Infraestrutura da GPO

...

Objetos de Diretiva de Grupo

- Para gerenciar a configuração de usuários e computadores, você cria GPOs que contêm as configurações de diretiva necessárias.
- Cada computador tem vários GPOs armazenados localmente no sistema - São as *Local GPO*
- E podem estar dentro do escopo de qualquer número de GPOs baseados em domínio

Local GPO

- Independente se o computador faz parte de domínio ou não , sistemas Windows tem suas GPOs local que podem gerenciar localmente esse sistema
- Estão armazenadas em %SystemRoot%\System32\GroupPolicy e só afeta aquele sistema o qual estão armazenadas .
- Por padrão apenas políticas de segurança já estão pré-configuradas as demais estão definidas como *não configuradas*
- As políticas locais são usadas em ambientes onde não temos um AD Samba pois quando os temos a administração se torna bem mais fácil pois tudo estará centralizada no DC
- As configurações nos GPOs vinculados ao site, ao domínio ou às UOs substituirão a GPO local

- Você pode configurar GPO local para dois grupos padrão : *Administradores e Usuários sem privilégio de administrador*
- Você pode refinar ainda mais configurações do usuário com um GPO local que se aplica a uma conta de usuário específica.
- As configurações do usuário em um GPO específico do usuário substituirão as configurações conflitantes nos grupos *Administradores e Usuários sem privilégio de administrador*
- Tenha em mente que os GPOs locais são projetados para ambientes não-domínio.
- Configure-os para seu computador em casa, por exemplo, para gerenciar as configurações de seu cônjuge ou filhos.

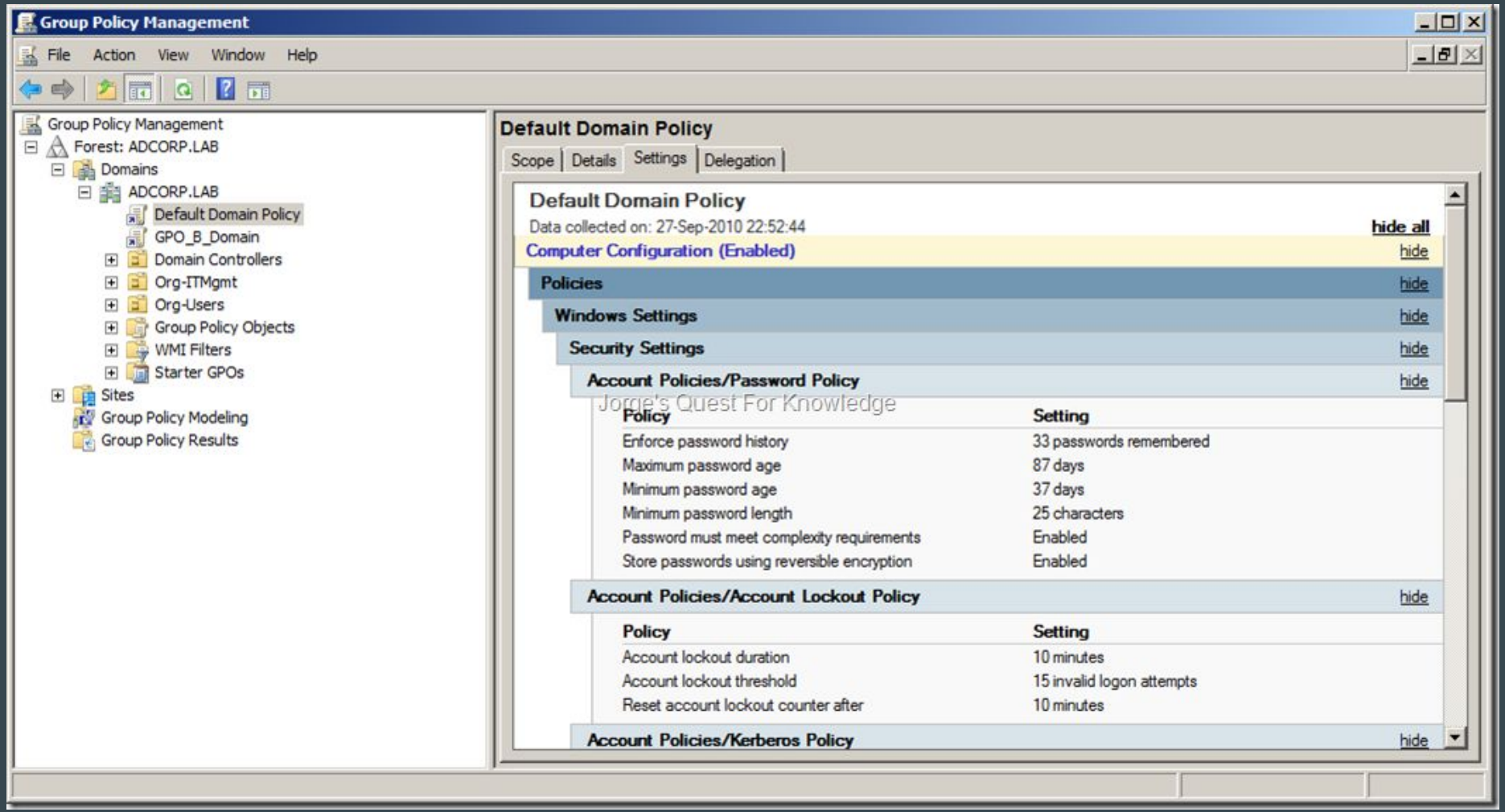
GPO baseada em domínio

- Os GPOs baseados em domínio são criados no Active Directory e armazenados em controladores de domínio.
- Eles são usados para gerenciar a configuração centralmente para usuários e computadores no domínio.

Quando o Samba AD é instalado , dois GPOs padrão são criados:

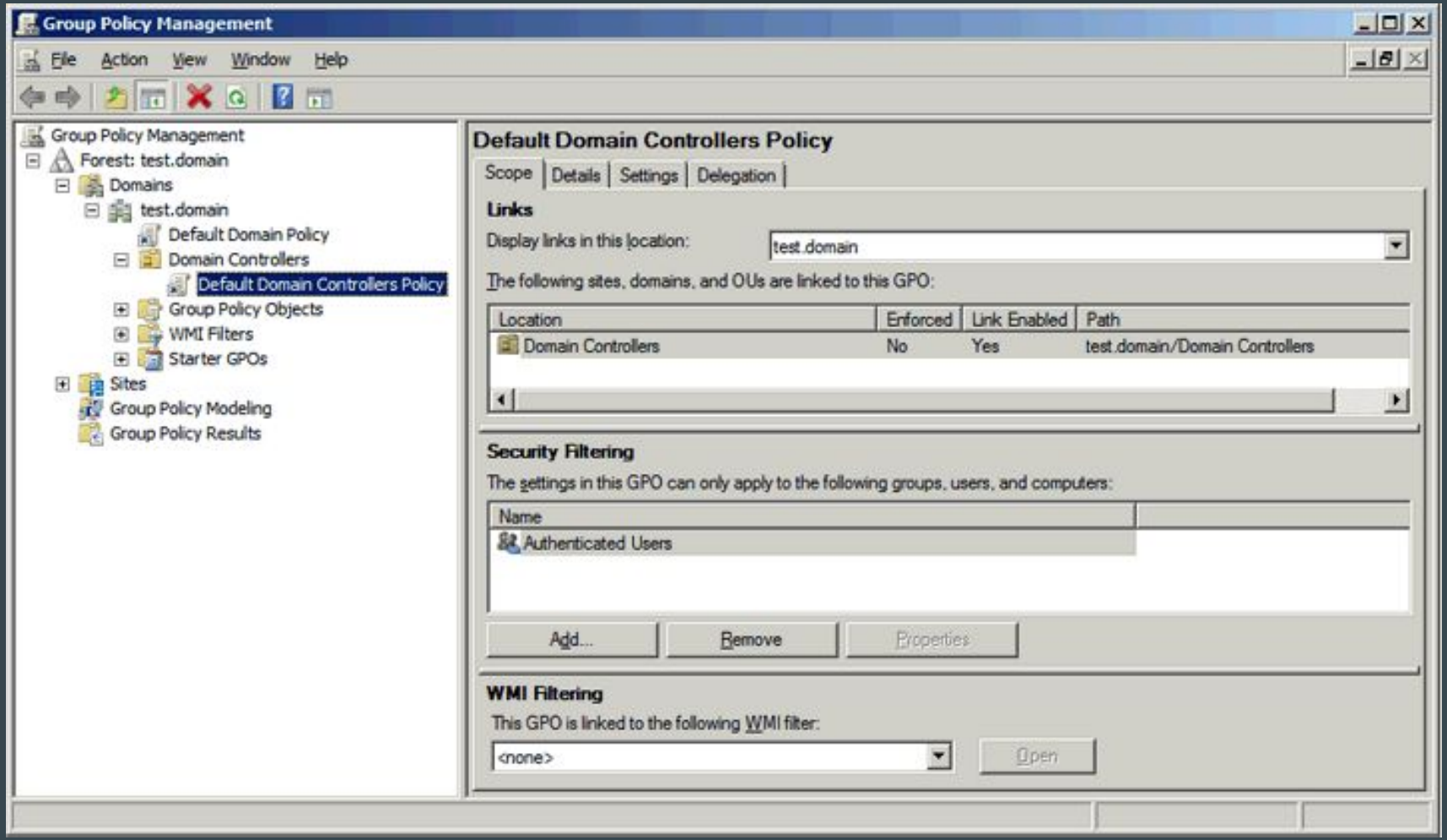
Default Domain Policy

- Este GPO está vinculado ao domínio e não tem grupo de segurança ou Filtros WMI. Portanto, afeta todos os usuários e computadores no domínio (incluindo computadores que são controladores de domínio).
- Esse GPO contém configurações de diretiva que especificam senha, bloqueio de conta e etc..
- *Em um ambiente com Samba 4 não vem nada configurado nesse GPO mas existe para efeito de compatibilidade .*
- Não edite esse GPO crie os seus próprios GPO


Group Policy Management
File Action View Window Help
Group Policy Management
Forest: ADCORP.LAB
Domains
ADCORP.LAB
Default Domain Policy
GPO_B_Domain
Domain Controllers
Org-ITMgmt
Org-Users
Group Policy Objects
WMI Filters
Starter GPOs
Sites
Group Policy Modeling
Group Policy Results
Default Domain Policy
Scope Details Settings Delegation
Default Domain Policy
Data collected on: 27-Sep-2010 22:52:44
hide all
Computer Configuration (Enabled)
hide
Policies
hide
Windows Settings
hide
Security Settings
hide
Account Policies/Password Policy
hide
Jorge's Quest For Knowledge
Policy
Setting
Enforce password history
33 passwords remembered
Maximum password age
87 days
Minimum password age
37 days
Minimum password length
25 characters
Password must meet complexity requirements
Enabled
Store passwords using reversible encryption
Enabled
Account Policies/Account Lockout Policy
hide
Policy
Setting
Account lockout duration
10 minutes
Account lockout threshold
15 invalid logon attempts
Reset account lockout counter after
10 minutes
Account Policies/Kerberos Policy
hide

Default Domain Controllers Policy

- Este GPO está vinculado à UO de Controladores de Domínio.
- Porque contas de computador para controladores de domínio são mantidas exclusivamente na OU Controladores de domínio e outras contas de computador devem ser mantidos em outras unidades organizacionais, esse GPO afeta apenas os controladores de domínio
- *Em um ambiente com Samba 4 não vem nada configurado nesse GPO mas existe para efeito de compatibilidade .*


Group Policy Management
File Action View Window Help
Group Policy Management
Forest: test.domain
Domains
test.domain
Default Domain Policy
Domain Controllers
Default Domain Controllers Policy
Group Policy Objects
WMI Filters
Starter GPOs
Sites
Group Policy Modeling
Group Policy Results
Default Domain Controllers Policy
Scope Details Settings Delegation
Links
Display links in this location: test.domain
The following sites, domains, and OUs are linked to this GPO:
Location Enforced Link Enabled Path
Domain Controllers No Yes test.domain/Domain Controllers
Security Filtering
The settings in this GPO can only apply to the following groups, users, and computers:
Name
Authenticated Users
Add... Remove Properties
WMI Filtering
This GPO is linked to the following WMI filter:
<none>
Open

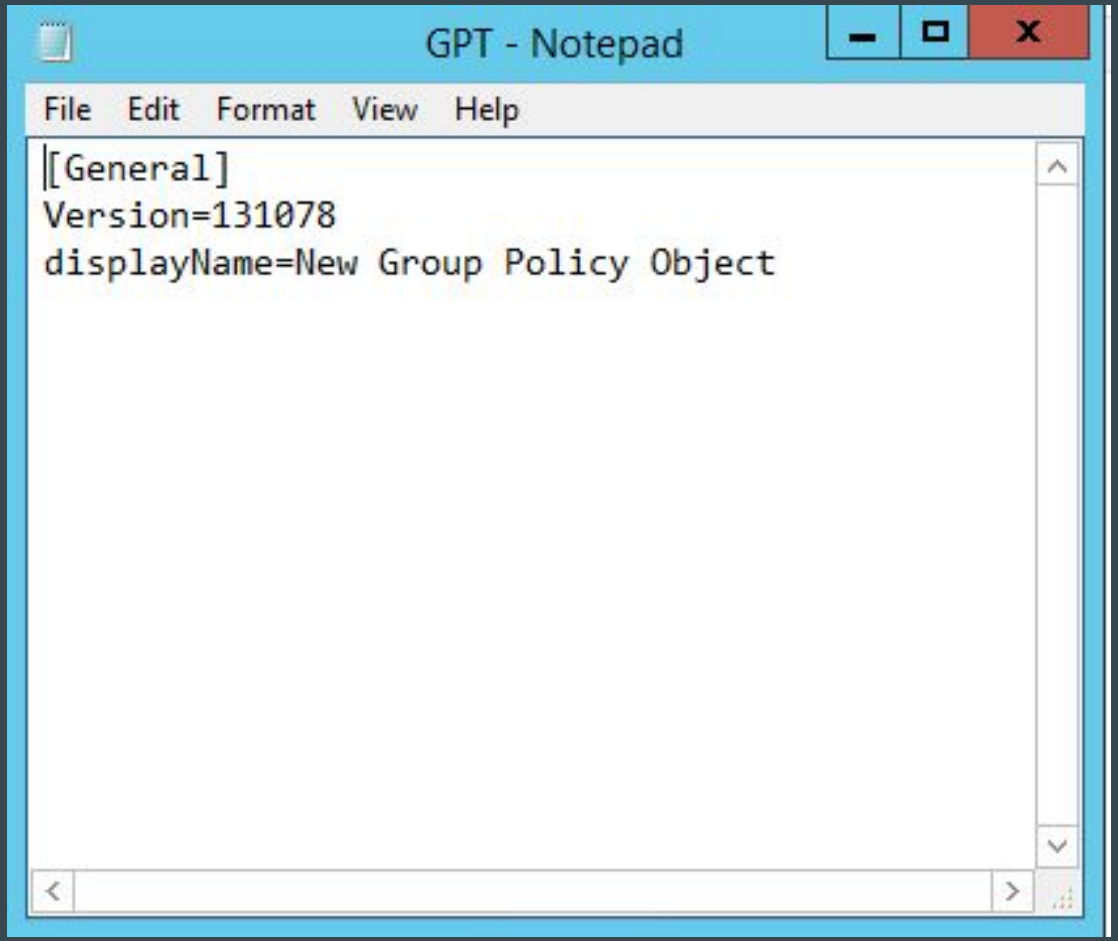
Criando, vinculando e editando GPOs

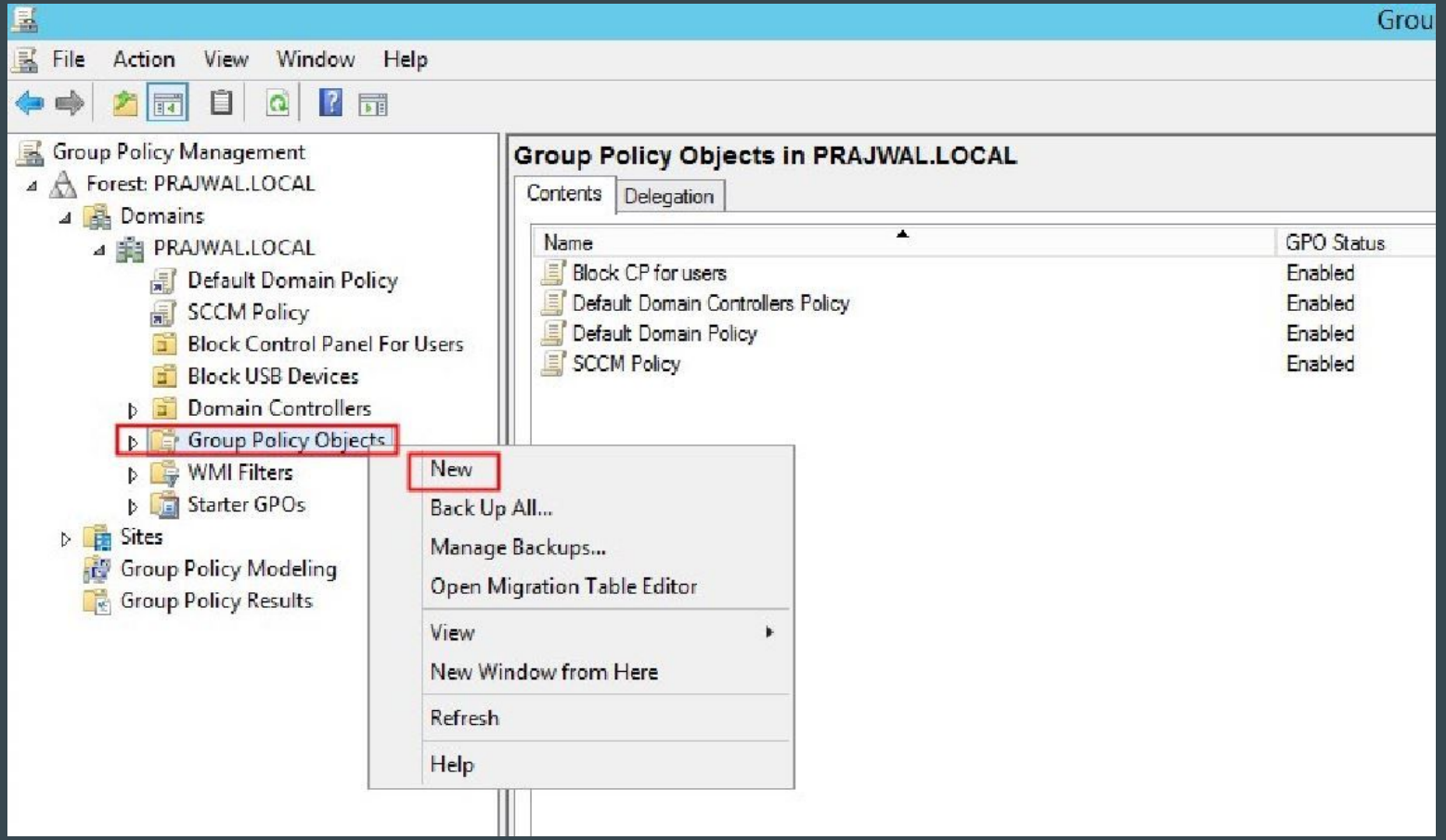
- Você deve ter permissão para o contêiner Objetos de Política de Grupo para criar um GPO.
- Por padrão, o grupo `Domain admins` e o grupo `Group Policy Creator Owners` têm a capacidade de criar GPOs.
- Para delegar permissões a outros grupos, selecione o contêiner Objetos de Políticas de Grupo na árvore de console do GPME e clique na guia Delegação no painel de detalhes do console.

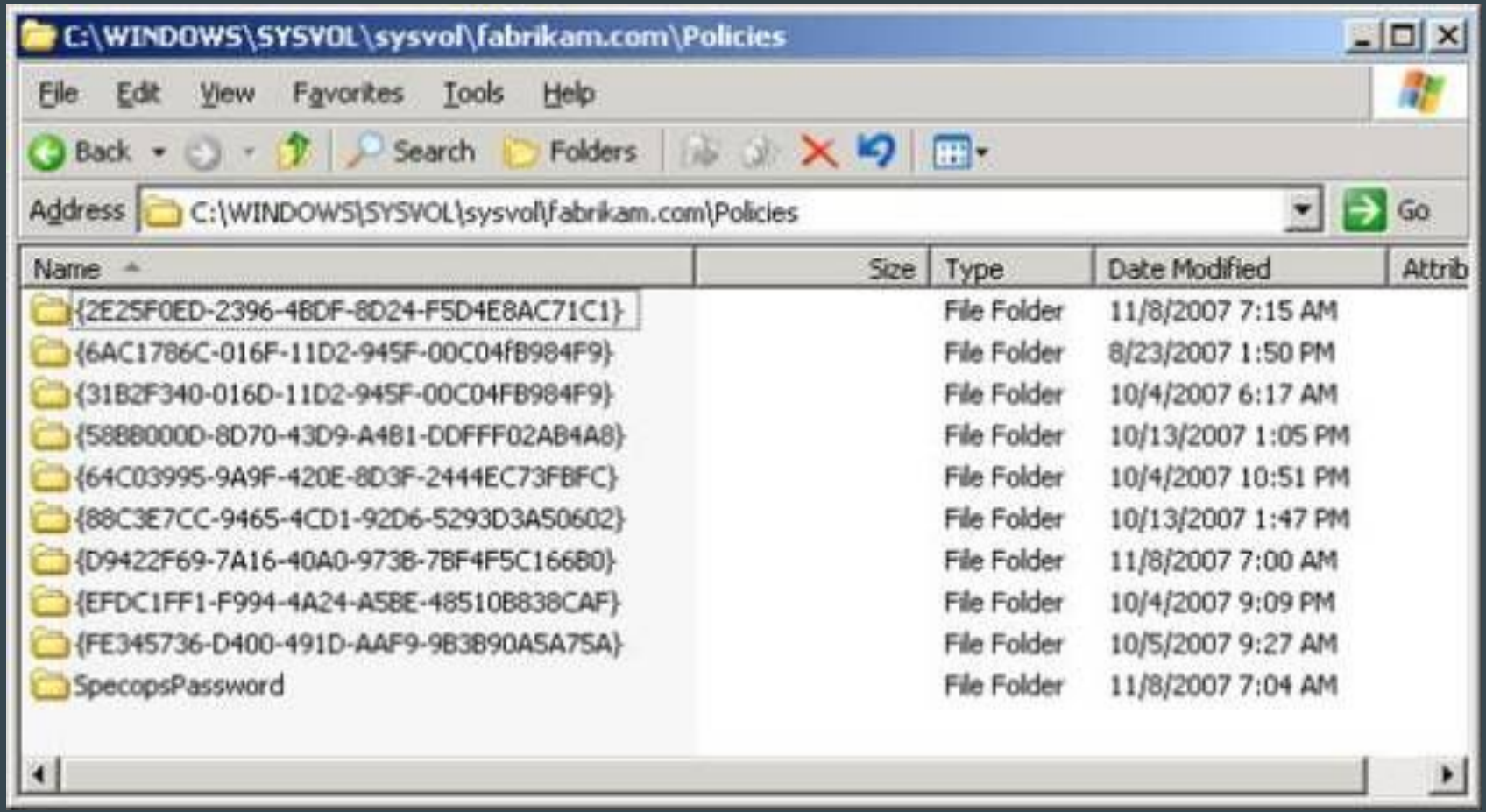
Armazenamento de GPO

- As configurações da Diretiva de Grupo são apresentadas como GPOs nas ferramentas de interface do usuário do Active Directory, mas um O GPO é, na verdade, dois componentes:
  - Contêiner de diretiva de grupo (GPC)
  - Modelo de diretiva de grupo (GPT)
- O GPC é um objeto do Active Directory armazenado no contêiner Objetos de Diretiva de Grupo.
- Possui um atributo de identificador global exclusivo (GUID) que identifica exclusivamente o objeto no Active Directory.

- O GPC define os atributos básicos do GPO, mas não contém qualquer uma das configurações.
- As configurações estão contidas no GPT, uma coleção de arquivos armazenados no SYS-VOL do DC ,no seguinte caminho `%SystemRoot%\SYSVOL\Domain\Policies\GPO GUID`
- As alterações na GPO são armazenadas no GPT e ele tem um número de versão que começa com zero , se ele foi atualizado esse número é alterado com a incrementação de +1.
- Esse número de versão fica gravado no arquivo `gpt.ini`
- O cliente de GPO sabe o número anterior e sabe se foi alterado, então os CSEs são informados e as GPO são atualizadas .


GPT - Notepad
File Edit Format View Help
[General]
Version=131078
displayName=New Group Policy Object


Grou
File Action View Window Help
Group Policy Management
Forest: PRAJWAL.LOCAL
Domains
PRAJWAL.LOCAL
Default Domain Policy
SCCM Policy
Block Control Panel For Users
Block USB Devices
Domain Controllers
Group Policy Objects
WMI Filters
Starter GPOs
Sites
Group Policy Modeling
Group Policy Results
New
Back Up All...
Manage Backups...
Open Migration Table Editor
View
New Window from Here
Refresh
Help
Group Policy Objects in PRAJWAL.LOCAL
Contents
Delegation
Name
GPO Status
Block CP for users
Enabled
Default Domain Controllers Policy
Enabled
Default Domain Policy
Enabled
SCCM Policy
Enabled


C:\WINDOWS\SYSVOL\sysvol\fabrikam.com\Policies
File Edit View Favorites Tools Help
Back Search Folders
Address C:\WINDOWS\SYSVOL\sysvol\fabrikam.com\Policies
Go
Name Size Type Date Modified Attrib
{2E2SF0ED-2396-4BDF-8D24-F5D4E8AC71C1} File Folder 11/8/2007 7:15 AM
{6AC1786C-016F-11D2-945F-00C04fB984F9} File Folder 8/23/2007 1:50 PM
{31B2F340-016D-11D2-945F-00C04FB984F9} File Folder 10/4/2007 6:17 AM
{5888000D-8D70-43D9-A4B1-DDFFF02AB4A8} File Folder 10/13/2007 1:05 PM
{64C03995-9A9F-420E-8D3F-2444EC73FBFC} File Folder 10/4/2007 10:51 PM
{88C3E7CC-9465-4CD1-92D6-5293D3A50602} File Folder 10/13/2007 1:47 PM
{D9422F69-7A16-40A0-973B-7BF4F5C166B0} File Folder 11/8/2007 7:00 AM
{EFDC1FF1-F994-4A24-A5BE-48510B838CAF} File Folder 10/4/2007 9:09 PM
{FE345736-D400-491D-AAF9-9B3B90A5A75A} File Folder 10/5/2007 9:27 AM
SpecopsPassword File Folder 11/8/2007 7:04 AM

Replicação de GPO

- As duas partes de um GPO são replicadas entre controladores de domínio usando mecanismos distintos.
  - O GPC no Active Directory é replicado pelo Directory Replication Agent (DRA),
- O GPT no SYSVOL é replicado usando uma das duas tecnologias.
  - O serviço de replicação de arquivos (FRS)
  - A Replicação do Sistema de Arquivos Distribuídos (DFS-R)
- No em ambientes com o Samba 4 como DCs não é assim que funciona. Ambos, o GPC e o GPT são replicados usando a mesma tecnologia de replicação usada para replicar a pasta sysvol , no caso usamos `osync` .
- Em ambientes com DC samba 4 você deve escolher um DC para que sejam feitas as configurações a serem replicadas para os outros DCs

Preferências

- Abaixo de Configuração do Computador e Configuração do Usuário, há um nó Preferências.
- As preferências fornecem mais de 20 CSEs para ajudá-lo a gerenciar um número de configurações adicionais, incluindo:
  - Aplicativos como o Microsoft Office
  - Drives mapeados
  - Configurações do registro

- Opções de energia
- Opções de pasta
- Opções regionais
- Opções do menu iniciar
- Arquivos e pastas
- Impressoras
- Tarefas agendadas
- Conexões de rede

- Você pode usar as preferências para desabilitar dispositivos de hardware ou classes de dispositivos.
- Por exemplo, você pode usar Preferências para impedir que discos rígidos USB, incluindo players de mídia pessoais, sejam conectados a computadores.
- Pode usar para mapear impressoras , e até configurar opções de energia dos computadores
- As preferências só funcionam em Windows vista SP1 ou superior para XP é necessário CSEs que podem ser baixadas nesse link - https://www.microsoft.com/en-us/download/details.aspx?id=23680
- Depois que você instalar no XP confirme a instalação verificando se o arquivo `Gpprefcl.dll` existe no seguinte caminho `c:\windows\system32`

Modelos administrativos

- São GPOs que manipula o registro de estação de trabalho e modificam basicamente as seguintes chaves no registro:
  - HKLM\Software\Policies (computer settings)
  - HKCU\Software\Policies (user settings)
  - HKLM\Software\Microsoft\Windows\CurrentVersion\Policies (computer settings)
  - HKCU\Software\Microsoft\Windows\CurrentVersion\Policies (user settings)

- Um modelo administrativo é um par de arquivos XML,
  - Extensão `.admx` que especifica as alterações a serem feitas no registro
  - Extensão `.adml` que fornece uma interface de usuário específica do idioma no GPME.
- Quando é necessário fazer alterações nas configurações gerenciadas pelo modelo administrativo, elas podem ser feitas no único arquivo ADMX.
- Qualquer administrador que modifique um GPO que use o modelo acessa o mesmo arquivo ADMX e chama o arquivo ADML apropriado para preencher a interface de usuário.
- Alguns fornecedores de software fornecem modelos administrativos como um mecanismo para gerenciar a configuração de sua aplicação centralmente.
- Por exemplo, você pode obter modelos administrativos para todas as versões recentes do Microsoft Office.

Repositório central

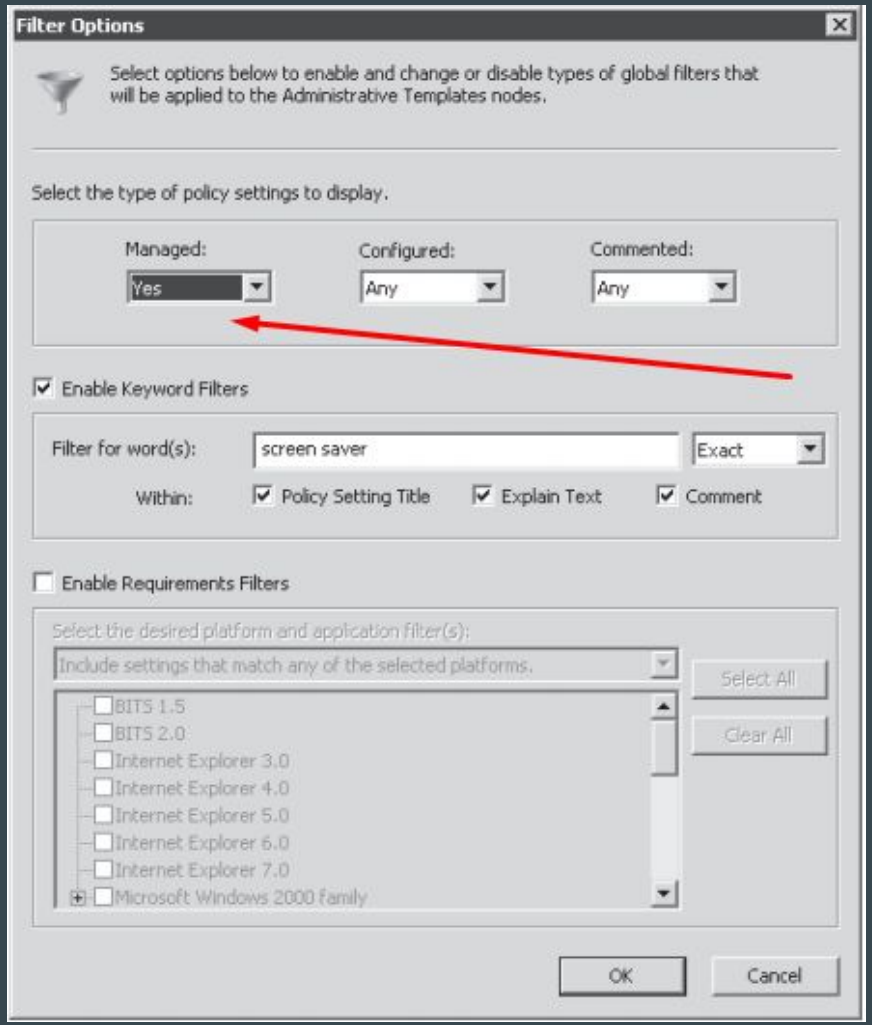
- Quando os arquivos ADMX / ADML são usados como modelos administrativos, o GPO contém apenas os dados que o cliente precisa para processar a Diretiva de Grupo
- Quando editamos o GPO, o GPME extrai os arquivos ADMX e ADML da estação de trabalho local
- Isso funciona bem para organizações menores e não empresas de medio e grande porte , para isso você tema o repositório central .
- O repositório central é uma única pasta no SYSVOL no DC que contém todos os arquivos ADMX e ADML necessários.
- O GPME então reconhece e carrega todos os modelos administrativos do repositório central em vez do computador local.

GPO de início

- É um template de GPO que podemos usar para criar GPO a partir dele.
- Assim você pode pré-criar várias configurações e em cada cliente usar esses GPO de início como um templete .
- Assim o trabalho será feito uma única vez.

Configurações de política gerenciadas e não gerenciadas

- Quando trabalhamos com modelos administrativos devemos entender o que são políticas gerenciadas e não gerenciadas .
- Normalmente quando configuramos uma política e depois removemos o objeto de GPO e ou mudamos a configuração de não configurada isso reflete imediatamente no estação de trabalho .
- Mas em alguns casos isso não acontece e acontece o que se chama de tatuagem de registro .
- Nesse caso deve-se configurar uma política contrária , não basta só remover ou desconfigurar .
- Por padrão o sistema oculta esse tipo de política que tatua o registro.


Filter Options
Select options below to enable and change or disable types of global filters that will be applied to the Administrative Templates nodes.
Select the type of policy settings to display.
Managed:
Yes
Configured:
Any
Commented:
Any
Enable Keyword Filters
Filter for word(s):
screen saver
Exact
Within:
Policy Setting Title
Explain Text
Comment
Enable Requirements Filters
Select the desired platform and application filter(s):
Include settings that match any of the selected platforms.
Select All
Clear All
BITS 1.5
BITS 2.0
Internet Explorer 3.0
Internet Explorer 4.0
Internet Explorer 5.0
Internet Explorer 6.0
Internet Explorer 7.0
Microsoft Windows 2000 family
OK
Cancel

FIM

...