



PRINCIPAL SISTEMAS HOSPEDAGEM PRODUTOS SOLUÇÕES UTILITÁRIOS FALE CONOSCO PÁGINA INICIAL

Total Produtos = 0
Total Preço = R\$ Consulte!

Meu Carrinho de Produtos

Entendendo o UAC do Windows Vista



por Marcos Elias Picão - Guiadohardware.net

O Windows Vista possui um sistema especial de controle de contas dos usuários, diferente de tudo o que existia nas versões anteriores do Windows. Todos os programas são executados por padrão com uma conta limitada, mesmo quando rodados com conta de administrador. Para efetivamente rodar um programa com direitos de administrador, é necessário aprovar conscientemente isso.

Um sério problema (não necessariamente “do” Windows) existente há muito tempo, a principal falha que permite que vírus, spywares e malwares em geral sejam instalados no Windows, foi reduzido – para muitos, emilinado – nessa nova versão do Windows. Antes de começarmos, é bom saber brevemente sobre as contas de usuários.

O Windows NT e seus sucessores, como o 2000, XP, 2003 e o Vista, baseiam-se no conceito de contas de usuário. Para cada conta são atribuídos direitos sobre o que podem e o que não podem fazer no sistema. Há basicamente dois tipos de contas “essenciais”: administrador e usuário. As preferências do computador (cores da tela, programas no menu, papel de parede, etc.) são separadas para cada usuário. Os usuários comuns, também chamados de usuários restritos ou limitados, só podem alterar os seus próprios arquivos e configurações (essa configuração pode variar dependendo de outras opções, mas é a base padrão). Eles não podem instalar programas que afetam todo o sistema, nem alterar configurações que são válidas para todos os usuários, como algumas configurações do painel de controle do Windows, de firewall, anti-vírus, nem alterar arquivos nas pastas do sistema ou instalar boa parte dos dispositivos de hardware – o que envolve a escrita de dados dentro da pasta do sistema. Os programas executados por usuários limitados seguem com seus mesmos bloqueios. Já os administradores têm acesso completo ao computador, podendo instalar e alterar qualquer coisa, em qualquer pasta. Isso é usado em muitos sistemas operacionais, como no Linux também, mas não existia tal controle no Windows 95, 98 nem no Me.

Devido o uso doméstico e a construção de muitos programas, que foram feitos (ou tiveram suas primeiras versões) pensando no Windows 9x e cia, eles precisam gravar coisas no registro em locais onde só os administradores poderiam, por afetar a máquina toda. Muitos programas ainda hoje fazem isso, uns porque herdaram versões projetadas para o 98, outros porque os programadores não atualizaram, e uma boa parte foi descontinuada mas continua sendo usada – os chamados “aplicativos de legado”.

Isso impede que o programa seja executado corretamente no Windows NT com uma conta limitada, porque entre outras coisas, o programa não pode:

- Gravar arquivos em pastas do sistema (em partições NTFS). Muitos programas gravavam configurações nas suas próprias pastas, ou na pasta do Windows (por exemplo, num arquivo INI). Se o programa foi instalado na pasta Arquivos de programas, ocorre o mesmo erro, pois só os administradores podem gravar coisas nela. Isso é um grande problema em muitos programas. Por outro lado, alguns programas móveis precisam gravar suas configurações na mesma pasta em que estão, o que se for a Arquivos de programas, gera esse erro.
- Gravar configurações nas chaves do registro onde só os administradores podem alterar: HKEY_LOCAL_MACHINE, para configurações, ou na HKEY_CLASSES_ROOT, para associações de arquivos. Essas opções afetam a todas as contas de usuário, por isso não podem ser alteradas por usuários limitados.

No tempo do Windows 9x/Me, onde não existia controle de acesso às pastas e ao registro, esses programas funcionavam com qualquer conta. Na família NT, precisam ser executados como administrador, ou é necessário fazer algumas alterações nas permissões de pastas e chaves do registro específicas – o que, convenhamos, não é nenhum pouco prático nem agradável, além de variar de programa para programa.

A Microsoft certifica os programas para Windows, quando eles seguem a configuração e as regras do sistema. Um programa certificado deve guardar as configurações em locais que o usuário possa escrever. Seja na pasta Dados de Aplicativos, ou no registro, sob a chave HKEY_CURRENT_USER. Sempre no perfil do usuário, nunca em locais globais. No Linux isso sempre ocorreu, veja que não é um problema “do” Windows ou dos usuários, e sim dos programadores. No Linux, por exemplo, os programas são instalados numa pasta onde só o administrador (root) pode alterar coisas, como a /usr/bin, ou /usr/local/bin. As configurações são salvas no perfil de cada usuário, sem afetar os demais. No Windows isso praticamente sempre esteve disponível, mas quase nunca foi usado na época do Windows 9x.

Como o pessoal usa muitos programas que não se adequam a isso, acabam tendo que rodá-los como administrador. É aí que mora o perigo: o programa funciona, mas usar o computador com conta de administrador abre inúmeras brechas: um vírus ou malware, se executado, poderá ferrar a máquina toda, arquivos de todos os usuários, se infiltrar no sistema e ser de difícil remoção.

O Vista e o UAC

O Windows Vista veio com um Controle de Conta de Usuário (User Account Control, UAC). Ele trabalha dessa forma:

- Se o usuário é um usuário limitado, todos os programas são executados como usuário limitado. Se algum programa precisar gravar arquivos em pastas globais do sistema ou configurações globais no registro, será necessário executá-lo como administrador. Isso pode ser feito clicando com o botão direito num programa e então escolhendo “Executar como”. No Windows NT4/2000 é necessário segurar SHIFT para que apareça a opção “Executar como” no menu. Até então, no Vista é basicamente a mesma coisa deste o Windows NT 4.0.
- Se o usuário é um administrador, até o Windows Server 2003, todos os programas executados eram rodados como administrador, tendo acesso completo/irrestrito ao sistema. Agora entra uma diferença no Vista: mesmo logado como administrador, os programas executados pelos administradores são executados com privilégios limitados. Para executar um programa realmente com direitos de administrador, deve-se conscientemente aceitar isso, o que pode ser feito de algumas formas diferentes (veremos logo mais).

Essa medida de segurança torna, por si só, o Windows Vista muito mais seguro do que qualquer versão anterior, pois a maioria, grande maioria dos problemas de vírus e spywares, são executados porque o usuário executa. Não é culpa do sistema. Se você mandar um vírus abrir, ótimo, ele será aberto. No Vista, será aberto com recursos de usuário limitado, poderá causar alguns

estragos, mas não globais. Normalmente bastará entrar com outra conta e tudo estará resolvido. Cabe aos usuários fazerem backup dos seus arquivos, claro. E todo o bla bla bla de não rodar programas suspeitos, que todo mundo está careca de saber, e uma vez comentei num texto aqui, sobre “como remover malwares na raça”: <http://www.guiadohardware.net/tutoriais/removendo-malware-raca/>

No processo de logon, o “explorer.exe” do Vista é executado com a conta de administrador (se o usuário for um administrador), porém com direitos de usuário limitado. Conseqüentemente, todos os processos iniciados após isso, como os programas do menu Iniciar, cliques em telas, em sites, etc, são rodados sem direitos administrativos. Nenhum deles pode gravar ou alterar nada em pastas do sistema, nem na chave HKEY_LOCAL_MACHINE do registro, entre outras.

Alguns programas que precisam ser executados como administrador, contém um recurso chamado “elevação”. Eles vêm preparados para o Windows NT, e quando rodados por um usuário limitado até o Windows Server 2003, o Windows exibia uma tela solicitando credenciais de administrador (usuário e senha). Isso é muito usado em instaladores de programas, e cabe aos programadores aplicarem o devido recurso nos seus programas (o que foge ao objetivo deste texto, que é para os usuários). Até então, esses mesmos programas rodavam diretamente se fossem executados por um administrador. No Vista, quando os administradores rodam os programas que pedem elevação, o Windows pára tudo e exhibe uma confirmação, perguntando se a pessoa tem certeza que quer executar o programa. É a tradicional tela do UAC que enche o saco de tanta gente

Se o mesmo for executado por um usuário limitado, aí vem a solicitação de uma conta de administrador, o que é basicamente como nas versões anteriores. Isso alerta os administradores de que aquele programa precisa de direitos de administrador. Ou o administrador executa, ou cancela a execução.

Acontece que programas que não pedem elevação na inicialização, serão executados diretamente. Como falei, cabe aos programadores isso. Como o Windows 9x/Me reinou por muito tempo, boa parte dos programas até 2001/2002 não se preocupava com isso. O ideal é que o programa possa ser instalado apenas por um administrador, mas usado por todos. Quando instalado por um usuário limitado, fica disponível apenas para o usuário que o instalou (assim como é no Linux), porém vários programadores não ligam para isso deixando tudo dependente de uma conta de administrador.

Então, os programas que não pedem elevação são executados diretamente, seja por um usuário restrito ou não. Como falei, eles serão rodados com direitos limitados, mesmo quando executados pelos administradores. Não conseguirão gravar coisas em pastas do sistema, como um arquivo de configuração sob a pasta do programa, dentro da Arquivos de programas; um arquivo INI na pasta do Windows; alterar uma chave global no registro; etc.

E como rodar os programas efetivamente como administrador?

Tudo isso traz segurança, mas traz ao mesmo tempo, incompatibilidade com alguns programas, que não funcionam sem direitos de administrador. O ambiente de programação Borland Delphi 7, por exemplo, na primeira inicialização, precisa renomear um arquivo que fica na pasta dele, dentro da Arquivos de programas. No Vista ele não consegue, mesmo sendo rodado com uma conta de administrador. O programa recebe uma mensagem do sistema operacional de acesso negado, e faz o que quiser depois (não mostra nada, ou mostra um erro para o usuário dizendo que não conseguiu gravar um arquivo, no exemplo do Delphi 7). Outro exemplo são as versões antigas do Winamp (acontece ainda com alguns reprodutores de mídia de programadores independentes). Ele salvava a playlist e as configurações na pasta dele. No Vista, não conseguirá.

A saída para esses casos é executar o programa com direitos administrativos. Isso pode ser feito clicando com o botão direito no ícone do programa e escolhendo “Executar como administrador” (não repare as imagens de tela, estou com o Vista em

espanhol/inglês):

Se for um programa que você precisa rodar sempre, pode ser chato. Calma, nas propriedades do arquivo (“botão direito no ícone > Propriedades”), escolha a aba “Compatibilidade”. Marque a opção “Executar como administrador”

Isso continuará exibindo o alerta de segurança ao tentar rodar o programa, mas pelo menos ele funcionará. Caso haja outras contas de usuário no computador, você pode clicar no botão “Mostrar a configuração para todos os usuários”, para permitir que eles rodem esses programas com direitos administrativos.

Cuidado: dependendo de como um programa chamar outro, o programa chamado herda os direitos atribuídos ao processo pai. Um programa rodado como administrador, poderá abrir outros programas, que também receberão direitos de administrador.

Alguns instaladores de programas não vêm preparados com a solicitação de elevação. Nesse caso, ao tentar executá-los, você não veria nenhum aviso, eles rodariam – mas não teriam acesso às pastas do sistema com suporte a escrita, nem à configuração global do registro. Como resultado, a instalação não se efetivaria, ou o programa não funcionaria. Basta executá-los novamente mas desta vez como administrador, clicando com o direito no ícone e escolhendo “Executar como administrador”.

Desativando o UAC

Apesar que eu, particularmente, também acho incômodo ter que confirmar toda vez que se quer rodar um programa com direitos administrativos, valeria a pena experimentar deixar ativado esse recurso, que fará parte também do Windows Server 2008. Muita gente critica indevidamente o Windows (não é que estou defendendo também), mas há de se concordar que o UAC é muito bom e barra o usuário de fazer várias besteiras, muitas vezes sem saber. O Linux também age assim. Se você quer rodar um programa como root (a conta de “Administrador” do Linux), sabe que não é só executar diretamente, deve usar o “Executar como” e fornecer credenciais de administrador, ou usar o comando su ou sudo que torna o usuário administrador, quando no prompt de comando (terminal ou console, como queira). Muitas distribuições nem deixam o usuário se logar como administrador no ambiente gráfico, tendo que alterar as configurações os que realmente querem. No caso do Vista, mais pessoas podem ser administradores, a segurança será maior, mas ainda depende, claro, da consciência do usuário.

Bom, se você quiser desativar o UAC, pode fazê-lo de 3 formas. Uma global, válida para todos os usuários, feita via interface, pelo MSConfig. Clique em “Iniciar > Executar” e digite msconfig. Na aba “Ferramentas”, escolha “Desativar UAC” e clique em “Iniciar”. O comando que é executado na verdade é este:

```
C:\Windows\System32\cmd.exe /k  
%windir%\System32\reg.exe ADD  
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System /v EnableLUA /t REG_DWORD /d 0 /f
```

(trocando C: pela unidade do Windows, claro)

Ele basicamente altera uma chave do registro. Depois de desativar, será necessário reiniciar o computador para que a alteração tenha efeito. Para ativar novamente, volte aí e faça a mesma coisa, escolhendo apenas o item “Ativar UAC”. Nota: no Windows Vista, o item “Executar” não aparece no menu Iniciar por padrão. Para exibi-lo, clique com o direito no menu Iniciar e a seguir em “Propriedades”, e ative o item “Executar” na aba “Menu Iniciar”. Você também pode usar o atalho de teclado da tecla de logotipo do Windows junto com a letra R, para abrir o Executar, independentemente de ele estar sendo exibido no menu ou não.

Outra forma é fazer a edição manual diretamente no registro, fazendo aquilo que o comando incluso no MSConfig faria. Abra o editor do registro (regedit), vá até a chave:

HKEY_LOCAL_MACHINE > SOFTWARE > Microsoft > Windows > CurrentVersion > Policies > System
... e edite o valor dword "EnableLUA", deixando-o com o valor 0 para desativá-lo, ou 1 para ativá-lo. Da mesma forma, é necessário reiniciar o computador para que entre em vigor a nova configuração.

Outra forma é usando as políticas de grupo de segurança. Essas podem ser usadas para ativar ou desativar o UAC para os administradores, mas mantendo ativada para os usuários limitados (o que também não seria recomendável, mas caso queira...).

No "Executar", digite secpol.msc. Em "Políticas locais", clique em "Opções de segurança". Role a tela e localize o item "Controle de Conta de Usuário: Executar todos os administradores no Modo de Aprovação de Administrador". Dê um duplo clique, e escolha a opção "Desativado". Confirme, feche a janela e reinicie o computador (ou faça logoff, agora). Nessas políticas locais de segurança há várias outras configurações relativas a esse tema, vale a pena dar uma olhada. Nota: no Windows em português poderá estar um pouco diferente, pois como falei estou usando ele em espanhol :p

É isso, mais segurança no Vista, no controle do usuário, pois o usuário é o principal responsável por baixar e executar os programas.

<< Voltar

Copyright© - Tera Sistemas. Todos os Direitos Reservados