**Políticas de Segurança no AD - Parte III**

**Gerenciando as Diretivas de Grupo:**  
  
As GPOs simplificam e aumentam a performance a administração ao oferecer aos administradores da rede um controle centralizado eficaz.  Nestas configurações, a centralização sobre privilégios, permissões e recursos de usuários e computadores, podemos:  
- Criar diretórios gerenciados de forma centralizada para pastas especiais.  
- Controlar o acesso a componentes Windows, a recursos de sistema, de rede, Painel de Controle, Área de Trabalho e Menu Iniciar.  
- Definir scripts de usuário e computador para executar funções específicas e em momentos específicos.

|  |
| --- |
|  |
| Imagem TechNet - Microsoft |

**Entendendo as GPOs!**  
  
É necessário o estudo da estrutura lógica do AD. De acordo com Stanek, no livro Guia de Bolso do Administrador - Windows Server 2003, se refere ao Active Directory, como:  
Os agrupamentos lógicos do domínio são chamados de sites e os subgrupos dentro de um domínio são chamados de Unidades Organizacionais.  
  
As configurações das GPOs são armazenadas em um container para diretivas. É possível criar várias GPOs e em 2 divisões:  
- Computador  
- Usuário  
  
**Quando as Diretivas de Grupo são aplicadas?**  
  
**As que são aplicadas aos Computadores**  
**As que são aplicadas aos Usuários**  
  
As GPOs de computadores são aplicadas durante a inicialização do sistema, as diretivas de usuário normalmente são aplicadas durante o logon. A sequência de eventos exata é muito importante na solução de problemas de comportamento do sistema e da própria rede.  
  
**Quais os eventos que ocorrem durante a inicialização e o logon?**  
- A rede começa a funcionar, o Windows Server aplica as diretivas de computador. Por padrão, é carregada e aplicada uma de cada vez. Nenhuma interface de user é exibida enquanto as GPOs de computador estão sendo processadas.  
- O Server executa scripts de inicialização. Não é exibida ao user  
- Quando o user pressiona CTRL ALT DEL, o server, com seus componentes específicos carrega o perfil do user. Após ele ser autenticado.  
- O Server aplica diretivas de usuário. Uma de cada vez. A interface do user, que pertence ao seu perfil, é exibida a ele.  
- O Server então, executa os scripts de logon. São executados simultaneamente. **Todos os scripts de logon estão no compartilhamento NetLogon.**  
  
Por padrão, as GPOs do usuário são atualizadas no momento do logon, ou quando o protocolo**Kerberos revalida os tickets de serviço**. Nestes momentos, podemos sugerir ao usuário refazer o seu logon para que as diretivas sejam aplicadas. **Por outro lado, também podemos utilizar o comando gpupdate/logoff para desconectar o usuário logado.**  
Para as configurações do computador, **podemos usar o comando gpupdate/boot - reinicia o computador após a atualização.**  
 **Criando as Configurações e trabalhando heranças**  
Para criarmos uma estrutura de GPOs de grupos, é necessário fazermos a nossa estrutura lógica do AD para conter nossos objetos de Domínio.

|  |
| --- |
|  |
| Usuários e Computadores do AD |

Esta estrutura lógica será replicada no console Gerenciamento de Política de Grupo.

|  |
| --- |
|  |
| Console Gerenciamento de Política de Grupo |

Para criarmos uma nova GPO associada à UO, basta clicarmos com o botão direito sobre o objeto (como na imagem acima) e selecionarmos Criar um GPO neste domínio e fornecer um link aqui.  
  
Sempre podemos configurar as GPOs para o computador e para o usuário (como mencionado acima), lembrando que para o computador, encontramos as GPOS que são carregadas enquanto o sistema inicia ou reinicia. É bom salientar que neste nível configuramos as diretivas de contas, senhas, kerberos, auditorias, opções de segurança. São diretivas mais "gerais" porque aplicam no objeto acima do user.  
  
As diretivas de grupo aplicadas no nível do usuário são mais avançadas e profundas. Detalhadas necessitam de um projeto especificado e analisado de forma correta.  
  
Na imagem abaixo, vemos a configuração de recipientes, os quais, o administrador de domínio pode configurar de acordo com as políticas de segurança exigidas.

|  |
| --- |
|  |
| Detalhe das pastas que o Administrador acessa nas GPOs de grupo |

**Entendendo as GPOs de Grupo e o console:**  
  
**- Configuração do Computador:** permite a configuração de diretivas que devem ser aplicadas a computadores, independente de quem se conecte.  
  
**- Configuração do usuário:** permite a configuração de diretivas que devem ser aplicadas a usuários.  
  
**- Configuração de Software:** define diretivas para configurações e instalação dos softwares da rede. Podemos adicioná-los aqui.  
  
**- Configurações do Windows:** configura diretivas para redirecionamento de pastas, scrips, segurança e processos do sistema.  
  
**- Modelos Administrativos:** configura diretivas para o sistema operacional, componentes do windows e programas. Os Modelos Administrativos são configurados por meio de templates, os quais podemos adicionar ou remover módulos de GPO sempre que necessitarmos. Estas GPOs são mais detalhadas e profundas, mas mesmo assim, proporcionam fácil acesso às configurações de diretivas baseadas em registro.

|  |
| --- |
|  |
| Console das GPOs Modelos Administrativos - No caso, Área de Trabalho |

As GPOs de grupos, na parte das configurações do usuário são armazenadas em um arquivos.adm. Esses arquivos são formatados com texto ASCII, e podemos editar usando modo gráfico. Todas as alterações destas diretivas são armazenadas no Registro do sistema servidor por arquivos **registry.pol** e usados por:  
**HKEY\_LOCALMACHINE (HKLM) e HKEY\_CURRENT\_USER (HKCU)**.  
  
 **As configurações padrões das diretivas podem ser:**  
 **- Não-Configurado:** a diretiva não é usada e nenhuma configuração foi salva no registro.  
**- Ativado**: a diretiva está sendo ativamente imposta aos objetos de domínio e replicada em usa hierarquia.  
**- Desativado:** a diretiva está apenas desligada e sua configuração não é imposta, porém foi salva no registro.  
  
**Reforçando que: estamos falando de diretivas de usuário, porém as diretivas do computador têm precedência no Windows Server 2012 (e anteriores). Portanto, se houver um conflito entre uma configuração de diretiva de computador e uma diretiva de usuário, sempre a diretiva do computador será imposta, ou seja, possui precedência.**  
  
  
 **Algumas diretivas importantes dos Modelos Administrativos/Usuários:**

|  |
| --- |
|  |
| Componentes do Windows |

|  |
| --- |
|  |
| Menu Iniciar e Barra de Tarefas |

|  |
| --- |
|  |
| Painel de Controle |

|  |
| --- |
|  |
| Rede |

|  |
| --- |
|  |
| Uma das mais importantes: Sistema |