

Microsoft Desktop Optimization Pack - MDOP

Advanced Group Policy Management - AGPM

Advanced Group Policy Management (AGPM) 2.5

Última revisão feita em 02 de Setembro de 2008.

Objetivo

Neste artigo iremos conhecer um dos cinco componentes do MDOP 2008. Você vai aprender sobre o Advanced Group Policy Management (AGPM), boa leitura.

Introdução

O AGPM é uma solução que incrementa a aplicação Group Policy Management Console (GPMC) adicionando a possibilidade de trabalhar com delegação de permissões, de fazer alterações em GPOs em modo offline, de controlar as versões destas GPOs e muito mais, a versão que acompanha o MDOP 2008 é o AGPM 2.5. O MDOP é um pacote de ferramentas destinado a melhorar o gerenciamento de sistemas operacionais e aplicações em ambiente Windows, esta suíte é formada por cinco produtos, entre eles o Advanced Group Policy Management (AGPM) que conheceremos neste artigo. Para mais informações sobre o MDOP leia o artigo MDOP Visão geral da suíte de produtos.

Características

Ao implementar o AGPM (instalar o AGPM Server e o AGPM Client) no ambiente podemos trabalhar com o que é chamado de GPO Controlada. Uma GPO Controlada é uma GPO criada através do AGPM e que se beneficia do seu controle de versão. O AGPM utiliza a interface do GPMC, ao ser instalado um novo nó será adicionado na console do GPMC, este nó se chama Change Control e será através dele que todas as novas características oferecidas pelo AGPM poderão ser utilizadas e configuradas. Entre estas características estão:

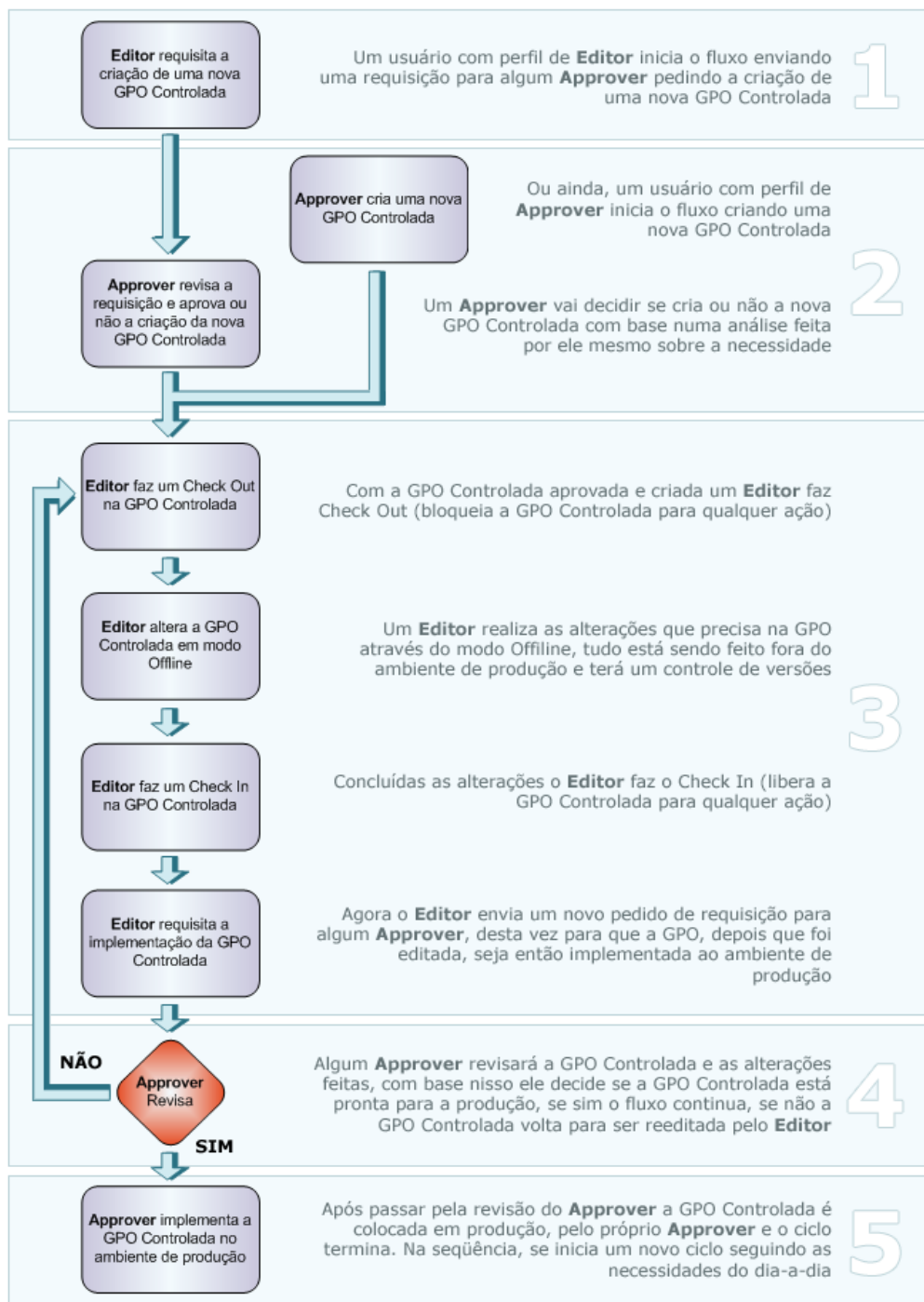
Delegação de Permissões	Possibilita compartilhar a tarefa de criar, editar e aprovar GPOs Controladas.
Modo Offline	Possibilita criar e testar GPOs antes de implementar no ambiente de produção, onde cada GPO é copiada e armazenada em um arquivo central.
Controle de Versões	Possibilita manter um arquivo central com diversas versões de cada GPO, podendo fazer Rollback de versões, análise de alterações nas GPOs, comparação entre versões e criação de novas GPOs com base em templates definidos.
Check-in/Check-out	Possibilita evitar sobrescrever GPOs que estão sendo editadas por outro usuário.

Para que todas estas características sejam realizadas de forma organizada existe a tal delegação de permissões, funcionalidade que permite segmentar as tarefas realizadas através do AGPM. Para cada tarefa existe um papel, estes papéis são integrados a usuários ou grupos do Active Directory. Acompanhe abaixo os quatro papéis oferecidos pela delegação de permissões no AGPM:

Reviewer	O papel mais simples entre os quatro possíveis, usuários com este perfil terão acesso apenas em modo de leitura para revisar e auditar as GPOs, realizando comparações simples entre elas. Por este ser um papel de pouca permissão todos os outros papéis incluem as permissões de um Reviewer.
Editor	Este é o papel de quem vai fazer edições nas GPOs já criadas, estas edições incluem desde renomear e importar GPOs até criar templates. Quando um Editor precisa criar uma nova GPO ou

	implementar uma GPO alterada no ambiente de produção ele deverá requisitar para que um Approver realize estas ações, esta requisição é feita por e-mail, você verá como, ainda neste artigo.
Approver	O Approver recebe requisições de um Editor para criar, implementar ou deletar uma GPO, porém estas ações podem ser executadas pelo Approver sem mesmo haver uma requisição de um Editor.
Administrator	É o papel com mais permissões, também chamado de Administrator (Full Control) ele inclui todas as permissões dos outros papéis.

Acompanhe abaixo um exemplo de atividades envolvendo os principais papéis do AGPM, eu usei como base um fluxo feito pela própria Microsoft.



Obs.: Para que um usuário tenha acesso somente leitura as GPOs Controladas ele deve ser um Reviewer, este tipo de acesso geralmente é concedido aos usuários que terão a tarefa de simplesmente auditar o que foi realizado pelos outros usuários administradores do AGPM.

Obs.: É necessário que o usuário ou grupo utilizado como Approver tenha uma conta de e-mail configurada, pois será para esta conta que a requisição feita pelo Editor vai ser enviada.

Componentes

Um ambiente com o AGPM instalado é formado por no mínimo dois componentes principais, o primeiro é o AGPM Server, componente que deve ser instalado em um Domain Controller ou um Member Server, durante a instalação do AGPM Server é que será definido o local do Archive (Repositório com as GPOs Controladas). O segundo componente é o AGPM Client, este será necessário instalar para que se tenha acesso às novas funcionalidades do AGPM através do GPMC, ele não necessariamente deve ser instalado junto com o AGPM Server, porém se você quiser instalar os dois componentes juntos não há problemas. Como percebido o GPMC é um pré-requisito para a instalação do AGPM Server e Client.

Obs.: É importante saber que ao instalar um AGPM Client ele deverá apontar sempre para o mesmo servidor que mantém o Archive, pois este arquivo é centralizado, logo isso pode e deve ser feito através de um template administrativo, esta configuração você confere logo mais neste artigo.

Requisitos

Antes de começarmos a instalação de qualquer componente do AGPM vamos observar alguns requisitos, para que ficasse mais intuitivo eu separei cada um deles em três categorias:

Requisitos Gerais

Quatro contas devem ser criadas, uma para cada papel: Administrator (Full Control), Approver, Editor e Reviewer. Lembrando que as contas para os papéis Administrator e Approver devem ter e-mails habilitados. Durante a instalação do AGPM Server você será perguntado pela conta de serviço a ser utilizada pela aplicação, neste caso você pode usar a mesma conta do papel Administrator (Full Control) ou seguir as políticas da sua organização.

Obs.: A prática de usar um usuário para cada papel é sugestão da Microsoft, porém você pode utilizar grupos de usuários quando a quantidade de profissionais envolvidos com as tarefas for muito grande. Logo cabe a você planejar o que melhor atende a sua necessidade.

Requisitos para o AGPM Server 2.5

Este componente pode ser instalado tanto em Windows Vista (32bit) quanto Windows 2003 (32bit), porém como a instalação é recomendada que seja feita em um Domain Controller ou Member Server você acabará instalando em um Windows 2003. O Windows 2003 deverá ter instalado o GPMC 2.0 (embora o AGPM funcione com versões anteriores do GPMC 2.0, como a 1.1, algumas políticas e configurações não ficarão disponíveis). Toda a instalação deve ser feita com um usuário membro do grupo Domain Administrators.

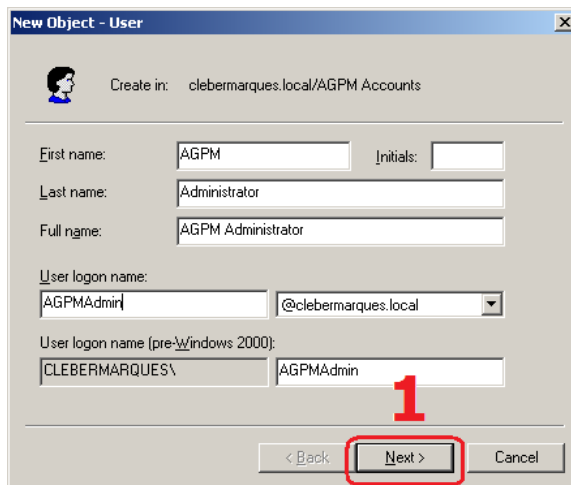
Requisitos para o AGPM Client 2.5

Este componente pode ser instalado tanto em Windows Vista (32bit) quanto Windows 2003 (32bit). O Windows deverá ter instalado o GPMC 2.0 (embora o AGPM funcione com versões anteriores do GPMC 2.0, como a 1.1, algumas políticas e configurações não ficarão disponíveis). Não tem problemas se você quiser instalar o cliente junto com o servidor, ou seja, os dois componentes podem ser instalados juntos.

Obs.: O AGPM não é suportado por sistemas x64, mesmo porque ele é dependente do GPMC e este não pode ser instalado em sistemas x64.

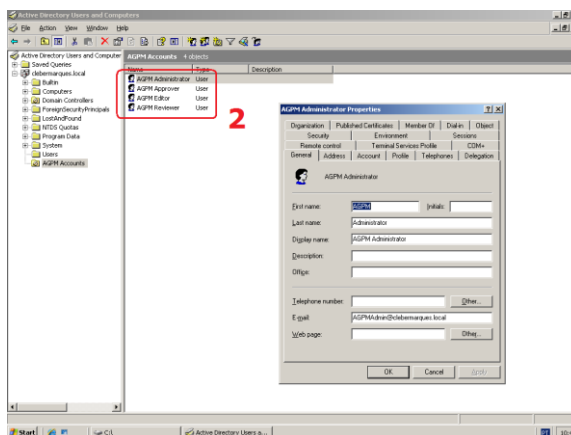
Criar contas administrativas

Como já vimos antes, para trabalhar com o AGPM será necessário delegar permissões e isso será feito para alguns usuários ou grupos de usuários. Seguindo a recomendação da Microsoft vamos criar um usuário para cada papel oferecido pelo AGPM, confira:



Passo 01 – Acesse o Active Directory.

01. Acesse o **Active Directory Users and Computers** através do **Administrative Tools**, crie os usuários no local que você achar necessário, seguindo a política da sua empresa.



Passo 02 – Crie quatro usuários.

02. É importante lembrar que seguindo a recomendação da Microsoft geralmente são criados **4 usuários**:

- AGPM Administrator
- AGPM Approver
- AGPM Editor
- AGPM Reviewer

Obs.: Para trabalhar com notificações por emails recomenda-se que os usuários Administrator e Approver tenham **e-mails habilitados**.

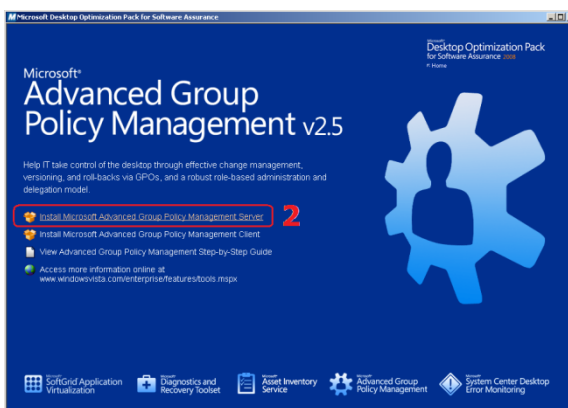
Instalar o AGPM Server

Hora de instalar o primeiro componente, o AGPM Server, lembrando que para iniciar a instalação devemos estar logados com um usuário que faça parte do grupo Domain Admins. O processo de instalação é simples, será feito através da mídia de instalação do MDOP 2008, vale atentar que o servidor escolhido para instalação do AGPM Server deve ter o GPMC já instalado, acompanhe:



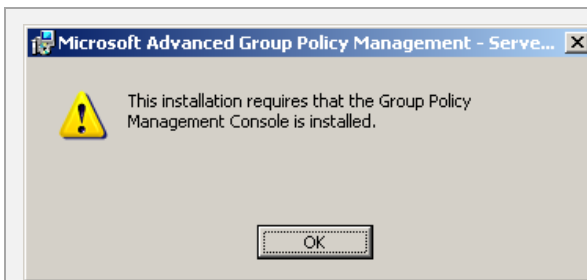
Passo 01 – Acesse o MDOP 2008.

01. Acesse a mídia de instalação dos componentes do **MDOP 2008**, clique na opção **Advanced Group Policy Management v2.5**.



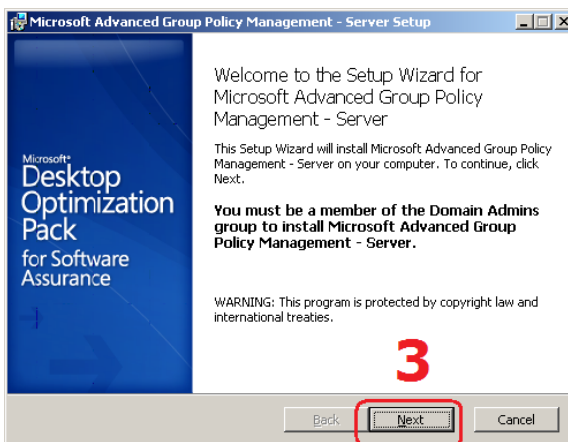
Passo 02 – Selecione a opção AGPM 2.5.

02. Agora clique na opção **Install Microsoft Advanced Group Policy Management Server**.



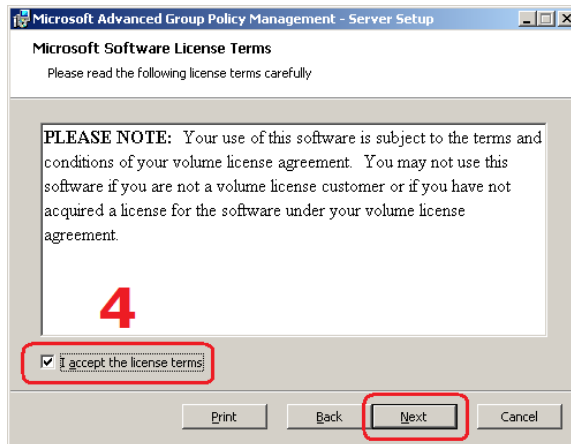
Um ponto importante que deve ser considerado antes de realizar a instalação do AGPM é a existência do **GPMC 2.0**. Este componente é um pré-requisito para a instalação do AGPM Server e Client, pois serve de interface para eles.

Embora o AGMP funcione com versões anteriores do GPMC 2.0, como a 1.1, algumas políticas e configurações não ficarão disponíveis



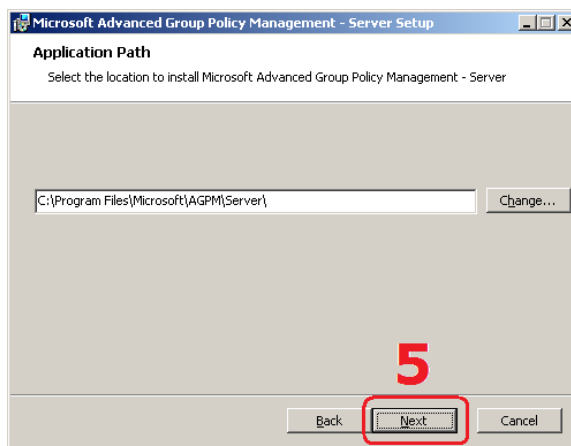
Passo 03 – Tela de boas vindas.

03. Na tela de boas vindas apenas clique no botão **Next** para continuar com a instalação.



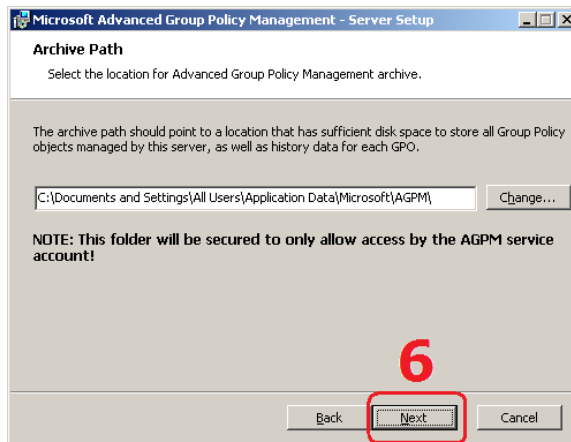
Passo 04 – Termo de uso.

04. Estes são os termos de uso, leia com atenção e marque a caixa **I Accept**. Clique em **Next**.



Passo 05 – Diretório de instalação.

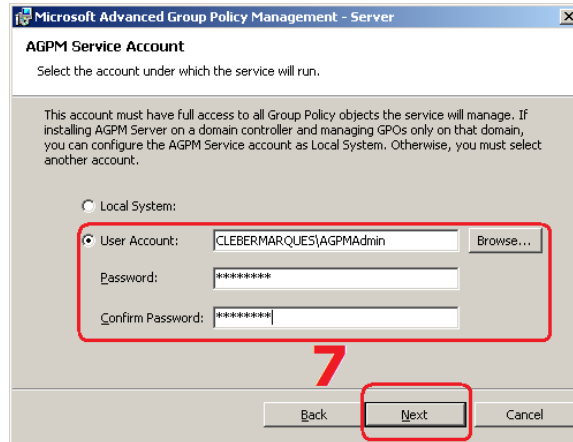
05. Nesta tela você pode definir o **local de instalação** para o AGPM Server, não há necessidade de alterar o padrão, apenas clique no botão **Next** para continuar.



Passo 06 – Diretório do Arquivo.

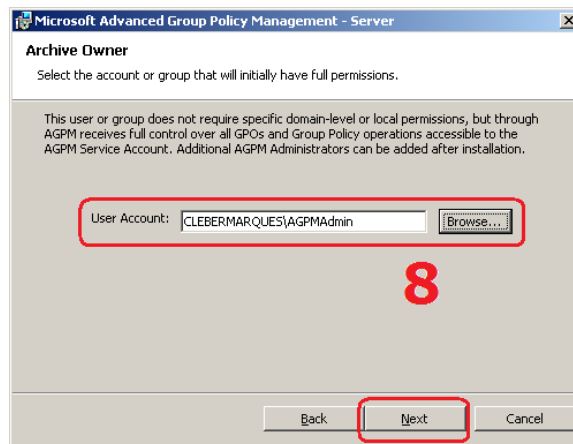
06. Uma parte muito importante da instalação, é hora de definir qual será o local que armazenará o **Archive**, arquivo centralizado que contém os dados das GPOs Controladas. Clique **Next**.

Obs.: Embora seja prático armazenar o Archive no mesmo servidor de instalação podemos instalar também em outro servidor ou diretório.



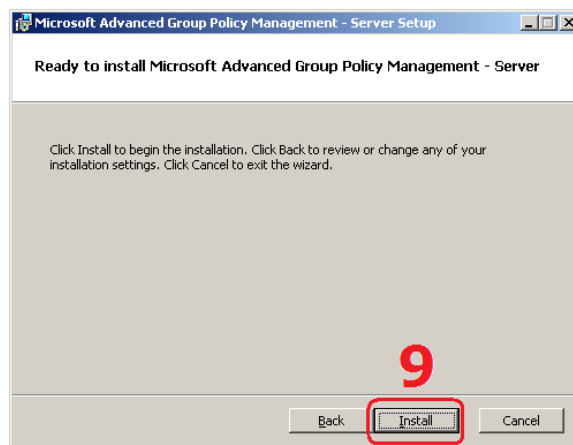
Passo 07 – Conta de serviço.

07. Aqui você terá que definir a conta utilizada como **Service Account** para o AGPM, siga a política de contas da sua empresa, ou se for o caso, use a mesma conta que você criou para ser o **AGPM Administrator**. Clique em **Next** para continuar.



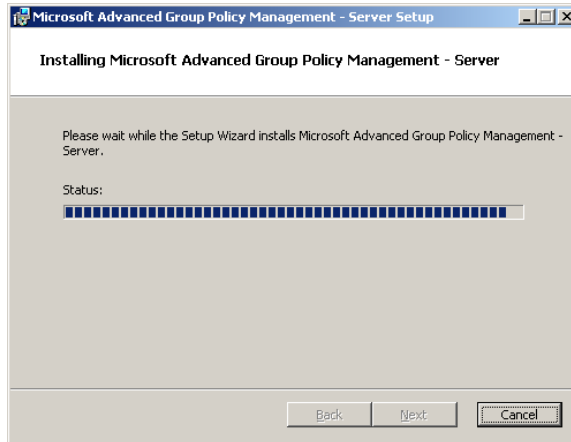
Passo 08 – Conta de AGPM Administrator.

08. Hora de definir a conta que será o **AGPM Administrator**, que você deve ter criado lá no primeiro passo. Apenas busque a conta clicando em **Browse** e clique **Next** para continuar.



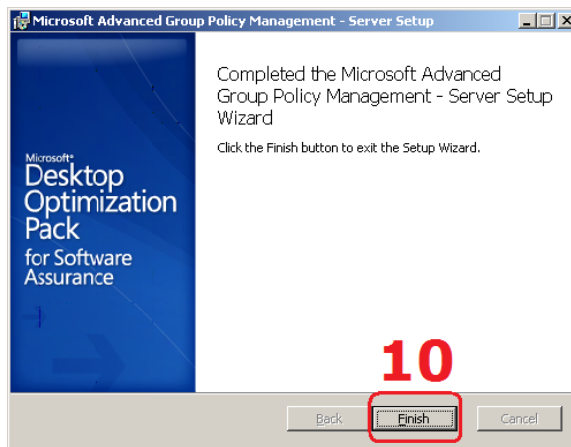
Passo 09 – Pronto para instalar.

09. Se estiver pronto para começar a instalação clique no botão **Install** ou utilize a opção **Back** para voltar e fazer alguma alteração.



Processo de instalação.

Aguarde alguns instantes até que a instalação seja concluída.



Passo 10 – Instalação concluída com sucesso.

10. E pronto, o **AGPM Server** foi instalado com sucesso, clique no botão **Finish** para fechar o assistente.

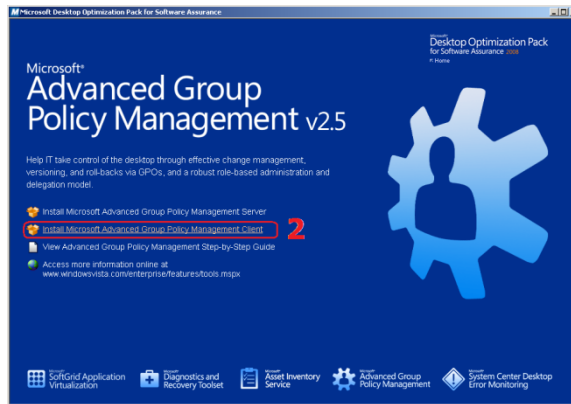
Instalar o AGPM Client

Após a instalação do AGPM Server é necessário instalar também o AGPM Cliente que vai possibilitar o acesso das novas funcionalidades via GPMC. Para isso o processo vai ser bem semelhante ao anterior, veja:



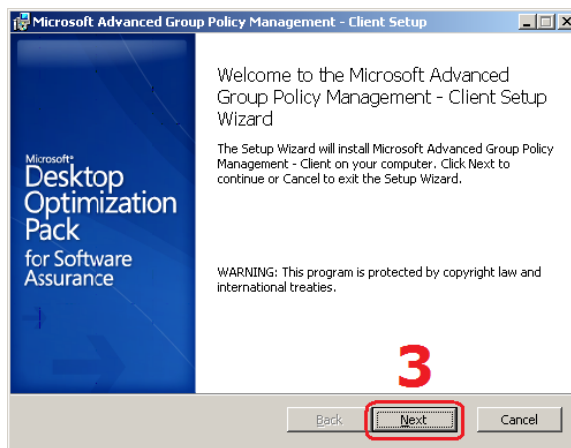
Passo 01 – Acesse o MDOP 2008.

01. Acesse a mídia de instalação dos componentes do **MDOP 2008**, clique na opção **Advanced Group Policy Management v2.5**.



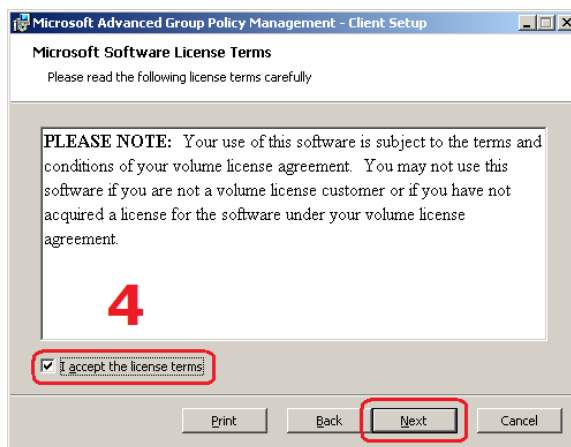
Passo 02 – Selecione a opção AGPM 2.5.

02. Agora clique na opção **Install Microsoft Advanced Group Policy Management Client**.



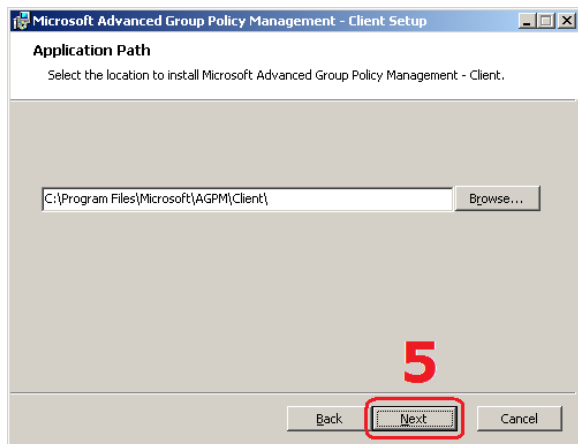
Passo 03 – Tela de boas vindas.

03. Na tela de boas vindas apenas clique no botão **Next** para continuar com a instalação.



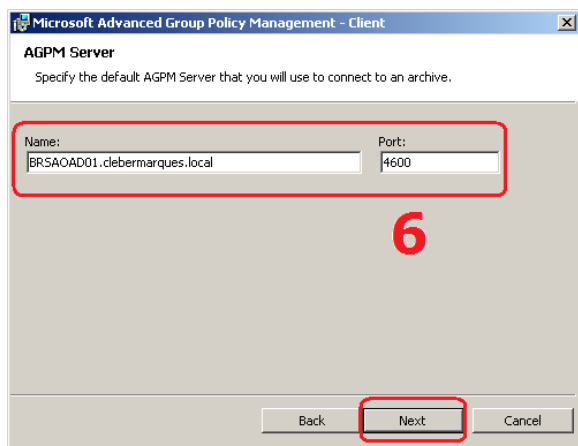
Passo 04 – Termo de uso.

04. Estes são os termos de uso, leia com atenção e marque a caixa **I Accept**. Clique em **Next**.



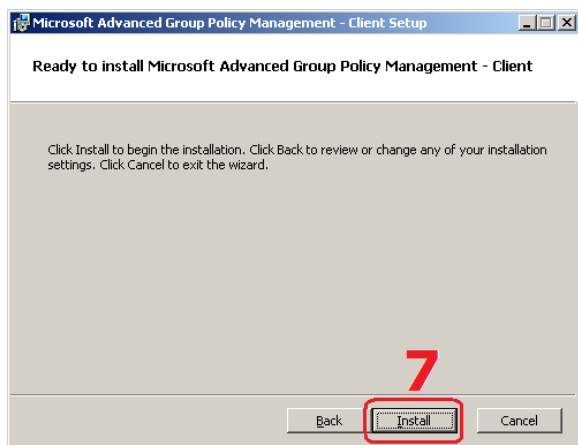
Passo 05 – Diretório de instalação.

05. Nesta tela você pode definir o **local de instalação** para o AGPM Client, não há necessidade de alterar o padrão, apenas clique no botão **Next** para continuar.



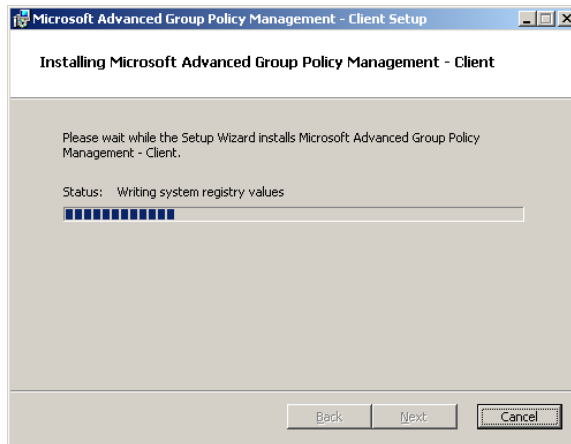
Passo 06 – Endereço do AGPM Server.

06. Digite o **endereço FQDN** do servidor AGPM padrão para o qual o cliente vai apontar, a porta já vem preenchida, clique em **Next** para continuar.



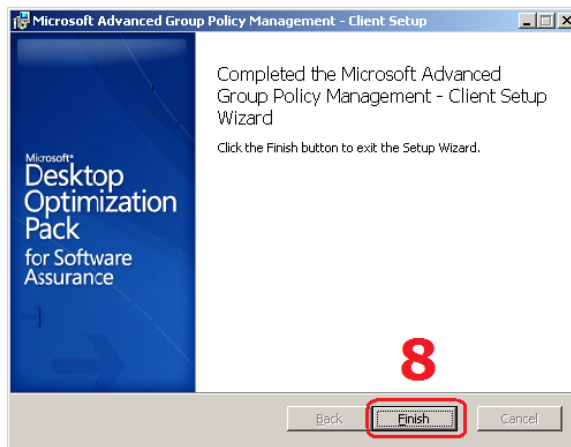
Passo 07 – Pronto para instalar.

07. Se estiver pronto para começar a instalação clique no botão **Install** ou utilize a opção **Back** para voltar e fazer alguma alteração.



Processo de instalação.

Aguarde alguns instantes até que a instalação seja concluída.



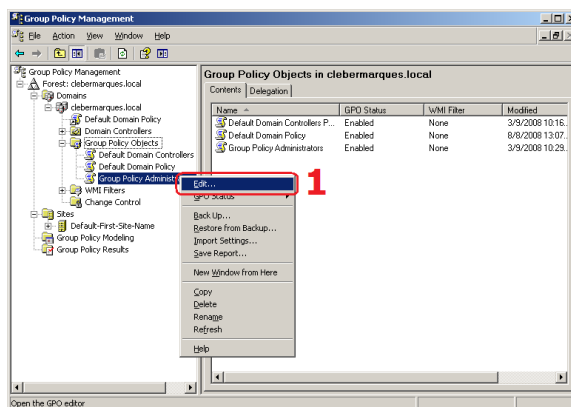
Passo 08 – Instalação concluída com sucesso.

08. E pronto, o **AGPM Client** foi instalado com sucesso, clique no botão **Finish** para fechar o assistente.

Se você acessar o **Group Policy Management** através do **Administrative Tools** verá que o nó **Change Control** foi criado.

Configurar a conexão com o Servidor

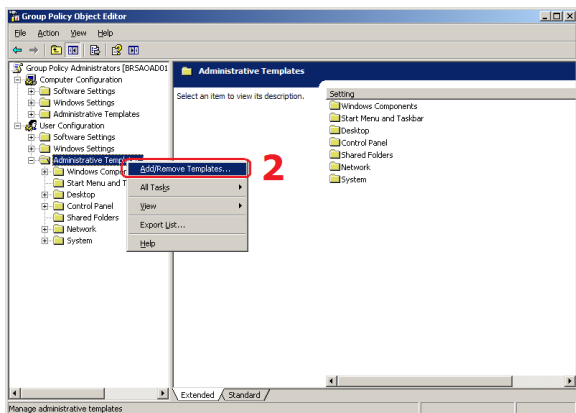
Quando um cliente do AGPM se conecta a um Server ele deve saber onde se encontra o Archive, pois será com base neste local que o cliente vai carregar as GPOs Controladas, sendo assim através de uma configuração no template administrativo fornecido com a solução nós iremos definir um servidor padrão que mantém o Archive, acompanhe:



Passo 01 – Console do AGPM (GPMC).

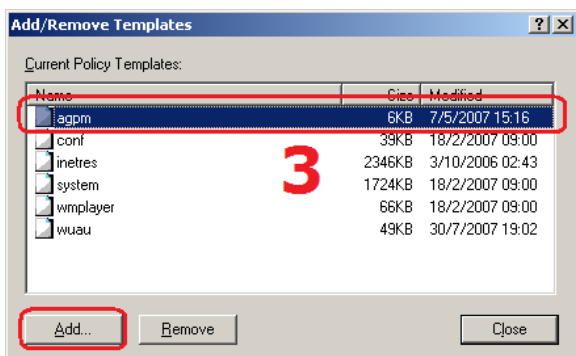
01. Acesse o **Group Policy Management** através do **Administrative Tools**, em **Group Policy Objects** clique com o botão direito no nome de uma política que se aplique a todas as contas utilizadas como os administradores do AGPM e escolha a opção **Edit**.

Obs.: No meu caso eu **criei uma OU** e coloquei os usuários criados para administrar o AGPM dentro dela, e então eu criei uma GPO e apliquei nessa OU.



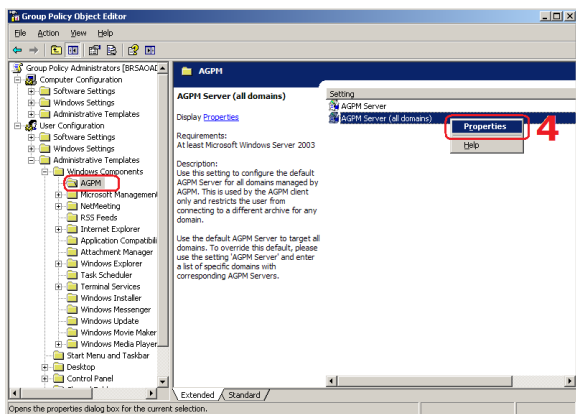
Passo 02 – Templates administrativos.

02. A janela do **Group Policy Object Editor** vai se abrir, abaixo de **User Configuration** clique com o botão direito em **Administrative Templates** e clique em **Add/Remove Templates**.



Passo 03 – Selecione o template.

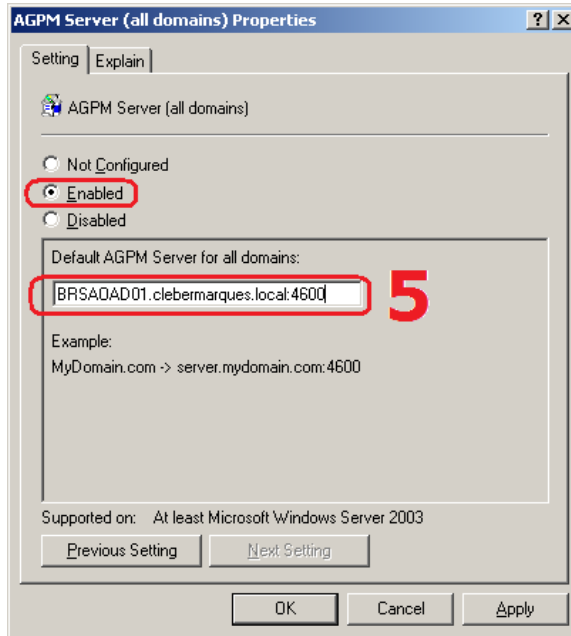
03. Na janela que aparecer clique no botão **Add** e procure pelo template **AGPM.adm** ou **AGPM.admx**, clique no botão **Open**. De volta a janela apenas clique no botão **Close**.



Passo 04 – Acesse as propriedades.

04. Agora é só expandir a árvore de opções **Windows Componentes** dentro de **Administrative Templates** que você terá acesso a uma nova opção chamada **AGPM**.

Clique na opção AGPM e na tela do lado direito acesse as propriedades de **AGPM Server (All Domains)**.



Passo 05 – Propriedades da política.

05. Marque a opção **Enable** e no campo em branco digite o nome do servidor AGMP seguido da porta de conexão. No meu caso ficou:

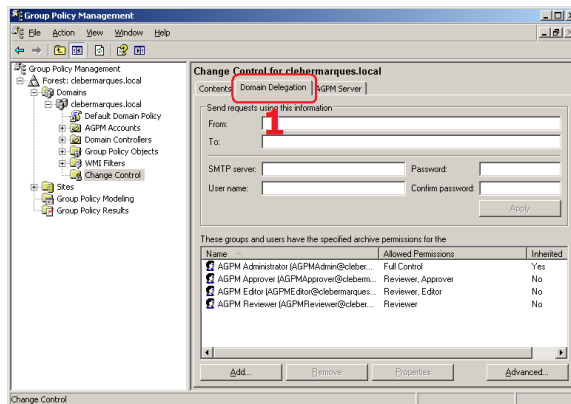
BRSAD01.clebermarques.local:4600

Com esta configuração você está definindo a conexão de todos os AGPM Clients para um único AGPM Server e seu **Archive**.

Clique no botão **Apply** e **OK**.

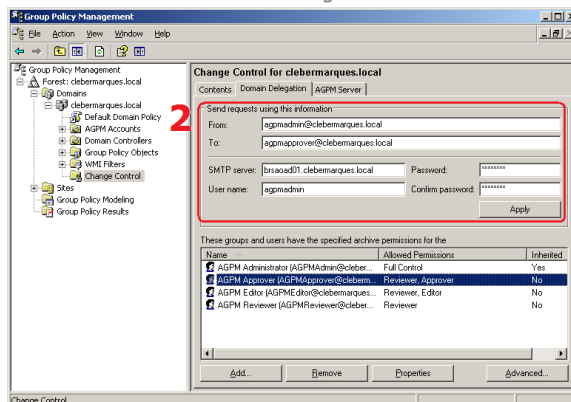
Configurar a notificações por E-mail

Sempre que um Editor precisar que uma nova GPO Controlada seja criada, removida ou implementada no ambiente de produção um e-mail deve ser enviado ao Approver para tal, logo o envio deste email depende de uma configuração prévia, acompanhe como fazer isso:



Passo 01 – Guia Domain Delegation.

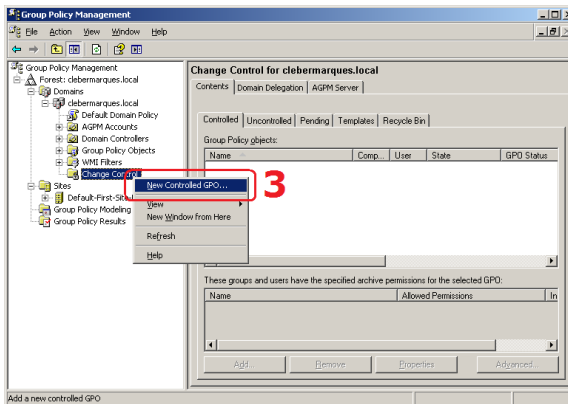
01. Acesse o **Group Policy Management** através do **Administrative Tools**. Na console clique na opção **Change Control** e selecione a guia **Domain Delegation**.



Passo 02 – Informações do e-mail.

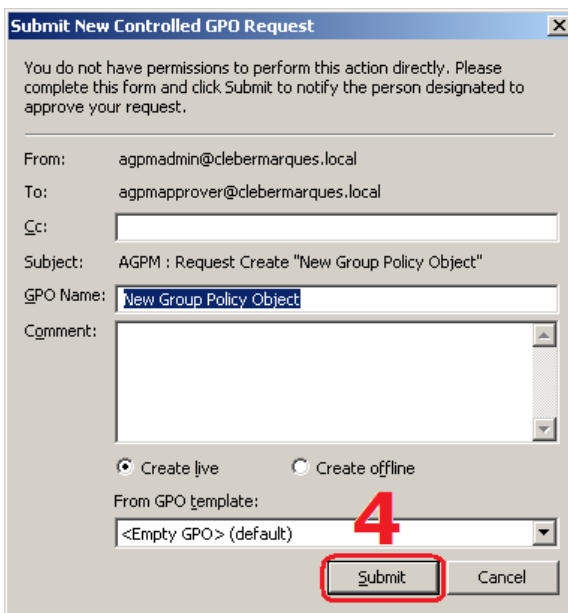
02. Nesta janela será necessário preencher todos os campos relacionados com o **envio de notificações** por e-mail. Preencha o campo **From** com o endereço de e-mail do AGPM Administrator, o campo **To** deve conter o e-mail do Approver, no campo **SMTP Server** digite o nome FQDN do seu servidor de e-mails bem como o nome do usuário e a senha (nos dois campos).

Clique em seguida no botão **Apply**.



Passo 03 – Pedido de requisição.

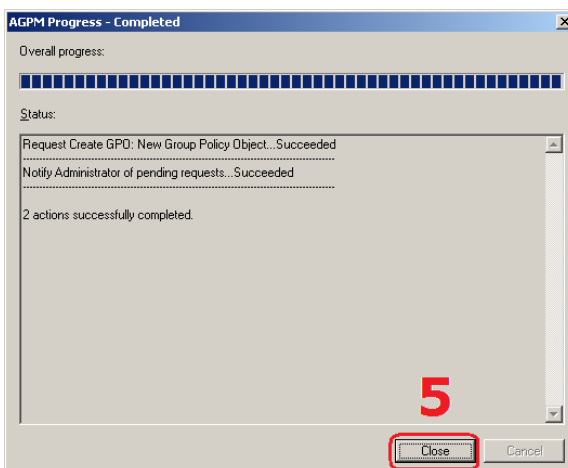
03. Simulando uma necessidade onde um usuário com o papel de Editor deve pedir por e-mail a criação de uma GPO Controlada para um Approver, acesse a console com um usuário **Editor**, clique com o botão direito na opção **Change Control** e selecione a opção **New Controlled GPO**.



Passo 04 – Dados da requisição.

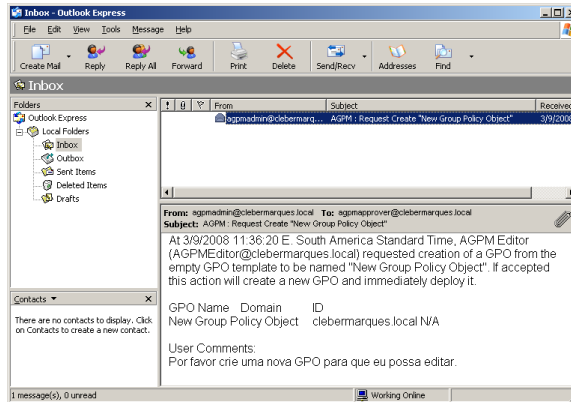
04. Desta forma você tem a possibilidade de **enviar um e-mail**, com todas as informações necessárias, para um usuário com o perfil de Approver criar, apagar ou implementar uma nova GPO Controlada.

Quando for este o caso preencha o que precisar e clique no botão **Submit**.



Passo 05 – Enviando o e-mail.

05. Você verá uma tela com o **status** do envio deste e-mail para o Approver, no final clique em **Close** para fechar a janela.

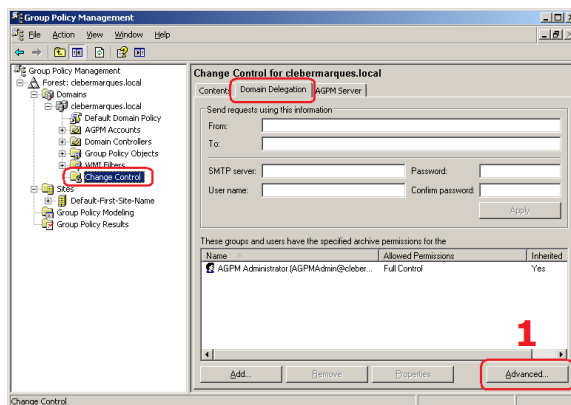


Passo 06 – E-mail recebido pelo Approver.

06. Certamente o Approver receberá em sua caixa de e-mail a **requisição** feita pelo Editor.

Delegar Permissões

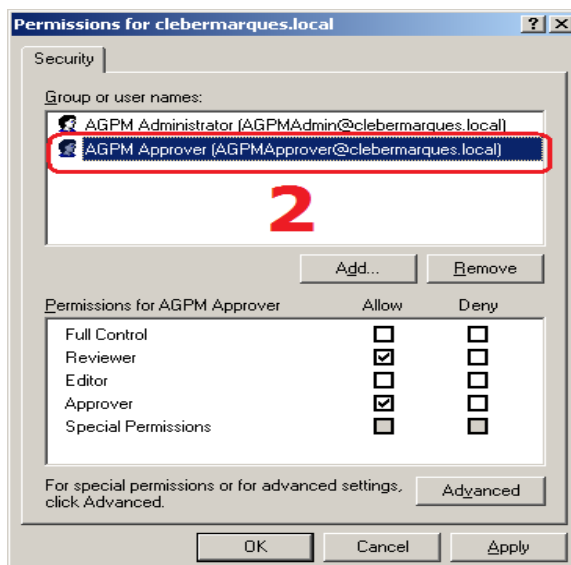
Como também já vimos neste artigo, todas as ações realizadas através da console do AGPM integrada ao GPMC deverão ser feitas por algum usuário ou grupo que faz parte de determinado papel, veja a seguir como delegar aos usuários as permissões de cada um destes papéis oferecidos pelo AGPM.



Passo 01 – Guia Domain Delegation.

01. Acesse o **Group Policy Management** através do **Administrative Tools**. Na console clique na opção **Change Control** e selecione a guia **Domain Delegation**.

Em seguida Clique no botão **Advanced**.



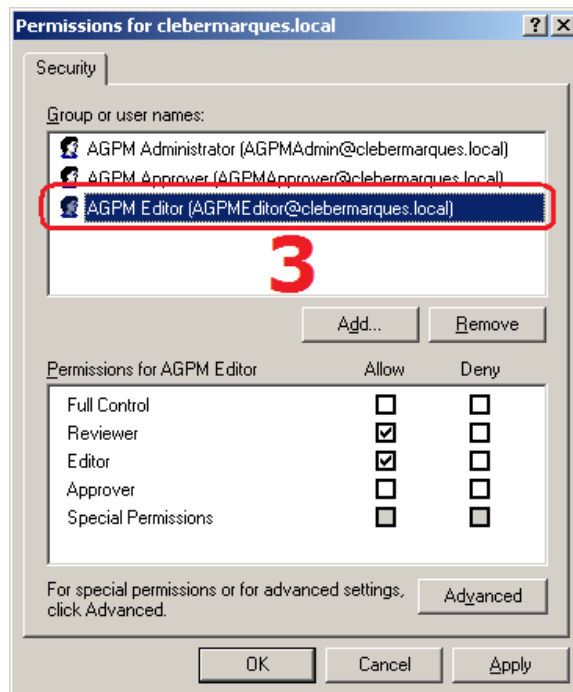
Passo 02 – Adicione o usuário Approver.

02. Na janela de permissões será necessário adicionar os usuários criados como Administradores do AGPM.

Clique no botão **Add** e adicione a conta de usuário que terá o papel de **Approver**. Deixe marcadas como **Allow** as permissões:

- Reviewer
- Approver

Obs.: Deixe marcada a opção **Reviewer** porque todos os papéis devem conter este papel.

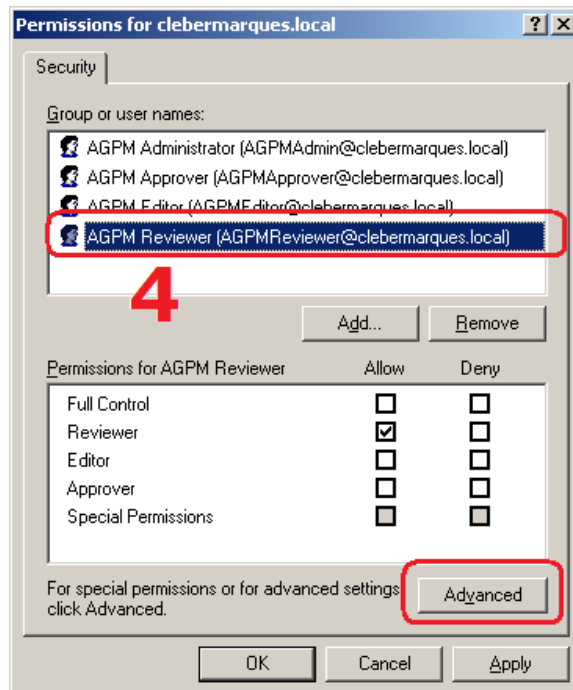


Passo 03 – Adicione o usuário Editor.

03. Clique no botão **Add** e adicione a conta de usuário que terá o papel de **Editor**. Deixe marcadas como **Allow** as permissões:

- Reviewer
- Editor

Obs.: Deixe marcada a opção **Reviewer** porque todos os papéis devem conter este papel.

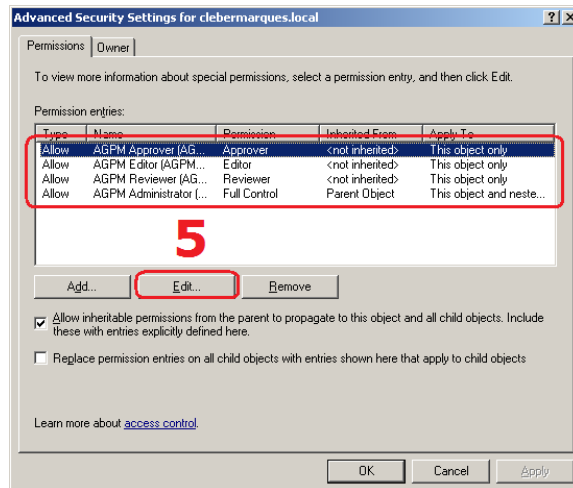


Passo 04 – Adicione o usuário Reviewer.

04. Clique no botão **Add** e adicione a conta de usuário que terá o papel de **Reviewer**. Deixe marcada como **Allow** a permissão:

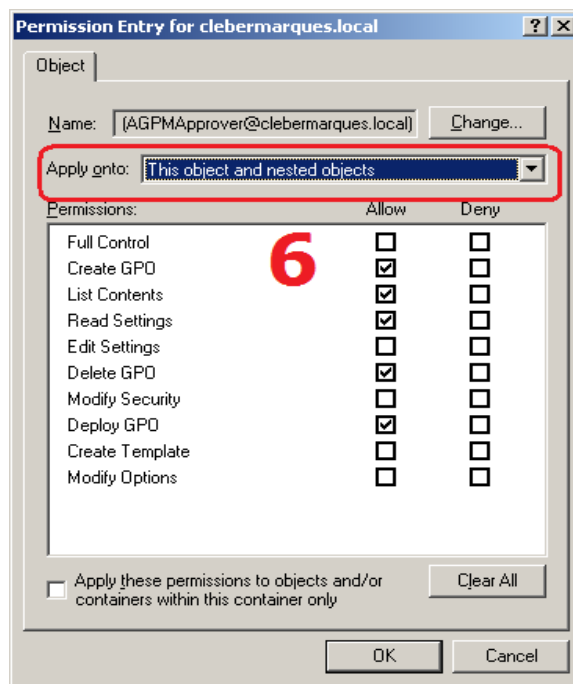
- Reviewer

Em seguida clique no botão **Advanced**.



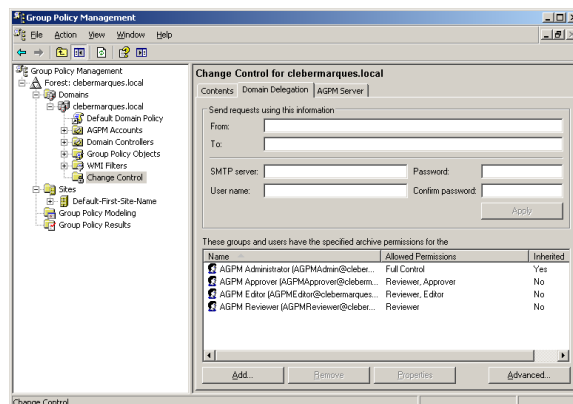
Passo 05 – Configurações avançadas.

05. Na janela de configurações avançadas de segurança selecione um usuário e clique no botão **Edit**.



Passo 06 – Permissões em todos objetos.

06. Na janela que abrir, no campo Apply Onto, selecione a opção **This object and nested objects**. Repita este passo para todos os usuários.

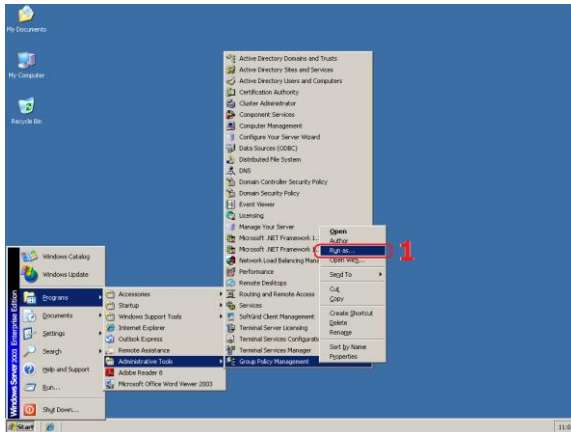


Passo 07 – Delegação concluída.

07. Por fim você delegou opções para cada tipo de papel permitido pelo AGPM.

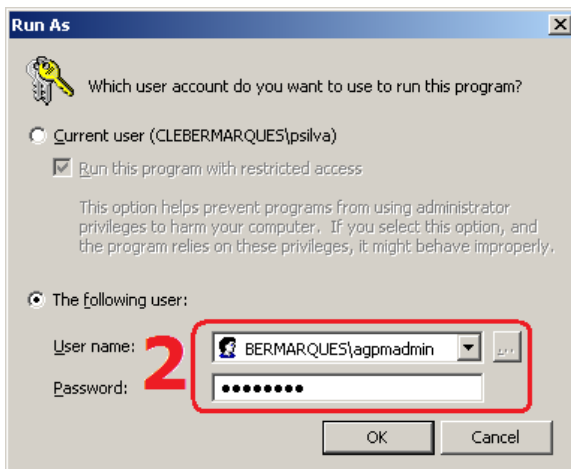
Acessando o AGPM utilizando Run As

Quando for necessário acessar a console do AGPM com permissões de outro usuário que não o logado atualmente nós podemos utilizar a facilidade do Run As, acompanhe a seguir:



Passo 01 – Opção Run As na GPMC.

01. Acesse o **Group Policy Management** através do **Administrative Tools**, clique com o botão direito e selecione a opção **Run As**.



Passo 02 – Acesse com outro usuário.

02. Marque a opção **The Following user** e digite um **usuário** e **senha**, como mostra a figura ao lado, clique em **OK** ara acessar.

A console vai abrir e permitirá o acesso de acordo com o **perfil do usuário** utilizado no momento do Run As.

Conclusão

E assim vimos de forma geral as características do AGPM, um dos produtos do pacote MDOP, desde seu funcionamento até sua instalação. Fique atento nos demais artigos para conhecer também as outras ferramentas, muito obrigado pela leitura e até a próxima oportunidade.

Escreveu,

Cleber Marques

contato@clebermarques.com

Terça-feira, 02 de Setembro de 2008.