

# O que é e como funciona a GPO

...

# Definição

- A GPO também conhecida como group policy ou diretiva de grupo é um conjunto de configurações que permite que você personalize diversos recursos dos usuários e dos computadores seja localmente (stand-alone) ou em um ambiente do domínio do Active Directory



- A Política de Grupo fornece uma infraestrutura dentro da qual as configurações podem ser definidas centralmente e implantada para usuários e computadores na empresa.
- Em um ambiente gerenciado por uma infraestrutura de Diretiva de Grupo bem implementada, pouco ou nenhuma configuração precisa ser feita tocando diretamente em uma Estação de trabalho.
- Toda as configurações definidas aplicadas e atualizadas usando configurações em Objetos de Diretiva de Grupo (GPOs) que afetam a empresa, é tão **ampla** quanto um site ou domínio inteiro ou tão **estreita** quanto uma única unidade organizacional (OU) ou grupo.

Uma infra-estrutura de Diretiva de Grupo possui muitas partes móveis. É importante que você entenda não apenas o que cada parte faz, mas também como as partes funcionam juntas e por que você pode querer montá-las em várias configurações.

*Nesta lição, você obterá uma visão geral abrangente da Diretiva de Grupo: seus componentes, suas funções e seu funcionamento interno.*

# Configurações de política

- Algumas configurações de política afetam um **usuário**, independentemente do computador no qual o usuário faz logon.
- Outras configurações de diretiva afetam um **computador**, independentemente de qual usuário efetua logon nesse computador



# Objetos de diretiva de grupo (GPOs)

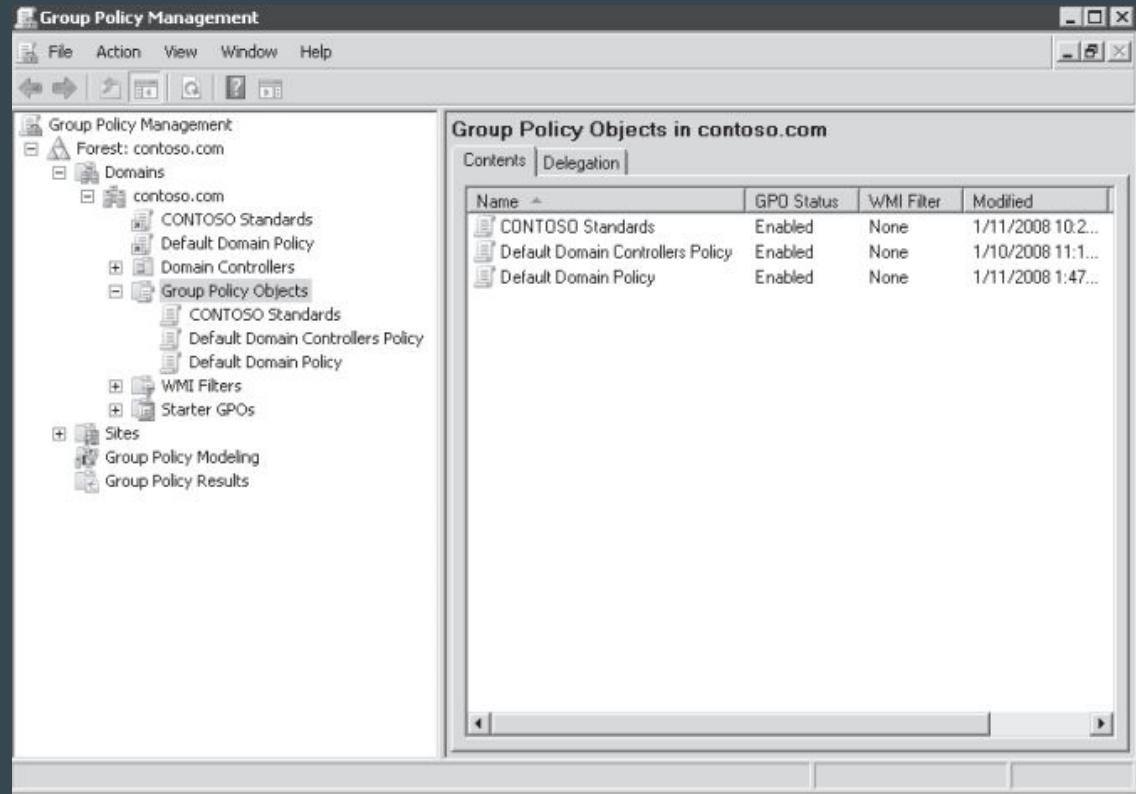
- As configurações de diretiva são definidas e existem dentro de um objeto de diretiva de grupo (GPO).
- Um GPO é um objeto que contém uma ou mais configurações de política e, portanto, aplica uma ou mais configurações para um usuário ou computador.

The screenshot shows the Windows Group Policy Management console. On the left, the navigation pane displays the forest (RWVDEV.INTRA), domains (RWVDEV.INTRA), and various GPOs like Default Domain Policy, DNS Suffix Configuration, and several Filter-GPOs. A red box highlights the 'Group Policy Objects' folder under 'RWVDEV.INTRA'. To the right, a detailed list of Group Policy Objects is shown in a table:

Name	GPO Status	WMI Filter	Modified	Owner
Default Domain Controllers P...	Enabled	None	2/26/2010 7:46...	Domain Admin...
Default Domain Policy	Enabled	None	1/9/2011 10:40...	Domain Admin...
DNS Suffix Configuration	Enabled	None	9/28/2010 11:5...	Domain Admin...
Filter-GPO-ComputerAccounts	Enabled	None	9/29/2010 11:4...	Domain Admin...
Filter-GPO-ServerOS	Enabled	None	1/6/2011 12:27...	Domain Admin...
Filter-GPO-UserAccounts	Enabled	None	9/29/2010 11:5...	Domain Admin...
Filter-GPO-UserAccounts	Enabled	None	5/13/2011 12:4...	Domain Admin...
Filter-GPO-UserAccounts	Enabled	None	9/29/2010 11:3...	Domain Admin...
Filter-GPO-ComputerAccounts	Enabled	None	3/15/2011 4:26...	Domain Admin...
Filter-GPO-ComputerAccounts	Enabled	None	3/17/2011 10:0...	Domain Admin...
Filter-GPO-ComputerAccounts	Enabled	None	9/9/2010 6:12...	Domain Admin...
Filter-GPO-ComputerAccounts	Enabled	None	9/8/2010 10:08...	Domain Admin...
Filter-GPO-ComputerAccounts	Enabled	None	8/6/2010 12:59...	Domain Admin...
Filter-GPO-ComputerAccounts	Enabled	None	8/6/2010 12:35...	Domain Admin...
ZONA-IPSEC	Enabled	None	8/14/2010 2:18...	Domain Admin...
ZONA-IPv6	Enabled	None	3/17/2011 10:1...	Domain Admin...

# Criando e gerenciando GPOs

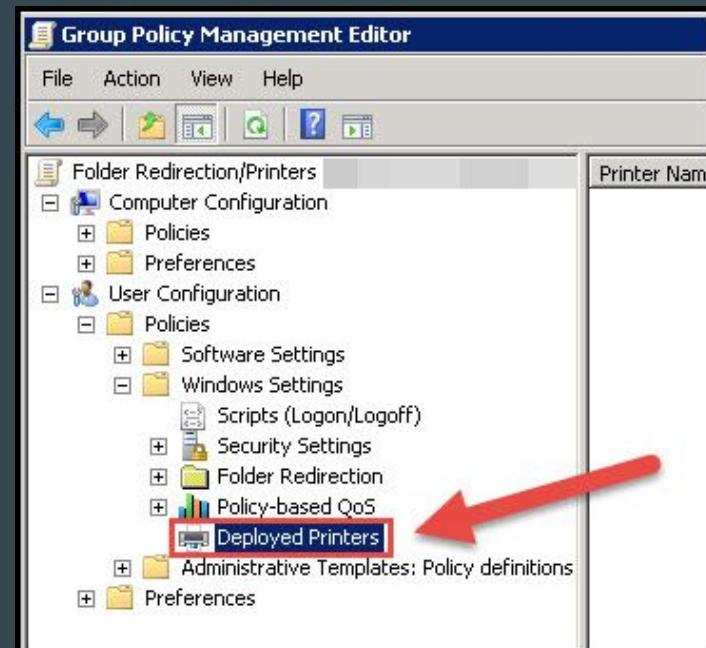
- Os GPOs podem ser gerenciados no Active Directory usando o console do Gerenciamento de Diretiva de Grupo (GPMC).
- Eles são exibidos em um contêiner denominado Objetos de Política de Grupo.



# Editando um GPO

- Para modificar as configurações de um GPO, clique com o botão direito do mouse no GPO e escolha Editar.
- O GPO é aberto no Snap-in Editor de Gerenciamento de Diretiva de Grupo (GPME).
- O GPME exibe as milhares de configurações de diretiva disponíveis em um GPO em uma hierarquia organizada que começa com a divisão entre as configurações do computador e as configurações do usuário: *o nó Configuração do computador e o nó Configuração do usuário*.

- Os próximos níveis da hierarquia são dois nós Polices e Preferências.
- Aprofundando na hierarquia, o GPME exibe pastas, também chamadas de nós ou grupos de configurações de políticas.
- Dentro das pastas estão as políticas e configurações próprias.. Para definir uma configuração de política, clique duas vezes na configuração de política.



# Configurando uma Configuração de Política

- Uma configuração de política pode ter três estados: *Não configurado*, *Ativado* e *Desativado*.
- Em um novo GPO, todas as configurações de política não são configuradas. Isso significa que o GPO não modificará a configuração existente dessa configuração específica para um usuário ou computador.
- E se você habilitar ou desabilitar uma configuração de política, será feita uma alteração na configuração dos usuários e computadores aos quais o GPO é aplicado.

**Group Policy Management Editor**

File Action View Help

CONTOSO Standards [SERVER01.c]

Computer Configuration

- Policies
  - Software Settings
  - Windows Settings
  - Administrative Template
- Preferences

User Configuration

- Policies
  - Software Settings
  - Windows Settings
  - Administrative Template
    - Control Panel
    - Desktop
    - Network
    - Shared Folders
    - Start Menu and Taskbar
    - System
    - Windows Components
    - All Settings
- Preferences

**System**

**Prevent access to registry editing tools**

Display Properties

Requirements:  
At least Microsoft Windows 2000

Description:  
Disables the Windows registry editor Regedit.exe.

If this setting is enabled and the user tries to start a registry editor, a message appears explaining that a setting prevents the action.

To prevent users from using other administrative tools, use the "Run only specified Windows applications" setting.

**Setting**

Setting	State
Ctrl+Alt+Del Options	Not configured
Driver Installation	Not configured
Folder Redirection	Not configured
Group Policy	Not configured
Internet Communication Management	Not configured
Locale Services	Not configured
Logon	Not configured
Performance Control Panel	Not configured
Power Management	Not configured
Removable Storage Access	Not configured
Scripts	Not configured
User Profiles	Not configured
Windows HotStart	Not configured
Download missing COM components	Not configured
Century interpretation for Year 2000	Not configured
Restrict these programs from being launched from Help	Not configured
Don't display the Getting Started welcome screen at logon	Not configured
Custom User Interface	Not configured
Prevent access to the command prompt	Not configured
<b>Prevent access to registry editing tools</b>	<b>Not configured</b>
Don't run specified Windows applications	Not configured
Run only specified Windows applications	Not configured
Windows Automatic Updates	Not configured

Extended Standard

10 setting(s)

**Prevent access to registry editing tools Properties**

Setting Explain Comment

**Prevent access to registry editing tools**

Enabled

Not Configured

Disabled

Disable regedit from running silently?

Yes

Supported on: At least Microsoft Windows 2000

Previous Setting Next Setting

OK Cancel Apply

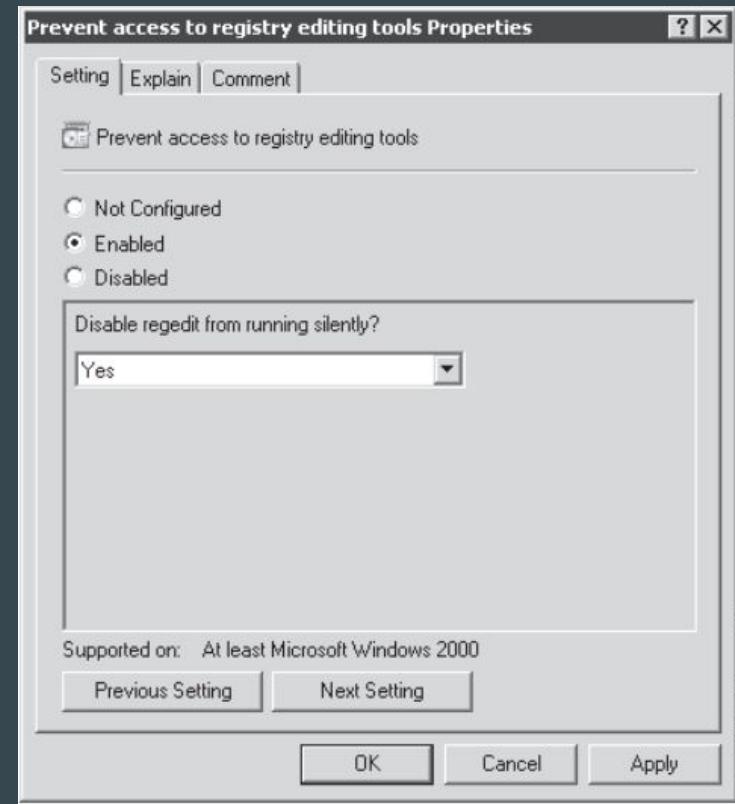
- O efeito da mudança depende da configuração de política em si.
- Por exemplo, se você habilitar a configuração de diretiva Impedir acesso a ferramentas de edição do Registro, os usuários não poderão iniciar o Editor de Registro Regedit.exe.
- Se você desabilitar a configuração de política, você garante que os usuários possam iniciar o Editor do Registro.
- Observe o duplo negativo nesta política: *você desabilita uma política que impede uma ação, permitindo a ação.*

Muitas configurações de política são complexas, e o efeito de habilitar ou desabilitar essas configurações pode não ficar imediatamente claro. Além disso, **algumas configurações de política afetam apenas determinadas versões do Windows.**

- Certifique-se de revisar um texto explicativo da configuração de política no painel de detalhes do GPME,
- Além disso, sempre teste os efeitos de uma configuração de política e suas interações com outras configurações de política, antes de implantar uma alteração no ambiente de produção



Algumas configurações de política combinam várias configurações em uma política e podem exigir parâmetros adicionais. Na Figura você pode ver que, ao permitir que a política restrinja as ferramentas de edição do registro, também é possível definir se os arquivos de registro podem ser mesclados no sistema silenciosamente, usando regedit / s.



# Escopo

- A configuração é definida pelas configurações de política em objetos de política do grupo. No entanto, as alterações de configuração em um GPO não afetam computadores ou usuários em sua empresa até que você especifique os computadores ou usuários aos quais o GPO se aplica.
- Isso é chamado de escopo de um GPO. O escopo de um GPO é a coleção de usuários e computadores que aplicará as configurações no GPO.
- Você pode usar vários métodos para gerenciar o escopo dos GPOs. O primeiro é o link do GPO.
- GPOs podem estar vinculado a sites, domínios e OUs.

- O site, domínio ou unidade organizacional torna-se o escopo máximo do GPO. Todos os computadores e usuários do site, domínio ou OUs, incluindo aquelas em UOs filhas, será afetada pelas configurações especificadas pelas configurações de diretiva no GPO.
- Um único GPO pode ser vinculado a mais de um site ou OU.
- Você pode restringir ainda mais o escopo do GPO com um dos dois tipos de filtros: filtros de **segurança** e **WMI** que especificam um escopo, usando características de um sistema como versão do sistema operacional ou espaço livre em disco.

# Conjunto de política resultante

- Computadores e usuários dentro do escopo de um GPO aplicarão as configurações de política especificadas no GPO.
- É provável que um usuário ou computador individual esteja no escopo de vários GPOs vinculados aos sites, domínio ou UOs em que o usuário ou computador existe.
- Isso leva à possibilidade as configurações de política podem ser configuradas de maneira diferente em vários GPOs.
- Você deve ser capaz de entender e avaliar o Conjunto de Políticas Resultante (RSoP), que determina as configurações que são aplicados por um cliente quando as configurações são configuradas de forma divergente em mais de um GPO.

# Atualização de Política de Grupo

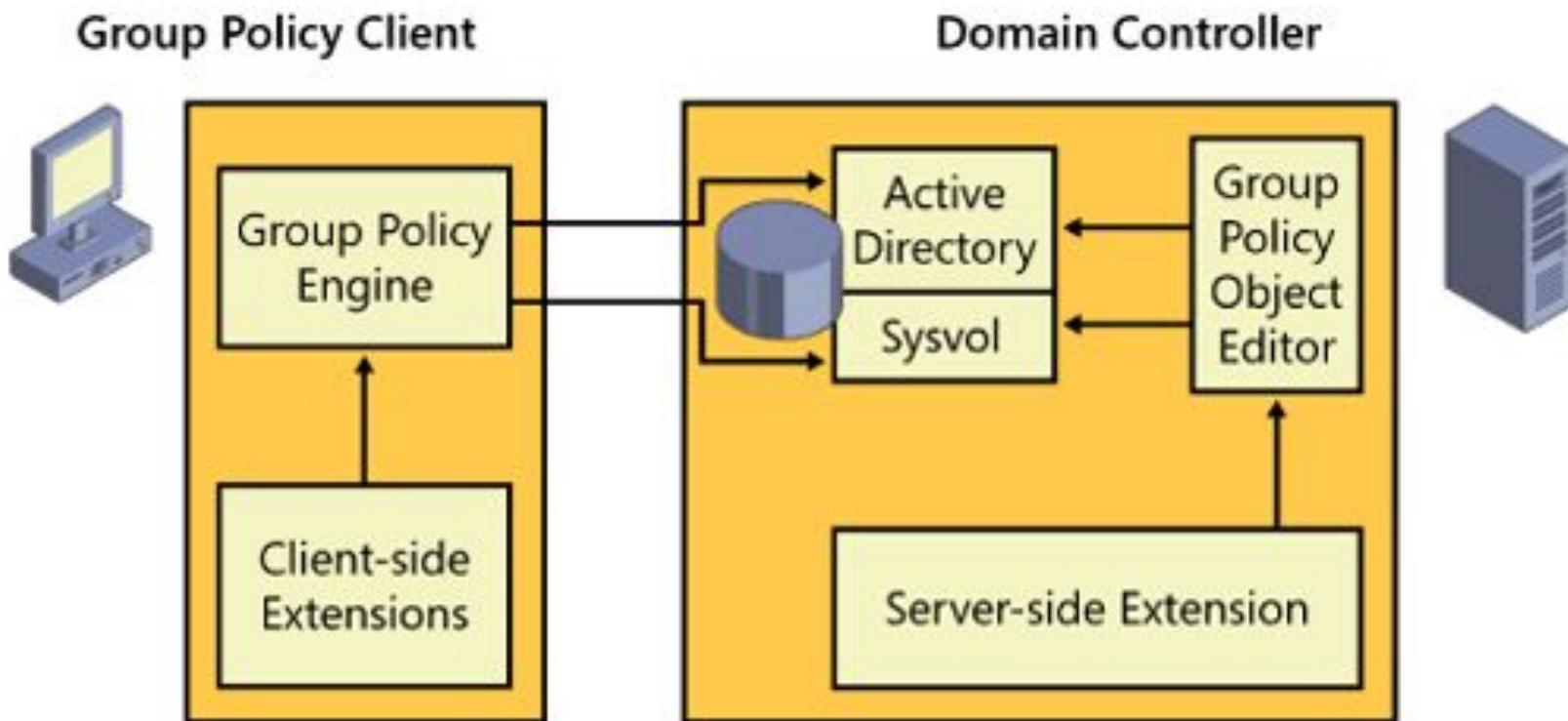
- As configurações de política no nó **Configuração do Computador** são aplicadas em inicialização do sistema e a cada 90–120 minutos depois disso.
- As configurações da política de **configuração do usuário** são aplicada no logon e a cada 90–120 minutos depois disso.
- A aplicação de políticas é chamada Atualização da Política de Grupo.

- Quando você está tentando solucionar problemas de Diretiva de Grupo talvez seja necessário iniciar manualmente uma atualização da Diretiva de Grupo para que você não tenha que esperar pela próxima atualização.
- O Gpupdate.exe pode ser usado para iniciar uma atualização da Diretiva de Grupo.
- Usado sozinho, Gpupdate.exe processa idêntico a uma atualização de Diretiva de Grupo em segundo plano. Tanto a política do computador quanto a política do usuário são atualizadas.
- Use o parâmetro de usuário /target:computer ou /target:user para limitar a atualização a configurações de computador ou usuário, respectivamente.

- Durante a atualização em segundo plano, por padrão, as configurações são aplicadas somente se o GPO tiver sido atualizado.
- O parâmetro /force faz com que o sistema reaplique todas as configurações em todos os GPOs com escopo definido para o usuário ou computador.
- Algumas políticas requerem um logoff ou reinicialização antes que elas realmente entrem em vigor.
- Os parâmetros /logoff e /boot causam um logoff ou reinicialização, respectivamente, se as configurações forem aplicadas

# Cliente de Política de Grupo e Client-Side Extensions(CSE)

- Quando a atualização da Diretiva de Grupo é iniciada, um serviço é executado em todos os sistemas Windows (chamado de cliente de Diretiva de Grupo )
- Ele Transfere qualquer GPO que já não tenha armazenado em cache. Então, uma série de processos chamados de Client-Side Extensions (CSE) que são os componentes em execução no sistema do cliente ,processam e aplicam as configurações do grupo a esse sistema. Há várias extensões pré-instaladas no Windows .
- O cliente de política de grupo puxa os GPOs do domínio, acionando os CSEs para aplicar configurações localmente.
- Diretiva de Grupo não é uma tecnologia "push".



- A maioria das CSEs aplicará configurações em um GPO somente se esse GPO tiver sido alterado. Esse comportamento melhora o processamento geral de diretivas
- Usuários padrão não podem alterar a configuração em seu sistema - eles sempre estarão sujeitos à configuração imposta pela Diretiva de Grupo.
- No entanto, algumas configurações podem ser alteradas por usuários padrão, e muitas podem ser alteradas se um usuário for um Administrador nesse sistema.

- Se os usuários em seu ambiente são administradores em seus computadores, considere configurar os CSEs para
- reaplique as configurações de política, mesmo que o GPO não tenha sido alterado.
- Dessa forma, se um usuário administrativo
- altera uma configuração para que ela não seja mais compatível com a política, a configuração será redefinida para seu estado compatível na próxima atualização de diretiva de grupo.



# CSE de segurança

- Uma exceção importante para as configurações padrão de processamento de políticas é a configuração gerenciada pelo CSE de segurança.
- As configurações de segurança são reaplicadas a cada 16 horas, mesmo que um GPO não tenha sido alterado.

- É altamente recomendável que você ative a configuração de política para Sempre esperar a rede na inicialização e no logon para todos os clientes Windows
- Os clientes executam apenas atualizações em segundo plano, o que significa que um cliente pode iniciar e um usuário pode efetuar logon sem receber as políticas mais recentes do domínio.



# Links lentos e sistemas desconectados

- Uma das tarefas que podem ser automatizadas é a instalação de software. A instalação do software de diretiva de grupo (GPSI) é suportada pelo CSE de instalação do software.
- Mas você não iria querer isso se rede estiver lenta
- O cliente da Diretiva de Grupo detecta a velocidade da conexão e determina se a conexão deve ser considerada um link lento.
- A determinação é então usada por cada CSE para decidir se será aplicada as configurações.
- Então a extensão, dispensa o processamento de políticas, e não instala o software. Por padrão, um link é considerado lento se for menor que 500 kilobits por segundo (kbps).

- Se um usuário estiver trabalhando **desconectado da rede**, as configurações aplicadas anteriormente pela Política de Grupo continuarão a entrar em vigor.
- Assim, a experiência de um usuário é idêntica, seja na rede ou trabalhando longe da rede.
- Há exceções a essa regra, casos como os scripts de logon e logoff.
- Se um usuário remoto **se conectar à rede** o cliente da Diretiva de Grupo é ativado e determina se uma janela de atualização da Diretiva de Grupo foi esquecido.
- Em caso afirmativo, ele executa uma atualização da Diretiva de Grupo para obter os GPOs mais recentes do domínio.

FIM

• • •