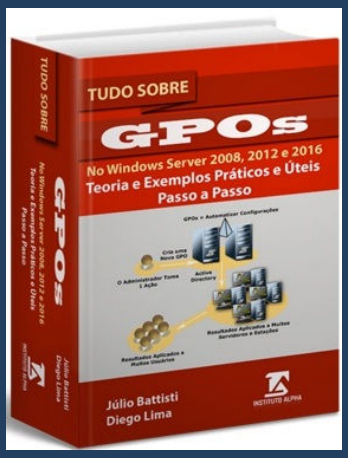
IMPORTANTE:

Este e-book é um Trecho de Demonstração do livro:

Tudo Sobre GPOs no Windows Server 2008, 2012 e 2016

Teoria e Exemplos Práticos e Úteis - Passo a Passo



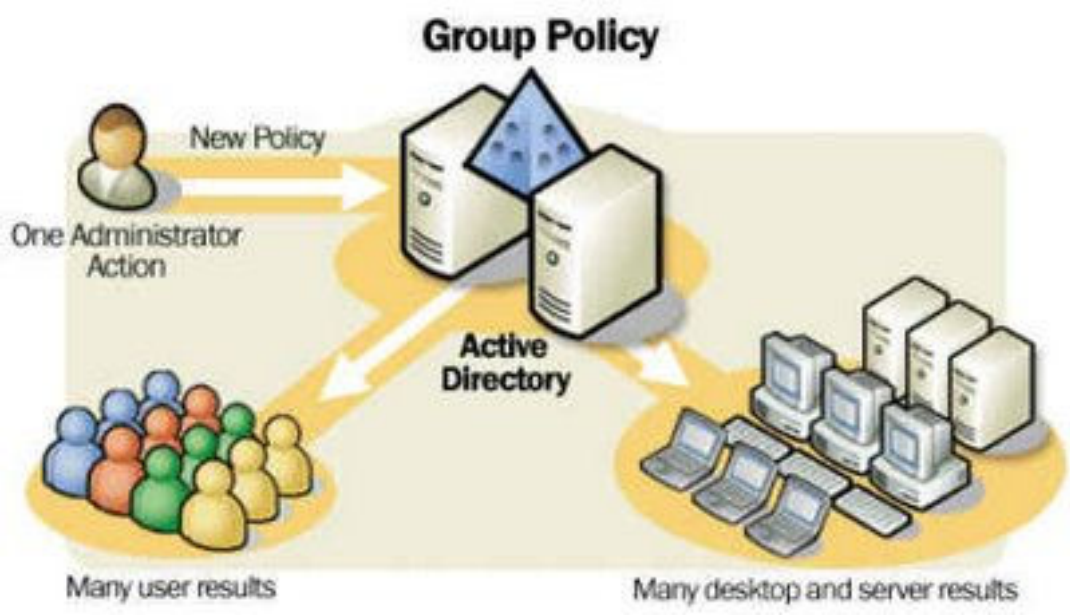
Páginas: 654 | Autores: Júlio Battisti e Diego Lima

Para Comprar o Livro Completo, com 50% de Desconto e Ainda Ganhar um Pacote de Bônus que Valem 20 Vezes o Valor do Livro, Acesse o Seguinte Endereço:

https://juliobattisti.com.br/loja/detalheproduto.asp?CodigoLivro=LIV0001525

Tudo Sobre GPOs no Windows Server 2008, 2012 e 2016 Teoria e Exemplos Práticos e Úteis - Passo a Passo

Autores: Júlio Battisti e Diego da Silva Lima



Autor: Júlio Battisti | Site: http://www.juliobattisti.com.br

Autor: Diego da Silva Lima | Site: https://diegogouveia.com.br

Introdução e Algumas palavras dos Autores:

Este livro foi criado com o objetivo de ajudá-lo a dominar desde a fundamentação teórica sobre GPOs no Active Directory, até a parte prática de Implementação, Configuração e Administração de GPOs no Windows Server 2008, Windows Server 2012 e Windows Server 2016.

Muitos Administradores de Rede tem inúmeras dúvidas sobre como utilizar GPOs, quais as reais capacidades deste recurso, o que pode e o que não pode ser feito com GPOs, como implementar, como administrar e assim por diante. Este livro procura preencher esta lacuna, ou seja, ser um livro onde o Administrador irá encontrar tudo o que ele precisa para dominar o recurso de GPOs, em diferentes versões do Windows Server.

GPOs - Group Policy Objects, ou, na tradução Oficial da Microsoft: Diretivas de Grupo. Mas o que vem a serem as tais de GPOs?

Nota: Neste livro usarei o termo mais conhecido e utilizado pela comunidade de TI, que é, simplesmente: GPOs. Prefiro usar GPOs do que a tradução Diretivas de Grupo.

O recurso de GPOs permite o gerenciamento centralizado e automatizado de centenas, milhares de configurações relacionadas com usuários e computadores de um Domínio. As GPOs se aplicam a todas as versões do Windows, a partir do Windows 2000. Claro que existem configurações que só existem em determinadas versões, por serem novidades na respectiva versão (não existirem nas versões anteriores). Ao invés de fazer as configurações individualmente, para milhares de usuários e em milhares de computadores, usando GPOs, o Administrador pode aplicar, automaticamente, estas configurações usando GPOs. Não se preocupe em entender como funciona este recurso neste momento, pois você terá este livro inteiro para isso.

Além de usar a Diretiva de Grupo para definir configurações para grupos de usuários e computadores, você também pode usar as GPOs para ajudar a gerenciar e configurar servidores, inclusive DCs - Domain Controllers (Controladores de Domínio), aplicando configurações de segurança, políticas de senha para o domínio, configurações para a conta Administrador, configurações para grupos de segurança. São muitos, MUITOS MESMO, os recursos e configurações que podem ser feitas via GPOs. Por exemplo, você pode até mesmo fazer instalação automatizada de software, via GPOs, definir o papel de parede para grupos de usuários, restringir o

acesso a opções do menu Iniciar ou do Painel de Controle, definir que usuários que não sejam Administradores possam instalar impressoras e assim por diante.

Poupando Tempo e Dinheiro:

Usando o recurso de GPOs, como Administrador da Rede, você pode reduzir significativamente o custo total de propriedade de uma organização (custo anual para manter um computador em rede e funcionando), ao automatizar dezenas, centenas de configurações, tanto de usuários quanto de computadores.

Vários fatores, como o grande número de configurações de diretiva disponíveis, a interação entre várias diretivas e opções de herança, podem tornar o projeto de implementação das GPOs bastante complexo. Planejando, projetando, testando e implantando cuidadosamente uma solução baseada nos requisitos de negócios da sua organização, você pode fornecer a funcionalidade, segurança e controle centralizado de gerenciamentos padronizados que sua organização precisa.

As configurações de Diretivas de Grupo que você cria estão contidas em um GPO. Para criar e editar um GPO o Administrador utiliza o Console de Gerenciamento de Diretiva de Grupo (GPMC). Ao usar o console GPMC para vincular um GPO a sites, domínios e unidades organizacionais (OUs) selecionados do Active Directory, você aplica as configurações de diretiva no GPO aos usuários e computadores nesses objetos do Active Directory. Uma OU é o contêiner do Active Directory de nível mais baixo ao qual você pode atribuir configurações de Diretiva de Grupo personalizadas.

Para orientar suas decisões de projeto de Diretiva de Grupo, você precisa entender claramente as necessidades de negócios da sua organização, os contratos de nível de serviço e os requisitos de segurança, rede e TI. Analisando o ambiente atual e os requisitos dos usuários, definindo os objetivos de negócios que você deseja atender usando a Diretiva de Grupo e seguindo estas diretrizes para projetar uma infraestrutura de Diretiva de Grupo, você pode estabelecer a abordagem que melhor atenda às necessidades da sua organização.

Muito bem. Este será um livro SÓ SOBRE GPOS. Mostraremos como Planejar, Implementar e Administrar GPOs em redes baseadas no Windows Server 2008 R2, Windows Server 2012 R2 ou Windows Server 2016.

Um bom estudo a todos e espero, sinceramente, que este curso possa ajudá-los a entender e, principalmente, a planejar, implementar e administrar, corretamente, o recurso de GPOs em diferentes versões do Windows Server.

Cordialmente,

Júlio Battisti,

Diego da Silva Lima

Pré-requisitos Para Acompanhar Este Livro:

Para que você possa acompanhar as lições deste curso é necessário que você já tenha preenchido os seguintes pré-requisitos:

- Conhecimentos da Instalação e Administração dos Recursos Básicos do Windows Server.
- Conhecimentos Básicos sobre o Active Directory e Seus Elementos (domínios, árvores, florestas, sites, Unidades Organizacionais, Usuários e Grupos).
- É recomendado já ter alguma experiência, mesmo que básica, com a implementação e administração de servidores baseados no Windows Server 2008, Windows Server 2012 ou Windows Server 2016.

Sumário Do Livro Completo:

Capítulo 03 – Tudo Sobre GPOs no Windows Server 2016

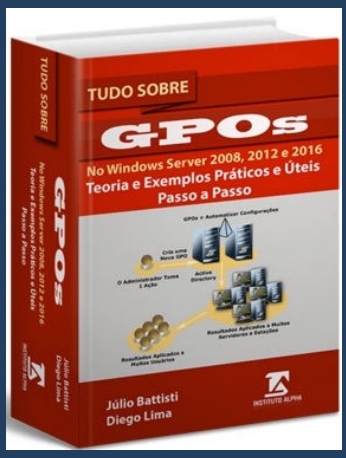
Capítulo 04 – GPOs - Só Tópicos Avançados

IMPORTANTE:

Este e-book é um Trecho de Demonstração do livro:

Tudo Sobre GPOs no Windows Server 2008, 2012 e 2016

Teoria e Exemplos Práticos e Úteis - Passo a Passo



Páginas: 654 | Autores: Júlio Battisti e Diego Lima

Para Comprar o Livro Completo, com 50% de Desconto e Ainda Ganhar um Pacote de Bônus que Valem 20 Vezes o Valor do Livro, Acesse o Seguinte Endereço:

https://juliobattisti.com.br/loja/detalheproduto.asp?CodigoLivro=LIV0001525

:: Capítulo 01 – GPOs no Windows Server 2008

Introdução:

O recurso de Group Policy Objects (GPO) é de "**ENORME**" utilidade para o administrador da rede. Com o uso de GPOs o administrador pode definir as configurações de vários elementos das estações de trabalho do usuário, como por exemplo, os programas que estarão disponíveis, os atalhos do Menu Iniciar que estarão disponíveis, os atalhos dentro do Painel de Controle que estarão disponíveis para o usuário, as configurações de Internet, habilitar ou desabilitar itens do Painel de Controle, configurar redirecionamento de pastas, configurações de rede e assim por diante. Por exemplo, o administrador pode configurar, via GPOs, quais grupos de usuários deverão ter acesso ao comando Executar e quais não terão, pode configurar a página inicial do Internet Explorer, do Firefox ou do Chrome para um grupo de usuários ou para toda a empresa, pode fazer configurações de Proxy e por aí vai. São milhares (literalmente "milhares") de opções de configurações que estão disponíveis via GPOs.

As configurações feitas via GPOs são aplicadas para usuários, computadores, Member Servers e DCs (Domain Controllers = Controladores de Domínio), mas somente para computadores executando Windows 2000 (Server ou Professional), Windows XP, Windows Vista, Windows 7, Windows 8, Windows 10, Windows Server 2003, Windows Server 2008, Windows Server 2012 ou Windows Server 2016. Para versões mais antigas do Windows, tais como Windows 95/98/Me e NT 4.0, o recurso de GPOs não é aplicado.

Devido à importância deste recurso e da grande quantidade de configurações disponíveis, este capítulo será todo dedicado ao recurso de GPOs no Windows Server 2008. Este capítulo será de grande utilidade para quem utiliza o Windows Server 2008 nos servidores da rede e quer automatizar uma série de configurações, usando o recurso de GPOs.

Vamos iniciar o capítulo com a teoria necessária para que você entenda exatamente o que é o recurso de GPOs, como ele se aplica em um domínio, em que níveis ele pode ser configurado e quais as opções que o administrador tem para garantir que as configurações definidas via GPOs, sejam aplicadas nas estações de trabalho dos usuários, em um domínio baseado no Windows Server 2008 R2.

Em seguida passarei as ações práticas relacionadas com GPOs. Desde a alteração da GPO padrão do domínio, passando pela criação de novas políticas de segurança e aplicações destas políticas em diferentes níveis, dentro do domínio.

Também falaremos sobre as configurações de segurança e definição de permissões, relacionadas com GPOs. Com a configuração das permissões de acesso a uma determinada GPO, o administrador pode fazer com que um conjunto de políticas de segurança sejam aplicados apenas a um determinado grupo de usuários ou computadores (é importante lembrar que no Windows Server 2008 R2, é possível adicionar as contas de computadores como membros de um grupo). Apresentarei o conceito de herança de GPOs, conceito importante quando se aplicam diferentes políticas em diferentes níveis dentro do domínio.

Outro ponto abordado em detalhes será o uso das políticas de segurança para redirecionamento das pastas de dados pessoais dos usuários, tais como a pasta Documentos. Combinando o uso dos recursos de GPOs e de "roaming profiles", o administrador pode redirecionar, por exemplo, a pasta Documentos dos usuários para um servidor da rede, de tal maneira que o usuário terá acesso a esta pasta, independentemente do computador em que estiver logado. Combinando estes dois recursos, com o recurso de pastas off-line, o usuário poderá ter acesso aos seus documentos, mesmo sem estar conectado à rede.

Para encerrar o capítulo vou apresentar as ferramentas de gerenciamento relacionados com GPOs, tais como:

- Resultant Set of Policy – RSoP.
- Console Group Policy Management – GPMC.
- Comandos para o gerenciamento de GPOs.

GPOs - O Que São e Para o Que Servem

Quem já trabalhou na administração de uma rede baseada no Windows sabe o quanto é trabalhoso (e com um custo elevado), manter a configuração de milhares de estações de trabalho rodando diversas versões do Windows. Existem diversas questões/problemas que tem que ser enfrentados:

- Como definir configurações de maneira centralizada, para que seja possível padronizar as configurações das estações de trabalho?

- Como impedir que os usuários possam alterar as configurações do Windows em suas estações de trabalho (diversas versões: Windows XP, Windows Vista, Windows 7, Windows 8 e Windows 10), muitas vezes inclusive causando problemas no Windows, o que faz com que seja necessário um chamado à equipe de suporte técnico, para colocar a estação de trabalho novamente em funcionamento, corrigindo alterações que o usuário fez e que não deveria ter feito e, nem mesmo, deveria ter permissões para fazer as alterações?

- Como aplicar configurações de segurança e bloquear opções que não devam estar disponíveis para os usuários de uma maneira centralizada, sem ter que fazer estas configurações em cada estação de trabalho? Quando houver alterações, eu gostaria de poder fazê-las em um único local e ter estas alterações aplicadas em toda a rede ou em partes específicas da rede?

- Com fazer a instalação e distribuição de software de uma maneira centralizada, sem ter que fazer a instalação em cada estação de trabalho da rede?

- Como definir um conjunto de aplicações diferentes, para diferentes grupos de usuários do Active Directory ou para computadores de um determinado departamento, de acordo com as necessidades específicas de cada grupo?

- Como aplicar diferentes configurações aos computadores de diferentes grupos de usuários, de acordo com as necessidades específicas de cada grupo??

- Como configurar as políticas de senha e políticas de bloqueio de conta para todo o domínio, de maneira centralizada??

- Como configurar o redirecionamento de pastas especiais, tais como a pasta Documentos, para compartilhamentos em servidores de rede??

- Como configurar scripts de logon e logoff do usuário e scripts para serem executados na inicialização e/ou desligamento da estação de trabalho??

A primeira tentativa de "responder" a estas necessidades, recorrentemente levantadas pelos Administradores de redes baseadas no Windows foi a introdução das chamadas Polices e do Police Editor, juntamente com o Windows NT 4.0. Com o uso das Polices era possível definir uma série de configurações, as quais eram aplicadas à registry da estação de trabalho do usuário quando ele fizesse o logon no domínio. Por exemplo, era possível utilizar as Polices para impedir que um usuário do Windows 95/98/Me pressionasse a tecla ESC para cancelar a tela de logon e ter acesso ao Windows sem fazer o logon no domínio. Eu digo "uma primeira tentativa", porque o uso de Polices não passou muito disso, uma tentativa, uma vez que muitas das demandas não foram atendidas por este recurso (mas confesso que usei, bastante, as Polices e me foram bastante úteis na época).

Já com o lançamento do Windows 2000 Server e com a introdução do recurso de GPOs, o administrador passou a ter um recurso realmente poderoso, capaz de atender todas as demandas descritas anteriormente e muito, muito mais mesmo.

Nota: É importante salientar que as GPOs somente são aplicadas a computadores com o Windows 2000, Windows XP, Windows Vista, Windows 7, Windows 8, Windows 10, Windows Server 2003, Windows Server 2008, Windows Server 2012 ou Windows Server 2016. Estações de trabalho que ainda estejam com versões mais antigas do Windows, tais como Windows 95, Windows 98, Windows Me ou Windows NT 4.0, terão como único recurso de configuração o uso de Polices e do Police Editor. O recurso de GPOs não é aplicado a estas versões mais antigas. Então, em uma rede onde você tem estações de trabalho com as novas versões do Windows e estações de trabalho com versões mais antigas (95, 98, Me e NT 4.0), você terá que utilizar os dois recursos. Polices para as versões mais antigas do Windows, sempre levando em consideração as limitações deste recurso, em comparação com o uso de GPOs e usar GPOs para as estações de trabalho com versões mais novas do Windows.

As GPOs incluem configurações que são aplicadas a nível de usuário (ou seja, em qualquer estação de trabalho do domínio em que o usuário faça o logon, as políticas associadas a sua conta de usuário serão aplicadas) e a nível de computador (ou seja, qualquer usuário que faça o logon no computador terá as políticas de computador serão aplicadas).

Por exemplo, se o administrador definiu uma política de usuário para o grupo do usuário jsilva, de tal maneira que o comando Executar não deva estar disponível para este grupo, em qualquer estação de trabalho que o jsilva fizer o logon, o comando Executar não estará disponível. Agora imagine que o administrador configurou uma política de computador, para o grupo de computadores da seção de contabilidade, definindo que o comando Executar não deve estar disponível nestes computadores. Qualquer usuário que faça o logon em qualquer um dos computadores da seção de contabilidade, não terá disponível o comando Executar, independentemente dos grupos aos quais pertença o usuário, uma vez que a política está sendo aplicada ao computador (independentemente do usuário que esteja utilizando-o).

Mas Enfim, o que as GPOs Podem Fazer?

- **Podem gerenciar, de maneira centralizada, configurações definidas na registry do Windows, com base em templates de administração (Administrative Templates):** As GPOs criam arquivos com definições da registry. Estes arquivos são carregados e aplicados na estação de trabalho do usuário, nas partes referentes a configuração de Usuários e configuração de Computador da registry. As configurações de usuário são carregadas na opção HKEY_CURRENT_USER (HKCU), da registry. As configurações de computador são carregadas na opção HKEY_LOCAL_MACHINE (HKLM), da registry. A idéia é relativamente simples. Ao invés de ter que configurar estas opções em cada estação de trabalho, o administrador cria elas centralizadamente, usando GPOs. Durante o logon, o Windows aplica as configurações definidas nas GPOs que se aplicam ao usuário e ao computador.

- **Atribuição de scripts:** Com o uso de GPOs o administrador pode configurar um script para ser executado na inicialização e também no desligamento do Windows. Também podem ser definidos scripts de logon e logoff.

- **Redirecionamento de pastas:** O administrador pode configurar uma GPO para que pastas tais como Documentos, Imagens, Downloads, etc. sejam redirecionadas para uma pasta compartilhada em um servidor. Com isso os dados do usuário passam a estar disponíveis no servidor e poderão ser acessados de qualquer estação de trabalho da rede, na qual o usuário faça o logon no domínio. Além disso, com os dados no servidor, é possível criar e implementar uma política de backup centralizada.

- **Gerenciamento de software:** Com o uso de GPOs o administrador pode fazer a instalação de software de uma maneira centralizada. É possível associar uma aplicação com um grupo de usuários. Quando o usuário fizer o logon, o ícone da aplicação já é exibido no menu Iniciar. Quando ele clicar neste ícone a aplicação será instalada, automaticamente, a partir de um servidor da rede, cujo caminho dos arquivos de instalação foi configurado via GPOs. Também é possível publicar aplicações. Neste caso, ao fazer o logon, o usuário tem que acessar a opção Adicionar ou remover programas do Painel de controle (a partir do Windows Vista esta opção foi renomeada para Programas e Recursos) e solicitar que a aplicação seja instalada.

- **Definir configurações de segurança:** Para computadores executando o Windows 2000 Server ou Professional, Windows XP Professional, Windows Vista, Windows 7, Windows 8, Windows 10, Windows Server 2003, Windows Server 2008, Windows Server 2012 ou Windows Server 2016, existe uma GPO localmente nestes computadores. Esta GPO pode ser utilizada para configurar uma série de opções do ambiente de trabalho do usuário. As configurações definidas na GPO local somente se aplicam ao computador onde as configurações estão sendo definidas. Algumas funcionalidades tais como distribuição de software e redirecionamento de pastas não estão disponíveis na GPO local. Estão disponíveis somente em GPOs aplicadas no Active Directory, conforme descrito logo a seguir. A GPO local somente deve ser utilizada quando houver necessidade de uma configuração específica em um determinado computador. As configurações que se aplicam a grupos de computadores e usuários devem ser configuradas via GPOs no Active Directory, já que isso facilita a configuração e atualização das configurações de uma maneira centralizada.

Nota: A GPO local é gravada, por padrão, na pasta %systemroot%\System32\GroupPolicy

Além da GPO local, podem ser aplicadas GPOs definidas no Active Directory, para aplicação nos computadores que fazem parte do domínio. Pode inclusive acontecer de haver "conflitos" de configurações entre a GPO local e uma ou mais GPOs do domínio. Neste caso existem configurações (que você aprenderá mais adiante), que definem, em caso de conflito, se deve ser aplicada a definição da GPO local ou a definição da GPO do domínio.

Dica: Existe uma GPO padrão para o domínio. Configurações feitas nesta GPO serão aplicadas a todos os usuários e computadores do domínio. Configurações gerais, que devam ser aplicadas a todos os objetos do domínio, devem ser definidas nesta GPO. Você aprenderá a configurar a GPO padrão do domínio, nos exemplos práticos deste capítulo.

Outra GPO que existe por padrão é uma GPO associada com a OU Domain Controllers (Controladores de domínio). Esta GPO é aplicada somente aos DCs do domínio. Embora seja possível mover a conta de um DC para outra unidade organizacional, este não é um procedimento recomendado. Ao mover a conta de um DC da unidade organizacional Domain Controllers para outra unidade organizacional, a GPO padrão para os DCs deixará de ser aplicado ao DC que foi movido, pois esta GPO está ligada a unidade organizacional Domain Controllers.

Políticas de Usuários e Políticas de Computador:

As políticas de usuários, isto é, políticas associadas a conta do usuário, são configuradas na opção Configurações do Usuário, do console Editor de Gerenciamento da Diretiva de Grupo (o qual você aprenderá a utilizar mais adiante, neste capítulo) e são aplicadas quando o usuário faz o logon.

Políticas de computador são configuradas através da opção Configurações de Computador e são aplicadas quando o computador e inicializado. Existe também um intervalo de atualização, dentro do qual as políticas são reaplicadas e quaisquer mudanças que tenham sido feitas pelo Administrador, serão aplicadas aos usuários e computadores.

Nota: As políticas definidas no Active Directory são aplicadas somente a objetos do tipo usuário e computador. Por questões de desempenho, as políticas não podem ser configuradas para objetos do tipo Grupos. Porém é possível utilizar o mecanismo de permissões de acesso das GPOs, para limitar a aplicação de uma GPO somente a um ou mais grupos de usuários e computadores, conforme você aprenderá na parte prática deste capítulo, mais adiante.

É possível criar objetos do tipo GPO e associá-los a diferentes objetos do Active Directory. Um objeto do tipo GPO pode ser criado e associado com um domínio, com uma unidade organizacional ou com um site. Além da GPO que pode ser criada localmente em cada computador com o Windows a partir do Windows 2000, conforme descrito anteriormente.

Ordem de Aplicação das GPOs:

As GPOs são aplicadas em uma ordem específica, caso esteja definida mais de uma GPO para o usuário que estiver fazendo o logon ou para o computador que está sendo inicializado. Por exemplo, quando o usuário faz o logon, são aplicadas a GPO do domínio e mais (se houver), a GPO da unidade organizacional a qual pertence a sua conta e a GPO local da estação de trabalho que ele está utilizando. A ordem de aplicação das GPOs é a seguinte:

- A GPO local.
- GPO definida para o site ao qual pertence o computador.
- GPOs do domínio.
- GPOs definidas a nível de unidade organizacional, da OU pai para a OU filho. Por exemplo, se foi criada uma OU "Divisão Sul" e, dentro desta OU as divisões: Finanças, Contabilidade e Vendas e a conta do usuário jsivla está na OU Vendas, primeiro será aplicada a GPO da OU "Divisão Sul" e depois a GPO da OU Vendas.

Por padrão, as políticas aplicadas por último, tem precedência sobre as políticas aplicadas anteriormente.

Por exemplo, a GPO de domínio é aplicada. Em seguida vem a GPO definida na Unidade Organizacional. Se houver um conflito entre a GPO de domínio e a GPO da unidade organizacional, irá prevalecer a configuração definida na GPO da unidade organizacional (aplicada por último). O administrador pode configurar a GPO de domínio (ou outras GPOs em qualquer nível), para que suas configurações não possam ser sobrescritas (substituídas) pelas configurações de GPOs de nível mais baixo, em caso de conflito.

Por exemplo, o administrador pode definir na GPO de domínio, que nenhum usuário terá acesso ao comando Executar e marcar a GPO onde está esta configuração com a opção No Override (Não Sobrescrever). Com isso, mesmo que exista um GPO em uma unidade organizacional, permitindo o uso do comando Executar, esta configuração não será aplicada, uma vez que a GPO do domínio não permite que sejam alteradas suas configurações em caso de conflito. Este mecanismo é uma maneira que o administrador tem, de garantir que determinadas configurações sejam aplicadas em todo o domínio, independentemente das configurações que são efetuadas em nível de unidade organizacional.

Novidades das GPOs no Windows Server 2008:

Uma série de novos recursos foram adicionados no Windows Server 2008. Com as GPOs a história não é diferente, aliás, muitos novos recursos foram adicionados ou aprimorados no Windows Server 2008. Vou apresentar rapidamente uma visão geral desses novos recursos de GPOs e, no decorrer deste capítulo, exploraremos alguns desses novos recursos na prática.

- **Novas categorias de gerenciamento de diretivas:** no Windows Server 2008 uma série de novas diretivas podem agora ser gerenciadas através das GPOs, como por exemplo, gerenciamento das opções de energia, gerenciamento de instalação e uso de dispositivos USB o outras mídias removíveis, criação de políticas de firewall e IPSec, novas opções de gerenciamento do Internet Explorer, atribuição de impressoras para os usuários de acordo com a localização física do usuário e permitir que os usuários instalem drivers de impressoras. Perceba que no Windows Server 2008, com o uso das GPOs você pode ter um controle maior sobre as estações de trabalho e laptops, elevando ainda mais o nível de segurança da sua rede.

- **Novos formato e funcionalidades de arquivos de modelo Administrativo (ADMX):** os modelos administrativos nada mais são do que arquivos que descrevem a Diretiva de Grupo baseado no registro do Windows. Esses modelos existem desde a época do Windows NT 4.0, porém o formato de arquivo utilizado era o ADM. Já no Windows Server 2008, esses arquivos passarem a ser baseados no padrão XML, e possuem a extensão ADMX. Um detalhe interessante é que os arquivos ADMX oferecem suporte multilíngue, armazenamento de dados centralizado opcional e recursos de controle de versão.

- **Objetos de Diretiva de Grupo Iniciais (GPOs Iniciais):** esse recurso é muito interessante e funciona basicamente da seguinte forma: suponha que você crie muitas GPOs, e a maioria dessas GPOs possuem muitas configurações em comum. Ao invés de você ter que configurar esses mesmos parâmetros em cada uma das GPOs, você pode criar uma Diretiva de Grupo Inicial e definir todas essas configurações nessa diretiva. Após isso, você cria suas GPOs baseado nessa Diretiva de Grupo Inicial. Em outras palavras, ao invés de você criar uma GPO do zero, você cria uma GPO baseada em uma GPO Inicial já existente, a qual possui as configurações que você desejar. Imagine um modelo de GPO, a partir do qual você cria suas GPOs baseada nesse modelo. É para isso que servem as GPOs Iniciais.

- **Comentários sobre GPOs e configurações de diretivas:** imagine um domínio que possua 20 GPOs (concordo que eu exagerei mas vamos imaginar esse cenário). Como é que você faz para saber o que faz cada uma das GPOs? Com certeza você utilizará nomes intuitivos. Mas com 20 GPOs ficará difícil você encontrar nomes intuitivos e curtos. Ao invés disso, você pode utilizar o recurso de comentários. Ou seja, você pode editar as propriedades das GPOs e das GPOs Iniciais e colocar um comentário em cada GPO. Com isso, você poderá rapidamente identificar o que faz cada uma das suas 20 GPOs.

- **Reconhecimento de Locais de Rede:** em domínios baseados em versões anteriores do Windows Server 2008, a detecção de vínculo de GPOs baseava-se no uso do protocolo ICMP, ou seja, no famoso “ping”. Já no Windows Server 2008, as GPOs são processadas mesmo que você desabilite o ICMP nos computadores, o que não acontece em domínios anteriores ao Windows Server 2008. Isso se deve ao fato do cliente de GPOs no Windows Server 2008 usar o Reconhecimento de Locais de Rede para determinar a largura de banda da rede e continuar a processar a aplicação das GPOs. Esse novo recurso permite que as GPOs trabalham de uma melhor forma em redes que tenham mudanças constantes em suas condições de uso e em sua configuração física. O primeiro benefício oferecido por esse recurso, já citado anteriormente, é o fim da dependência do protocolo ICMP (ping). Outra vantagem que esse recurso apresenta é a diminuição no tempo de inicialização das estações de trabalho e servidores. O Reconhecimento de Locais de Rede possui uma funcionalidade que indica com precisão para a GPO quando a rede está pronta. A GPO pode também determinar se o adaptador está desabilitado ou desconectado, permitindo assim que as GPOs diminuam o tempo de espera daqueles cenários nos quais a rede não estiver disponível.

- **Preferências:** as preferências, que estão disponíveis tanto em configurações de computador quanto em configurações de usuário, aumentam ainda mais o nosso controle sobre as estações de trabalho do domínio. O objetivo é simples: diminuir a quantidade de scripts que precisam ser desenvolvidos e implementados através das GPOs. As preferências nos permitem gerenciar, através da interface gráfica, mapeamentos de rede, habilitar ou desabilitar determinados dispositivos de hardware, criar variáveis de ambiente, configurar as opções de pasta do Windows Explorer, associar extensões de arquivos com softwares específicos, configurar serviços, impressoras, tarefas agendadas, criação de usuários e grupos locais, e assim por diante.

- **Serviço Diretiva de Grupo:** toda a infraestrutura das GPOs foi aprimorada com o isolamento completo do Winlogon, proporcionando assim uma nova arquitetura para a forma na qual as GPOs executam ações de notificação e processamento. Como as GPOs exigem menos recurso de processamento em segundo plano e menos utilização de memória, a aplicação das GPOs é mais eficaz e mais rápida.

- **Eventos e log:** conforme já dissemos anteriormente, a infraestrutura das GPOs foi totalmente modificada no Windows Server 2008. Por exemplo, o processamento das GPOs não existe mais no processo Winlogon do Windows. Ao invés disso, está hospedado como seu próprio serviço. Outra alteração é que o mecanismo de GPOs não se baseia mais no registro de rastreamento encontrado na DLL Userenv. Em versões anteriores ao Windows Server 2008, grande parte da resolução dos problemas com GPOs baseava-se nos logs gerados pela DLL Userenv. Quem já precisou trabalhar com esses logs sabe que não era na fácil entender as mensagens que eram gravadas nos logs. No Windows Server 2008 as GPOs possuem um componente próprio, com um novo serviço de GPO. Esse serviço é executado sobre o processo Svchost, com a finalidade de ler e aplicar as GPOs. Uma novidade também é que os eventos relacionados as GPOs são armazenados agora no log de sistema do Windows, e não mais no log de aplicativo. E a origem desses eventos é identificada como Microsoft-Windows-GroupPolicy.

- **Localizando configurações específicas da diretiva de modelos Administrativos:** no Windows Server 2008 temos muitas configurações que podem ser habilitadas via GPO. Quando digo muitas, estou me referindo a mais de 2400 configurações, contra cerca de 1700

no Windows Server 2003. E como é que você localiza as opções desejadas rapidamente? Realmente é um processo complicado, e para quem não tem muita experiência com GPOs, algumas horas podem ser perdidas até que as configurações desejadas sejam localizadas. No Windows Server 2008 você tem a possibilidade de criar filtros e localizar rapidamente as configurações desejadas. Tanto nas configurações de computador quanto nas configurações de usuários, dentro da opção Modelos Administrativos temos uma opção chamada Todas as Configurações. Essa categoria nos mostra, por padrão, todas as opções disponíveis nos Modelos Administrativos. E aqui você pode criar os filtros desejados para encontrar rapidamente as configurações que precisa configurar.

Sobre as novidades de GPOs no Windows Server 2008 é basicamente isso. Vamos agora entender como é feito o processamento e aplicação das GPOs.

Entendendo como é Feito o Processamento e Aplicação das GPOs:

Este é um item que eu considero de fundamental importância para o administrador. Configurar as GPOs, conforme você verá mais adiante, é relativamente simples com o uso do console de administração das GPOs.

Porém, mais do que saber configurar as GPOs, o administrador precisa entender exatamente como as GPOs são processadas e aplicadas às estações de trabalho e aos usuários. Com este entendimento, o Administrador tem condições de planejar as políticas a serem implementadas e também de resolver problemas relacionados a aplicação das GPOs. Por isso é fundamental que o administrador entenda, exatamente, como é feito o processamento e aplicação das GPOs.

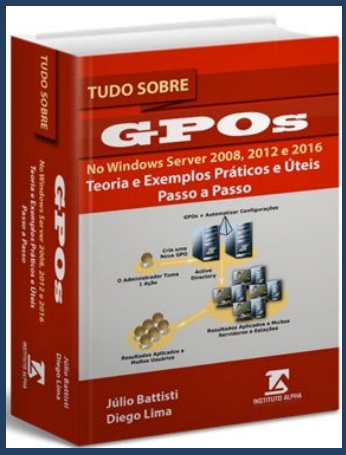
No NT Server 4.0 as configurações de Polices eram armazenadas em um arquivo com a extensão .pol, arquivo este que é gravado no compartilhamento NETLOGON do PDC e de todos os BDCs do domínio. Para clientes Windows 9x/Me o arquivo deve ter o nome config.pol e para clientes com o NT 4.0, o arquivo deve ter o nome ntconfig.pol. As configurações definidas neste arquivo são carregadas durante o logon e aplicadas à registry da estação de trabalho do usuário. As configurações de usuário são carregadas na opção HKEY_CURRENT_USER (HKCU) da registry. As configurações de computador são carregadas na opção HKEY_LOCAL_MACHINE (HKLM) da registry.

IMPORTANTE:

Este e-book é um Trecho de Demonstração do livro:

Tudo Sobre GPOs no Windows Server 2008, 2012 e 2016

Teoria e Exemplos Práticos e Úteis - Passo a Passo



Páginas: 654 | Autores: Júlio Battisti e Diego Lima

Para Comprar o Livro Completo, com 50% de Desconto e Ainda Ganhar um Pacote de Bônus que Valem 20 Vezes o Valor do Livro, Acesse o Seguinte Endereço:

https://juliobattisti.com.br/loja/detalheproduto.asp?CodigoLivro=LIV0001525

A partir do Windows 2000 Server, Windows Server 2003 e Windows Server 2008, o processamento das GPOs segue caminhos bem diferentes, os quais serão descritos neste item.

No NT Server 4.0 um único conjunto de políticas é aplicado ao usuário/computador, conjunto este que é definido no arquivo .POL, carregado quando o computador é inicializado e o usuário faz o logon. Já no Windows Server 2008, mais de um conjunto de políticas pode ser aplicado ao mesmo usuário/computador. Por exemplo, imagine o usuário jsilva, do domínio abc.com, cuja conta está na Unidade Organizacional Vendas, dentro da Unidade Organizacional (OU) RegiãoSul. Para este usuário, será aplicada a GPO local, mais a GPO do domínio (uma ou mais GPOs que estiverem definidas no domínio abc.com), mais o conjunto de GPOs definidas para a OU RegiãoSul e mais o conjunto de GPOs definidas para a OU Vendas.

As configurações das GPOs são armazenadas em uma estrutura de pastas e arquivos dos DCs do domínio. Estas informações são gravadas na pasta SYSVOL e são replicadas para todos os DCs do domínio. Na Figura 1.1 apresento uma visão geral da pasta onde ficam gravadas as informações sobre as GPOs do domínio abc.com (C:\WINDOWS\SYSVOL\sysvol\abc.com\Policies), onde o Windows Server 2008 está instalado na pasta Windows, no drive C:

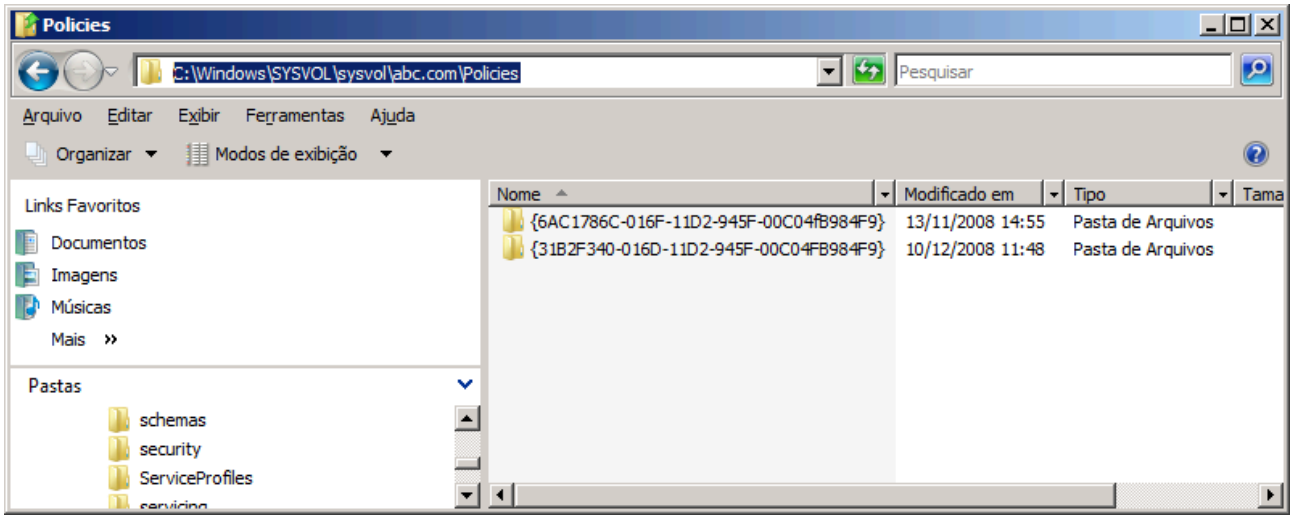


Figura 1.1 - A pasta com informações das GPOs em um DC do domínio abc.com.

Cada pasta representa uma determinada GPO. Ao abrir uma destas pastas, será exibido o seguinte conteúdo:

- **Pasta Adm ou Admx:** Contém os arquivos com os templates administrativos. Uma das novidades no Windows Server 2008 são os templates baseados no padrão XML, os quais usam a extensão .Admx.

- **Pasta Scripts:** Se houver scripts definidos neste template, esta pasta conterá os scripts e arquivos relacionados.

- **Pasta MACHINE:** Contém as configurações que se aplicam a computadores. Esta pasta contém um arquivo chamado Registry.pol, o qual contém as configurações de registry que serão aplicadas ao computador durante a inicialização (veja os passos de aplicação das polices durante a inicialização do computador, mais adiante). Quando o computador é inicializado, é feito o download do arquivo Registry.pol e são aplicadas as configurações definidas neste arquivo. As configurações são aplicadas na opção HKEY_LOCAL_MACHINE, da registry, da estação de trabalho.

- **Pasta USER:** Contém as configurações que se aplicam a usuários. Esta pasta contém um arquivo chamado Registry.pol, o qual contém as configurações de registry que serão aplicadas ao usuário quando este fizer o logon (veja os passos de aplicação das polices durante a inicialização do computador, mais adiante). Quando o computador é inicializado, é feito o download do arquivo Registry.pol e são aplicadas as configurações definidas neste arquivo. As configurações são aplicadas na opção HKEY_CURRENT_USER, da registry

- **Arquivo GPT.INI:** Informações sobre a versão da GPO. Utilizada pelo serviço de replicação.

Em resumo: As informações sobre as GPOs são gravadas em uma estrutura de pastas e arquivos, dentro da pasta SYSVOL, nos DCs do domínio. Esta estrutura é replicada para todos os DCs do domínio. As informações gravadas na pasta SYSVOL são os chamados modelos de GPOs, oficialmente conhecidos como Group Policy Template (GPTs). O template é que define quais opções de configuração estarão disponíveis. Por exemplo, o template de GPO para usuários define quais opções de usuários poderão ser configuradas via GPO. Quando uma nova GPO é criada, o Windows Server 2008 cria a GPO com base nos templates da pasta Sysvol. A nova GPO que é criada e as configurações nela definidas são armazenadas no Active Directory. Esta GPO é conhecida como GPC – Group Policy Container. Ou seja, uma GPO é criada com base em um

modelo (GPT, armazenado na pasta SYSVOL). O modelo define quais opções de configuração estarão disponíveis. Após criada e configurada, a GPO é salva na base de dados do Active Directory, quando é conhecida como GPC – Group Policy Container. Estas definições muitas vezes se confundem. Nos exemplos práticos, quando você aprenderá a criar e a configurar as políticas, usarei sempre o termo genérico GPO.

Toda GPO é dividida em duas partes também conhecidas como seções:

- Seção do usuário.
- Seção do computador.

Conforme o próprio nome sugere, estas seções contém as configurações específicas aplicadas a usuários ou computadores especificamente. Quando um computador com o Windows 2000, Windows XP Professional, Windows Vista, Windows 7, Windows 8, Windows 10, Windows Server 2003, Windows Server 2008, Windows Server 2012 ou Windows Server 2016, pertencente ao domínio é inicializado, o Windows verifica se existem novas GPOs ou alterações nas GPOs existentes e aplica as configurações definidas na seção do computador (independentemente de algum usuário ter feito o logon ou não). Quando o usuário faz o logon no domínio (em qualquer computador da rede com uma das versões do Windows descritas no início do parágrafo), o Windows verifica se existem GPOs a serem aplicadas a este usuário ou alterações nas GPOs já aplicadas e aplica as configurações definidas na seção de usuário destas GPOs. Estas informações ficam gravadas no Active Directory. Conforme descrito anteriormente (estou insistindo neste ponto porque ele é muito importante), uma GPO é criada com base nos modelos armazenados na pasta Sysvol (GPT- Group Policy Templates). Uma vez criada e configurada, a GPO é salva no Active Directory (tornando-se uma GPC – Group Policy Container). Quando um usuário faz o logon o Windows Server 2008 verifica no Active Directory se existem GPOs a serem aplicadas para o usuário. Quando um computador é inicializado, o Windows Server 2008 verifica no Active Directory, se existem GPOs a serem aplicadas ao computador. É isso.

Detalhando a Ordem de Processamento das GPOs:

As GPOs são processadas na seguinte seqüência:

1. **GPO Local:** Cada computador com o Windows 2000, Windows XP Professional, Windows Vista, Windows 7, Windows 8, Windows 10, Windows Server 2003, Windows Server 2008,

Windows Server 2012 ou Windows Server 2012, possui uma GPO local, a qual é aplicada em primeiro lugar, antes das demais GPOs que possam estar disponíveis.

2. **GPOs do Site:** Em seguida é aplicada a GPO associada (ou GPOs associadas, caso exista mais de uma) ao site do qual faz parte o computador que está sendo inicializado. Lembre-se que um site do Active Directory é definido por uma ou mais sub-redes. O Windows Server 2008 identifica a qual site pertence um computador, pela identificação de rede do computador (propriedades do Protocolo TCP/IP).

3. **GPOs associadas ao domínio:** Em seguida são processadas as GPOs associadas ao domínio ao qual pertence o computador, conforme a ordem de execução definida pelo administrador. Na parte prática deste capítulo você aprenderá a criar GPOs de domínio e a definir a ordem de aplicação destas GPOs.

4. **GPOs associadas a todas as OUs do caminho:** Por exemplo, se um computador pertence a OU Vendas, que está dentro da OU RegiãoSul, primeiro serão aplicadas as GPOs da OU RegiãoSul, para depois serem aplicadas as GPOs associadas a OU Vendas. Quando houver mais de uma GPO associada a mesma OU, as GPOs serão aplicadas na seqüência que foi definida pelo administrador.

Com esta seqüência, as GPOs aplicadas por último tem preferência em relação as que são aplicadas anteriormente. Por exemplo, se na GPO do domínio está que o usuário não deve ter acesso ao comando Iniciar -> Executar, porém na GPO da OU do usuário este comando está habilitado, valerá a configuração da GPO da OU, ou seja, comando habilitado, uma vez que esta GPO será aplicada por último. O administrador tem meios para fazer com que uma GPO de nível mais alto, como por exemplo uma GPO de domínio, não tenha suas configurações sobrescritas por GPOs de nível mais baixo, aplicadas por último, como uma GPO associada a uma unidade organizacional. Para implementar esta configuração, o administrador marca a opção “No Override” (Não sobrescrever), conforme você aprenderá na parte prática deste capítulo.

Algumas exceções na ordem de aplicação das GPOs:

- Qualquer GPO que estiver associada a um site, domínio ou unidade organizacional (a única exceção é a GPO local), poderá ser configurada com a opção “No Override”, de tal maneira que suas configurações não possam ser sobrescritas pelas GPOs que serão aplicadas depois. Caso duas GPOs, no mesmo caminho, tenham esta opção marcada, valerá a configuração da

GPO que estiver mais acima na hierarquia de objetos. Por exemplo, se uma GPO de domínio está marcada com a opção No Override e uma GPO de uma unidade organizacional também esta marcada com a opção No Override, em caso de conflito nas configurações destas duas GPOs, valerá a configuração da GPO de domínio, que é a que está mais acima na hierarquia de objetos do Active Directory.

Importante: Deve ser observado que a propriedade No Override é uma propriedade da ligação da GPO com o domínio, site ou unidade organizacional. Esta não é uma propriedade da GPO propriamente dita. Uma GPO poderá ser associada em diferentes locais no Active Directory. Por exemplo posso associar uma determinada GPO com o domínio e também com uma ou mais unidades organizacionais do domínio. Em uma das associações posso habilitar a opção No Override, em outras não e assim por diante. Lembre (principalmente para os exames de certificação do Windows Server 2008): A propriedade No Override é uma propriedade da ligação (objeto do tipo link) entre uma GPO e um domínio, site ou unidade organizacional e não uma propriedade da GPO propriamente dita.

- Computadores que não façam parte do domínio, como por exemplo computadores configurados para fazer parte de um Workgroup, irão processar e aplicar apenas a GPO local, uma vez que todas as demais GPOs são carregadas a partir do Active Directory. Como o computador não faz parte do domínio, ele não tem acesso ao Active Directory.

O Recurso de Loopback:

Existe um recurso avançado das polices, o qual é conhecido como Loopback. Este recurso é especialmente recomendado para computadores que estão conectados à rede da empresa mas com acesso ao público externo, como por exemplo em quiosques de informação ao público, terminais de autoatendimento e computadores de salas de treinamentos.

O recurso de Loopback permite que você defina uma ordem alternativa para aplicação das GPOs. Lembrando que a ordem padrão é: local, site, domínio e unidade organizacional. O recurso de Loopback pode ser configurado com os valores Not configured (Não configurado), Enabled (Habilitado) ou Disabled (Desabilitado). Se este recurso for habilitado, ele poderá ser configurado com as opções Merge ou Replace, conforme descrito a seguir:

- **Loopback configurado com a opção Replace:** Com este método, a lista de execução padrão (que define a seqüência de aplicação das GPOs) será substituída pela lista definida no próprio computador.

- **Loopback configurado com a opção Merge:** Com este método, a lista de execução padrão (que define a seqüência de aplicação das GPOs) será concatenada com lista definida no próprio computador. As GPOs obtidas a partir da lista definida no próprio computador serão aplicadas por último, o que fará com que estas GPOs tenham precedência em relação as GPOs definidas pela lista padrão, obtida a partir do Active Directory.

Ordem de Eventos quando o Computador é Inicializado e o Usuário faz o Logon:

Neste item descrevo a ordem de eventos que ocorrem quando um computador é inicializado e quando o usuário faz o logon. Considerando um computador que pertence ao domínio e possui o Windows 2000, Windows XP Professional, Windows Vista, Windows 7, Windows 8, Windows 10, Windows Server 2003, Windows Server 2008, Windows Server 2012 ou Windows Server 2016 instalado:

1. O computador é ligado, o Windows é inicializado e os serviços de rede são carregados.

2. Uma lista ordenada de objetos do tipo GPO é obtida pelo computador. A maneira como esta lista é obtida, depende dos seguintes fatores:

    2.1. O computador deve fazer parte do domínio e obter esta lista a partir das informações do Active Directory. Se o computador não fizer parte do domínio, apenas a GPO local será aplicada.

    2.2. A lista depende de onde está contida a conta do computador, no Active Directory. Por exemplo, a unidade organizacional onde encontra-se a conta, definirá quais GPOs serão aplicadas, as configurações de rede definem a qual site pertence o computador e quais GPOs de site (se houver alguma), serão aplicadas e assim por diante.

    2.3. De a lista de GPOs ter sido alterada desde a última inicialização. Se a lista de GPOs não foi alterada, nenhum processamento será feito.

3. As configurações relativas a computador serão aplicadas, a partir da lista de GPOs obtidas. As GPOs são aplicadas na ordem descrita anteriormente: local, site, domínio e unidade organizacional.

4. Se houver um script de inicialização configurado ele será executado. Pode haver mais de um script de inicialização configurado, conforme veremos na parte prática. Neste caso eles serão executados na ordem em que foram definidos e de maneira síncrona, ou seja, um script é executado e somente depois que ele concluir a sua execução, o próximo será executado e assim por diante. Existem também um tempo máximo de execução para cada script, que por padrão é de 600 segundos. Se o script não terminar a sua execução neste tempo, ele será encerrado e o próximo script (se houver) será inicializado.

5. Após terem sido feitos estes processamentos, a tela de logon é exibida. O usuário faz o logon.

6. O usuário digita as suas informações de logon e é autenticado por um dos DCs do domínio. Após a validação do usuário, a sua profile é carregada.

7. Uma lista ordenada de objetos do tipo GPO é obtida pelo usuário. A maneira como esta lista é obtida, depende dos seguintes fatores:

    7.1. Se o usuário está fazendo o logon no domínio e, portanto, recebendo a lista de GPOs a serem aplicadas a partir do Active Directory.

    7.2. Se o recurso de Loopback está habilitado e, estando habilitado, qual opção está definida (Merge ou Replace).

    7.3. A lista depende de onde está contida a conta do usuário, no Active Directory. Por exemplo, a unidade organizacional onde encontra-se a conta, definirá quais GPOs serão plicadas.

    7.4. De a lista de GPOs ter sido alterada desde o último logon. Se a lista de GPOs não foi alterada, nenhum processamento será feito. Este comportamento pode ser alterado.

8. As configurações relativas ao usuário serão aplicadas, a partir da lista de GPOs obtidas. As GPOs são aplicadas na ordem descrita anteriormente: local, site, domínio e unidade organizacional.

9. Os scripts de logon definidos nas GPOs serão executados. Estes scripts são executados sem que seja exibida uma tela de execução dos scripts e de maneira síncrona, ou seja, um após o outro, conforme descrito para a execução de scripts de inicialização. O script de logon, definido nas propriedades da conta do usuário, no Active Directory, será executado após a execução dos scripts definidos via GPOs. Este script é executado e uma janela do Prompt de comando é exibida. Observe que podem ser executados vários scripts de logon, em seqüência, sendo que estes scripts são definidos nas GPOs que se aplicam ao usuário e o último script a ser executado é o script de logon definido nas propriedades da conta do usuário, no Active Directory.

10. A área de trabalho do usuário é carregada e o Windows está pronto para ser utilizado.

Alguns casos especiais em relação à execução das polices:

- Pode acontecer uma situação em que o usuário está fazendo o logon em um computador que pertence a um domínio do NT Server 4.0, porém fazendo o logon em um domínio baseado no Windows Server 2008 (sendo que existem relações de confiança entre os domínios). Neste caso, para as configurações de computador serão aplicadas as configurações definidas no sistema de Polices do NT 4.0 e para o usuário, será aplicada a parte relativa as configurações de usuário, das GPOs definidas no domínio de origem do usuário. Pode ocorrer o contrário, ou seja, a conta de computador ser de um domínio do Windows Server 2008 e a conta do usuário de um domínio do NT Server 4.0. Neste caso serão aplicadas as configurações de computador, obtidas via GPO e as configurações de polices definidas para o usuário, no domínio de origem da conta.

- Se for um computador com o Windows XP Professional, Windows Vista, Windows 7, Windows 8, Windows 10, Windows 2000 Server, Windows Server 2003, Windows Server 2008, Windows Server 2012 ou Windows Server 2016, porém pertencente a um domínio baseado no NT Server 4.0, somente serão aplicadas as polices do NT Server 4.0, já que em um domínio baseado no NT Server 4.0 não existe o conceito de GPOs.

Entendendo como Funciona o Mecanismo de Herança – Policy Inheritance:

Por padrão, as GPOs são aplicadas a partir do objeto pai (a raiz do domínio), passando pelos objetos filho, até a unidade organizacional onde está a conta do usuário ou do computador. É importante salientar este funcionamento é dentro de um mesmo domínio, não existe uma herança de GPOs

entre domínios. Por exemplo, as GPOs aplicadas em um domínio raiz abc.com, não serão herdadas e aplicadas nos domínios filho, tais como vendas.abc.com e rh.abc.com.

Porém dentro do domínio, o funcionamento é o padrão descrito nos itens anteriores. Se você associar uma GPO com um determinado elemento do Active Directory (um domínio ou uma unidade organizacional), as configurações desta GPO também serão aplicadas a todos os objetos contidos nos elementos filho. Por exemplo, se você aplicar uma GPO no domínio, todos os objetos do domínio receberão as configurações desta GPO. Se você aplicar uma GPO a uma unidade organizacional, todos os objetos (inclusive objetos contidos em unidades organizacionais dentro da unidade organizacional que está sendo configurada) contidos nesta unidade organizacional receberão estas configurações. Porém é importante lembrar que, ao associar uma GPO com um objeto filho (por exemplo uma unidade organizacional), as configurações desta GPO irão sobrescrever as configurações do objeto Pai (por exemplo o domínio), pois são executadas por último, a não ser que o mecanismo de No Override tenha sido habilitado na GPO do objeto Pai.

Para entender melhor os conceitos apresentados, vamos considerar o exemplo de um domínio chamado abc.com, no qual foi criada uma unidade organizacional chamada Sul. Dentro desta unidade organizacional foi criada uma outra unidade organizacional chamada Vendas. Para a discussão que apresentarei a seguir, Sul é referenciada como OU pai (em Inglês é usado o termo Parent) e Vendas é referenciada como OU filho (em Inglês é usado o termo child).

Se nas configurações de GPO da OU pai, houver itens que estão marcados como Não configurados, a OU filho não irá herdar estes itens “não configurados”. Lembrando que a maioria das opções pode ser marcada como Enabled (Habilitada), Disabled (Desabilitada) ou Not deffined (Não definida). As opções que tiverem o valor padrão como desabilitado, também serão definidas como desabilitado na OU filho. As opções que estiverem configuradas na OU pai, habilitadas ou desabilitadas (não confundir com aquelas que tem o valor padrão como desabilitada) e as respectivas opções não estiverem configuradas na OU filho, serão herdadas pela OU filho, com o mesmo valor definido na OU pai (habilitada ou desabilitada). Se uma determinada opção estiver configurada na OU filho, valerá o que está configurado na OU filho, a não ser que a opção No Override tenha sido definida na GPO da OU pai. Se as configurações definidas na OU pai e as políticas definidas em uma OU filho são compatíveis, isso é, se não houver conflito, a OU filho irá herdar as definições da OU pai e irá aplicá-las normalmente na OU filho.

Se houver configurações definidas na OU pai, as quais são incompatíveis com as configurações definidas na OU filho (por exemplo, uma determinada Police está habilitada na GPO da OU pai e desabilitada na Police da OU filho), estas configurações não serão herdadas pela OU filho. Será aplicada a configuração definida na OU filho.

Como bloquear a herança (Blocking inheritance):

A herança pode ser bloqueada tanto em nível de domínio quanto em nível de unidade organizacional. Esta opção é configurada nas propriedades do domínio ou da OU respectivamente, conforme você aprenderá na parte prática deste capítulo, mais adiante.

Forçando a herança (Enforcing inheritance):

Para forçar a herança, ou seja, para fazer com que os objetos filho, obrigatoriamente, tenham que aplicar as configurações definidas no objeto pai, você utiliza a opção No Override, já descrita anteriormente e que será exemplificada na parte prática. Ao marcar esta opção, você força todos os objetos filho a herdarem as configurações definidas no objeto Pai, mesmo que existam conflitos de configuração e mesmo que a opção Blocking inheritance tenha sido habilitada no objeto filho.

Algumas observações importantes:

- Polices que foram configuradas com a opção No Override serão aplicadas, independentemente das configurações existentes nos objetos filho.

- As opções No Override e Block Policy inheritance devem ser utilizadas com cautela, pois o uso muito intensivo destes recursos, torna difícil o trabalho de identificar e resolver problemas de configuração, quando não se está obtendo o resultado desejado.

Exemplos de Situações Práticas de uso das Opções "No Override" e "Block Policy Inheritance"

Neste tópico vamos descrever algumas situações práticas, onde o uso das configurações "No Override" e "Block Policy inheritance" se aplica.

Situação 01: Como administrador do domínio abc.com você gostaria de implementar um conjunto de configurações usando GPOs. Este conjunto deve ser aplicado a todos os computadores e usuários

do domínio. Essas configurações não devem ser sobrescritas por GPOs ligadas a objetos filhos, tais como GPOs ligadas a OUs do domínio. Qual a solução para a situação descrita?

Solução: Esta é uma situação de solução bastante simples e ao mesmo tempo muito comum. Neste caso, como as configurações devem ser aplicadas a todos os usuários e computadores do domínio, elas devem ser feitas na GPO padrão do domínio, com a qual você aprenderá a trabalhar mais adiante, na parte prática deste capítulo. Para que estas configurações não possam ser sobrescritas por configurações definidas nas GPOs dos objetos filho, você deve acessar a GPO no console GPMC, clicar na guia Escopo, clicar com o botão direito do mouse no link da GPO e, no menu de opções que é exibido, clicar em Imposto. Veremos exemplos práticos, passo a passo, na parte prática do capítulo, mais adiante.

Situação 02: Como administrador do domínio abc.com você gostaria de implementar um conjunto de configurações usando GPOs. Este conjunto deve ser aplicado a todos os computadores e usuários dos domínios. Existe uma única OU do domínio, na qual devem ser aplicadas configurações especiais e não devem ser aplicadas as configurações definidas na GPO padrão do domínio. Nesta OU estão as contas de usuários e computadores do setor de pesquisa, e uma série de configurações especiais de segurança devem ser aplicadas via GPO. Qual a solução para a situação descrita?

Solução: Nesta situação o administrador deve configurar a GPO padrão do domínio, com as configurações que serão utilizadas pela maioria dos usuários e computadores, com exceção dos usuários e computadores da OU Pesquisa. Na OU pesquisa, crie e configure uma GPO com as configurações exigidas pelos usuários e computadores desta OU. Para isso basta abrir o console GPMC, navegar até o domínio abc.com, clicar com o botão direito do mouse no domínio abc.com e, no menu de opções que é exibido, clicar em Bloquear Herança. Veremos exemplos práticos, passo a passo, na parte prática do capítulo, mais adiante. Com esta configuração a OU pesquisa não herdará as definições de GPOs aplicadas ao domínio e somente serão aplicadas as GPOs definidas na própria OU Pesquisa, que é exatamente o que deve ser feito para solucionar a questão proposta.

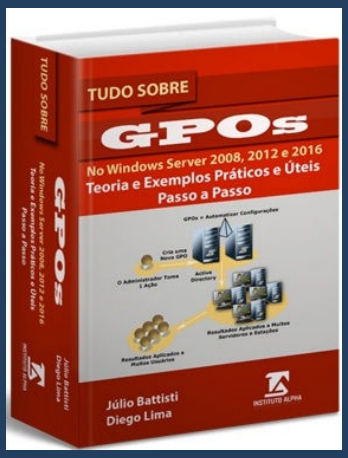
Bem, sobre a teoria inicial de GPOs era isso. Agora você aprenderá uma série de ações práticas sobre GPOs. Após as ações práticas falarei sobre uma outra funcionalidade muito importante das GPOs que é a distribuição de software. Durante os exemplos práticos serão apresentados diversos conceitos relacionados com o tópico que está sendo exemplificado.

IMPORTANTE:

Este e-book é um Trecho de Demonstração do livro:

Tudo Sobre GPOs no Windows Server 2008, 2012 e 2016

Teoria e Exemplos Práticos e Úteis - Passo a Passo



Páginas: 654 | Autores: Júlio Battisti e Diego Lima

Para Comprar o Livro Completo, com 50% de Desconto e Ainda Ganhar um Pacote de Bônus que Valem 20 Vezes o Valor do Livro, Acesse o Seguinte Endereço:

https://juliobattisti.com.br/loja/detalheproduto.asp?CodigoLivro=LIV0001525