Escopo de GPO

...

Definição

- Um GPO é, por si só, apenas uma coleção de instruções de configuração que serão processadas pela CSEs de computadores.
- Até o escopo do GPO, ele não se aplica a nenhum usuário ou computador. o escopo do GPO determina quais CSEs dos computadores receberão e processarão o GPO.
- E somente os computadores ou usuários dentro do escopo de um GPO aplicarão as configurações nesse GPO.
- Várias mecanismos são usados para definir um GPO

- O link do GPO para um site, domínio ou unidade organizacional e se esse link está habilitado
- A opção forçar uma GPO
- A opção Bloquear Herança em uma UO
- Filtragem do grupo de segurança
- filtragem WMI
- Nó de política, habilitando ou desabilitando
- Segmentação de preferências
- Processamento de política de loopback

- Você deve ser capaz de definir os usuários ou computadores nos quais a configuração é implantada e portanto, você deve dominar a arte de delimitar os GPOs.
- Nesta Aula, você aprenderá cada um dos mecanismos com os quais você pode definir um GPO e, no processo, os conceitos de aplicação , herança e precedência do GPO

Links do GPO

- Um GPO pode ser vinculado a um ou mais sites, domínios ou unidades organizacionais do Active Directory.
- Depois que uma política é vinculados a um site, domínio ou unidade organizacional, os usuários ou computadores desse contêiner estão no escopo do GPO, incluindo computadores e usuários em OUs filhas.
- Por padrão, os sites do Active Directory não ficam visíveis no GPME; você deve primeiro clique com o botão direito do mouse em Sites e escolha Mostrar sites.

Pulo do Gato I

- Um GPO vinculado a um site afeta todos os computadores do site sem considerar o domínio a que pertencem os computadores (desde que todos os computadores pertençam à mesma floresta).
- Como o GPO é armazenado no DC onde foi criado , deve haver conectividade com o DC onde o GPO está para que os computadores apliquem o GPO .

Pulo do gato 2

- Você pode vincular um GPO a mais de um site, domínio ou unidade organizacional. É comum, por exemplo, aplicar configuração para computadores em várias OUs.
- Você pode definir a configuração em um único GPO e vincular esse GPO a cada UO.
- Se você alterar posteriormente as configurações no GPO, suas alterações serão aplicadas para todas as UOs às quais o GPO está vinculado.

- Você pode excluir um link de GPO escolhendo Excluir no menu de contexto. Excluindo um link de GPO não exclui o próprio GPO, que permanece no contêiner Objetos de Diretiva de Grupo.
- Excluindo o link altera o escopo do GPO para que ele não se aplique mais a computadores e usuários dentro de um site, domínio ou UO ao qual foi vinculado anteriormente.
- Você também pode modificar um link de GPO desativando-o. Clique com o botão direito no link do GPO e desmarque o link Opção ativada.
- Desabilitar o link também altera o escopo do GPO para que ele não seja mais aplicável a computadores e usuários dentro deste contêiner.
- No entanto, o link permanece para que ele possa ser facilmente reativado.

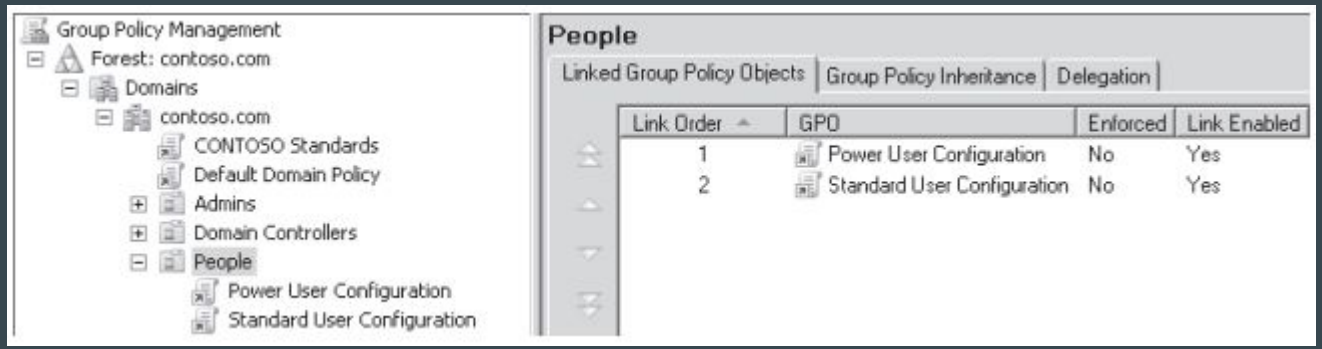
Herança e Precedência do GPO

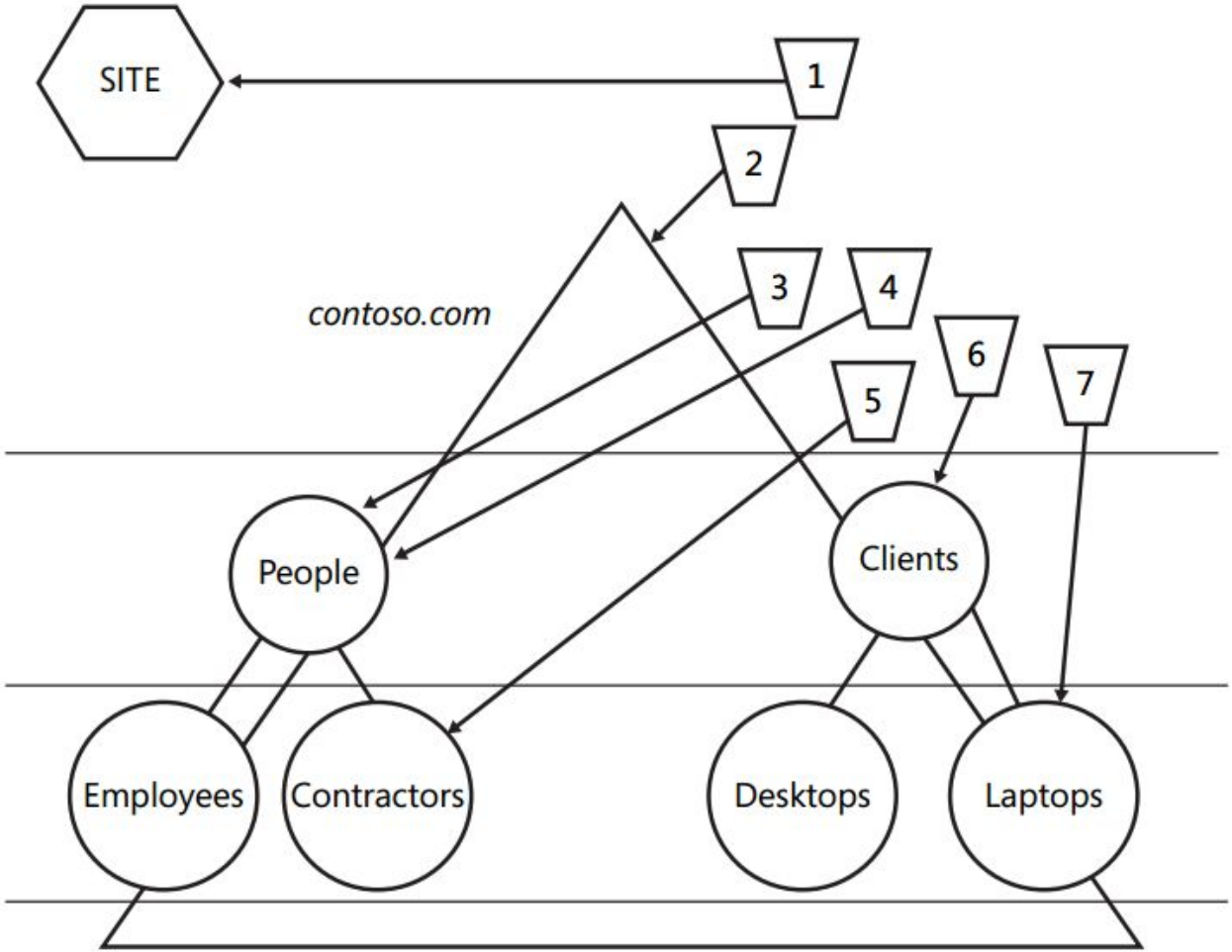
- Uma configuração de política pode ser configurada em mais de um GPO e os GPOs podem estar em conflito com um outro.
- Por exemplo, uma configuração de política pode ser ativada em um GPO, desativada em outro GPO e não configurado em um terceiro GPO. Nesse caso, a precedência dos GPOs determina qual configuração de política o cliente aplica.
- Um GPO com maior precedência prevalecerá sobre um GPO com menor precedência.
- Precedência é mostrada como um número no GPMC. Quanto menor o número - ou seja, quanto mais próximo de 1 - maior a precedência, portanto, um GPO com uma precedência de 1 irá prevalecer sobre outros GPOs.
- Selecione o domínio ou UO e clique na guia Herança de Diretiva de Grupo para exibir a precedência de cada GPO.

- Você pode excluir um link de GPO escolhendo Excluir do menu de contexto. Excluindo um link de GPO não exclui o próprio GPO, que permanece no contêiner Objetos de Diretiva de Grupo.
- Excluindo o link altera o escopo do GPO para que ele não se aplique mais a computadores e usuários dentro de um site, domínio ou UO ao qual foi vinculado anteriormente.
- Você também pode modificar um link de GPO desativando-o. Clique com o botão direito no link do GPO e desmarque o link Opção ativada.
- Desabilitar o link também altera o escopo do GPO para que ele não seja mais aplicável a computadores e usuários dentro deste contêiner.
- No entanto, o link permanece para que ele possa ser facilmente reativado.

Precedência de vários objetos de diretiva de grupo vinculados

- Uma UO, domínio ou site pode ter mais de um GPO vinculado a ele.
- No caso de múltiplos Objetos de Diretiva de Grupo, a ordem dos links dos objetos determina sua precedência.




SITE
1
2
3
4
5
6
7
contoso.com
People
Clients
Employees
Contractors
Desktops
Laptops

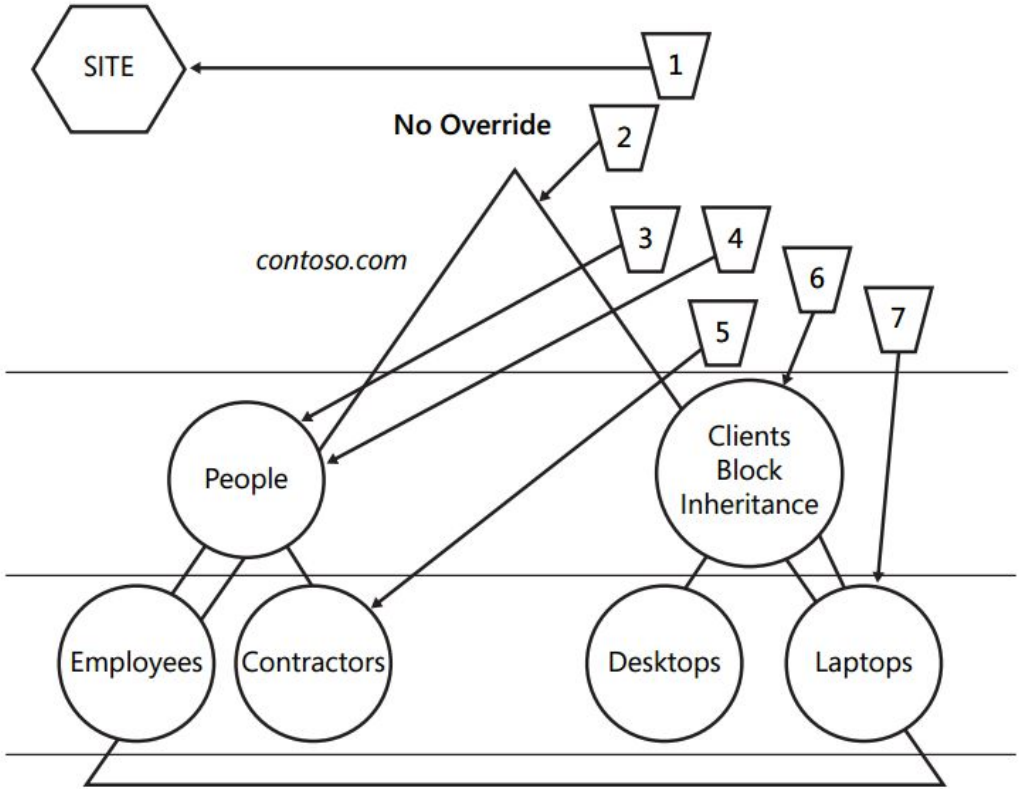
Pulo do gato 2

- Você pode vincular um GPO a mais de um site, domínio ou unidade organizacional. É comum, por exemplo, aplicar configuração para computadores em várias OUs.
- Você pode definir a configuração em um único GPO e vincular esse GPO a cada UO.
- Se você alterar posteriormente as configurações no GPO, suas alterações serão aplicadas para todas as UOs às quais o GPO está vinculado.

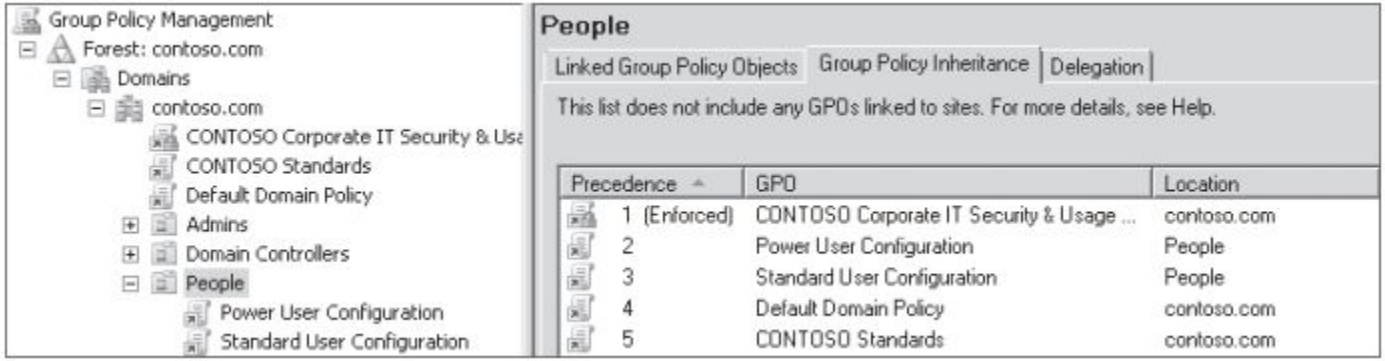
Bloqueio de herança

- Um domínio ou uma unidade organizacional pode ser configurado para impedir a herança de configurações de diretiva.
- A opção Bloquear Herança é uma propriedade de um domínio ou UO, portanto, bloqueia todas as configurações de Diretiva de Grupo dos GPOs vinculados a pais na hierarquia da Diretiva de Grupo.
- Quando você bloqueia herança em uma UO, por exemplo, o aplicativo de GPO começa com qualquer GPO vinculado diretamente a essa UO
- Os GPOs vinculados a unidades organizacionais de nível superior, o domínio ou o site não serão aplicados.
- A opção Block Inheritance deve ser usada com moderação, se for o caso.

- Bloquear herança faz com que mais difícil avaliar a precedência e a herança da Diretiva de Grupo.
- O interessante é aprender como definir um GPO para que ele se aplique para apenas um subconjunto de objetos ou para que seja impedido de se aplicar a um subconjunto de objetos.
- Com filtragem de grupo de segurança, você pode definir com cuidado um GPO para que ele se aplique somente usuários e computadores em primeiro lugar, tornando desnecessário o uso da herança.


SITE
1
No Override
2
contoso.com
3
4
6
7
5
People
Clients
Block
Inheritance
Employees
Contractors
Desktops
Laptops

- Quando você configura um GPO que define a configuração determinada por sua segurança de TI corporativa e políticas de uso, você deseja garantir que essas configurações não sejam substituídas por outros GPOs.
- Você pode fazer isso impondo o link do GPO.
- O link do GPO tem um cadeado - o indicador visual de um link imposto.
- Para facilitar a avaliação da precedência do GPO, basta selecionar uma OU (ou domínio) e clicar em na guia Herança de Diretiva de Grupo.
- Essa guia exibirá a precedência resultante dos GPOs,responsáveis pelo link de GPO, ordem dos links, bloqueio de herança e aplicação de link.
- Esta aba não conta para políticas que estão vinculadas a um site, nem conta para segurança de GPO ou filtragem WMI.
-


Group Policy Management
Forest: contoso.com
Domains
contoso.com
CONTOSO Corporate IT Security & Usa
CONTOSO Standards
Default Domain Policy
Admins
Domain Controllers
People
Power User Configuration
Standard User Configuration
People
Linked Group Policy Objects
Group Policy Inheritance
Delegation
This list does not include any GPOs linked to sites. For more details, see Help.
Precedence
GPO
Location
1 (Enforced)
CONTOSO Corporate IT Security & Usage ...
contoso.com
2
Power User Configuration
People
3
Standard User Configuration
People
4
Default Domain Policy
contoso.com
5
CONTOSO Standards
contoso.com

Usando o filtro de segurança para modificar o escopo do GPO

- Até agora, você aprendeu que pode vincular um GPO a um site, domínio ou unidade organizacional.
- No entanto, você pode precisar aplicar GPOs somente a determinados grupos de usuários ou computadores, e não a todos os usuários ou computadores dentro do escopo do GPO.
- Embora você não possa vincular diretamente um GPO a um grupo de segurança , existe uma maneira de aplicar GPOs a grupos de segurança específicos.
- As políticas em um GPO são aplicadas somente para usuários que têm permissão para Permitir Ler e Permitir Aplicar Diretiva de Grupo ao GPO.
-

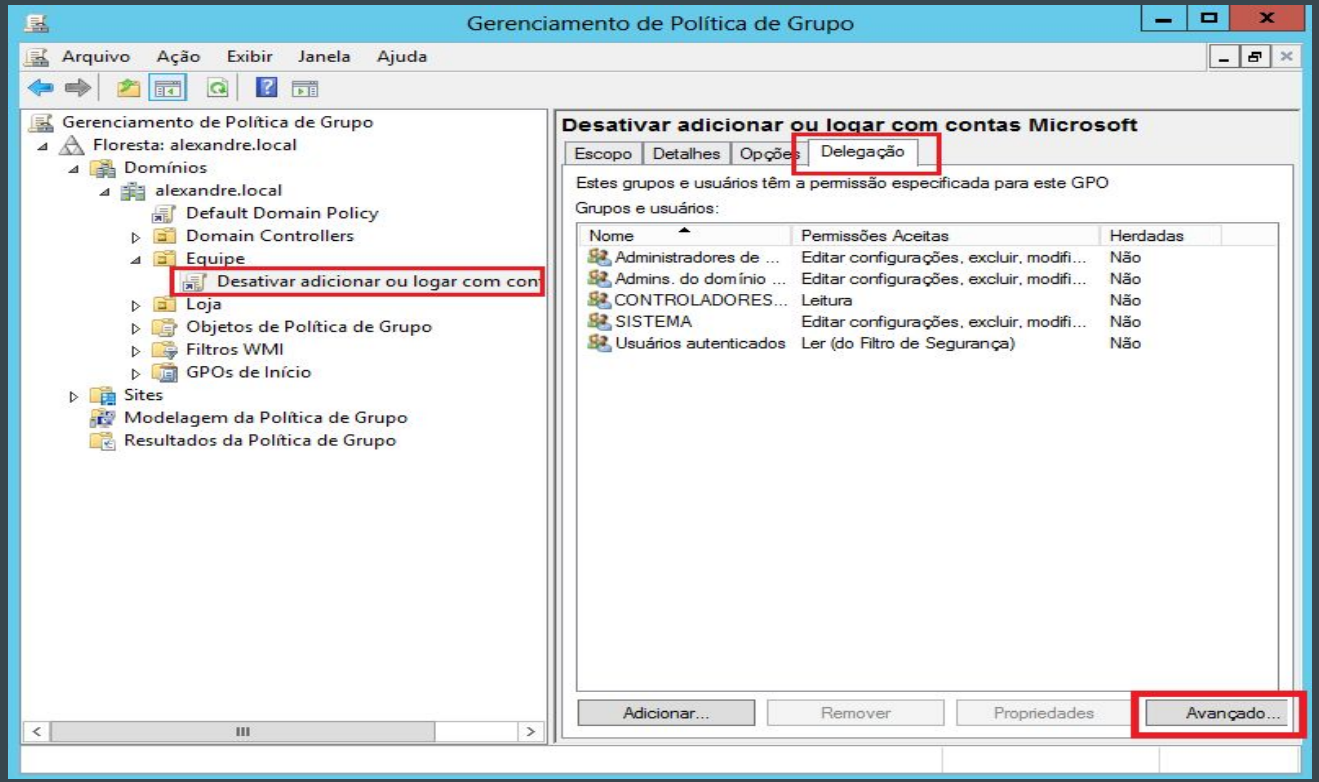
- Cada GPO tem uma lista de controle de acesso (ACL) que define permissões para o GPO.
- Duas permissões, Permitir Ler e Permitir Aplicar Diretiva de Grupo são necessárias para que um GPO seja aplicado a um usuário ou computador.
- Se um GPO tiver um escopo definido para um computador, por exemplo, por seu link para a UO do computador, mas o computador não tem permissões para Ler e Aplicar Diretiva de Grupo, ele não fará o download e aplicará o GPO.
- Portanto, definindo as permissões apropriadas para grupos de segurança, você pode filtrar um GPO para que suas configurações se apliquem apenas aos computadores e usuários especificados.
- Por padrão, os Usuários Autenticados recebem a Permissão de Diretiva de Grupo Permitir Aplicação em cada novo GPO.

- Isso significa que, por padrão, todos os usuários e computadores são afetados pelos GPOs definidos para seu domínio, site ou unidade organizacional, independentemente dos outros grupos em que possam ser membros.
- Portanto, há duas maneiras de filtrar o escopo do GPO:
  - **Remova a permissão Aplicar Diretiva de Grupo (atualmente definida como Permitir)** para o grupo Usuários autenticados, mas não defina essa permissão para Negar. Em seguida, determine os grupos a que o GPO deve ser aplicado e defina as permissões Ler e Aplicar Diretiva de Grupo para esses grupos para permitir.
  - **Determine os grupos aos quais o GPO não deve ser aplicado e defina a opção Aplicar para Negar.** Se você negar a política de grupo para um GPO o usuário ou computador não aplicará as configurações no GPO, mesmo se o usuário ou computador é um membro de outro grupo permitido ao grupo Aplicar Política .

- Para aplicar um GPO a um grupo de segurança específico, selecione o GPO no contêiner Objetos de Diretiva de Grupo no GPMC.
- Na seção Filtragem de segurança, selecione o grupo Usuários autenticados e clique em Remover.
- Clique em OK para confirmar a alteração e clique em Adicionar.
- Selecione o grupo ao qual você deseja que a política seja aplicada e clique em OK.
- Grupo Usuários Autenticados não está listado, e o grupo específico ao qual a política deve ser aplicada é listado.
- Os GPOs podem ser filtrados apenas com grupos de **segurança globais** - não com grupos de segurança locais de domínio

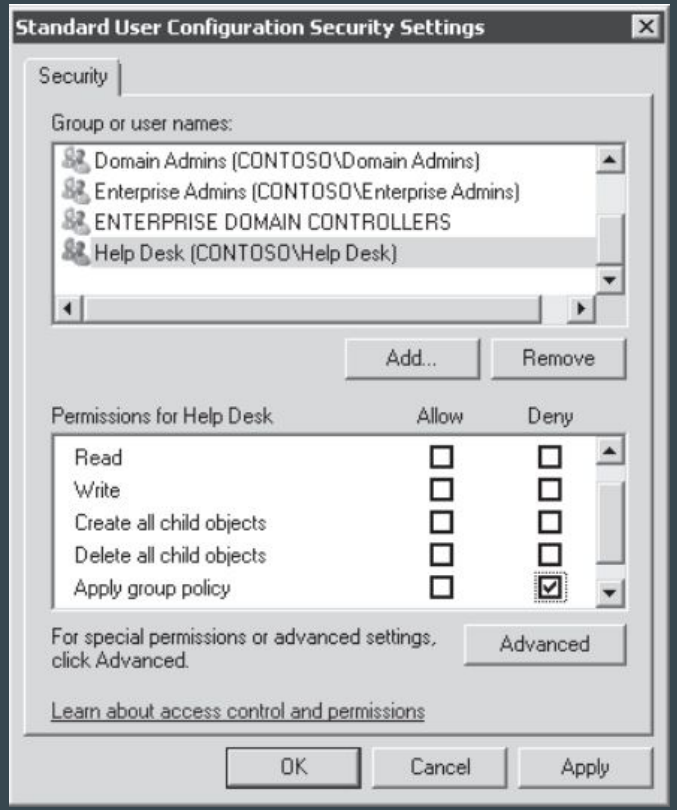
Filtrando um GPO para excluir grupos específicos

- Infelizmente, a guia Escopo de um GPO não permite excluir grupos específicos.



Filtrando um GPO para excluir grupos específicos

- Infelizmente, a guia Escopo de um GPO não permite excluir grupos específicos.



- Negar permissões substituem outras permissões. Por isso, é recomendável usar as permissões Negar com moderação.

Filtros WMI

- A Instrumentação de Gerenciamento do Windows (WMI) é uma tecnologia de infraestrutura de gerenciamento que permite aos administradores monitorar e controlar objetos gerenciados na rede.
- Uma consulta WMI é capaz de filtrar sistemas baseados em características, incluindo RAM, velocidade do processador, capacidade de disco, endereço IP, versão do sistema operacional e nível do service pack, aplicativos instalados e propriedades da impressora.
- Porque o WMI expõe quase todas as propriedades de cada objeto dentro de um computador, a lista de atributos que podem ser usados em uma consulta WMI é virtualmente ilimitada.

- As consultas do WMI são gravadas usando a linguagem de consulta WMI (WQL).
- Você pode usar uma consulta WMI para criar um filtro WMI, com o qual um GPO pode ser filtrado.
- Por exemplo podemos criar um GPO que instala um software e depois filtra aplicação desse GPO para Windows xp com SP3 por exemplo .

```
Select * FROM Win32_OperatingSystem WHERE Caption="Microsoft
Windows XP Professional" AND CSDVersion="Service Pack 3"
```

- Quando o cliente de Diretiva de Grupo avalia os GPOs, ele é baixado para determinar o que deve ser entregue aos CSEs para processamento, ele executa a consulta no sistema local.
- Se o sistema atende aos critérios da consulta, o resultado da consulta é um True lógico e os CSEs processarão o GPO.
- Para filtrar um GPO com um filtro WMI, clique na guia Escopo de um GPO, clique na lista suspensa WMI,
- e selecione o filtro WMI. Um GPO pode ser filtrado por apenas um filtro WMI, mas esse filtro WMI pode ser uma consulta complexa, usando vários critérios.
- Um único filtro WMI pode ser usado para filtrar, um ou mais GPOs.

3 coisas que você precisa saber

1. Existem três advertências significativas em relação aos filtros WMI. Primeiro, a sintaxe de WQL das filas WMI pode ser difícil de dominar.
2. Em segundo lugar, os filtros WMI são caros em termos de desempenho de processamento da Diretiva de Grupo. Porque o cliente de Diretiva de Grupo deve executar a consulta WMI em cada intervalo de processamento de diretivas, um pequeno impacto no desempenho do sistema a cada 90–120 minutos.
3. Terceiro, os filtros WMI não são processados por computadores que executam o Windows 2000. Se um GPO for filtrado com um filtro WMI, um sistema Windows 2000 sinalizará o filtro e processará o GPO como se os resultados do filtro foram verdadeiros.

Habilitando ou desabilitando GPOs e nó de GPOs

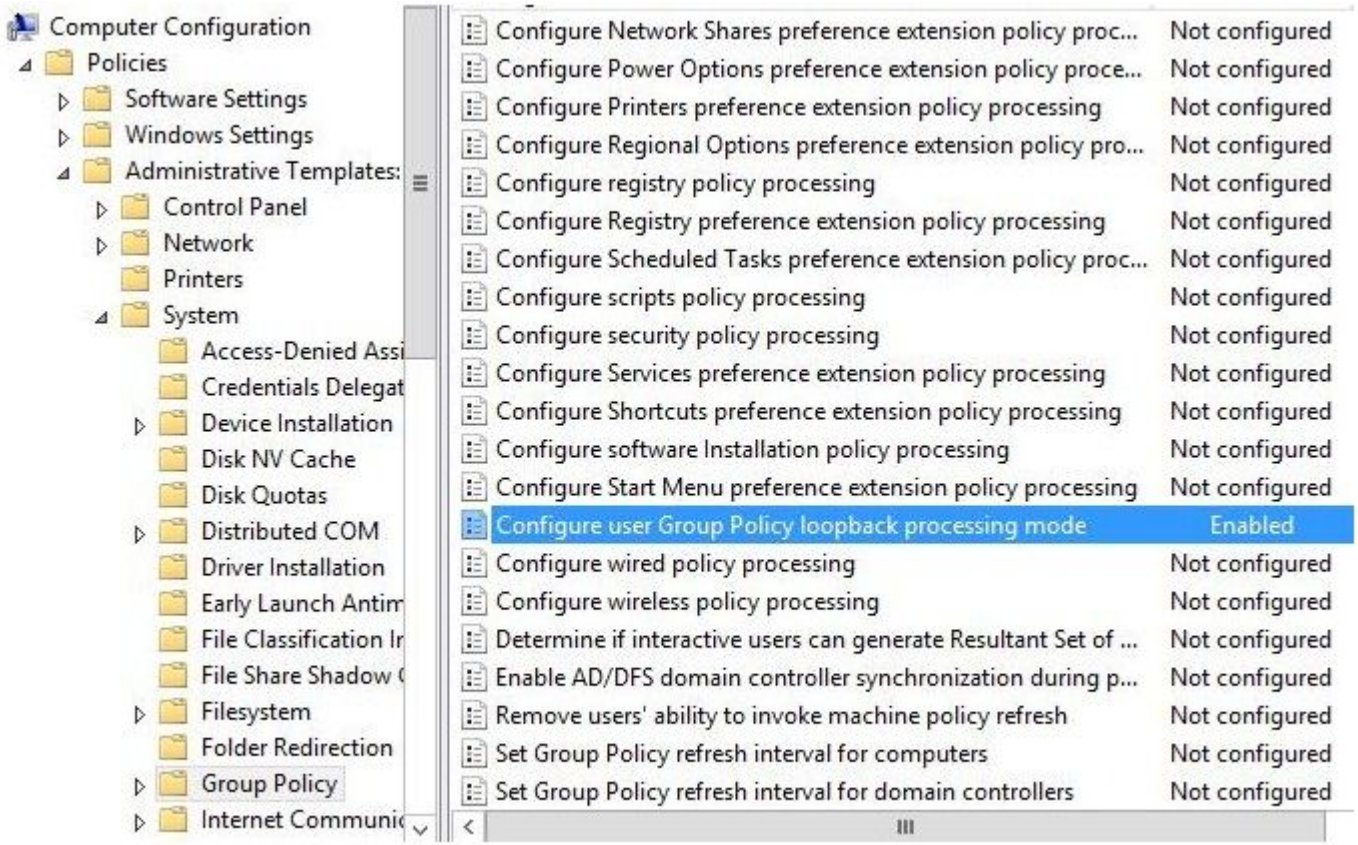
- Você pode impedir que as configurações nos nós Configuração do Computador ou Configuração do Usuário sejam processadas durante a atualização da política, alterando o status do GPO.
- Na guia Detalhes de um GPO, clique na lista suspensa Status do GPO e escolha uma das seguintes opções:
  - **Habilitado** As configurações do computador e as configurações do usuário serão processadas por CSEs durante a atualização da política.
  - **Todas as configurações desabilitadas** CSEs não processarão o GPO para atualização de política.
  - **Configurações do computador desabilitadas** - O GPO não será processado durante atualização da política do usuário.
  - **Definições de configuração do usuário desabilitadas** - O GPO não será processado durante a política do computador..

Loopback Processing Mode

- 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 contêm contas de usuários.

- Na OU-TERMINALSERVERS você cria e configura uma GPO.
- Então existem políticas 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 política da OU-TERMINALSERVERS
  - **User Configuration** -> São as configurações criadas na política da OU-SUPORTE
- Isso é o padrão, mas se você configurar a Loopback Processing Mode que está no caminho `Computer Configuration\Policies\Administrative Templates\System\Group Policy`, não será assim você pode então mudar o padrão


Computer Configuration
Policies
Software Settings
Windows Settings
Administrative Templates:
Control Panel
Network
Printers
System
Access-Denied Assi
Credentials Delegat
Device Installation
Disk NV Cache
Disk Quotas
Distributed COM
Driver Installation
Early Launch Antim
File Classification In
File Share Shadow
Filesystem
Folder Redirection
Group Policy
Internet Communic
Configure Network Shares preference extension policy proc... Not configured
Configure Power Options preference extension policy proce... Not configured
Configure Printers preference extension policy processing Not configured
Configure Regional Options preference extension policy pro... Not configured
Configure registry policy processing Not configured
Configure Registry preference extension policy processing Not configured
Configure Scheduled Tasks preference extension policy proc... Not configured
Configure scripts policy processing Not configured
Configure security policy processing Not configured
Configure Services preference extension policy processing Not configured
Configure Shortcuts preference extension policy processing Not configured
Configure software Installation policy processing Not configured
Configure Start Menu preference extension policy processing Not configured
Configure user Group Policy loopback processing mode Enabled
Configure wired policy processing Not configured
Configure wireless policy processing Not configured
Determine if interactive users can generate Resultant Set of ... Not configured
Enable AD/DFS domain controller synchronization during p... Not configured
Remove users' ability to invoke machine policy refresh Not configured
Set Group Policy refresh interval for computers Not configured
Set Group Policy refresh interval for domain controllers Not configured

replace e marge

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

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

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 política de redirecionamento de pastas não será aplicada.

- Em caso de conflito das politicas de usuários da OU-TERMINALSERVERS terá precedência. Como os GPOs do computador são processados após as GPOs do usuário, elas têm precedência para resolver conflitos.

FIM

...