GPO

Group Policy Objects

Da teoria à prática – Ajudando administradores a automatizar tarefas

"Um guia prático e didático destinado a administradores de redes, que facilitará o trabalho diário de todos."

Group Policy Objects

Da teoria à prática – ajudando a Administradores a automatizar tarefas

“Um guia prático e didático destinado a administradores de redes, que facilitará o trabalho diário de todos.”

Esse é um trabalho da Comunidade de TI Microsoft. Todas as informações aqui escritas são de responsabilidades dos autores!

Autores:

Alexandro Prado: Profissional com projetos de implantação de sistemas operacionais Desktop/Client, desde o Windows 2000 Professional até o Windows 7, SCCM, SCOM, SCVMM, FEP, WAIK, MDT e outros. Possui as certificações: MCP/MCDST/MCTS/MCITP. MVP - Windows Expert-Consumer. Instrutor Oficial MCT - Microsoft Certified Trainer. Na comunidade Technet Brasil, atua com moderador dos Fóruns Technet. Líder do Grupo MS-InfraRio (ug.gitca.org/sites/MS-InfraRio/default.aspx) e Co-Líder do Grupo MSRio.NET (blog.msriodotnet.com), organiza, coordena e realiza palestras, eventos e seminários em todo o estado do Rio de Janeiro. Líder do Grupo MS-InfraRio (Líder), e outros, organizando palestras, eventos e encontros técnicos. Atua como Analista de Infraestrutura e Consultor em ambientes Microsoft. Ministra Treinamentos Oficiais. Atua ainda como moderador e colaborador no Forum Technet e Wiki: http://msdn.microsoft.com/pt-br/library/default.aspx, ajudando na tradução para o português. Beta Tester de vários produtos Microsoft. PASS Chappter Regional Mentor. **Twitter: @alexandroprado**

Daniel Donda: Especializado em sistemas operacionais de rede e segurança. Atua no mercado de TI desde 1996. MVP Windows Expert-IT Pro possui as seguintes certificações MCP,MCT,MCITP-EA, MCSA+Security, MCSE+Security, MCSE+Messaging, EC-Certified Ethical Hacker V7, EC-Council Instructor (CEI),autor de diversos artigos técnicos e autor dos livros “MCSE/MCSA Guia de Certificação Windows Server 2003" e ”Administração do Windows Server 2008 R2 - Server Core". Lider do grupo MUGSS Mcsesolution.com e colaborador do MCPBrasil.com. Atua ainda como palestrante dp Microsoft TechDay www.mstechday.com e colaborador ativo do TechNet Wiki www.technet.com/wiki . Beta-tester oficial de sistemas operacionais Microsoft. **Twitter: @danieldonda**

Sumário

Prefácio 4

O que é GPO? 5

Herança de GPOS, qual GPO ganha? 6

Bloquear Herança 7

Forçar a aplicação de uma GPO 7

Criar uma GPO. 8

Vinculando GPO. 8

Criando Filtros de segurança e WMI 9

Starter GPOs 11

Configurar (Editar) uma GPO 12

Filtro de diretivas 13

Group Policy Preferences (GPP) 14

Item Level targeting 16

Algumas diretivas interessantes: 17

Instalação de Softwares via GPO. 18

Entendendo o User Group Policy Loopback Processing Mode 19

Prefácio

Quando fui convidado pelo Alexandro Prado e Daniel Donda a fazer o prefácio deste e-book fiquei feliz de poder contribuir com estes dois grandes profissionais.

A primeira vez que tive contato com recursos de Gerenciamento de Ambientes (Configuration Manager) foi em 1994 quando trabalhava com Novell 3.2 e tive contato com o NDS que já incluía algumas funções de automação, mas ainda eram poucas.

Em 1998 a Novell avaliou tornar essas funções um produto completo e com mais recursos. Foi quando surgiu o ZENworks que era um produto muito bom e permitia configurar muitos recursos das estações.

Até então falávamos da Microsoft como sendo a fabricante do SO Windows NT e já havia o SMS 1.0 e logo após o SMS 2.0. Porem, eram produtos que não permitiam gerenciamento do ambiente do usuário no mesmo nível que era feito pelo ZENworks.

Em 2000 com o lançamento do Windows 2000 nas versões Server e Workstation, tivemos contato com o Active Directory e vimos como a Microsoft se preocupou em cobrir esta lacuna deixada pelo SAM do Windows NT e SMS.

Com o Windows 2003 vimos o AD evoluir mais ainda nas configurações possíveis com GPOs e agora com o Windows 2008 tivemos a inclusão do recurso de “Preferencias” (Preferences) que incluiu recursos importantíssimos.

Windows 2000	Windows 2003	Windows 2008 RTM/R2
• Configuração dos principais componentes do Windows • Configuração dos principais recursos de desktop ativo • Configuração das regras de segurança (SecEdit) • Instalação de software no modelo Windows Installer • Configurações por computador ou usuário • Permite herança, bloquei de herança e regras mandatórias	• Novas configurações de componentes, desktop e segurança • Inclusão do novo console Group Policy Management Console • Inclusão de perfis para redes wireless	• Inclusão de “Preferences” que permite configurar o que antes era feito por scripts, como mapeamento de impressoras, discos e até aspectos do desktop do usuário • Inclusão de filtros WMI, permitindo GPOs especificas conforme o hardware da estação • Criação de modelos com o recurso “Starter GPO”

Aproveite este e-book para utilizar esta poderosa ferramenta de forma consistente e com eficiência.

O que é GPO?

Quando falamos sobre **GPO (*Group Policy Object*)** devemos pensar em **diretiva de grupo**. Diretiva de grupo é um conjunto de regras que podemos utilizar a fim de facilitar o gerenciamento, configuração e segurança de computadores e usuários.
As regras das diretivas de grupo se aplicam a usuários e computadores.

Você configura as diretivas em uma GPO. A GPO com estas regras (para usuários e computadores) podem ser aplicadas (vinculadas) no:

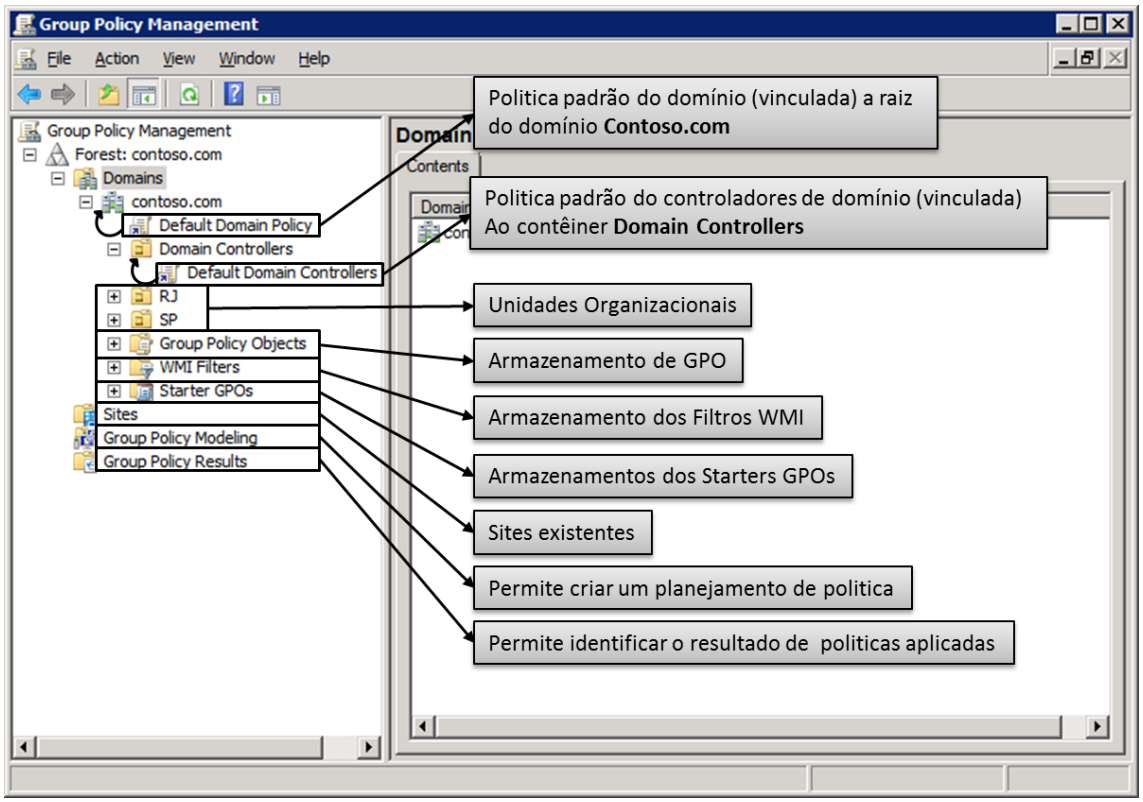
- **Site**
- **Domínio**
- **OU**

Definindo assim a **Hierarquia das GPOs** onde:

Sites: O mais alto nível. Todas as configurações feitas no site serão aplicadas a todos os usuários/computadores/domínios nesse site.

Domínios: É o segundo nível. Configurações feitas aqui afetarão todos os usuários/computadores dentro do domínio.

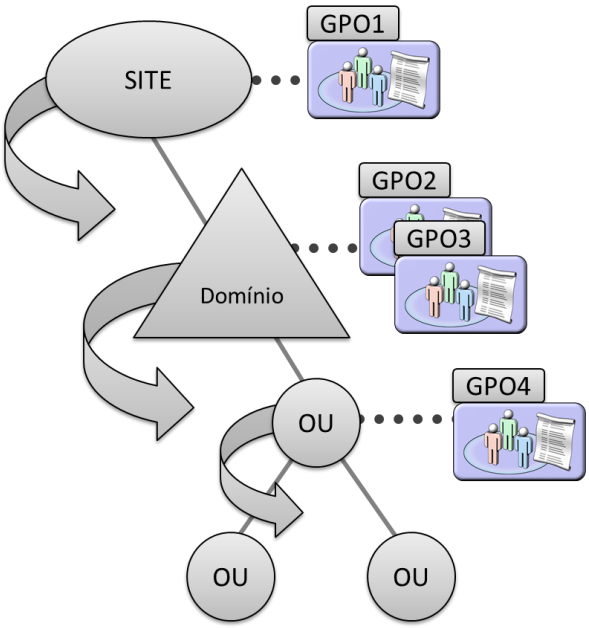
OUs: O que se aplica nas **OUs** afetarão todos os usuários/computadores dentro dela.
A ferramenta para trabalhar no gerenciamento de politica de grupo (GPO) é o Snap-in "**Group Policy Management**".



- Computadores fora do domínio também podem ter diretivas configuradas localmente (Use o GPEDIT.MSC).

Herança de GPOS, qual GPO ganha?

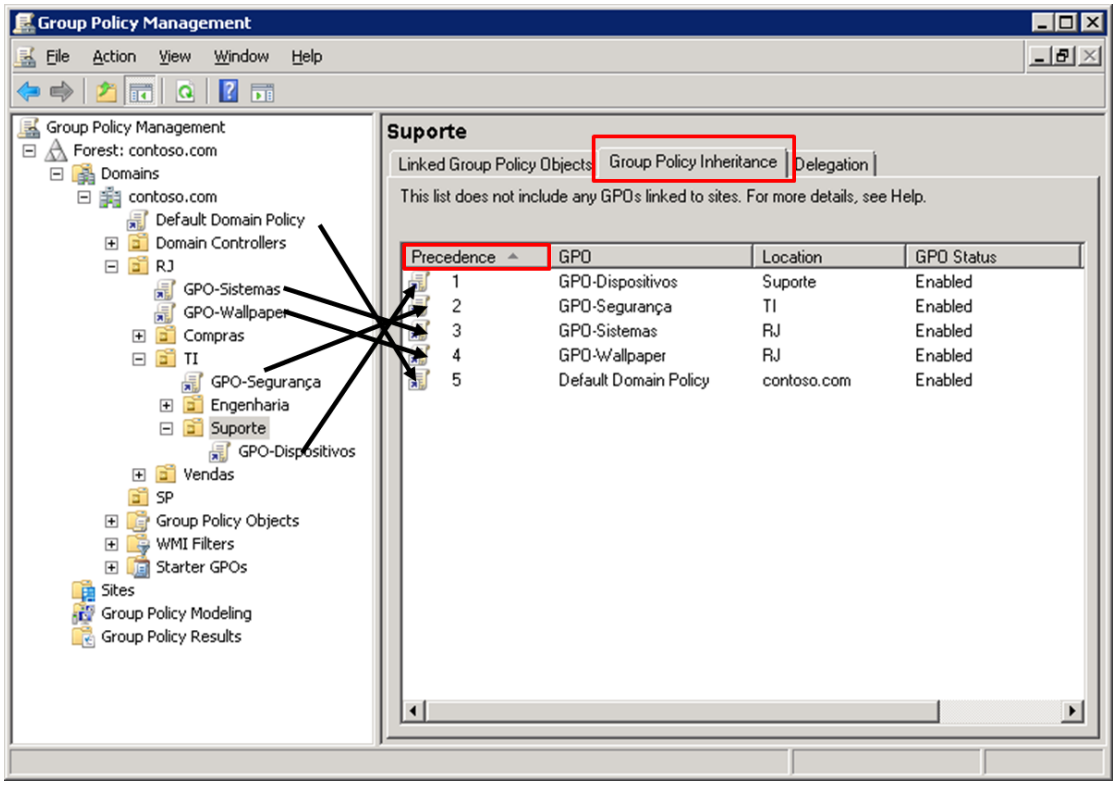
As diretivas são cumulativas, assim um computador/usuário pode receber configurações que vieram do Site, domínio e também da OU no qual ele pertence.



Na imagem, se houver um computador/usuários em qualquer OU este receberá a GPO1, depois a GPO2, depois a GPO3 e por ultimo a GPO4.

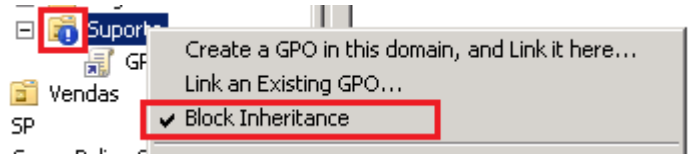
Caso as diretivas sejam conflitantes elas serão sobrescritas pelas diretivas aplicadas por ultimo. Vamos entender:
GPO1 – Acesso ao Painel de Controle – **Disabled**
GPO2 – Acesso ao Painel de Controle – **Enabled**
GPO3 – Acesso ao Painel de Controle – **Disabled**
GPO4 – Acesso ao Painel de Controle – **Enabled**

A ultima GPO aplicada foi a GPO4 por isso ela tem preferencia ou como alguns gostam de falar A GPO4 “Ganha”.



Bloquear Herança

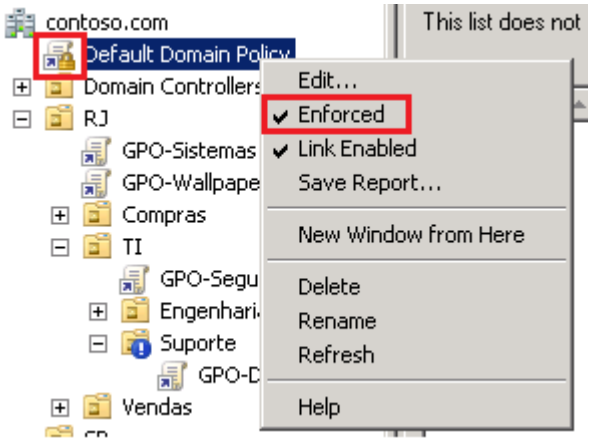
Você pode bloquear uma herança, marcando a opção "**Block Inheritance" sobre a Unidade Organizacional** que não quer aplicar diretivas herdadas.



Forçar a aplicação de uma GPO

Você pode também forçar a aplicação de uma diretiva, de modo que ela **terá precedência sobre todas as outras.**

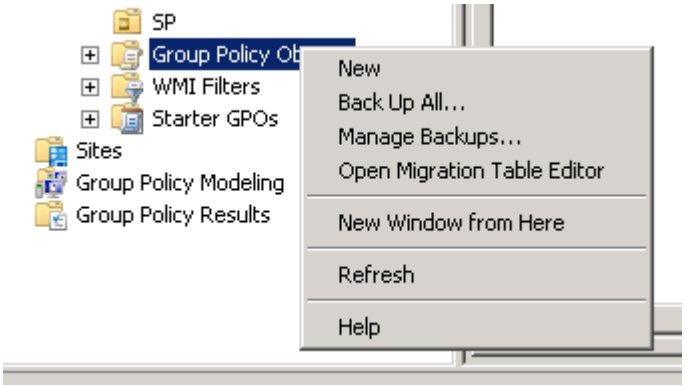
Para isso marque a opção **Enforce sobre a GPO**.



Criar uma GPO.

Criar uma GPO não significa que ela faz alguma coisa. Alias você pode criar um monte de GPO que nada acontece até você **configurar** e **vincular** (linkar).
Se você desejar você pode criar uma GPO já vinculando em um OU.

No **Group Policy Management** clique com o lado direito em **Group Policy Object** e selecione Novo.



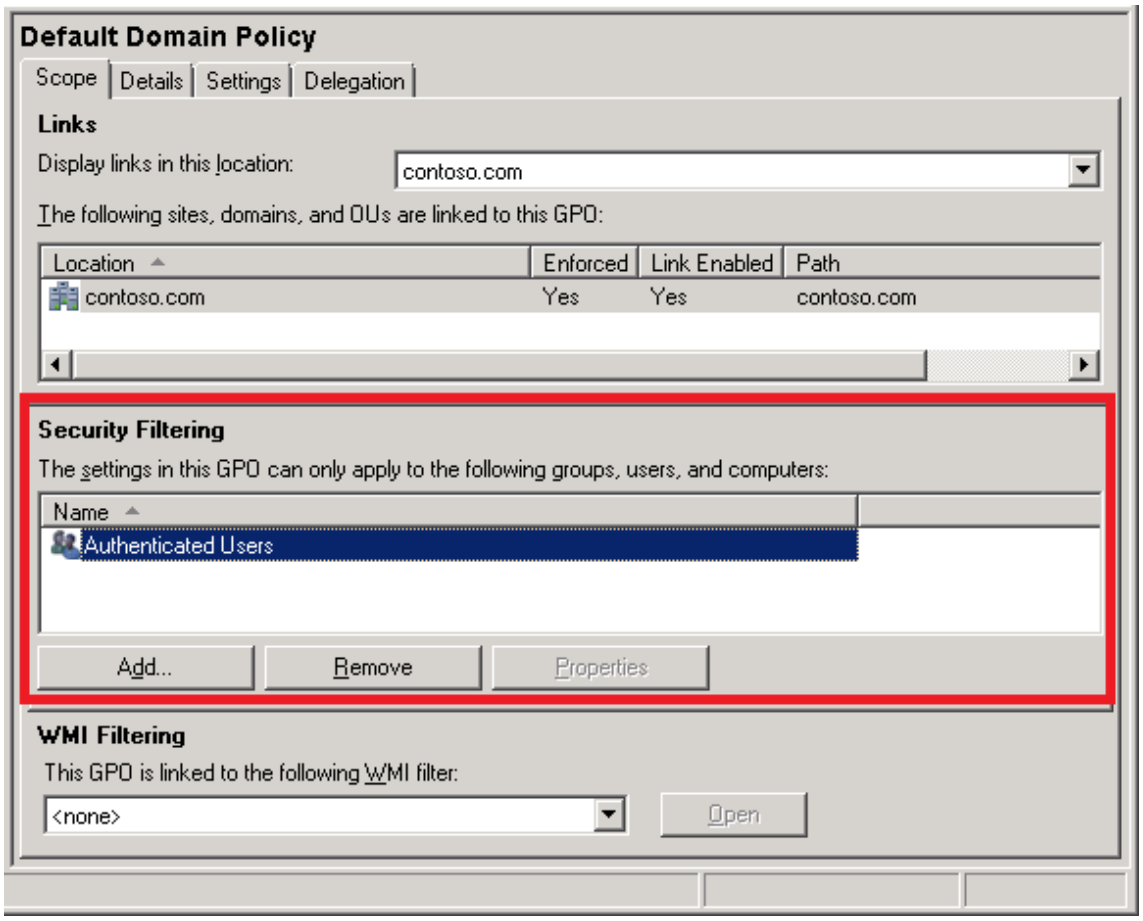
Vinculando GPO.

Você pode criar as **GPOs** no nó **Group Policy Objects** e depois vincular ou você pode criar uma GPO já vinculando a uma OU ou domínio.

Criando Filtros de segurança e WMI

Filtros de segurança.
Após vincular uma GPO você pode ainda criar filtros de usuários ou grupos, assim as diretivas somente serão aplicadas para os grupos de usuários ou computadores que você desejar.
Pense bem, você pode aplicar uma politica no Domínio, mas somente o grupo que você definir receberá a politica.
Por padrão recebem as politicas os usuários autenticados.

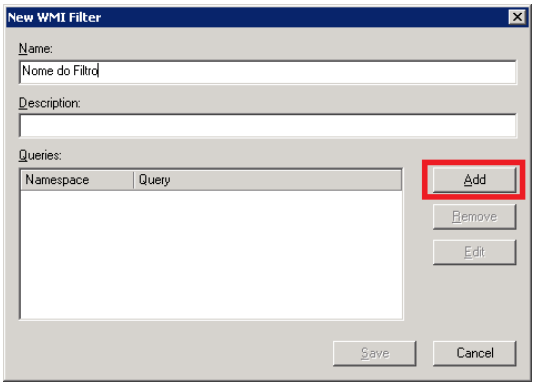
Clique sobre uma diretiva e o painel da direita exibe o escopo.



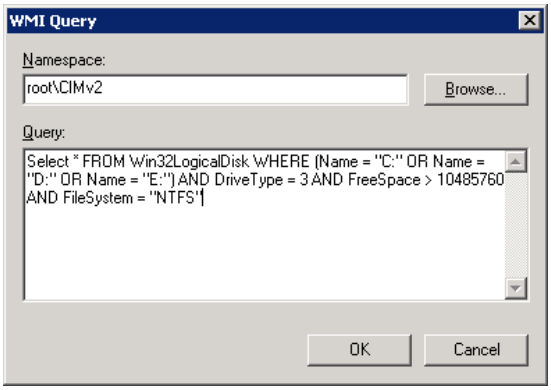
Filtros WMI

O WMI disponibiliza informações sobre o computador de destino. Essas informações podem ser dados de hardware e software, configurações e informações de configuração. Por exemplo, o WMI pode criar filtros baseados em hardware como CPU, memória, espaço em disco e fabricante, ou de software, tipo Registro, drivers, sistema de arquivos, Active Directory, serviço Windows Installer, configuração de rede etc.

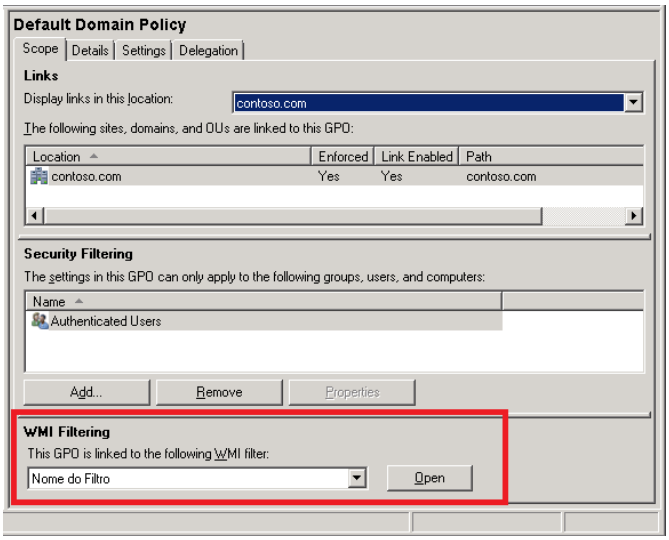
1. Para criar filtros WMI, acesse o nó **WMI Filters**, lado direito e selecione **NEW**.



2. Clique no botão Add e adicione a WMI query.
   Acesse http://technet.microsoft.com/pt-br/library/cc779036(WS.10).aspx para saber mais.



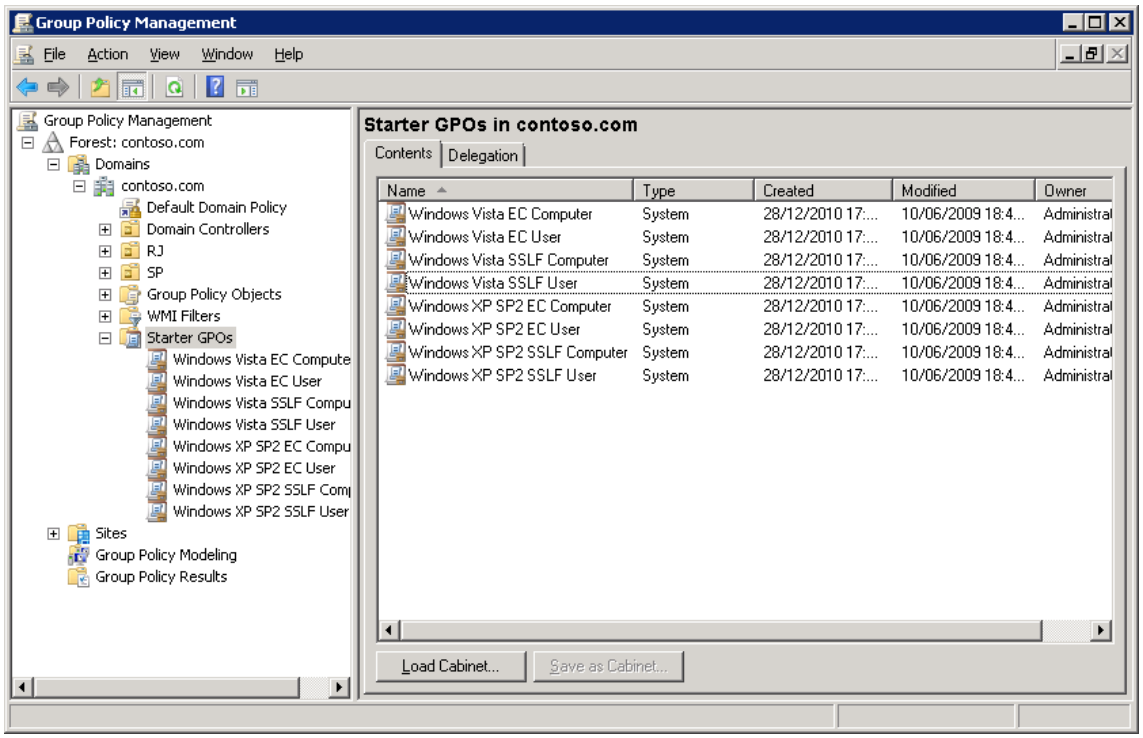
3. No escopo da GPO (quando clicar na GPO, do lado direito) selecione o filtro criado.



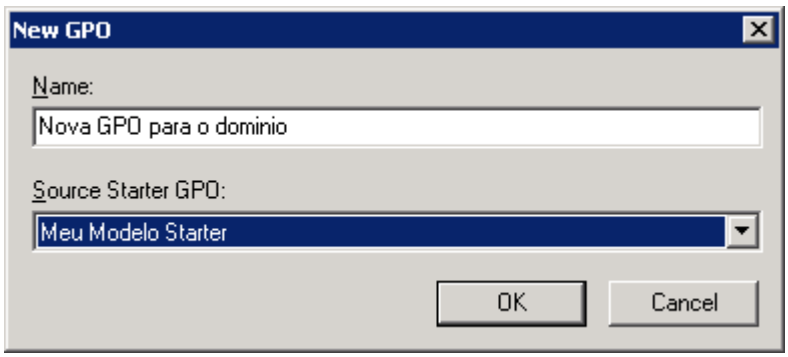
Starter GPOs

Quando você cria muitas GPOs com configurações similares você pode fazer uso do novo recurso do Windows Server 2008 chamado "**Starter GPOs**" que servirá de base para as GPOS que você criar no futuro. Ainda fornece a opção de **exportar** e **importar** para qualquer domínio usando a **extensão .CAB**.

Para trabalhar com Starter GPOs, clique no nó Starter GPOs e em seguida clique no botão "Create Starter GPOs Folder".
A criação da pasta vem com modelos para Windows Vista e XP (SSLF e EC) para entender mais sobre EC e SSLF acesse: http://www.mcsesolution.com/Windows-Server-2008/seguranca-melhores-praticas.html



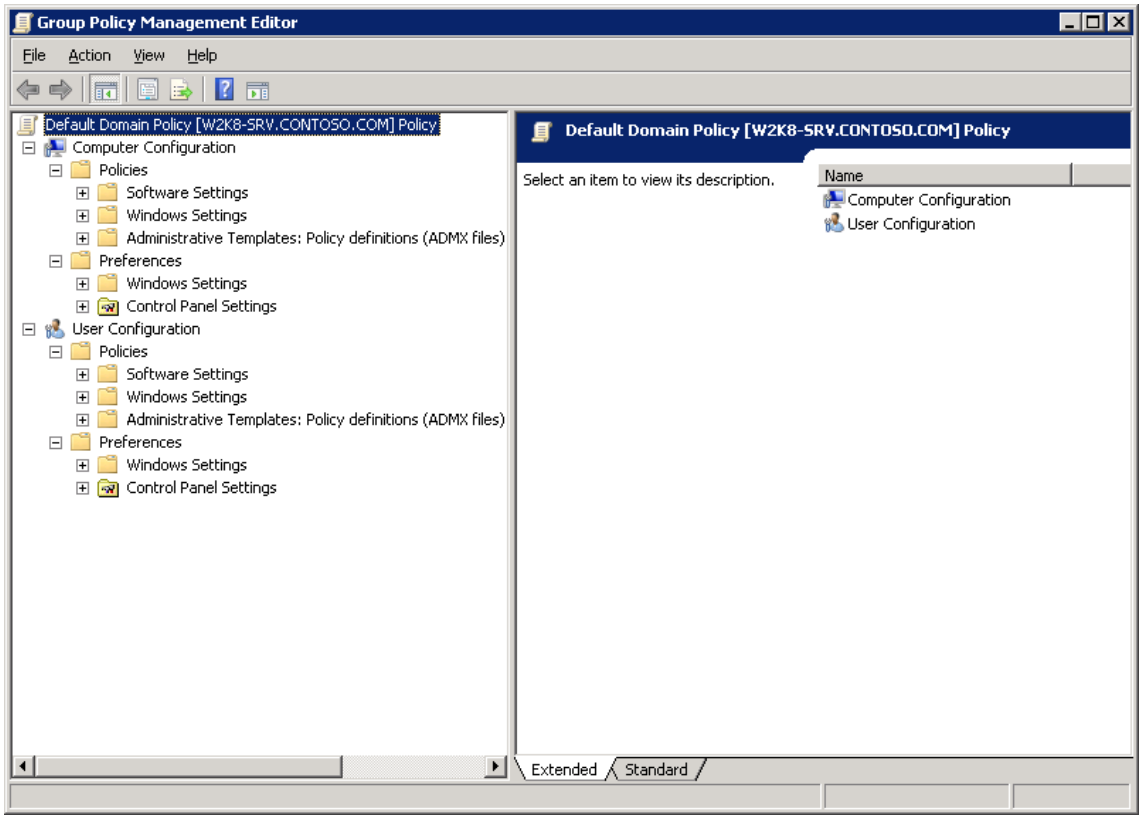
Você pode criar seu próprio modelo e sempre que criar um GPO para aplicar a um site, domínio, ou OU você pode cria-lo a partir do seu modelo de Starter GPOs.



Configurar (Editar) uma GPO

Agora sim vamos definir o que será aplicado ao computador/usuário.
Você criou e vinculou uma GPO agora é só clicar com o lado direito e selecionar Edit para que você escolha quais politicas serão definidas.

O Editor de politicas até que é bem simples:



Nele podemos definir diretivas para:

Computador que estas são aplicadas quando o Windows é carregado e depois entre 90 e 120 minutos.
Usuário que é aplicada quando um usuário faz logon e depois disso também é atualizada entre 90 e 120 minutos.

Computer Configuration

- **Policies**
  - **Software Settings** > Usado para instalação de softwares
  - **Windows Settings** > Configuração de Scripts, Segurança (senhas, auditoria), firewall, NAP, restrição de softwares.
  - **Administrative Templates** > São definições de configuração de registro. Nas versões anteriores ao vista a extensão era ADM, hoje ADMX (bem menor também). Você obter templates administrativos no Microsoft Download Center, por exemplo, para configurar o Office.
- **Preferences >** Recurso novo no Windows Server 2008.

- **Windows Settings**
- **Control Panel Settings**

User Configuration

- **Policies**
  - **Software Settings** > Usado para instalação de softwares
  - **Windows Settings** > Configuração de Scripts de logon/Logoff, restrição de softwares. Redirecionamento de pastas, Configuração do IE.
  - **Administrative Templates** > Assim como para computador são definições de configuração de registro.
- **Preferences >** Recurso novo no Windows Server 2008.
  - **Windows Settings**
  - **Control Panel Settings**

Não são poucas configurações não olha só, são mais de 3000 diretivas... Vamos ver só algumas nesse E-Book.

No site Microsoft Download Center você baixa planilhas com todas as Diretivas.

Filtro de diretivas

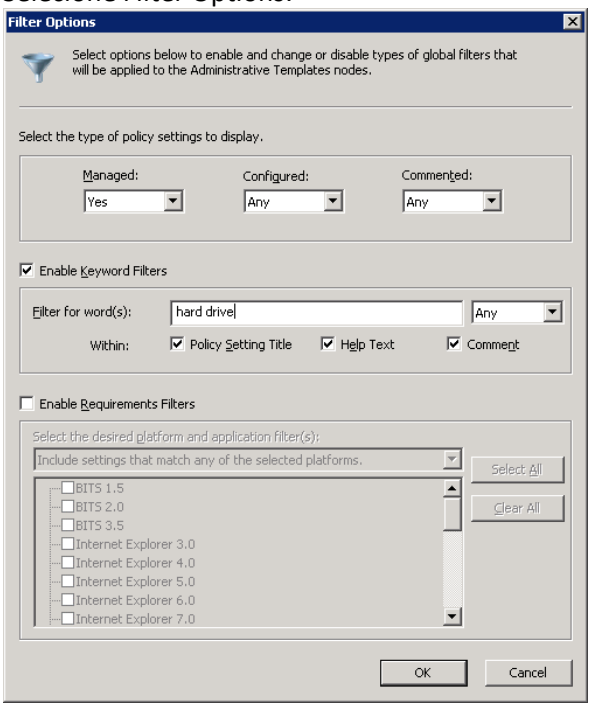
O melhor recurso do Windows 2008, pois as vezes queremos fazer determinada configuração e não sabemos onde está localizado o item que devemos configurar.
Por exemplo, eu quero ocultar o Disco C:, onde é que eu configuro?

Para isso é só criar um filtro:

1. Ao editar uma GPO, clique em **Administrative Templates** (pode ser tanto de user como de computer).
2. Clique no menu em VIEW.

Observe os passos a seguir:

3. Selecione Filter Options.



4. Em **Filter for word** digite a palavra que procura e clique OK.
5. Somente as diretivas que possuírem a palavra chave (No titulo, help ou comentário) serão exibidas.
6. Para facilitar ainda mais, selecione o nó **"All settings (*todas as configurações*)"** dentro de **administrative Templates**.

Group Policy Preferences (GPP)

Esses novos nós existentes apenas no Windows Server 2008 facilitam a vida do administrador incluindo mais de 20 novas extensões de Diretiva de Grupo.
Essas diretivas ajudam o gerenciamento criando-se um alvo especifico usando vários tipos de filtros.
Para que essa politicas funcionem é necessário a instalação do **Client Side Extension**.

- Group Policy Preference Client Side Extensions for Windows Vista (KB943729)
- Group Policy Preference Client Side Extensions for Windows Vista x64 Edition (KB943729)
- Group Policy Preference Client Side Extensions for Windows Server 2003 (KB943729)
- Group Policy Preference Client Side Extensions for Windows Server 2003 x64 Edition (KB943729)
- Group Policy Preference Client Side Extensions for Windows XP (KB943729)

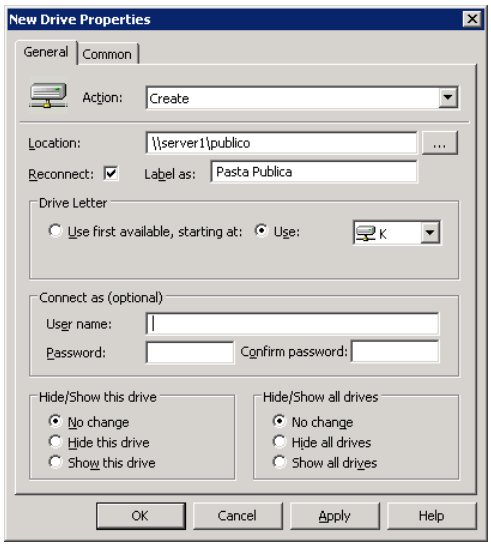
Windows Settings

Applications
Drive Maps
Environment
Files
Folders
Ini Files
Registry
Shortcuts

Control Panel Settings

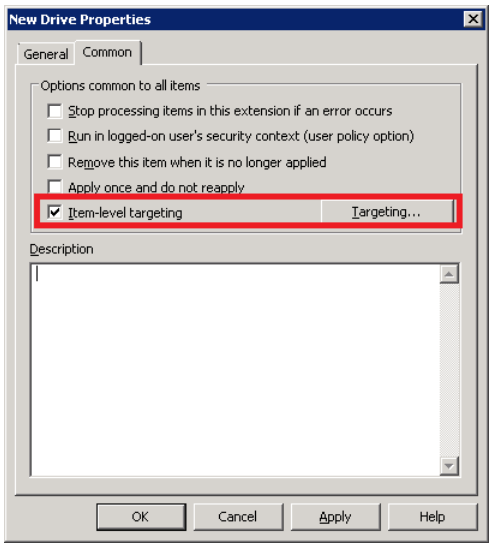
Data Sources
Devices
Folder Options
Internet Settings
Local Users and Groups
Network Options
Power Options
Printers
Regional Options
Scheduled Tasks
Start Menu

Para cada opção você tem varias configurações, por exemplo:
Criar um mapeamento.
Em Windows Settings > Drive Maps > New

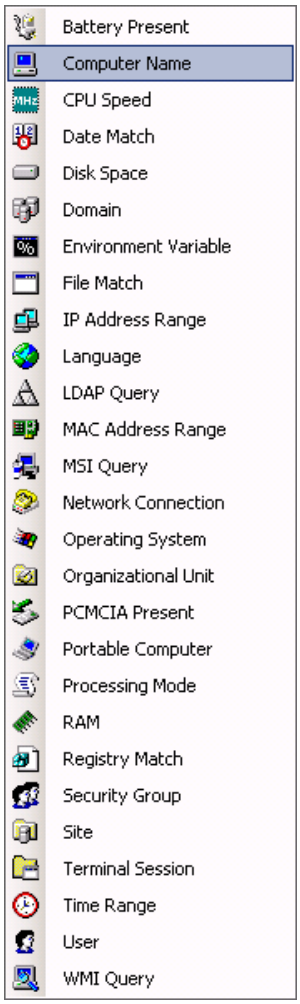


Se você clicar em Common você tem mais opções, como o exemplo abaixo:

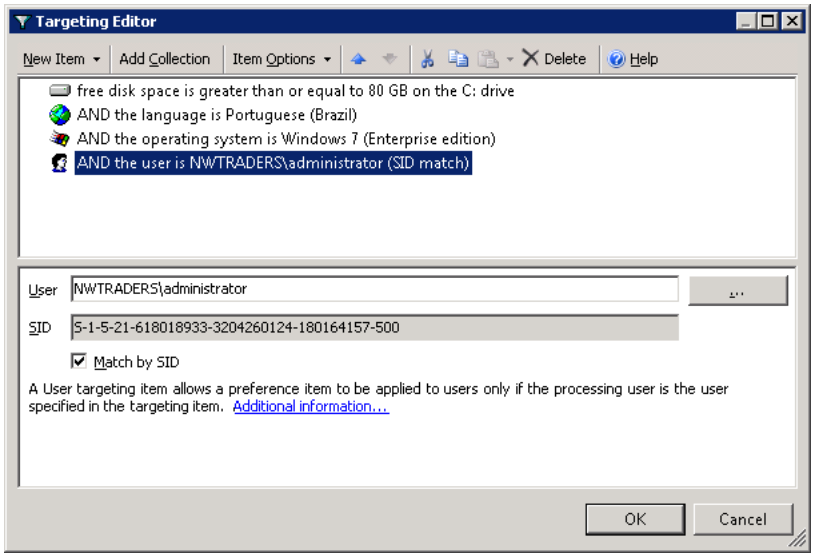
Item Level targeting



Onde você pode selecionar uma ou mais das seguintes opções:



E fazer uso de operadores booleanos para definir um "**Target**". Veja o exemplo o mapeamento somente irá acontecer se: O C: tiver 80 GB livre e o sistema for Windows 7 Enterprise e for em português e o se o usuário for o Administrador.



Algumas diretivas interessantes:

Bloquear USB com mensagem para o usuário.
Computer Configuration/Administrative Templates/System/Device Installation/Device Installation Restrictions
Display a custom message title when device installation is prevented by a policy setting
Display a custom message when installation is prevented by a policy setting
Prevent installation of removable devices

Esconder um disco (HD)
User configuration/Administrative Templates/Windows Components/Windows Explorer
Hide these specified drives in My Computer

Não deixar gravar CD/DVD
User configuration/Administrative Templates/Windows Components/Windows Explorer/
Remove CD Burning features

Colocar o RUN no menu iniciar
User configuration/Administrative Templates/Start Menu and Taskbar
Add the Run command to the Start Menu

Definir um papel de parede
User configuration/Administrative Templates/Desktop/Desktop
* Desktop Wallpaper
Disable all itens
Enable Active Desktop

Proibir acesso ao Painel de Controle
User configuration/Administrative Templates/Control Panel
Prohibit access to the Control Panel

Instalação de Softwares via GPO.

É possível criar uma diretiva de instalação de softwares. Podendo instalar arquivos do tipo **MSI** ou **EXE** (Utilizando um arquivo ZAP, veja mais adiante).
A instalação pode ser feita usando as configurações de computador e de usuários.

Computer Configuration (Instalação de softwares pensando nas maquinas)
Disponível apenas a opção **Assigned (*Atribuído*)** – ***Somente para arquivos MSI*** – > A instalação ocorre automaticamente quando a maquina ligar e o software ficara disponível no **menu iniciar.**

User Configuration (Instalação de softwares pensando nos usuários)
Permite a opção **Assigned (*Atribuído*)** – ***Somente para arquivos MSI*** – O software ficara disponível para instalação no **menu iniciar** (*Não é instalado automaticamente, instalação é iniciada pelo usuário ao primeiro clique*).

Disponível também a opção **Publish (*Publicado*) – *Aceita arquivos MSI e ZAP* -** que aceita tanto os arquivos **MSI** como os arquivos **ZAP**.
Arquivos ZAP são criados usando um editor de texto (**notepad.exe**) e apontam para a localização do arquivo EXE na rede.

Veja um modelo:

```
[Application]
; Este é um modelo de arquivo ZAP
; Somente é necessario utilizar as opções FriendlyName e SetupCommand

FriendlyName = "Nome do Programa"
SetupCommand = "\\server\compartilhamento\setup.exe"
DisplayVersion = 1.0
Publisher = Microsoft
```

 Para saber mais....

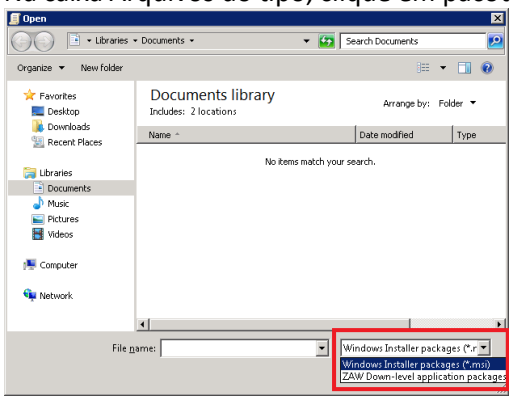
Antes de iniciar a distribuição de arquivos através de **GPO** – é interessante configurar o caminho da pasta com os softwares a serem instalados.
Esta pasta deverá ser compartilhada (Todos – Leitura).

Configurando o servidor.
Em **User Configuration** ou **Computer Configuration > Policies > Software Settings** , clique com o botão direito do mouse em **Software Installation** e selecione propriedades.

No campo **Default package location** digite o caminho \\server\compartilhamento\

Como publicar um EXE.

Em **User Configuration**, clique com o botão direito do mouse em **Software Installation** e em seguida, clique em novo.
Clique em **Package**.
Digite o caminho para a pasta que contém o **arquivo.zap**.
Clique em **Abrir**.
Na caixa Arquivos do tipo, clique em pacote de aplicativos de nível inferior ZAW (* .zap).



Clique em arquivo **.zap** e clique em **Abrir**.
Clique em **Publish** e clique em **OK**.

Entendendo o User Group Policy Loopback Processing Mode

Como você viu nesse e-book GPO possui configurações para usuários e computadores, assim a politica de computador é aplicada ao computador e a politica de usuário é aplicada ao usuário.

Agora vamos imaginar que você tenha domínio e que existam duas unidades organizacionais. **OU-TERMINALSERVERS** e **OU-SUPORTE**.
A **OU-TERMINALSERVERS** possui contas de computadores e a **OU-SUPORTE** contem contas de usuários.

Na **OU-TERMINALSERVERS** você cria e configura uma **GPO**.
Então existem politicas para:
•***Computer Configuration***
•***User Configuration***

Na **OU-SUPORTE** você cria e configura uma **GPO**.
Existem politicas de:
•***Computer Configuration***
•***User Configuration***

Se determinado usuário pertencente a **OU-SUPORTE** fizer logon em um computador pertencente a **OU-TERMINALSERVERS** o que acontece?

Aplica-se:

•**Computer Configuration** -> São as configurações criadas na politica da **OU-TERMINALSERVERS**
•**User Configuration** -> São as configurações criadas na politica da **OU-SUPORTE**

Isso é o padrão, agora vamos finalmente entender a politica: **User Group Policy Loopback processing Mode**
Ao configurar a politica, você pode escolher dois modos, Replace e Merge:

Modo Replace

Quando você definir o User Group Loopback processing Mode - No modo replace para a OU-TERMINALSERVERS.

Aplica-se:
•***Computer Configuration*** -> São as configurações criadas na politica da OU-TERMINALSERVERS
•***User Configuration*** -> São as configurações criadas na politica da OU-TERMINALSERVERS

Modo Merge

Quando você definir o **Loopback processing Mode** - No modo Merge para OU-TERMINALSERVERS.

Aplica-se:
•***Computer Configuration*** -> São as configurações criadas na politica da OU-TERMINALSERVERS
•***User Configuration*** -> São as configurações criadas na politica da OU-TERMINALSERVERS

Mais
•***User Configuration*** -> São as configurações criadas na politica da OU-SUPORTE

Atenção: Em caso de conflito das politicas de usuários (User Configuration) da OU-TERMINALSERVERS terá precedência. Como os GPOs do computador são processados após as GPOs do usuário, elas têm precedência se qualquer uma das definições de conflito

Por que essa configuração pode ser útil?

Digamos que você tem usuários em sua rede que possuem suas pastas redirecionadas via configurações de GPO. Mas você não deseja que o redirecionamento ocorra quando os usuários logarem via Terminal Server.

Neste caso habilite **o Loopback processing Mode (Replace)** nas GPO que está vinculada a OU onde estão as contas de computadores do Terminal Server e não habilite o redirecionamento de pastas. Assim quando os usuários fizerem logon no Terminal Services a politica de redirecionamento de pastas não será aplicada.

Como configurar o Loopback processing Mode?

No Group Policy Management Editor selecione Edit sobre a politica escolhida e em seguida expanda:
"Computer Configuration > Policies > Administrative Templates > System > Group Policy"

Clique duas vezes sobre "**User Group Policy Loopback processing Mode**"