode utilizar o espaço livre na partição estendida para criar múltiplas unidades de disco lógicas ou utilizar todo ou parte dele quando criar volumes ou outros tipos de volumes com a finalidade de tolerância a falhas.

Criando, formatando e deletando partições



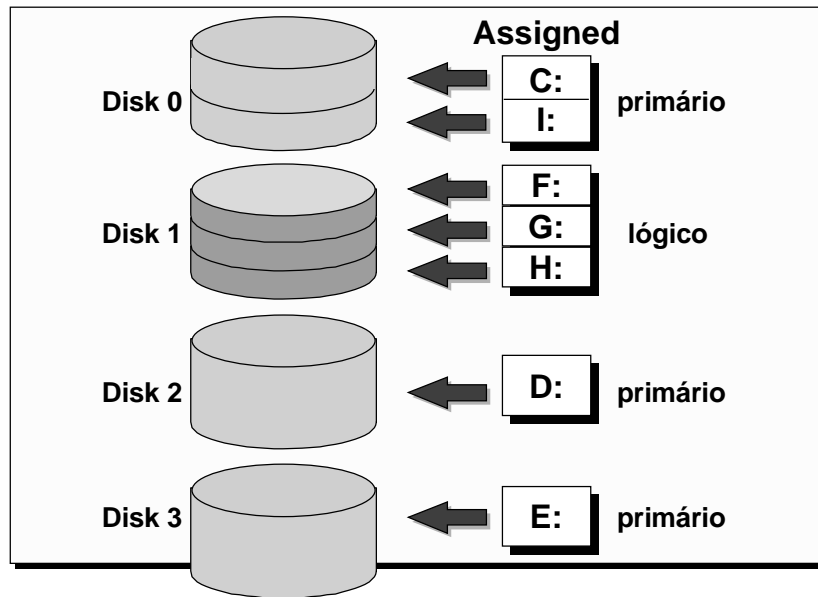
O gerenciamento de discos no Windows NT é muito flexível. Você pode criar até quatro partições no espaço livre de um disco rígido físico, criar múltiplas unidades lógicas no espaço livre de uma partição estendida e excluir partições. Também pode adicionar discos rígidos à configuração do seu sistema, recuperar informações de configuração de disco e atribuir letras de unidades de disco específicas a cada partição primária ou unidade lógica.

Cada partição pode ter um sistema de arquivos diferente, como FAT ou o sistema de arquivos do Windows NT (NTFS, Windows NT File System). Se você quer ter múltiplos sistemas de arquivos e o seu disco rígido existente tem somente uma partição, você deve criar mais de uma partição no disco antes de instalar o Windows NT.

O Windows NT faz certas restrições quanto à sua habilidade para fazer exclusões. Ele não permite que você exclua o volume que tem os arquivos de sistema (a partição de sistema), nem que exclua partições individuais que fazem parte de um conjunto, sem excluir o conjunto inteiro. No entanto, em um computador baseado em RISC, você pode excluir a partição de sistema com os arquivos necessários para carregar o Windows NT. Portanto, tenha muito cuidado. O Windows NT exige também que todas as unidades de disco lógicas ou outros volumes de uma partição estendida sejam excluídos para que você possa excluir a partição estendida.

Uma vez que cria ou exclui partições, volumes ou unidades lógicas, é preciso que você confirme as alterações para que qualquer outra coisa possa ser feita com as partições, volumes ou unidades lógicas.

Definindo letras para drives

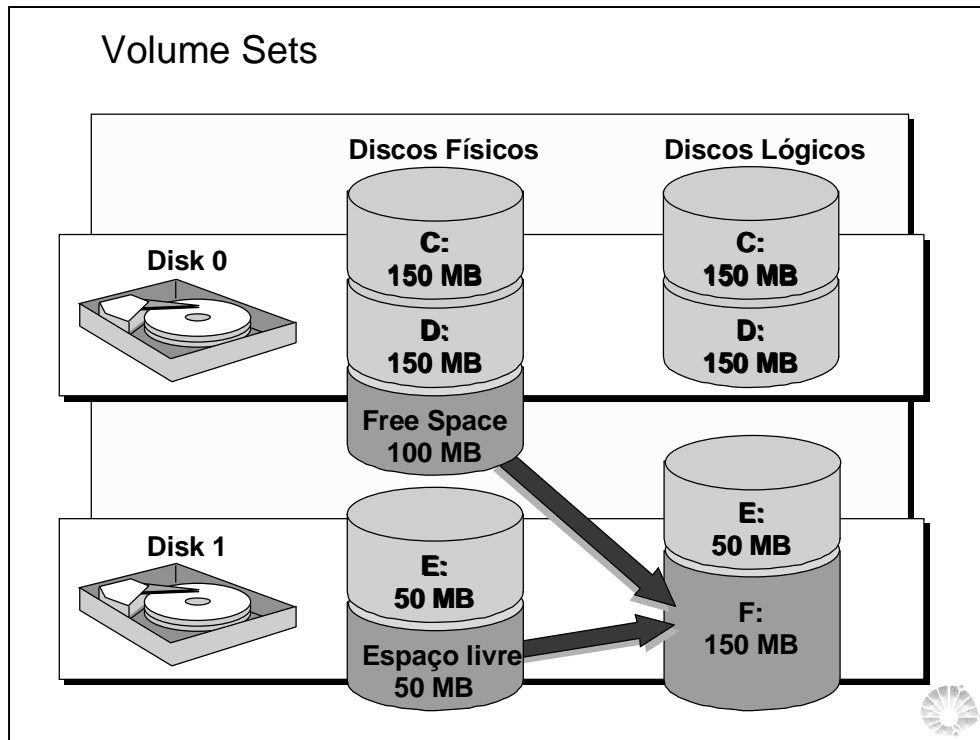


É possível criar mais de 24 volumes com o Windows NT, mas você não pode atribuir mais de 24 letras de unidades de disco para acessar esses volumes. As letras A e B são reservadas para unidades de disco flexível. No entanto, se você não tiver uma unidade B de disquete poderá utilizar a letra B para uma unidade de disco de rede.

O Windows NT permite a atribuição estática de letras de unidades de disco. O que significa que uma letra pode ser atribuída permanentemente a partição/volume em um disco rígido específico. Quando um novo disco rígido é acrescentado a um sistema de computador existente, ele não afeta as letras de unidade atribuídas estaticamente.

Além de suportar a atribuição estática de letras de unidades de disco em volumes e partições o Administrador de discos suporta também a atribuição de letras permanentes a unidades de CD-ROM.

No entanto, essa atribuição estática de letras de unidades ocorre somente depois que o Administrador de discos tenha sido utilizado no computador. Antes disso, as letras de unidades de disco são atribuídas pelo Windows NT de forma semelhante à utilizada pelo MS-DOS, que segue esta regra: primeiramente são atribuídas letras às partições primárias de cada disco rígido, começando pela letra C. Em seguida o Windows NT continua atribuindo as letras seguintes disponíveis, em ordem alfabética, às unidades lógicas de todos os discos rígidos e depois a outras partições primárias de cada disco. A partição de sistema ativa é normalmente a unidade de disco C.

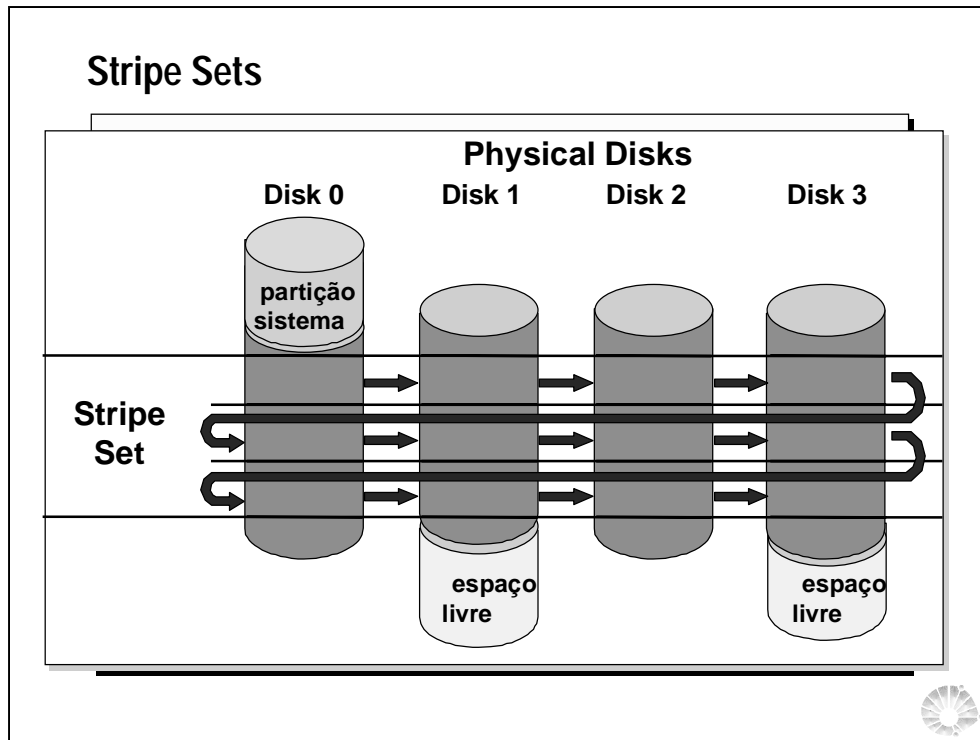


Os volumes constituem um mecanismo para a utilização mais eficiente do espaço livre total de diversos discos. Eles são criados, como é mostrado na ilustração acima, pelas de áreas de espaço livre de diversos tamanhos existentes em 1 a 32 discos, combinadas em um grande conjunto lógico de volumes que é reconhecido como uma partição única.

As áreas de espaço livre utilizadas para criar volumes podem ter tamanhos diferentes, como é mostrado na ilustração seguinte. Os conjuntos são organizados de tal forma que o espaço de um disco é preenchido, depois, começando no início do disco seguinte, todo o espaço é preenchido. E o processo continua da mesma forma para cada disco subsequente até o máximo de 32 discos.

Excluir as partições menores e combiná-las em um volume libera letras de unidades de disco para outros usos, permite a criação de um volume grande para ser utilizado pelo sistema de arquivos e pode melhorar o desempenho do sistema proporcionando melhor equilíbrio entre entrada e saída de dados (E/S) através das unidades de disco. Porém, os conjuntos de volume não têm tolerância a falhas.

Os volumes NTFS e os volumes existentes podem ser estendidos adicionando-se espaço livre. O Administrador de discos força o sistema a reinicializar depois que você sair e salvar as alterações, e então formata a nova área sem afetar os arquivos existentes no volume ou volume original.



As faixas de disco são criadas de maneira semelhante aos volumes, mas com mais restrições. Cada partição membro do conjunto de faixas deve estar em um disco diferente, até o limite de 32 discos. Além disso, o Administrador de discos fará todas as partições com o mesmo tamanho.

Os conjunto de faixas são criados combinando-se de áreas de espaço livre de 2 a 32 discos em um grande volume lógico. As partições nos conjunto de faixas têm aproximadamente o mesmo tamanho para que ao dados possam ser gravados em faixas ao longo da partição. Isto permite que os comandos de E/S sejam emitidos simultaneamente e melhora a taxa de transferência.

Quando você não precisar mais de um conjunto de faixas ou tiver problemas com falhas em um disco rígido, deve primeiro efetuar backup de todas as informações do conjunto de faixas e, somente então, excluir o conjunto, porque todas as informações serão também excluídas. As faixas de disco sem paridade não proporcionam tolerância a falhas.

Monitorando desempenho

- **Performance Monitor**
- **TaskMan**
- **Metas do monitoramento**
 - Melhorar performance
 - Traçar limites de capacidade
 - Manter hardware adequado
 - Detectar limitações no sistema



O Windows NT Server contém duas ferramentas para o monitoramento do desempenho do computador:

- O *performance monitor* permite que você veja a utilização dos recursos por componentes específicos e por processos de aplicativos mediante gráficos e relatórios. Com essa ferramenta, você pode medir a eficiência de seu computador para identificar e resolver possíveis problemas (como utilização desequilibrada dos recursos, hardware insuficiente ou programas mal estruturados) e planejar a necessidades de hardware adicional. Você pode também utilizar alertas para notificá-lo quando a utilização de um recurso atingir um valor especificado.
- O *Gerenciador de tarefas* oferece a você uma visualização rápida de como cada aplicativo, componente de aplicativo ou processo de sistema está utilizando os recursos da unidade central de processamento (CPU, Central Processing Unit) e da memória, bem como um resumo sobre o uso total da CPU e da memória.

Para executar o Gerenciador de tarefas, clique com o botão direito do mouse na Barra de ferramentas e depois clique em Gerenciador de tarefas. Para obter maiores informações sobre a sua utilização, consulte a Ajuda do Gerenciador de tarefas.

Performance Monitor

- **Ferramenta gráfica de análise de performance**
- **Charts, log files, set Alerts, format reports**
- **Entendendo objects, counters e instances**
- **Objetos de análise:**
 - Cache, Logical Disk, Memory, Paging File, Physical Disk, Process, Processor, Redirector, Server, System, Thread



O Desempenho do sistema utiliza uma série de contadores que monitoram dados como o número de processos aguardando por tempo do disco, o número de pacotes de rede transmitidos por segundo e a porcentagem de utilização do processador. Com esses dados, você pode criar gráficos, definir alertas e formatar relatórios que possibilitam medir e ajustar o Desempenho do sistema. Os dados podem ser exibidos enquanto são coletados, armazenados em logs para posterior utilização e comparação, ou ambos.

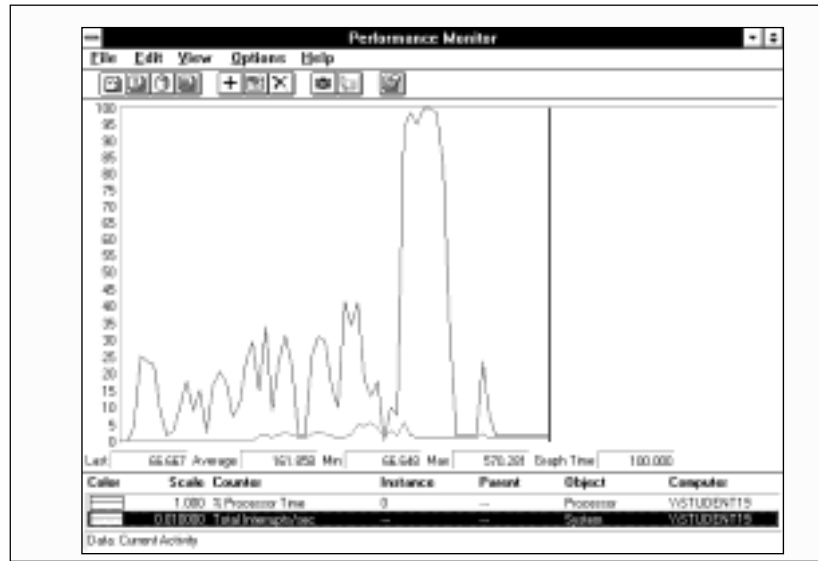
Com o Desempenho do sistema, você pode:

- Visualizar dados de qualquer número de computadores, simultaneamente.
- Receber imediato retorno sobre o modo como as alterações que você faz afetam o computador.
- Visualizar e alterar dinamicamente gráficos que representam os valores do contador da atividade atual.
- Exportar dados de gráficos, logs, logs de alerta e relatórios para programas de planilha eletrônica ou de banco de dados para posterior manipulação e impressão.
- Criar um log de alerta que lista (e, opcionalmente, notifica você) quando um valor de contador ultrapassar um limite configurado pelo usuário.
- Criar arquivos de log contendo dados sobre diversos objetos de diferentes computadores, de forma que você possa ver as informações reunidas ao longo do tempo. Você pode utilizar esses arquivos de log para registrar a utilização típica ou habitual dos recursos, identificar tendências e projetar as necessidades de hardware (planejamento de capacidade).
- Anexar a um arquivo selecionado seções de outros arquivos de log existentes para formar um arquivo de longo prazo.
- Visualizar relatórios de atividade atual ou criar relatórios a partir de arquivos de log existentes.
- Salvar configurações individuais de gráficos, alertas, logs ou relatórios, ou a instalação completa da Área de trabalho, e reutilizá-las quando necessário.

Apesar de sua ampla aplicabilidade, o Desempenho do sistema não responde a todas as questões sobre o ajuste do desempenho. Sendo uma ferramenta abrangente, proporciona uma visão geral do desempenho do computador. Pode, às vezes, isolar o problema; em outras ocasiões, pode indicar que ferramenta específica deve ser utilizada em seguida (como uma ferramenta para perfilar, um monitor de trabalho ou um analisador de rede, também denominado farejador (sniffer)).

Performance Monitor

(A ferramenta)



Inicie o Desempenho do sistema a partir do submenu Ferramentas administrativas do menu Iniciar ou da linha de comando. Ao iniciar o Desempenho do sistema na linha de comando, você pode especificar um arquivo de configurações. Se você não especificar esse arquivo, o Desempenho do sistema pesquisará na pasta de trabalho atual o arquivo de gráfico padrão, Default.pmc. A tabela a seguir mostra os tipos de arquivos de configurações suportados pelo Desempenho do sistema e as extensões que eles utilizam.

Tipo de arquivo de configurações Extensão do arquivo de configurações

Alerta .pma

Gráfico .pmc

Log .pml

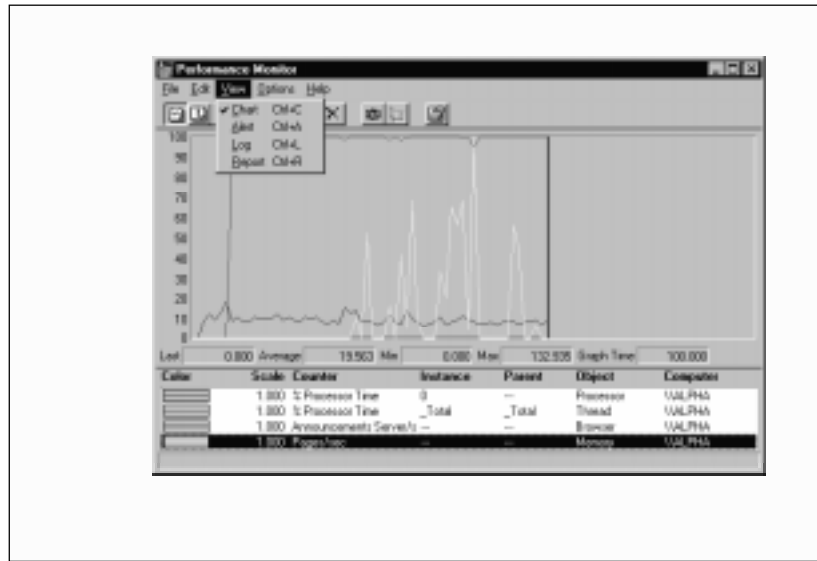
Relatório .pmr

Área de trabalho .pmw

Você pode também especificar o nome de um computador, além do arquivo de configurações ou no lugar dele. Esse computador aparecerá então como computador padrão quando você clicar no comando Adicionar ou no botão Adicionar contador.

Para sair do Desempenho do sistema, clique em Sair no menu Arquivo. Você pode salvar as configurações do desempenho do sistema para uma visualização específica (gráfico, alerta, log ou relatório), ou pode salvar a Área de trabalho inteira.

Visualizando dados do Performance Monitor



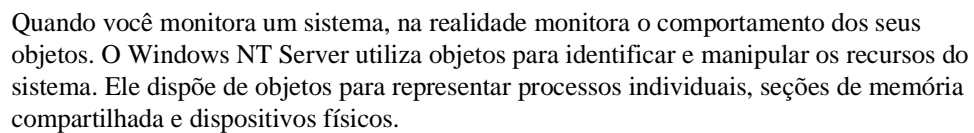
O Desempenho do sistema consiste de quatro janelas principais, que você visualiza escolhendo Gráfico, Alerta, Log ou Relatório. Os mesmos objetos e contadores estão disponíveis para monitoramento nos quatro modos de exibição.

Dica Para assegurar que o Desempenho do sistema seja visível em qualquer outra janela de sua tela, clique em Sempre visível no menu Opções.

Selecionando um objeto para ser monitorado na janela Log, todos os contadores desse objeto e todas as suas ocorrências serão monitorados quando você começar a coletar dados em um arquivo de log. Posteriormente, quando visualizar os resultados em uma das outras janelas, você poderá selecionar os contadores e as ocorrências de seu interesse.

O comando Dados de no menu Opções permite que você manipule um arquivo de log existente em vez de visualizar a atividade atual (isso é padrão).

A Barra de status indica a origem dos dados (atividade atual ou o nome do arquivo de log), o tamanho do arquivo (se você estiver registrando dados), e o número de ocorrências de alerta desde a última vez em que você esteve no modo de exibição Alerta (se você definiu alertas).



O Desempenho do sistema agrupa os contadores pelo tipo de objeto. Há um conjunto exclusivo de contadores para o processador, a memória, o cache, o disco rígido, os processos e outros tipos de objetos que produzem informações estatísticas. Certos tipos de objetos e seus respectivos contadores estão presentes em todos os sistemas; outros contadores, como os contadores de protocolos, aparecerão somente se o computador estiver executando o software associado. Os tipos de objetos a seguir acham-se disponíveis na maior parte dos computadores executando o Windows NT Server.

Cache	Arquivo de paginação		Redirecionador
DiscoLógico	Disco físico	Servidor	
Memória	Processo	Sistema	
Objetos	Processador	Segmento	

Alguns tipos de objeto dispõem de várias instâncias. Por exemplo, o objeto do tipo Processador terá múltiplas instâncias se o sistema dispuser de múltiplos processadores. O Disco Físico terá duas instâncias se o sistema tiver dois discos. Alguns tipos de objeto (Memória e Servidor) não dispõem de instâncias. Se um tipo de objeto dispuser de múltiplas instâncias, você poderá adicionar contadores para monitorar as estatísticas de cada instância ou, em muitos casos, de todas as instâncias de uma vez.

Dois tipos de objeto, processos e segmentos, possuem um relacionamento particularmente estreito.

- Os processos consistem de um programa executável, um conjunto de endereços de memória virtual e um segmento. Quando um programa é executado, é criado um processo do Windows NT. O processo pode ser um aplicativo (Microsoft Word para Windows, Corel® Draw), um serviço (Log de eventos, Computer Browser) ou um subsistema (spooler de impressão, POSIX).
- Segmentos são objetos dentro de processos que executam instruções de programa. Eles permitem que sejam realizadas operações simultâneas dentro de um processo e habilitam um processo a executar diferentes partes do seu programa em diferentes processadores, simultaneamente. Cada segmento em execução em um sistema é exibido como uma instância de objeto do tipo Segmento e é identificado pela associação com seu processo pai. (Por exemplo, se o Windows NT Explorer tiver dois segmentos ativos, o Desempenho do sistema os identificará como as instâncias Explorer=>0 e Explorer=>1 do objeto Segmento).

Observação Instâncias do tipo de objeto Processo aparecerão como números, se forem processos internos do sistema. Outros tipos de processos são identificados pelo nome do arquivo executável. Geralmente, somente processos de 32 bits aparecem na caixa Instância e os aplicativos de 16 bits, sendo executados em uma máquina com MS-DOS Virtual (VDM) aparecem apenas se tiverem sido iniciados em um espaço de memória separado.

Os valores de contador exibidos são a média dos dois últimos dados lidos ou o último valor do contador. Por exemplo, para contadores que cobrem um curto espaço de tempo, como Páginas de Memória/seg, a média é calculada sobre as duas últimas leituras de dados (separadas pelo intervalo de tempo); ao passo que os contadores de limiar, como o Contador de Segmentos do Processo, indicam o último valor que foi lido.

Quando você utiliza o Desempenho do sistema pela primeira vez, o número de contadores de desempenho pode parecer assustador. Mas não é necessário estar familiarizado com todos os contadores. Alguns são apropriados somente para os programadores que criam aplicativos baseados em plataforma Windows NT; outros são úteis para fornecedores que necessitam testar desempenho de hardware.

Dica Para obter ajuda para entender um contador selecionado, clique no botão Explicar da caixa de diálogo Adicionar para para exibir a caixa Definição do contador.

Categorias de análise de Performance

Análise

- ☐ Atividade do Processador
- ☐ Atividade do Disco
- ☐ Memória
- ☐ Atividade da Rede
- ☐ Workstation Service
- ☐ Server Service

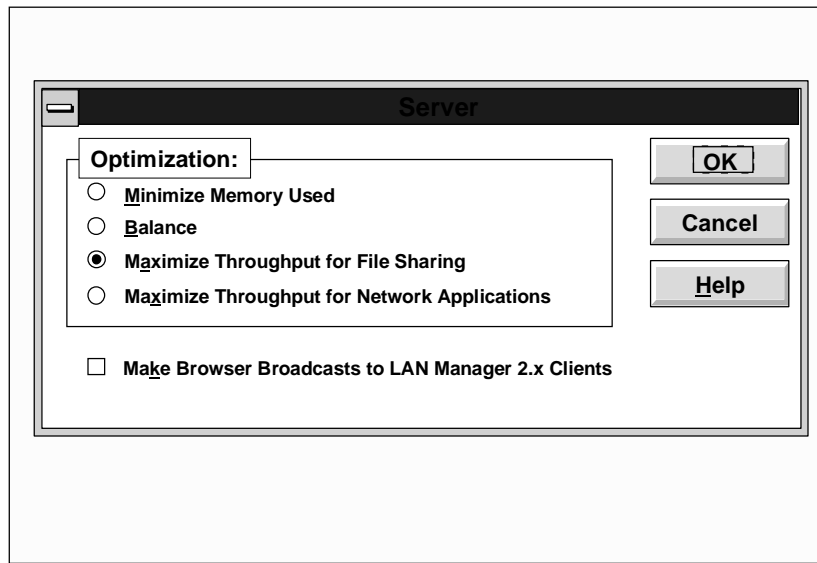
Conclusão

- ☐ Mais velocidade para um processo específico
- ☐ Melhor compartilhamento do processador para muitos processos
- ☐ Memória
- ☐ Disponibilidade do H.D.



Normalmente, os problemas referentes à taxa de transferência do sistema ocorrem quando a demanda por recursos (como microprocessadores, memória, discos rígidos e hardware e software de rede) excede a oferta. Para isolar problemas de desempenho, comece por determinar como usuários, aplicativos e sistema operacional interagem com cada recurso. O restante desta seção focaliza contadores que interessam a administradores de sistema, especialmente os contadores que indicam algo sobre a taxa de transferência do sistema e da rede.

Otimizando o Windows NT Server



A otimização de um servidor tem duas opções principais:

- *Maximize Throughput for File Sharing*: Selecionando essa opção seu servidor dará mais atenção às tarefas de servidor de arquivos, e se for um PDC fará uma média de 5 logons/segundo.
- *Maximize Throughput for Network Applications*: Essa opção é essencial estar selecionada num servidor PDC, pois ela configura a máquina para realizar até 20 logons/segundo.

Aumentando a performance

- ❑ **Criar múltiplos Paging Files**
- ❑ **Agendando aplicações de uso intensivo da memória**
- ❑ **Balance Server Load**
- ❑ **Utilizar melhor subredes “à toa”**
- ❑ **Planejar grupos de trabalho**



Event Viewer

- **Ferramenta de análise de Eventos**
- **Log records**
- **foco de análise: system, security, application**
- **tipo de eventos**



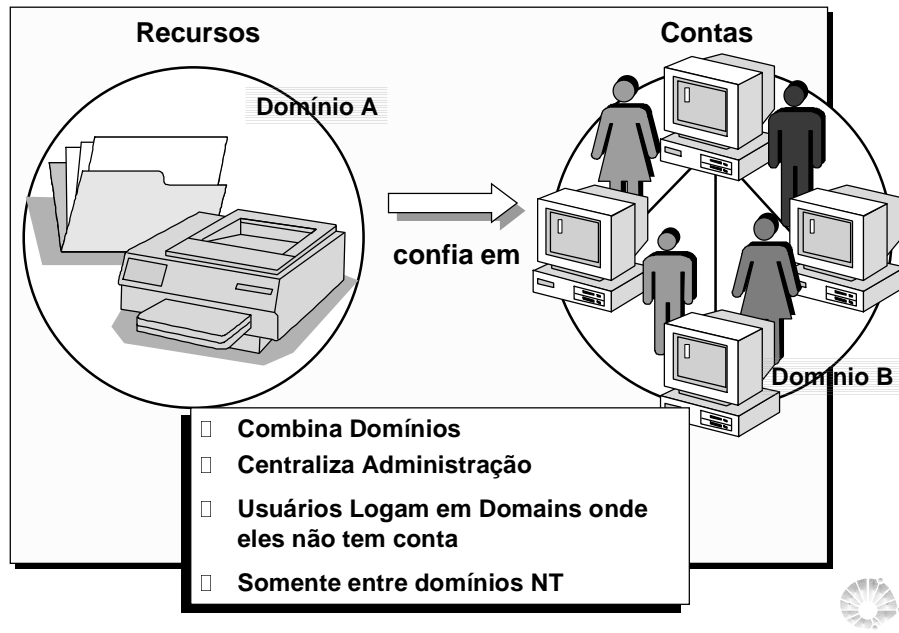
O Windows NT Server grava eventos em três tipos de log:

- O log de sistema contém eventos registrados pelos componentes do sistema do Windows NT Server. Por exemplo, a falha de um driver ou de outro componente do sistema ao ser carregado durante a inicialização é gravada no log de sistema. Os tipos de eventos registrados pelos componentes do sistema são predeterminados pelo Windows NT Server.
- O log de segurança pode conter tentativas de logon válidas ou inválidas, assim como eventos relacionados à utilização de recursos, como criar, abrir ou excluir arquivos ou outros objetos. Por exemplo, se você utiliza o Gerenciador de usuários para domínios para ativar a auditoria de logon e logoff, as tentativas para efetuar logon no sistema são gravadas no log de segurança.
- O log de aplicativo contém os eventos registrados pelos aplicativos. Por exemplo, um programa de banco de dados pode gravar um erro de arquivo no log de aplicativo. Os profissionais da área de desenvolvimento de aplicativos decidem quais eventos devem ser monitorados.

Os logs de aplicativo e de sistema podem ser visualizados por todos os usuários; os logs de segurança podem ser acessados somente pelos administradores do sistema.

Ativando o log de segurança Por padrão o log de segurança fica desativado. Para ativá-lo, o Gerenciador de usuários para domínios precisa ser executado para definir a Diretiva de auditoria. O administrador pode também definir diretivas de auditoria no Registro que paralise o sistema quando o log de segurança estiver cheio. Para obter maiores informações, consulte “Paralisando o computador quando o log de segurança estiver cheio”, mais adiante neste capítulo.

Trust Relationships



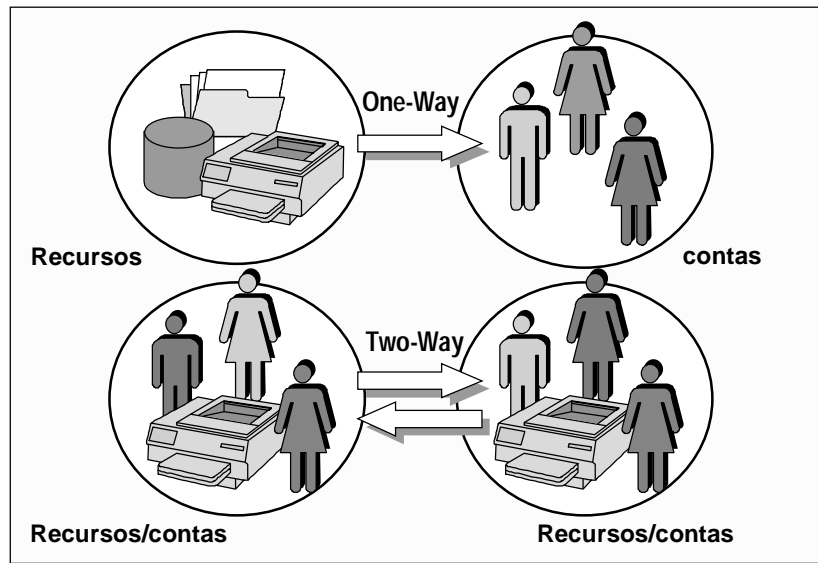
Embora pequenas organizações possam armazenar contas e recursos em um único domínio, as grandes organizações, tipicamente, estabelecem múltiplos domínios. Com múltiplos domínios, as contas são geralmente armazenadas em um único domínio e os recursos em outro domínio ou domínios.

Os serviços de diretório do Windows NT Server proporcionam segurança em múltiplos domínios mediante relações de confiança. Uma relação de confiança é um vínculo que combina dois domínios em uma única unidade administrativa que pode autorizar o acesso a recursos nos dois domínios.

Há dois tipos de relações de confiança:

- Em uma relação de confiança unidirecional, um domínio confia nos usuários do outro domínio para que utilizem os recursos. Mais especificamente, um dos domínios confia nos controladores de domínio no outro domínio a validação de contas de usuários para a utilização de seus recursos. Os recursos que são colocados à disposição estão no domínio confiante e as contas que podem utilizá-los estão no domínio confiável. Contudo, se as contas de usuário localizadas no domínio confiante precisarem utilizar recursos localizados no domínio confiável, essa situação requer uma relação de confiança bidirecional.
- Uma relação de confiança bidirecional são duas confianças unidirecionais: cada domínio confia nas contas de usuários do outro domínio. Os usuários podem efetuar logon a partir de computadores de qualquer um dos domínios para ao domínio que contenha a conta deles. Cada domínio pode ter contas e recursos. Contas de usuário globais e grupos globais podem ser utilizados a partir de um ou outro domínio para conceder direitos e permissões a recursos em um ou outro domínio. Em outras palavras, ambos os domínios são domínios confiáveis.

Confiança entre dois domínios



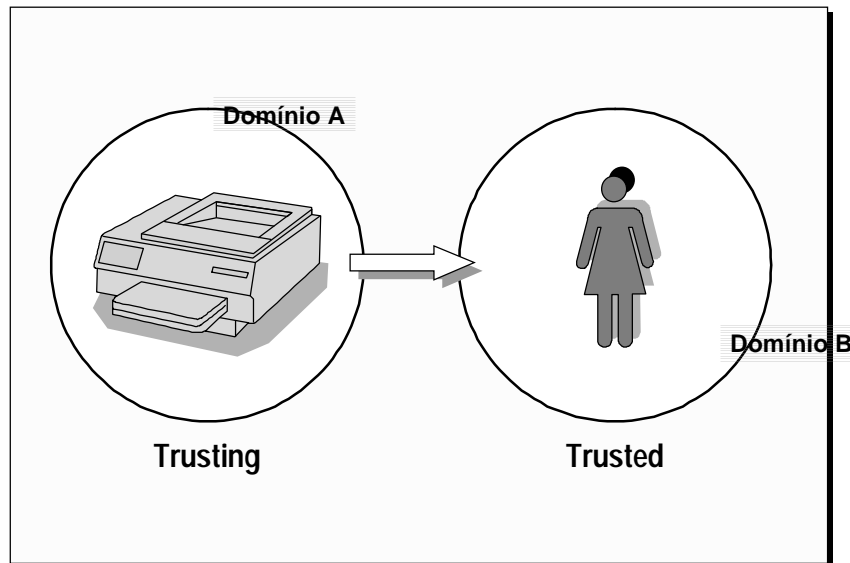
Através do agrupamento de computadores em domínios, os administradores e usuários de rede se beneficiam de duas maneiras principais:

- Os servidores em um domínio formam uma única unidade administrativa, compartilhando segurança e informações sobre contas de usuário e, desta forma, poupando tempo e trabalho dos administradores e usuários.
- Usuários que pesquisam a existência de recursos disponíveis na rede vêem a rede agrupada em domínios, e não como servidores e impressoras individuais na toda rede. (Essa vantagem dos domínios é idêntica ao conceito de grupo de trabalho no Microsoft Windows para Workgroups e Windows 95).

As relações de confiança transferem a praticidade de uma administração centralizada do nível do domínio para o da rede. Pelo estabelecimento de relações de confiança entre domínios na sua rede, você permite que contas de usuário e grupos globais sejam utilizadas em domínios que não o domínio onde essas contas estão localizadas. Você precisa criar uma só vez a conta de cada usuário e, já que os Serviços de diretório permitem a sincronização de todos os dados de segurança no banco de dados do diretório, é possível conceder à conta um acesso a qualquer computador da sua rede e não somente aqueles de um único domínio.

As relações de confiança são criadas somente entre domínios com Windows NT. Durante a administração de servidores membros, em computadores executando o Windows NT Workstation ou um domínio com LAN Manager 2.x, o comando Relações de confiança está indisponível.

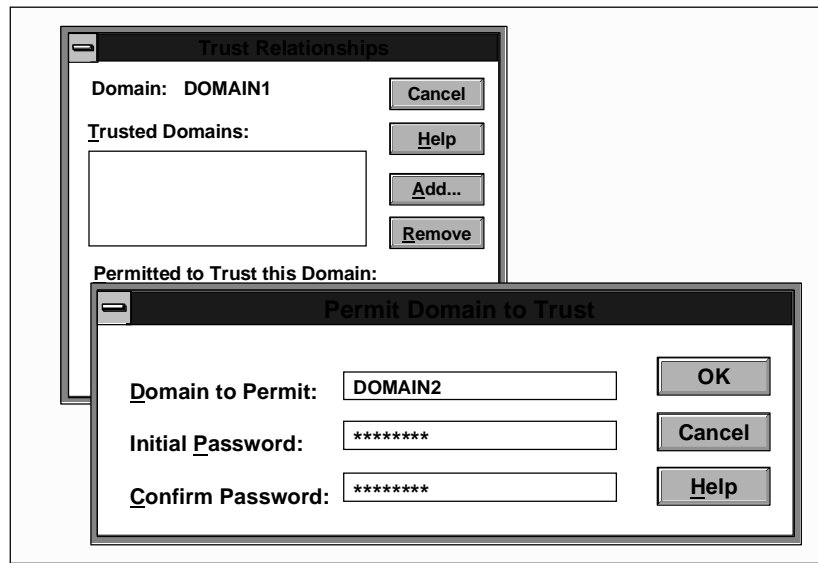
Trusting vs. Trusted Domains



Contas de computador e canais seguros permitem que os administradores gerenciem remotamente as estações de trabalho e os servidores membros. Também afetam a relação entre uma estação de trabalho e servidores do domínio e entre controladores de domínio primário e reserva:

- A conta de computador faz parte de uma relação de confiança unidirecional implícita entre o computador cliente e os controladores em seu domínio. As estações de trabalho solicitam autenticação de logon para uma conta de usuário de um servidor de domínio da mesma forma que um servidor em um domínio confiante solicita validação de um servidor em um domínio confiável. Essa relação de confiança permite que os administradores selecionem uma estação de trabalho ou um servidor membro para administração, da mesma maneira que eles selecionam um domínio.
- Ao ser criada uma conta de computador, o grupo global Admins. do Domínio é automaticamente adicionado à estação de trabalho ou ao grupo local Administradores do servidor membro. Os administradores de domínio podem então utilizar os utilitários do Windows NT Server para gerenciar remotamente o ambiente do usuário do computador e gerenciar as contas de computador de usuários e grupos, inclusive adicionando grupos globais do domínio aos grupos locais do computador. Adicionalmente, os administradores de domínio podem executar no próprio computador qualquer função que seja permitida pelo grupo local Administradores.
- Para controladores de domínio do Windows NT Server, contas de computador vinculam BDCs ao PCD e fazem pares de domínios confiantes com confiáveis. Contas de confiança do servidor criados durante a configuração do canal de comunicações seguro permitem que os BDCs obtenham cópias do banco de dados do diretório principal do PDC. As contas de confiança entre domínios permitem que os controladores de domínio em um domínio confiável transfiram a autenticação de contas de usuário ao domínio confiante.

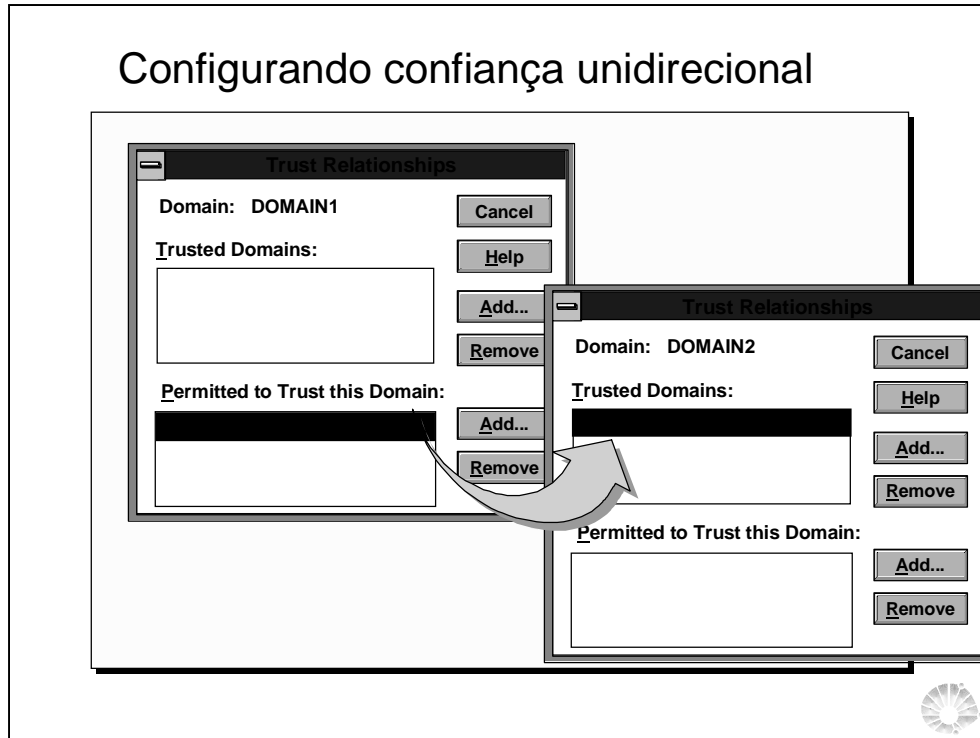
Estabelecendo Trusts



Para criar relações de confiança, você utiliza o comando Relações de confiança no menu Diretivas do Gerenciador de usuários para domínios. A criação de uma relação de confiança unidirecional requer duas etapas: em primeiro lugar, um domínio (o domínio que deverá ser o domínio confiável) deve adicionar um segundo domínio (o domínio que deverá ser o domínio confiante) à lista de domínios que confiam nele. Em seguida, o domínio confiante deve adicionar o domínio confiável à lista de domínios em que ele confia. Uma vez que a relação de confiança ainda não está estabelecida, é possível que essas duas etapas precisem ser executadas por administradores diferentes.

É melhor estabelecer primeiro a relação de Domínio confiante, seguida pela relação de Domínio confiável. Essa ordem permite que a senha utilizada para configurar a relação seja imediatamente verificada na primeira vez em que a relação for utilizada.

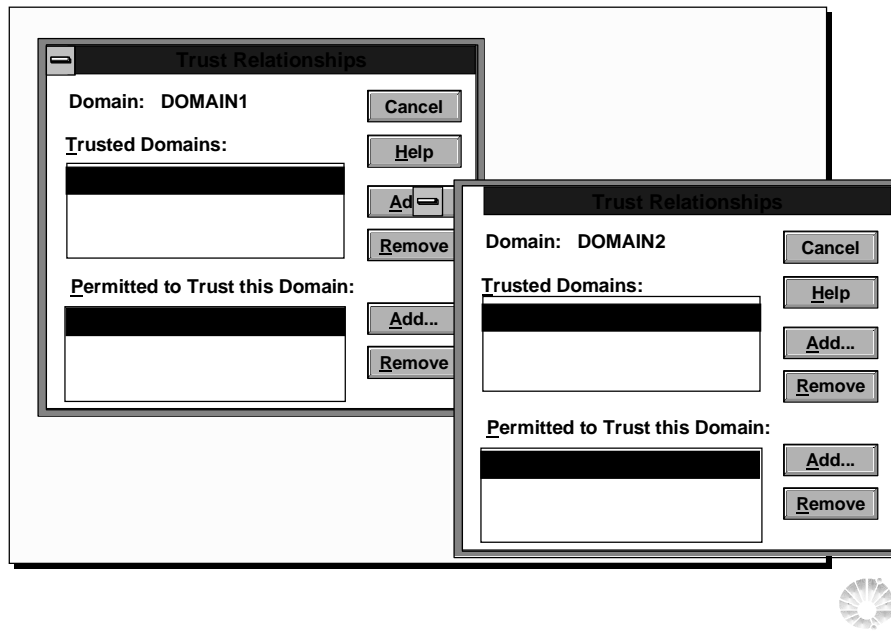
Configurando confiança unidirecional



Para criar relações de confiança, você utiliza o comando Relações de confiança no menu Diretivas do Gerenciador de usuários para domínios. A criação de uma relação de confiança unidirecional requer duas etapas: em primeiro lugar, um domínio (o domínio que deverá ser o domínio confiável) deve adicionar um segundo domínio (o domínio que deverá ser o domínio confiante) à lista de domínios que confiam nele. Em seguida, o domínio confiante deve adicionar o domínio confiável à lista de domínios em que ele confia. Uma vez que a relação de confiança ainda não está estabelecida, é possível que essas duas etapas precisem ser executadas por administradores diferentes.

É melhor estabelecer primeiro a relação de Domínio confiante, seguida pela relação de Domínio confiável. Essa ordem permite que a senha utilizada para configurar a relação seja imediatamente verificada na primeira vez em que a relação for utilizada.

Configurando confiança bidirecional



Uma relação de confiança bidirecional são duas confianças unidirecionais: cada domínio confia nas contas de usuários do outro domínio. Os usuários podem efetuar login a partir de computadores de qualquer um dos domínios para ao domínio que contenha a conta deles. Cada domínio pode ter contas e recursos. Contas de usuário globais e grupos globais podem ser utilizados a partir de um ou outro domínio para conceder direitos e permissões a recursos em um ou outro domínio. Em outras palavras, ambos os domínios são domínios confiáveis.

Concedendo permissões através de Trusts

Add Users and Groups

List Names From: DOMAIN2

Names: DOMAIN2

MacintoshU
 NETWORK
 SYSTEM
 User1
 Guest
 Mac1

Add **Show Users** **Members...** **Search...**

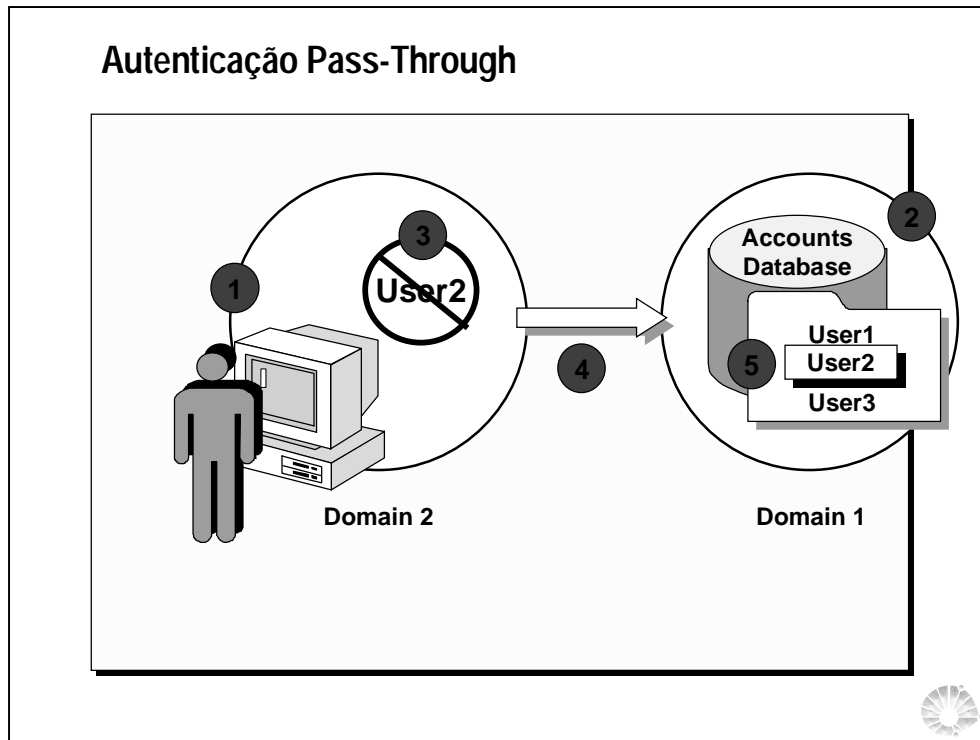
Add Names:

DOMAIN1\User1

Type of Access: Read

OK **Cancel** **Help**





A autenticação de passagem ocorre nos casos a seguir:

- No logon interativo, quando um usuário efetua logon em um computador executando o Windows NT Workstation ou em um computador executando o Windows NT Server e o nome na caixa Domínio na caixa de diálogo Informações de logon não é o nome do computador.

O computador de logon envia a solicitação de logon a um controlador de domínio, no domínio ao qual pertence a conta de computador. Inicialmente, o controlador verifica o nome do domínio. Se for o domínio ao qual pertence o controlador, o controlador autenticará as credenciais de logon verificando-as no seu banco de dados do diretório e passará as informações de identificação da conta de volta ao computador de logon, permitindo que o usuário se conecte aos recursos do computador de logon e do domínio.

Observação Se o computador de logon não estiver executando o Windows NT Workstation ou o Windows NT Server, a autenticação do controlador de domínio não terá efeito sobre a capacidade do usuário para utilizar os recursos do computador de logon.

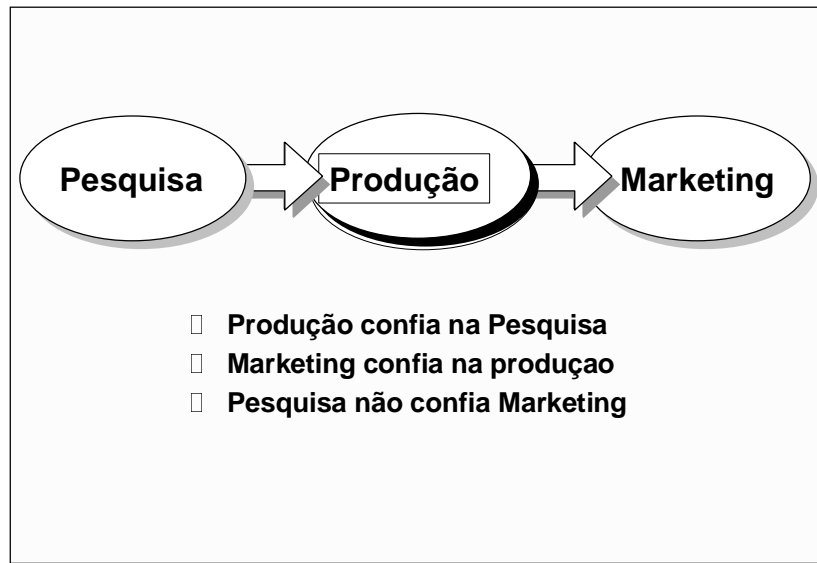
Se o nome de domínio não for o domínio ao qual pertence o controlador de domínio, o controlador de domínio verificará se o domínio é confiável. Se for, o controlador de domínio transfere a solicitação de logon a um controlador de domínio no domínio confiável. Esse controlador de domínio autentica o nome de usuário da conta e a senha, confrontando-as com o banco de dados do diretório do domínio, e devolve as informações de identificação da conta ao controlador de domínio inicial, que as envia de volta ao computador de logon.

Se o nome nas credenciais de logon não for o nome do computador, o nome do domínio ao qual pertence o computador nem o nome de um domínio confiável pelo domínio do computador, as credenciais serão consideradas como pertencentes a um domínio não confiável e o logon interativo não ocorrerá.

· No logon interativo, quando o computador no qual está sendo efetuado o logon é um controlador de domínio, mas o nome na caixa Domínio não é o domínio ao qual pertence o controlador.

O controlador verifica o nome do domínio para saber se é confiável. (O controlador de domínio não verifica o nome do computador pois seu banco de dados do diretório contém somente contas de domínio). Se o domínio for confiável, o controlador passará as informações de logon a um controlador de domínio no domínio confiável para autenticação. Se o controlador de domínio confiável autenticar a conta, as informações de logon serão passadas de volta ao controlador de domínio inicial e o logon do usuário será efetivado. Se a conta não for autenticada (não estiver definida no banco de dados do diretório do domínio confiável), ocorrerá falha de logon.

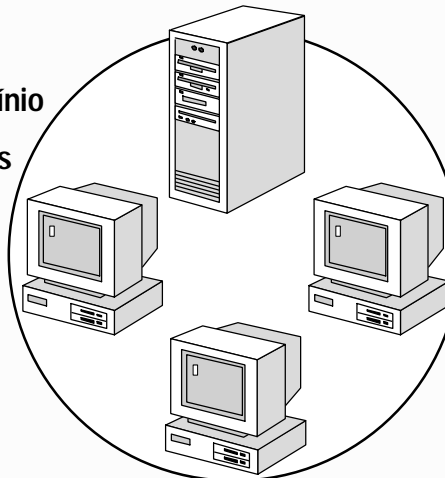
Trusts são intransitivos



Uma característica essencial que um administrador deve conhecer é a intransitividade das relações de confiança. Isso quer dizer que se o domínio Pesquisa confia na Produção e a produção confia no Marketing, a priori não existe nenhuma relação entre Marketing e Pesquisa. Essa característica se torna de extrema importância quando se planeja um grande domínio utilizando os 4 modelos básicos que veremos a seguir.

O modelo de domínio simples

- **Usuários e grupos globais em um domínio**
- **Não são necessários Trusts**



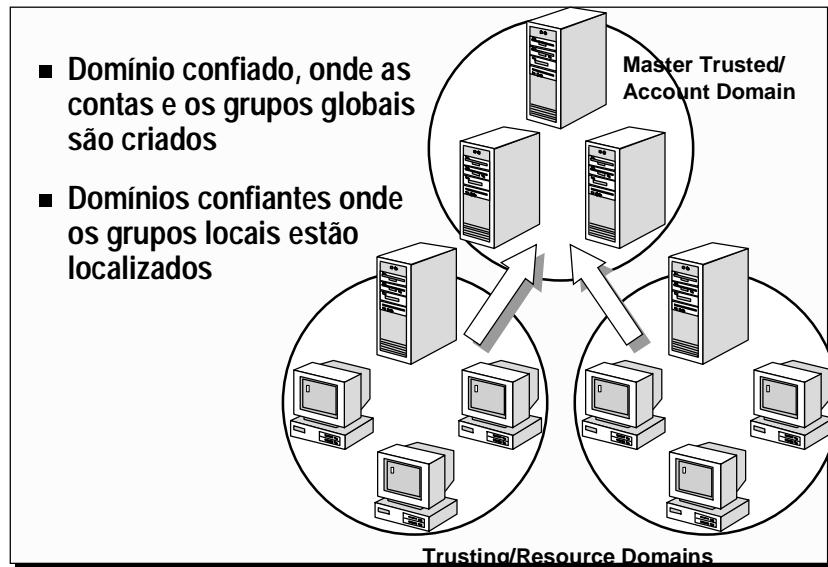
Na maioria dos casos, você pode utilizar o modelo de domínio único. Nesse modelo, a rede tem um único domínio. Você cria todos os usuários e grupos globais nesse domínio. O domínio único tem um PDC com um ou mais BDCs. O PDC e cada BDC podem suportar 2.000 a 2.500 contas de usuário para validar logons de usuário e proporcionar tolerância a falhas. O número de contas pode chegar a 5.000, dependendo do poder do computador.

O modelo de domínio único é uma opção adequada para organizações que requerem tanto gerenciamento centralizado de contas de usuário como facilidade de administração. Qualquer membro do grupo Administradores de Domínio pode administrar todos os servidores de rede e contas de domínio no PDC.

Uma rede pode utilizar o modelo de domínio único se tiver um número suficientemente pequeno de usuários e grupos para assegurar um bom desempenho (geralmente até 26.000). O número exato de usuários e grupos depende do número de servidores do domínio e do hardware dos servidores.

Ter um único domínio também significa que todos os administradores da rede podem administrar todos os servidores da rede. Dividir uma rede em domínios permite que você crie administradores que podem administrar somente alguns servidores, como os dos seus próprios departamentos.

Modelo de um domínio mestre



Quando a rede não precisa ser dividida em domínios para fins organizacionais, mas tem um número suficientemente pequeno de usuários e grupos, o modelo de domínio mestre poderá ser a melhor opção. Esse modelo oferece tanto a administração centralizada como as vantagens organizacionais de múltiplos domínios.

Com esse modelo, um dos domínios o domínio mestre age como a unidade administrativa central para contas de usuário e de grupo. Todos os outros domínios da rede confiam nesse domínio e isso significa que reconhecem os usuários e grupos globais ali definidos. Se sua empresa tem um departamento de Sistema de Gerenciamento de Informações (MIS, Management Information System) que gerencia sua LAN, é lógico fazer com que esse departamento administre o domínio mestre.

Todos os usuários efetuam login em suas contas no domínio mestre. Recursos como impressoras e servidores de arquivo, estão localizados nos outros domínios. Cada domínio de recursos estabelece uma confiança unidirecional com o domínio mestre (de contas), permitindo que os usuários com contas no domínio mestre utilizem os recursos de todos os outros domínios. O administrador de rede pode gerenciar a rede de múltiplos domínios inteira e seus usuários e recursos mediante o gerenciamento de um único domínio.

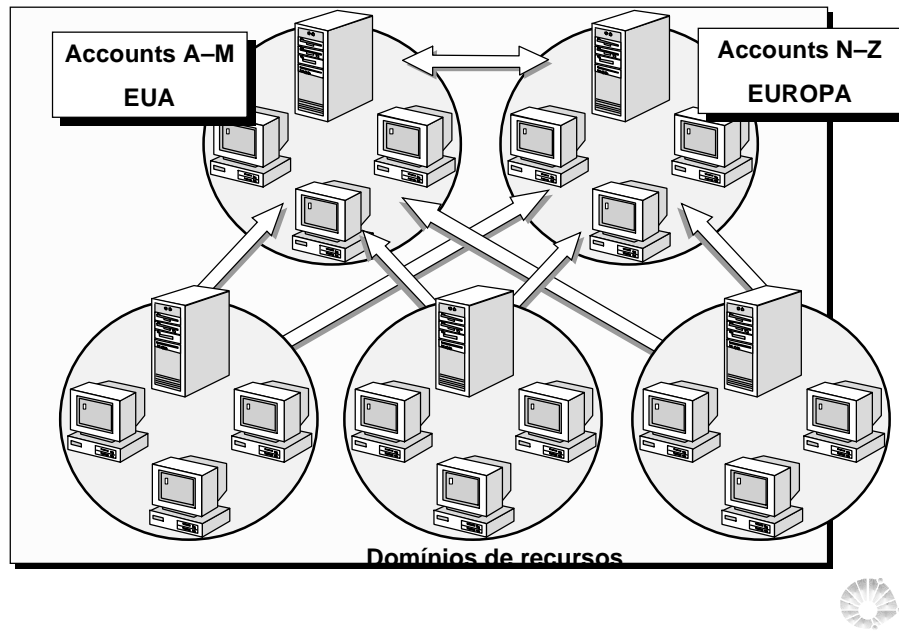
A vantagem do modelo de domínio mestre único está na sua flexibilidade de administração. Por exemplo, em uma rede que requer quatro domínios, à primeira vista poderia ser mais óbvio criar quatro bancos de dados de contas de usuário diferentes, um para cada domínio. Contudo, se você colocar todas as contas de usuário em um único banco de dados do diretório em um dos domínios e depois implementar relações de confiança bidirecionais, poderá consolidar a administração de contas de usuário e de computador. Também poderá administrar todos os recursos ou delegá-los aos administradores locais. E os usuários só precisarão de um nome de login e uma senha para utilizar os recursos de qualquer um dos domínios.

Esse modelo equilibra as necessidades de segurança de conta com a necessidade de recursos prontamente disponíveis na rede pois as permissões aos recursos são concedidas aos usuários com base em sua identidade de login no domínio mestre.

O modelo de domínio mestre único é particularmente adequado para:

- Gerenciamento centralizado de contas. As contas de usuário podem ser centralmente gerenciadas; adicionar/excluir/alterar contas de usuário a partir de um único ponto.
- Gerenciamento descentralizado de recursos ou capacidade local de administração do sistema. Os domínios de departamento podem ter seus próprios administradores que gerenciam os recursos do departamento.
- Os recursos podem ser agrupados logicamente, correspondendo aos domínios locais.

O modelo Multiple Master Domain



No modelo de múltiplos domínios mestres, existem dois ou mais domínios mestres simples. Como o modelo de domínio mestre único, os domínios mestres servem como domínios de contas, com todas as contas de usuário e de computador criadas e mantidas em um desses domínios mestres. Os grupos MIS de uma empresa podem gerenciar centralmente esses domínios mestres. Da mesma forma que o modelo de domínio mestre único, os outros domínios da rede são denominados domínios de recursos; não armazenam nem gerenciam contas de usuário, mas fornecem recursos à rede, como impressoras e servidores de arquivo compartilhados.

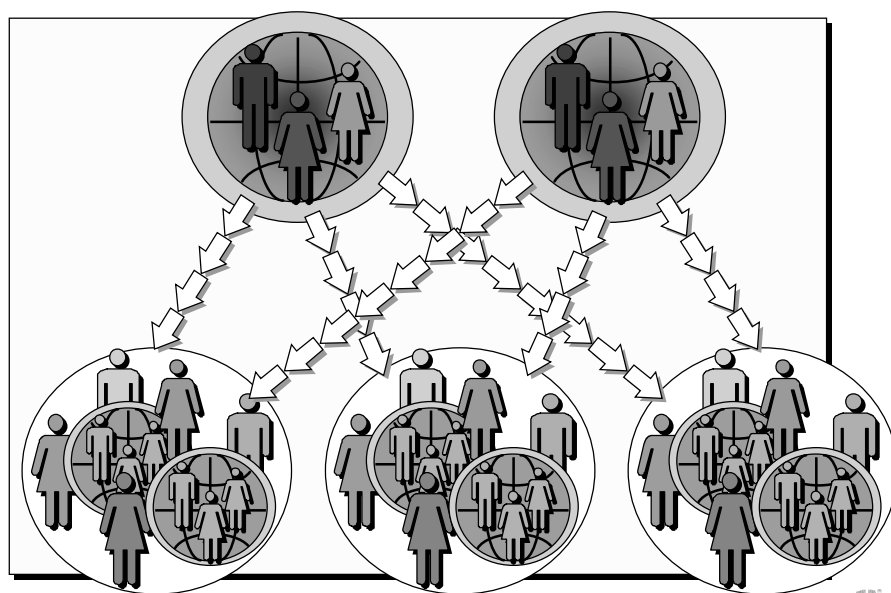
Nesse modelo, cada domínio mestre é conectado aos outros domínios mestres por uma relação de confiança bidirecional. Cada domínio de recursos confia em todos os domínios mestres com uma relação de confiança unidirecional. Os domínios de recursos podem confiar em outros domínios de recursos, embora isso não lhes seja exigido. Uma vez que toda conta de usuário está presente em um dos domínios mestres e já que cada domínio de recursos confia em todos os domínios mestres, toda conta de usuário pode ser utilizada em qualquer um dos domínios mestres.

Cada usuário efetua login no domínio que contém a sua conta. Cada domínio mestre contém um único PDC e pelo menos um BDC.

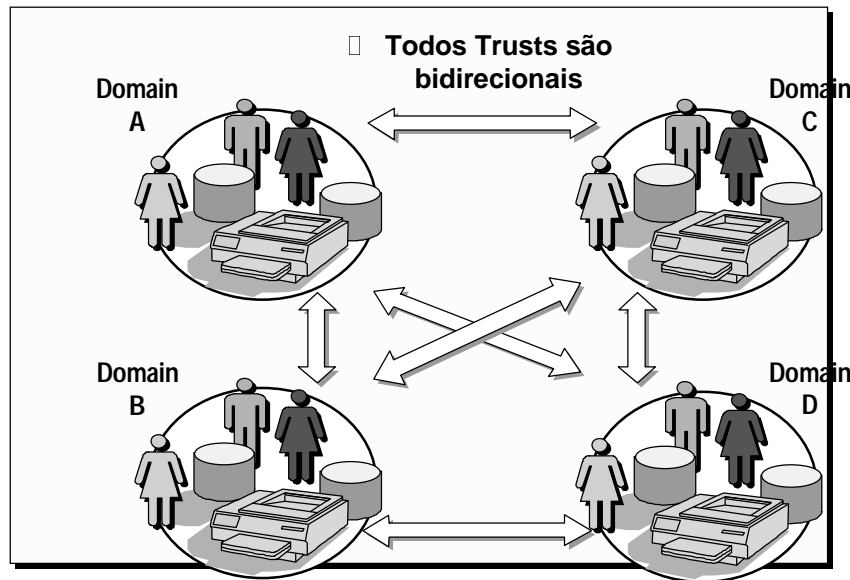
O modelo de múltiplos domínios mestres incorpora todos os recursos de um domínio mestre único e também acomoda:

- Organizações com mais de 40.000 usuários. O modelo de múltiplos domínios mestres é escalável para redes com qualquer número de usuários.
- Usuários móveis. Os usuários podem efetuar login de qualquer lugar da rede, de qualquer lugar do mundo.
- Administração centralizada ou descentralizada.
- Necessidades organizacionais. Os domínios podem ser configurados de forma a retratar departamentos específicos ou organizações internas da empresa.
- Os BDCs podem ser distribuídos entre os locais para facilitar interações entre redes remotas e redes locais.

Grupos nos modelos de domínio



O modelo Complete Trust



Número de relações de confiança no modelo Complete Trust Domain

