craptree 06-03-2008 04:35 PM

Guide to using FBWF on Windows XP Pro

Hi there. my first post, hope its of use to people here. I am using FBWF on a standard Windows XP Pro installation (SP3 RC1 to be exact). Finding no guide available online, I thought I'd write this one.

--EDIT--
Quick note for those of you who don't know what FBWF is. It is very similar to EWF, but FBWF (file based write filter) offers some important advantages. FBWF uses less ram (you can reclaim ram overlay space when you delete files), you can also commit on the fly (without restarting or disabling), and have persistent (write through) folders that write straight to the drive (so you can have a persistent My Documents for example).
--EDIT--

You will need the following files from the XPe feature pack 2007 trial.

fbwf.sys fbwfdll.dll fbwflib.dll fbwfmgr.exe

If you're not sure how to extract these files, please see the "New EWF + MinLogon and CF instructions" thread by SFiorito.

1.Copy fbwf.sys to \WINDOWS\system32\drivers
2.Copy all other files to \WINDOWS\system32\
3.Add the following to your registry (it's probably easiest to copy it into an empty txt file, rename it to fbwf.reg, and load)

Code:

```
Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\FBWF]
"Start"=dword:00000000
"Type"=dword:00000002
"ErrorControl"=dword:00000001
"ImagePath"=hex(2):73,00,79,00,73,00,74,00,65,00,6d,00,33,00,32,00,5c,00,44,00,\
  52,00,49,00,56,00,45,00,52,00,53,00,5c,00,66,00,62,00,77,00,66,00,2e,00,73,\
  00,79,00,73,00,00,00
"Group"="FSFilter System Recovery"
"DisplayName"="File-Based Write Filter"
"Description"="File-Based Write Filter driver"
"DependOnService"=hex(7):46,00,6c,00,74,00,4d,00,67,00,72,00,00,00,00,00
"DebugFlags"=dword:00000000
"EnabledOnAllSkus"=dword:00000001

[HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\FBWF\FBA]
"EnablePostFBA"=dword:00000001

[HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\FBWF\Instances]
"DefaultInstance"="Fbwf Instance"

[HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\FBWF\Instances\Fbwf Instance]
"Flags"=dword:00000000
"Altitude"="226000"
```

4.Reboot
5.Go to your command prompt, and type in the following commands.

fbwfmgr /enable
fbwfmgr /addvolume X:
fbwfmgr /setthreshold S

X is the drive you want to protect (most will want to protect c:). S is the size you want your ram drive to be in MB(mine is 256).

6. Reboot, and your done!

There are 4 other commands in fbwfmgr you may want to play with. /setpreallocation 1 reserves the ram space (I.E does not dynamically change with the amount of actual used space). /setcompression 1 compresses the date to save more ram space, but at the cost of CPU time. /overlaydetail tells you what files are being stored in ram, and how much ram space is being used. /addexclusion X: "\persistent\folder" enables write through on the folder X:\persistent\folder.

For those used to EWF, unfortunately there is no way to commit all data, and each file has to be committed manually with the following command /commit X: "\windows\file.exe"

I hope I haven't left anything out! Hopefully this guide will be usable and somewhat clear...and if it breaks your puter, well, I'm sorry :P