

Performance Optimization – Necessary Steps for PC Fast Performance

¹ MOHAMED ANVAR HAITHER M.Sc.IT

BITS Pilani, Dubai Campus
Computer Lab Instructor
Dubai International Academic City, PO Box no. 345055, UAE
+971 50 2098466

Abstract

Nowadays we keep receiving virus disturbance like GAMES.EXE, Generic Host Process for win32 services etc..in our PCs that too whenever we are in urgency and if our system slows down no words to express that feel right? IF virus utility is updated it doesn't mean that we are safe and PC performance will be faster. As a User it's our responsibility also to keep our PC perfect. People used to discuss great topics like Cloud computing, Bridge Networks etc. but small routine steps they fail to do in order to improve their PC better performance. In this paper we will see few initial and important steps for Performance optimization

Keywords: *Virus Removal, DATs Update, Removal of Generic Host process for Win32 services, Automatic Shutdown,*

1. Introduction

In this paper Performance Optimization and Maintenance has been discussed in simpler manner which will be very helpful for all the users. Instead of minimizing the warning messages and continuing the work, doing a basic initiative will improve the PC performance better.

Making the PC performance faster will help the user in delivering the output prompt and will also saves time. [1]Microsoft has clearly explained similar steps discussed in this journal to improve PC fast performance.[2] This paper develops a performance gap measure of reverse salience and applies this measurement in the study of the PC (personal computer) technological system, focusing on the evolutions of firstly the CPU (central processing unit) and PC game sub-systems, and secondly the GPU (graphics processing unit) and PC game sub-systems.

2. Basic Steps for PC Fast Performance

2.1. Utility to Remove Viruses from Net.

Check whether your virus Anti virus utility has Anti Spyware [removes viruses received while surfing the net] and Anti Malware [removes additional viruses from application installed].

2.2. DATs Update.

Check whether your DAT file is current date or not[right click on your Anti virus symbol click on about Virus Scan , then check DAT created on is current date it should not be >3days back.]

2.3. Regular Scanning of PCs.

At the end of every day start a full system scan and leave. If you are aware of how to setup a scheduled task in the control panel to full scan and Shut down after your work hours.

2.4. Awareness about Latest DATs update.

IF you're using McAfee as your Anti Virus, click this link <https://secure.mcafee.com/apps/mcafee-labs/dat-notification-signup.aspx> and enter your email id. McAfee will send you the latest DAT file notification. Keep downloading, after update restart your system and run full scan.

2.5. Removing unnecessary sharing.

Remove your old Printer, scanner, PC camera, Bluetooth drivers which you are not using it anymore and Avoid Network Sharing.

2.6. Regular Removable drives scanning.

Before using a USB drives its better to run a virus scan on it to avoid infections of your hard drive.

3. Preventing from regular virus information.

3.1. Generic Host Process for Win32 Services & Svchost Error.

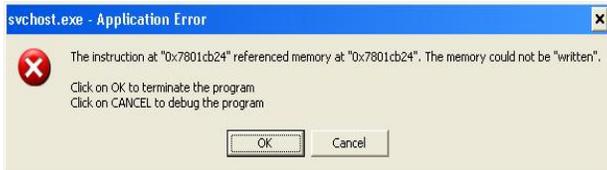


Fig. 1: SVCHOST.EXE error message box.



Fig. 2: Generic Host Process for Win32 Services message box.

The above fig.1 and fig.2 are the problems faced by lot of windows XP OS systems. There are several possible reasons of these error messages.

Reason 1: You have one of numerous worms, viruses and Trojans which pretend they to be legal svchost.exe or use legal svchost.exe to run themselves at windows startup. These threats include: Cash Toolbar Downloader-MY, System1060, CoolWebSearch Svchost32, ADCLICK-AG, ADCLICK-AX, ADUYO-A, AGENT-V, AGOBOT-KL, AUTOTROJ-C and many others.

Reason 2: Few legal DLL which uses svchost.exe to run itself at Windows startup crashed and causes crash of the whole svchost.exe service.

Reason 3: You may just installed update from Microsoft which contains erroneous version of Windows Installer or double-byte character set (DBCS) characters support (only occurs in Microsoft Windows XP Service Pack 2 (SP2)).

Reason 4: You installed old printer or scanner drivers from Hewlett-Packard which are incompatible with the current version of svchost.exe.

3.2. Solution to prevent from these error messages.

3.2.1 Automatic Solution

Download [Svhost Fix Wizard](#) Perform scan of your PC which will take up to 1 minute (usually faster) If Svhost Fix Wizard will find reason of the problem, you need to purchase it. The price of Svhost Fix Wizard is \$39.95. Mention that for \$39.95 you get not only solution of your problem but also quality anti-spyware scanner.

3.2.2 Manual Solution.

Go to Windows Automatic Updates properties (right-click on My Computer, then click on Properties and switch to Automatic Updates tab). Choose "Turn Off Automatic Updates", click OK and reboot your PC. Manually update Windows using "Windows Update" shortcut in the start menu. Turn automatic updates on. If your problem is not solved on this step, uninstall old Hewlett-Packard printer and scanner drivers (if any) and download new drivers from the manufacturer's web site. If your problem is not solved on this step, use the following command to show all svchost.exe instances and associated services or libraries: `tasklist /svc /fi "imagename eq svchost.exe"` Then search for each of services and libraries shown in that list in the Internet to find out whether the entry is malicious or not. In case you find malicious entry, use msconfig.exe utility to disable the appropriate service entry. This is long but effective way of Generic Host Process or svchost.exe repair.

3.2.3 Additional steps to remove Generic virus.

In the Run box, type: regedit then click the OK button. The Registry Editor will now have opened. Locate the following key in the registry:

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\NetBTParameters. In the right-hand side of the window find an option called TransportBindName. Double click that value, and then delete the default value, thus giving it a blank value. Then you must now navigate to the following registry key: HKEY_LOCAL_MACHINE\Software\Microsoft\OLE You will see there is a String Value called: Enabled COM Set the value to: N (it should currently be Y) Close the Registry Editor. Shutdown and Restart your computer.

3.3 Removing Games.exe virus.

Games.exe it's a regular file we use to see in our folders. IT may hit your machine due to a download from a P2P sharing. To remove games.exe, follow the below steps, First try to run your anti-virus and other spyware removal tools. If it doesn't help you could try Click Start > Run > type msconfig and click OK. Click the Startup tab and uncheck: Microsoft Tray = D:\DOWNLOADS\GAMES.EXE click apply/ok and reboot. Delete the file. OTHERWISE in the same Tray if u see Games .exe at any path just delete it.

[3]4. Similar Group policy for all users.

In your office or the place you are working is a computer laboratory and if you want to apply similar group policy for all users except administrator at your work place follow the below steps. **Warning** Microsoft strongly recommends that you perform a full backup before you start this procedure.

4.1 Starting with Group Policy Object Editor.

To start with Group Policy Object Editor, click **Start**, click **Run**, type **gpedit.msc**, and then click **OK**. **Note** If one of the policies that you want to apply is the removal of the **Run** command, Microsoft recommends that you use the Microsoft Management Console (MMC) to edit the policy and that you then save the results as an icon so that you will not have to use the **Run** command to complete some of the other steps in this procedure. To do this, follow these steps:

- a. Click **Start**, click **Run**, type **mmc**, and then click **OK**.
- b. Click **Console**, and then click **Add/Remove Snap-in**.
- c. On the **Standalone** tab, click **Add**.
- d. In the **Add Standalone Snap-in** window, click **Group Policy**, and then click **Add**.
- e. In the **Group Policy Object** box, type **Local Computer** (if it is not already there), and then click **Finish**.
- f. In the **Add Standalone Snap-in** window, click **Close**. In the **Add/Remove Snap-in** dialog box, click **OK**.
- g. Click **Console**, click **Save**. In the **Save in** list, click **Desktop**.
- h. In the **File Name** box, type a name for the console, and then click **Save**.

4.2 Expand **User Configuration**, and then expand **Administrative Templates**.

4.3 Click the folder that contains the policy that you want to enable, double-click a policy, and then enable it. For example, if you want to hide the My Network Places icon, click **Desktop**, double-click **Hide My Network Places icon on desktop**, click **Enabled**, click **Apply**, and then click **OK**. **Note** Make sure that you select the correct policies. Otherwise you may restrict the ability of the administrator to log on to the computer (and complete the necessary steps to configure the computer). Microsoft recommends that you record the changes that you have made.

4.4 Close the Group Policy Object Editor or MMC, and then log off.

4.5 Log on to the computer as an administrator. You can see in this logon session that the policy changes that you made are applied. By default, the local policies apply to all users, including administrators.

4.6 Log off from the computer, and then log on to the computer as one of the non-administrator users of this computer for whom you want these policies to apply. Repeat this step for each user of this computer for whom you want these policies to apply. The policies are implemented for all these users and for the administrator. **Note** You must log on as each user of the computer. User accounts that do not log on during this step will not have the policies implemented for that account.

4.7 Log on to the computer as an administrator.

4.8 Turn on the **Show hidden files and folders** option. To do so, follow these steps:

4.8.1 Click **Start**, point to **Settings**, and then click **Control Panel**.

4.8.2 Double-click **Folder Options**, click the **View** tab, click **Show hidden files and folders**, and then click **OK**.

4.9 Copy the Registry.pol file that is located in the %Systemroot%\System32\GroupPolicy\User folder to a backup location (for example, to a different hard disk, to a floppy disk, or to a folder).

4.10 Open your local policy again by using either the Group Policy Object Editor or your MMC console icon, and then reverse the changes that you made in step 3. For example, to reverse the changes that you made in step 3, double-click **Hide My Network Places icon on desktop**, click **Disabled**, click **Apply**, and then click **OK**. **Note** When you do this, Policy Editor creates a new Registry.pol file.

4.11 Close Group Policy Object Editor or MMC, and then copy the backup Registry.pol file that you created in step 9 back to the %Systemroot%\System32\GroupPolicy\User folder. When you are prompted to replace the existing file, click **yes**.

4.12 Log off from the computer, and then log on to the computer as an administrator. You can see that the changes that you made in step 3 are not implemented because you have logged on to the computer as an administrator.

4.13 Log off from the computer, and then log on to the computer as another user (or other users). You can see that the changes that you made in step 3 are implemented because you have logged on to the computer as a user (not as an administrator).

4.14 Log on to the computer as an administrator to verify that the local policy does not affect you as the local administrator of that computer.

4.15 Restore original local policies

To reverse the process that is described in the "Apply local policies to all users except administrators" section of this article, follow these steps:

4.15.1 Log on to the computer as an administrator.

4.15.2 Turn on the **Show hidden files and folders** option. To do so, follow these steps:

a. Click **Start**, point to **Settings**, and then click **Control Panel**.

b. Double-click **Folder Options**, click the **View** tab, click **Show hidden files and folders**, and then click **OK**.

4.15.3 Move, rename, or delete the Registry.pol file from the %Systemroot%\System32\GroupPolicy\User folder. Another default Registry.pol file is created by the Windows File Protection system after you log off from or restart the computer.

4.15.4 Open the local policy. To do this, click **Start**, click **Run**, and then type **gpedit.msc** or **mmc**, and then click **OK**. Load the local security policy. Then, set all the items that are set to either "Disabled" or "Enabled" to "Not defined" to reverse any policy changes that had been implemented to the Windows 2000 registry as specified by the Registry.pol file.

4.15.5 Log off from the computer, and then log on to the computer as an administrator.

4.15.6 Log off from the computer and then log on to the computer as one of the non-administrator users so that the changes can be reversed on that user's account also. Repeat this step for each non-administrator user of this computer.

Note If the profile does not load, the subsequent logon by the administrator will be locked down to the point that the computer cannot be unlocked.

Source/Reference: <http://support.microsoft.com/kb/293655>

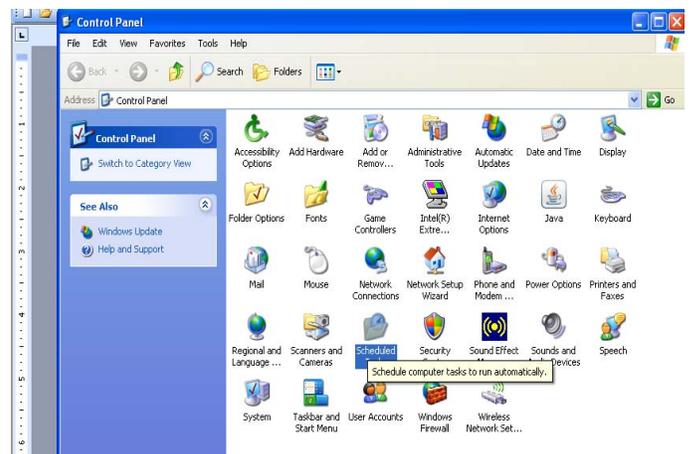
5. Setting Automatic Shut Down for PCs Manually.

Most of the users they used to ignore shutting down their PC at the end of the day its because they use to work until the last minute in their office or overnight at home. To avoid these situations we can set up automatic shut down according to our desire finishing time so that it will make CPU to take rest. Even though few auto shut down is available in the net its better to do ourselves in our PC and here are the easy steps illustrated with clear figures to set up Auto Shut Down in windows based Systems.

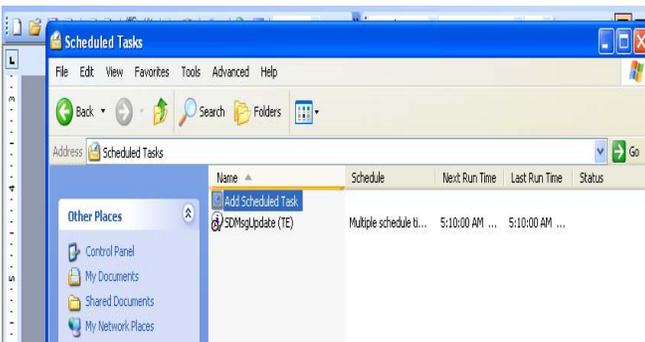
5.1. First check your system has been set to current time and date then .Open Control Panel.



5.2. Select Scheduled Task button and double click it



5.3. Inside Schedule Task window select ADD Schedule task



5.6. Browse for the file shutdown.exe from the path c:\windows\system32 shutdown.exe then you will get a window like below select daily and then click next

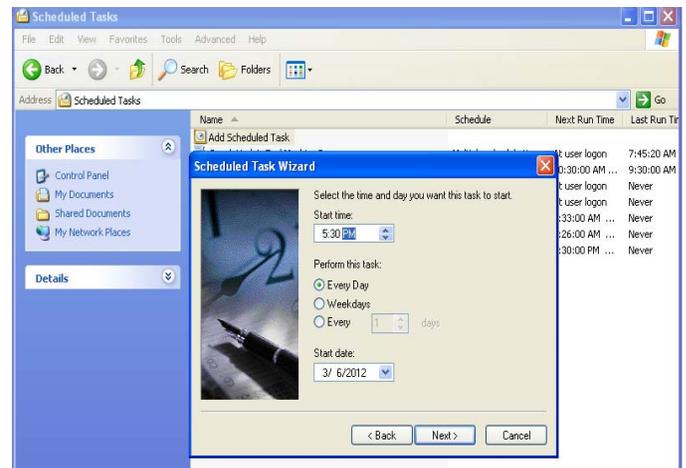
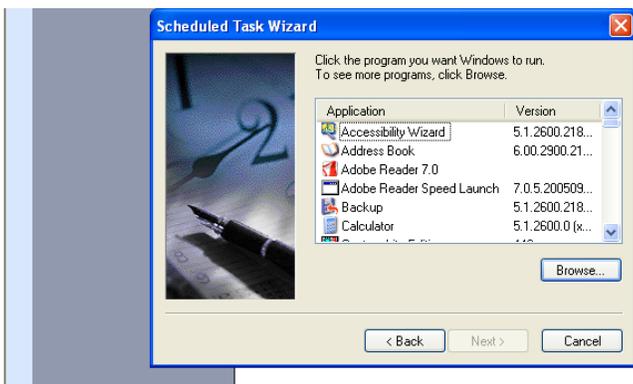


5.4. You will get a window as below then click next



5.7. Set the timing to 5.30pm or 10.30pm at home or else whichever your last time you used to finish your work in the system and the date. Make sure everyday option is selected and date should be the current date whenever you are creating this task. Then Click Next

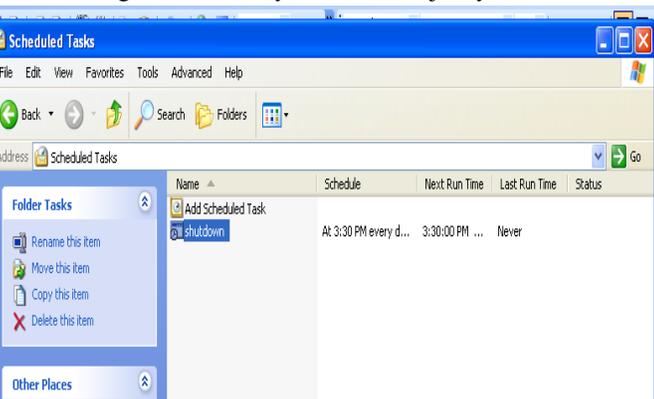
5.5 Click the browse button below.



5.8. Enter your Administrator Password then click Next. and Finish as below.



5.9. If you got any error message just ignore and open the Task schedule again u can see your new task just you created.



5.10. Double click on your task u will get the window as below.



For testing yourself you can give the nearest time and check whether the task you have just created is working properly then set back to the ending time.

Source: Own Practical Experience

6. Conclusions:

In this paper I have illustrated basic steps to prevent our PCs from slow performance and also routine maintain. Its not like no one know about these steps but most of us use to follow these steps and whenever in trouble all we are doing is just taking a back up and formatting the system, which will waste our time in between our busy schedule. It's always to prevent ourself before the problem attacks us rather than putting our self in a miserable condition after the problem attack us. Few of may know these steps but don't know how to implement that's why I made this paper user friendly.

Acknowledgments:

Author likes to thank IJCSI for accepting his first Journal.

References:

- [1] Microsoft has clearly explained similar steps to increase PC fast performance in this link <http://www.microsoft.com/atwork/maintenance/speed.aspx>.
- [2] Journal of technology management & innovation *version Online* ISSN 0718-2724 http://www.scielo.cl/scielo.php?pid=S0718-27242008000100006&script=sci_arttext
- [3] Chapter 4 you can refer to Microsoft.com with the following link <http://support.microsoft.com/kb/293655>

Author:

¹ MOHAMED ANVAR HAITHER completed his M.Sc. IT in 2004 from Annamalai University – INDIA and currently working in BITS Pilani Dubai campus as Computer Lab Instructor from 25 August 2005 to till now. His total IT experience is 16 years. He started his career as field servicing engineer from the day he completed is Advanced Diploma that is from March 1995. He also worked in Singapore Ministry of Education as Computer Technology Assistant from 1998 to 2000. During later 2000 he went back to his home country-India where he completed his Master in 2004 and Joined BITS Pilani in August 2005.