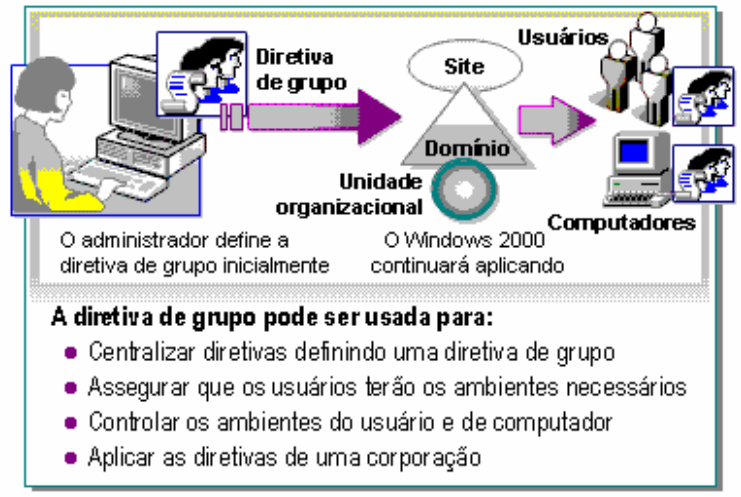
www.projetoderedes.com.br
www.redesdecomputadores.com.br
www.metrored.com.br

DIRETIVAS DE GRUPO

Introdução à diretiva de grupo



A diretiva de grupo pode ser usada para definir inicialmente as configurações; depois disso, as configurações serão periodicamente reaplicadas. Você pode vincular as configurações de diretiva de grupo a objetos, sites, domínios e unidades organizacionais do Active Directory. Uma vez vinculada, a diretiva de grupo afetará todos os usuários e computadores nesses recipientes (containers).

Com a diretiva de grupo, você pode:

- Centralizar diretivas definindo uma diretiva de grupo para uma organização inteira no nível de site ou de domínio ou descentralizar as configurações de diretiva de grupo definindo uma diretiva de grupo para cada departamento no nível de unidade organizacional.

- Assegurar que os usuários terão ambientes necessários para executarem seus trabalhos. Você pode verificar se os usuários possuem:

    - As configurações de sistema e de aplicativo necessárias no Registro; os scripts para modificar os ambientes do usuário e do computador.
    - Instalações automatizadas do software.
    - Configurações de segurança para computadores locais, domínios e redes.
    - Controle do local de armazenamento das pastas de dados dos usuários.

- Controlar os ambientes do usuário e de computador, reduzindo o nível de suporte técnico necessário aos usuários e diminuindo a perda de produtividade causada por um erro do usuário. Poe exemplo, com a diretiva de grupo, você pode evitar que os usuários instalem aplicativos desnecessários ou efetuem alterações nas configurações do sistema que possam tornar um computador inoperante.
- Aplicar as diretivas de uma corporação, como regras de negócios, objetivos e necessidades de segurança. Por exemplo, você pode assegurar que os requisitos de segurança para todos os usuários corresponderão à segurança exigida pela corporação ou que todos os usuários terão um conjunto específico de aplicativos instalados.

Observação As configurações de diretiva de grupo aplicam-se apenas aos sistemas baseados no Windows 2000 e Microsoft Windows XP Professional, e não a versões anteriores da família de sistemas operacionais Windows.

Tipos de configurações de diretiva de grupo

Tipos de configurações de diretiva de grupo	
Administrative Templates	Configurações de aplicativos e ambientes de área de trabalho do usuário
Security	Configurações de segurança do computador local, do domínio e da rede
Software Installation	Centralizam o gerenciamento de instalações, atualizações e remoções de software
Scripts	Especificam o momento em que o Windows 2000 executará scripts específicos
Remote Installation Services	Controlam as opções durante a execução do **Client Installation Wizard**
Internet Explorer Maintenance	Administram e personalizam o Microsoft Internet Explorer
Folder Redirection	Armazenam pastas específicas de perfil de usuário em um servidor de rede

A edição de um GPO permite que as configurações de diretiva de grupo sejam definidas a fim de determinar as diretivas que afetarão usuários e computadores. Estes são os tipos de configurações que podem ser definidos:

- *Administrative Templates* (Modelos Administrativos). Baseados no Registro, definem configurações de aplicativos e ambientes de área de trabalho do usuário. Essas configurações incluem os aplicativos e os componentes do sistema operacional que podem ser acessados pelo usuário, o nível de acesso às opções do **Control Panel** (Painel de controle) e o controle de arquivos off-line dos usuários.

- *Security* (Segurança). Definem configurações de segurança do computador local, do domínio e da rede. Essas configurações incluem controle de acesso dos usuários à rede, configuração de diretivas de conta e auditoria, além de controle dos direitos do usuário. Por exemplo, você pode definir o número máximo permitido de tentativas de logon com falha em uma conta de usuário antes que ela seja bloqueada.

- *Software installation* (instalação de Software). Centralizam o gerenciamento de instalações, atualizações e remoções de software. É possível fazer com que os aplicativos sejam automaticamente instalados, atualizados ou removidos de computadores cliente. Também é possível disponibilizar aplicativos para que sejam exibidos **Add/ Remove Programs** (Adicionar ou remover programas) no **Control Panel**, que fornece aos usuários um local central para obtenção de aplicativos para instalação.

- *Scripts* (Scripts). Especificam o momento em que o Windows 2000 executará scripts específicos. Você pode especificar que os scripts sejam executados quando o

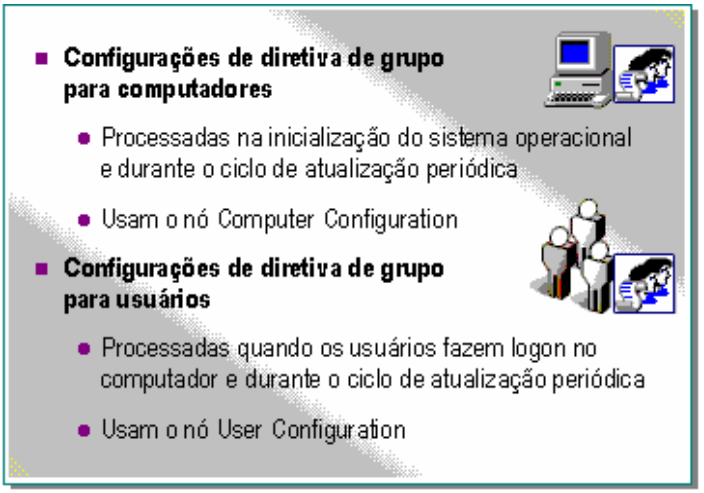
computador for iniciado e desligado ou quando o usuário fizer logon ou logoff. Você pode especificar que os scripts executem operações em lote, além de controlar vários scripts e determinar a ordem de sua execução.

- *Remote Installation Services* (Serviços de Instalação Remota). Controlam as opções durante a execução do **Client Installation Wizard** (Assistente para a instalação de cliente) usado pelos Remote Installation Services (RIS, serviços de instalação remota), disponíveis aos usuários.

- *Internet Explorer Maitenance* (manutenção de Internet Explorer). Administram e personalizam o Microsoft Internet Explorer.

- *Folder Redirection* (Redirecionamento de pastas). Armazenam pastas específicas de perfil de usuário em um servidor de rede. As configurações criam um link no perfil para a pasta compartilhada na rede, mas as pastas são exibidas localmente. O usuário pode obter acesso à pasta em qualquer computador da rede. Por exemplo, você pode redirecionar a pasta My Documents de um usuário para uma pasta compartilhada na rede.

Configurações de diretiva de grupo para computadores e usuários



Um GPO contém dois nós distintos: Computer Configuration (Configuração do computador) e User Configuration (Configuração do usuário). As configurações do nó Computer Configuration são processadas somente por contas de computador. As configurações do nó User Configuration são processadas somente por contas de usuário.

Configurações de diretiva de grupo para computadores

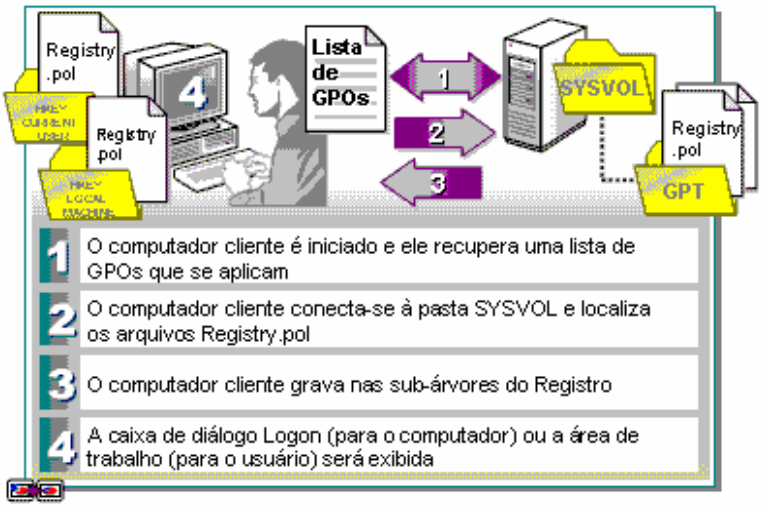
As configurações de diretiva de grupo para computadores especificam configurações do sistema operacional, da área de trabalho e de segurança, além de scripts de inicialização e

desligamento do computador, opções de aplicativos atribuídos a computadores e configurações de aplicativos. A diretiva de grupo relacionada a computadores é aplicada na inicialização do sistema operacional e durante o ciclo de atualização periódica. Em geral, a diretiva de grupo para computadores tem precedência sobre uma diretiva de grupo para usuários conflitante.

Configurações de diretiva de grupo para usuários

As configurações de diretiva de grupo para usuários especificam configurações do sistema operacional, da área de trabalho e de segurança, além de opções de aplicativos atribuídos e publicados, configurações de aplicativos, opções de redirecionamento de pastas e scripts de login e logoff. A diretiva de grupo relacionada a usuários é aplicada quando os usuários fazem logon no computador e durante o ciclo de atualização periódica.

Como a diretiva de grupo é aplicada



As configurações de diretiva de grupo e os valores das configurações aplicadas aos clientes do Windows 2000 e do Windows XP estão armazenados em um arquivo Registry.pol no GPT em controladores de domínio. Há dois Arquivos: Um para configurações no computador e outro para configurações do usuário.

Observação O caminho do arquivo Registry.pol é *raizdosistema*\SYSVOL\ sysvol*nome_de_domínio*\policies*identificador*_GUID_do_GPO\Machine ou \User.

Aplicando configurações durante o processo de inicialização

Este é um processo usado por um computador que executa o Windows 2000 ou o Windows XP Professional para aplicar as configurações da diretiva de grupo durante o processo de inicialização:

1. Quando o computador cliente é iniciado, ele recupera a lista de GPOs que contêm configurações de computador e determina a ordem de aplicação desses GPOs.

2. O computador cliente conecta-se à pasta SYSVOL do controlador de domínio que fez a autenticação e localiza os arquivos Registry.pol que se aplicam ao computador cliente na pasta Machine no GPT de cada GPO.

3. O computador cliente grava as configurações do registro e os respectivos valores contidos no arquivo Registry.pol na sub-árvore do Registro apropriada, a HKEY_LOCAL_MACHINE. O computador continua a inicializar o sistema operacional e aplica as configurações do Registro.

4. Depois que essas configurações tiverem sido aplicadas, a caixa de diálogo Logon (logon) será exibida.

Aplicando Configurações durante o processo de logon do usuário

Este é um processo usado por um computador que executa o Windows 2000 ou o Windows XP Professional para aplicar configurações de diretiva de grupo durante o processo de logon do usuário:

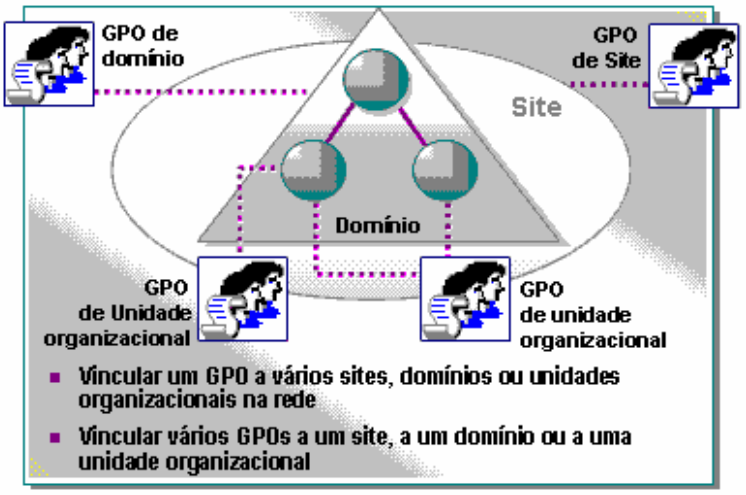
1. Depois que o usuário inicia o processo de logon, o computador cliente recupera a lista de GPOs que contêm configurações do usuário e determina a ordem de aplicação desses GPOs.

2. O computador cliente conecta-se à pasta SYSVOL do controlador de domínio que fez a autenticação e localiza os arquivos Registry.pol que contêm as configurações de diretiva de grupo que se aplicam ao usuário da pasta User no GPT de cada GPO.

3. O computador cliente grava as configurações do Registro e os respectivos valores contidos no arquivo Registry.pol na sub-árvore do Registro apropriada, a HKEY_CURRENT_USER. O computador continua o processo de logon e aplica as configurações do Registro.

4. Depois que essas configurações tiverem sido aplicadas, o computador cliente a área de trabalho do usuário.

Examinando vínculos de GPOs



Os GPOs são vinculados (ou seja, associados) a sites, domínios e unidades organizacionais. Devido a essa associação, é possível definir diretivas centralizadas que afetem toda a organização e diretivas descentralizadas que sejam determinadas pelo departamento. A vinculação de um GPO a um site, a um domínio ou a uma unidade organizacional faz com que as configurações de diretiva de grupo afetem objetos de usuário e de computador nesse site, domínio ou unidade organizacional.

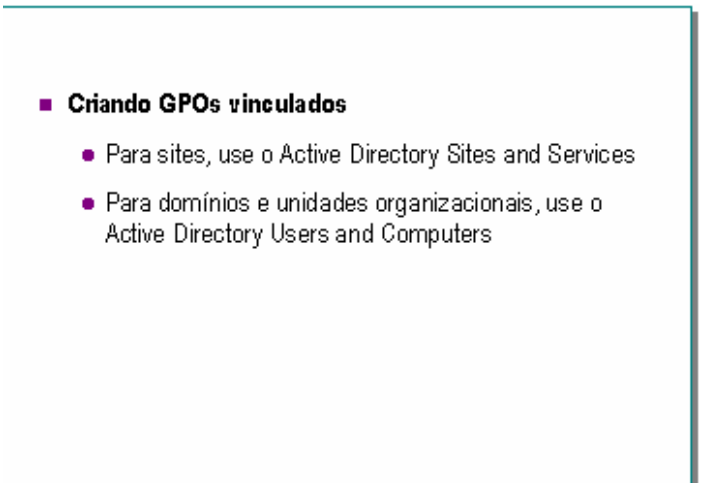
As informações que descrevem os GPOs vinculados a um recipiente do Active Directory estão armazenadas em dois atributos desse recipiente: **gPLink** e **gPOptions**. O atributo gPLink contém a lista priorizada de GPOs vinculados a um recipiente. O atributo gPOptions contém a configuração do recipiente que impede a herança de qualquer GPO.

A capacidade de vincular GPOs fornece flexibilidade na implementação de configurações de diretiva de grupo. É possível vincular GPOs de diversas maneiras:

- Vincular um GPO a vários sites, domínios ou unidades organizacionais na rede.

  Você pode usar esse método para definir as configurações de diretiva direta de grupo que se apliquem a usuários e a computadores em diferentes sites, domínios ou unidades organizacionais. Por exemplo, talvez seja necessário que todos os usuários dos departamentos de contabilidade, vendas e marketing executem o mesmo script de logon. Em vez de criar três GPOs separados, você pode criar um GPO que contenha o script de logon e vinculá-lo a todas as unidades organizacionais.

Criando GPOs vinculados e desvinculados



Ao criar um GPO vinculado a um site, a um domínio ou a uma unidade organizacional, você executa duas operações separadas: Você cria um novo GPO e, em seguida, vincula-o ao site, ao domínio ou à unidade organizacional. As condições a seguir são aplicáveis:

- É necessário que você tenha as permissões Read (Ler) e write (Gravar) nos atributos gPLink e gPOptions do recipiente ao qual o GPO está sendo vinculado.

- Por padrão, somente participantes dos grupos Domain Admins e Enterprise Admins possuem as permissões necessárias para vincular GPOs a domínios e unidades organizacionais, enquanto participantes do grupo Enterprise Admins possuem as permissões para vincular GPOs a sites.

- Participantes do grupo Group Policy Creator Owners criar GPOS, mas não podem vinculá-los.

Criando GPOs vinculados

Crie um GPO para domínios e unidades organizacionais usando o Active Directory Users and Computers.

Criar um novo GPO para um domínio ou uma unidade organizacional:

1. Abra o Active Directory Users and Computers.

2. Clique com o botão direito do mouse no domínio ou na unidade organizacional para a qual deseja criar um GPO e, em seguida, clique em Properties (propriedades).

3. Na linha Group Policy (Diretiva de grupo), clique em new (novo), digite o nome do novo GPO e pressione ENTER. O GPO criado será exibido na listas de GPOs associados à unidade organizacional ou ao domínio da guia Group Policy.

Observação Criar um novo GPO para um site é diferente de criar um GPO para um domínio ou para uma unidade organizacional, já que você usa o Active Directory Sites and Service (Serviços e sites do Active Directory) para administrar sites. É necessário que você seja participante do grupo Enterprise Admins para criar GPOs vinculados a sites.

Criando GPOs desvinculados

GPOs desvinculados podem ser criados em organizações nas quais um grupo seja responsável pela criação de GPOs e outro grupo vincule os GPOs ao site, domínio ou unidade organizacional necessários. Para criar um GPO desvinculado, adicione um snap-in Group Policy ao Microsoft Management Console (MMC).

Pra criar um GPO desvinculado:

1. No prompt de comando ou na caixa de diálogo Run (Executar). Digite mmc.exe e clique em OK ou pressione ENTER.

2. Adicione o snap-in Group Policy.

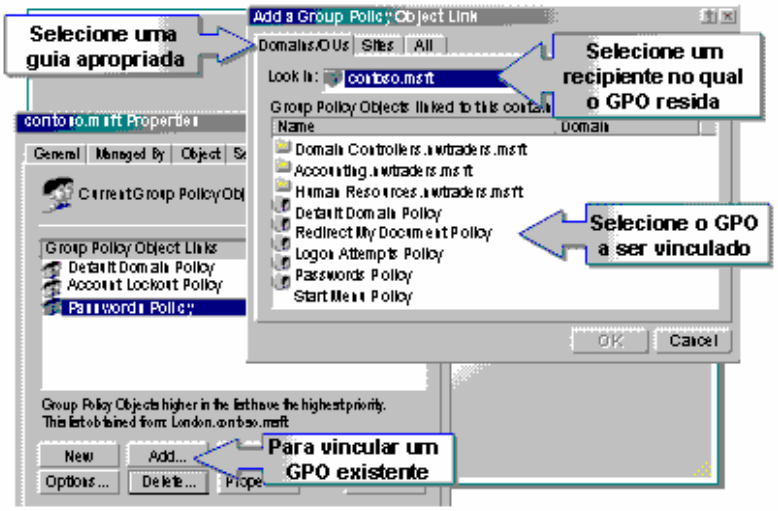
3. Na caixa de diálogo Select Group Policy Object (Selecionar objeto de diretiva de grupo), clique em Browse (procurar).

4. Na caixa de diálogo Browse for a Group Policy Object (Procurar um objeto de diretiva de grupo), na guia All (Tudo), clique com o botão direito do mouse em qualquer parte da lista All Group Policy Objects stored in this domain (Todos os objetos de diretiva de grupo armazenados neste domínio) e, em seguida, clique em new.

5. Digite um nome para o novo GPO e clique em OK para fechar a caixa de diálogo Browse for a Group Policy Object.

6. Para editar o novo GPO, clique em Finish (Concluir) na caixa de diálogo Select Group Policy Object. Caso contrário, clique em Cancel (Cancelar).

Vinculando um GPO existente



È possível aplicar as configurações de diretiva de grupo existentes a recipientes adicionais do Active Directory vinculando o GPO que contém as configurações necessárias a esses recipientes. Para vincular um GPO a um site, a um domínio ou a uma unidade organizacional, é necessário que você tenha as permissões Read e Write nos atributos gPLink e gPOptions desse site, domínio ou unidade organizacional.

Vinculando um GPO existente a domínios e unidades organizacionais

Vincule um GPO existente a domínios e unidades organizacionais usando o Active Directory Users and Computers executando as seguintes etapas:

1. Abra o Active Directory Users Computers.

2. Clique com o botão direito do mouse no domínio ou na unidade organizacional à qual deseja vincular um GPO existente e, em seguida, clique em Properties.

3. Na guia Group Policy, clique em Add (Adicionar)...

4. Clique na guia Domain/OUs (Domínio/OUs), na guia sites ou na guia All, conforme apropriado.

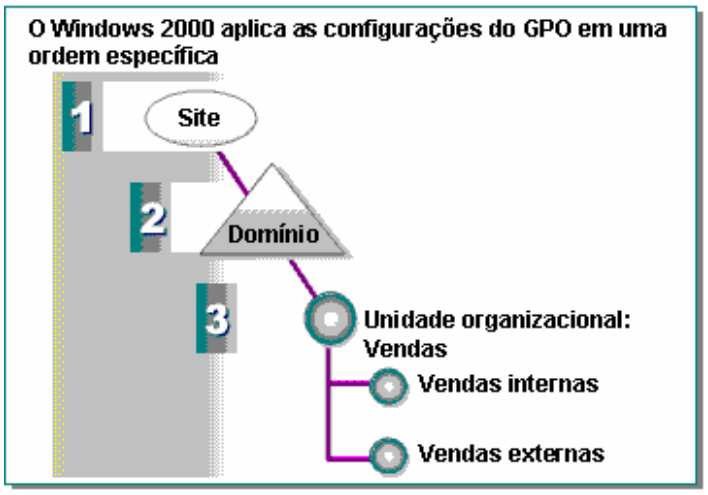
5. Na lista look in (Examinar), clique no domínio que contém o GPO a ser vinculado.

6. Na lista Group Policy Objects Linked to this container (Objetos de diretiva de grupo vinculados a esse recipiente), clique no GPO ao qual deseja se vincular e clique em OK.

Como as configurações de diretiva de grupo são aplicadas no Active Directory

As configurações de diretiva de grupo aplicadas a um usuário ou a um computador são determinadas por várias regras. Pra obter os resultados desejados, você precisa saber como elas são aplicadas.

Herança de diretiva de grupo



A herança de diretiva de grupo representa a ordem de configurações do GPO. A ordem na qual a diretiva de grupo é aplicada e o modo como as configurações de diretiva de grupo são herdadas determinam as configurações que afetarão usuários e computadores.

Fluxo da herança

Por padrão, as configurações do GPO são herdadas. A herança no Active Directory passa no site para o domínio, para a unidade organizacional e, por último, para qualquer unidade organizacional filho. Como os recipientes filhos herdam várias configurações de diretiva de grupo de seu recipiente pai, um filho pode ter várias dessas configurações aplicadas a seu conteúdo sem que um GPO esteja vinculado diretamente a ele. Se um recipiente filho tiver GPOs vinculados a ele, as configurações de outros recipientes pai em níveis superiores na árvore do Active Directory serão aplicadas primeiro; só depois serão aplicadas as configurações do recipiente filho.

Ordem de aplicação

A ordem de aplicação dos GPOs baseia-se no recipiente do Active Directory ao qual os GPOs estão vinculados. O Windows 2000 aplica os GPOs conforme a ordem de vinculação do GPO:

1. A um site
2. A domínios
3. A unidades organizacionais

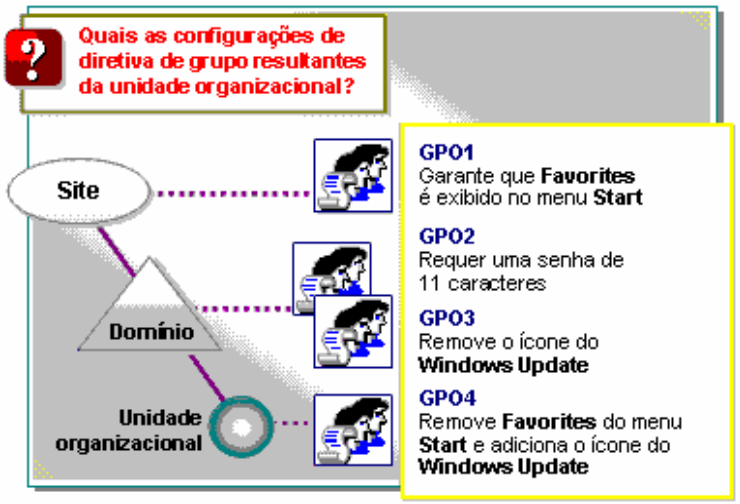
Portanto, as configurações de diretiva de grupo da unidade organizacional da qual um usuário ou um computador é participante são as configurações finais de diretiva de grupo aplicadas.

GPOs vinculados a sites

Como os sites representam a rede física, e os domínios e as unidades organizacionais representam a rede lógica, é importante entender como os GPOs vinculados a sites são aplicados.

- Qualquer site específico pode conter computadores de um ou mais domínios.
- Se um site contiver computadores de mais de um domínio, as configurações de diretiva de grupo definidas no GPO vinculado a esse site serão aplicadas a todos os computadores e a todos os usuários que fizerem logon em computadores desse site, independentemente do domínio no qual as contas de computador ou de usuário existem.

Discussão: Como a diretiva de grupo é aplicada



Em sua rede, os GPOs deScritos na tabela a seguir vinculados a recipientes do Active Directory.

GPO	Contém
GPO1	Uma configuração de diretiva de Grupo de conta que assegura a exibição da lista **Favorites** (Favoritos) no menu **Start** (Iniciar).
GPO2	Uma diretiva de grupo de conta que requer pelo menos 11 caracteres em uma senha.
GPO3	Uma configuração do menu **Start** que remove o ícone do Windows Update desse menu.
GPO4	Configurações do menu **Start** que asseguram a exibição do ícone do Windows Update nesse menu e que removem a lista **Favorites** do menu **Start**.

Quais são as configurações de diretiva de grupo resultantes para objetos de usuário na unidade organizacional? Por quê?

Estas são as configurações de diretiva de grupo resultantes:

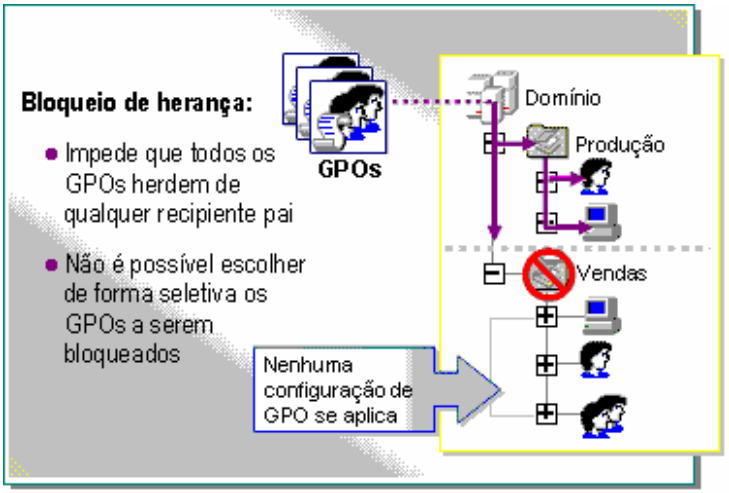
- **As senhas de usuário devem ter pelo menos 11 caracteres.**
- **O ícone do Windows Update deve ser exibido no menu Start.**
- **A lista Favorites não deve ser exibida no menu Start.**

A configuração de diretiva de grupo que remove a lista de Favorites do menu Start foi processada após a diretiva de grupo que inclui a lista de Favorites no menu Start. Esse processo assegura a não exibição da lista Favorites no menu Start. A configuração de diretiva de grupo que assegura a exibição do ícone do Windows Update no menu Start foi processada após a configuração de diretiva de grupo que removeu o ícone da área de trabalho. Esse processo assegura a exibição do ícone do Windows Update no menu Start.

Modificando a herança de diretiva de grupo

É possível controlar a herança de diretiva de grupo e a forma como as configurações de diretiva de grupo são aplicadas a computadores e usuários específicos. A modificação da herança permite bloquear, forçar ou filtrar a herança das configurações de diretiva de grupo.

Ativando o bloqueio da herança



Você pode impedir que um recipiente filho herde GPOs do recipiente pai ativando **Block Policy Inheritance** (Bloquear herança de diretiva) no recipiente filho. A ativação dessa opção em um recipiente filho impede que o recipiente herde todas as configurações da diretiva de grupo, mas não as configurações individuais.

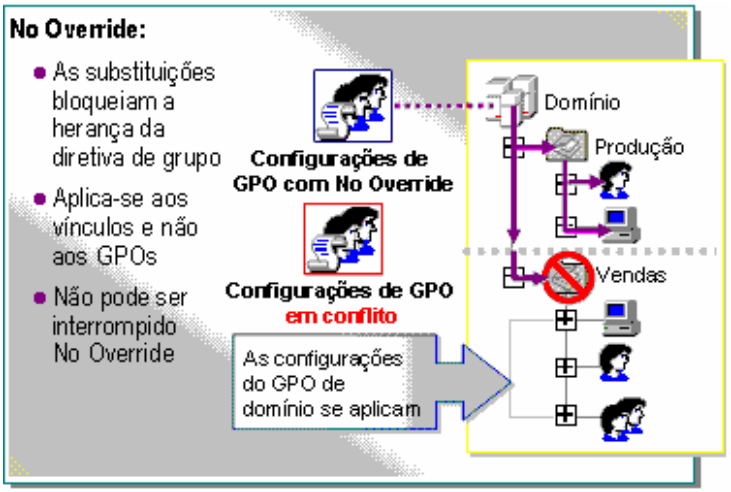
Isso é útil quando o Active Directory necessita de configurações de diretiva de grupo exclusivas e você deseja assegurar que as configurações não serão herdadas. Por exemplo, você pode usar a opção Block Policy Inheritance quando o administrador de uma unidade organizacional tiver de controlar todas as configurações de diretiva de grupo referentes a esse recipiente.

Não é possível escolher de forma seletiva de GPOs a serem bloqueados. O bloqueio de herança afeta todos os GPOs de todos os recipientes pai.

Para bloquear a herança de um GPO para um recipiente filho:

1. Abra a caixa de diálogo **Properties** do domínio ou da unidade organizacional na qual deseja bloquear a herança.
2. Na guia **Group Policy**, marque a caixa de seleção **Block Policy Inheritance**.

Ativando a opção No Override



A configuração Block Policy Inheritance não poderá interromper a herança de GPO vinculando a um recipiente pai se o vínculo estiver configurado com a opção No Override (Não substituir). A configuração No Override força a aplicação de todas as configurações de diretiva de grupo, mesmo que elas entrem em conflito com as configurações de GPO vinculado a um recipiente filho. A configuração No Override tem precedência sobre a configuração Block Policy Inheritance.

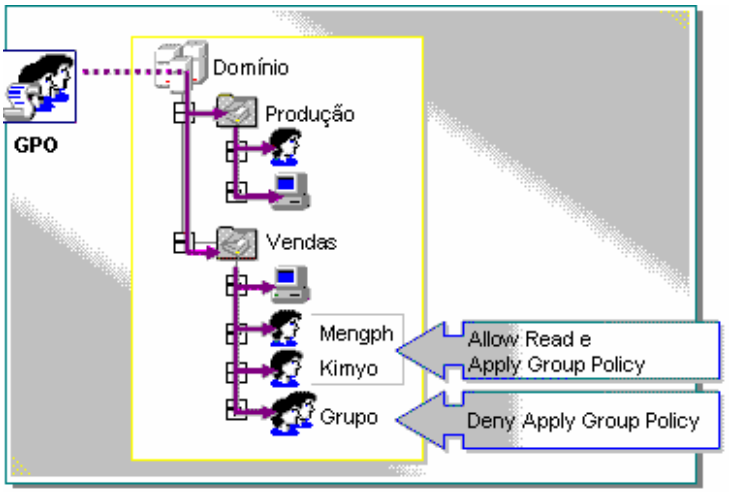
A opção No Override é definida no vínculo, e não no GPO. Caso haja um GPO vinculado a vários recipientes, você poderá configurar a opção No Override em cada recipiente, independentemente dos outros recipientes.

Quando mais de um vínculo é definido para a configuração No Override, o GPO de nível mais alto na hierarquia do Active Directory terá precedência.

Para definir a opção No Override:

1. Abra a caixa de diálogo Properties do recipiente ao qual o GPO está vinculado.
2. Na guia Group Policy, clique em Options (Opções).
3. Na caixa de diálogo Options, clique em No Override e, em seguida, clique em OK.

Filtrando configurações de diretiva de grupo



A filtragem é outro método que pode ser usado para modificar a herança da diretiva de grupo. A *filtragem* permite que você impeça que um GPO e sus as respectivas configurações sejam aplicados a computadores, usuários e grupos de segurança específicos em um recipiente.

Para que a diretiva de grupo seja aplicada a uma conta de usuário ou de computador, a conta deverá ter as permissões Allow Read (Permitir ler) e Allow Apply Group Policy (Permitir aplicar diretiva de grupo) para o GPO. As permissões padrão que afetam o processamento de um novo GPO são:

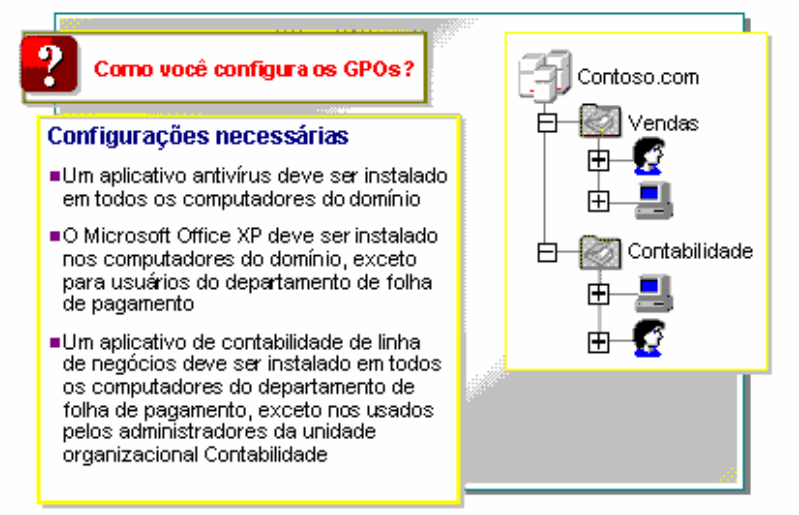
- *Authenticad Users.* Esse grupo oferece suporte às permissões Allow Read e Allow Apply Group Pplicy.

- *Domain Admins, Enterprise Admin e SYSTEM.* Esses grupos oferecem suporte às permissões Allow Read, Allow Write (Permitir gravar), Allow Creat All Child Objects (permitir criar todos os objetos filho), Allow Delete All Child Objects (permitir excluir todos os objetos filho).

Para filtrar um GPO de modo a impedir sua aplicação a um determinado objeto de computador, de usuário ou de grupo de segurança, você deve negar a permissão Apply Group Policy no GPO relevante.

Dica Se você precisa delegar tarefas de filtragem, delegue-as a um grupo de domínio local para filtrar as configurações de diretiva de grupo em um nível de domínio ou de unidade organizacional. Para filtrar as configurações de diretiva de grupo em um nível de site, delegue-as a um grupo global.

Discussão: Alterando a herança de diretiva de grupo



Você determinou que as seguintes condições devem ser aplicadas à sua rede:

- Um aplicativo antivírus deve ser instalado em todos os computadores de domínio.
- O Microsoft Office XP deve ser instalados nos computadores do domínio, exceto para usuários de departamento de folha de pagamento.
- Um aplicativo de contabilidade de linha de negócios deve ser instalado em todos os computadores do departamento de folha de pagamento, exceto nos usados pelos administradores da unidade organizacional Contabilidade.

Como você configuraria os GPOs para que as condições fossem aplicadas?

Primeiro crie um GPO vinculado ao domínio que instala o aplicativo antivírus e defina a opção No Override no vínculo. Em seguida, crie e vincule outro GPO no nível de domínio de instalação do Office XP.

Depois disso, na unidade organizacional Contabilidade, ative a opção Block Policy Inheritance. A opção No Override no vínculo referente ao GPO que implanta o aplicativo antivírus assegura que ele não estará bloqueado. Em seguida, crie e vincule um GPO à unidade organizacional Contabilidade que instala o aplicativo de contabilidade nos computadores cliente.
Finalmente, modifique a Discretionary Acces Control List (DACL, lista de controle de acesso discricional) desse GPO para que seja negada a permissão Apply Group Policy para as contas de computador usadas pelos administradores da unidade organizacional Contabilidade.