Win 10 Management Notes 1.1.20

Nofrillstech recently went delving into Win 10, to see what changes were to be found, and realised that XP was not far below the surface. So, short notes on managing Win 10 follow, to do with cleaning, defragging, optimising, et al, tho other program usage is all about heuristics...nothing changes in that respect. More such relevant notes can be found in the **Computer Management Factfiles** on the main **PDF and WORD Page.**

See also Windows 10 Bible, Tidrow, Boyce, Schapiro, Wiley 2015-->

Re basic Win 10 tweaks, go to **Control Panel**:

Turn off **Indexing**, (stops this always running in the background),

Settings/System Properties Turn off **Remote Access**, (security step, trust your IT dept does not require this), and,

Settings/System Properties/Visual Effects/Performance/Best Performance, all squares unticked.

(All of these are reachable via **Search**, as well)

Plus, install **Toolwiz**, for file and Registry cleaning/defrag, et al, also turns off some unwanted Services...never had any problems with this program, run once per week, interesting to check out various ancillaries as well. You will notice an immediate speed improvement, tho also note that, after any Defrag, a couple of boots may needed to get the OS to run optimally, this always being the case, as Win re-deploys various System files and Directories. **Use the native Defrag/Optimise Administrative Services.**

Note that **defrag does not apply in the case of SSDs,** make sure that is never happening. **Win 7, and above, should automatically take care of this, viz, SSDs instead need TRIM to free up/overwite vacant space on the drive.**

1) Use the **Windows key + X** keyboard shortcut to open the Power User menu and select **Command Prompt (Admin)**.

2) Type the following command and press **Enter**: fsutil behavior query DisableDeleteNotify

3) If **zero (0) is the result**, then TRIM is **enabled**

4) If not, to enable TRIM, command line is: fsutil behavior set DisableDeleteNotify 0

Bleachbit is a handy cleaner, complementary to **Toolwiz**, tho leave Passwords, Memory, Diskwipe, and RAM unticked, the rest should be OK. **Crapcleaner** and **Dustbuster** are also useful. Running a **ClamAV** virus check, with the HDD/SSD plugged into a **Linux** system, will be worth doing after initial full install, including the ancillary programs. (Tho note that native Win 10 anti-malware objects are protected.)

Libre Office and CDBurnerXP, Firefox, Thunderbird, all work well, plus, usual Win programs, such as Office 97/2003 also. Plus, **Seamonkey/Kompozer/Kompozer 0.7.10, Filezilla, PDFCreator, PDFSAM, Photoshop, VLC**, are all OK.

Crystal Disk, CPUID/Z, Easeus Clone, Clonezilla, SSD Life, Speedfan, HardwareMonitor, HardInfo, all OK too. Native **Win antivirus/antimalware** kept updated should be sufficient.

Heuristics will apply for other specific programs, especially legacy versions, OK!

To get rid of the new Index, install **Classic Shell**, if needed, then the system will look and feel more like XP again.

Drivers, if required, are obtainable by the usual methods, tho Win 10 seems to be well-supplied for modern systems.

To dig deeper re turning off Win 10 Services:

http:www.askvg.com/beginners-guide-to-configure-windows-10-services/ ...and, there are many other refs via Google, depending on how keen you are. Some of these links also deal with Win 10 Bloatware. **Well-resourced/fast Win 10 systems should not actually need any more tweaks, up to you...?**

Re installation and validation: Win 10 will install, boot, and run, including updating, installing ancillary programs, drivers, et al, and, the un-validated drive OS will be swappable, from one system to another, which would be useful for finding the best system match, and for cloning purposes. **Note that, when the OS installation is validated online, the request for validation no longer appears in Settings.**

Existing validation codes may be utilised, from Win 7 and above, tho, be sure to install the version that matches the label code chosen. However, **actual validation will then match that OS installation to that specific system .**

https://www.howtogeek.com/266072/you-can-still-get-windows-10-for-free-with-a-windows-7-8-or-8.1-key/

If needed: fix-windows-10-startup-problems, plus, reinstallation and updates are simpler and faster, currently.

Note that Win10 OS is quite resilient, so, look for hardware problems like failing HDD/SSD, RAM, DVD, et al, when problems first arise.

Some computer and Internet security notes, and also power security, using UPSs, et al.

1) **Recommend using a good-quality surge monitor powerboard, and a UPS.** 'The three major types of UPS system configurations are online double conversion, **line-interactive** and **offline** (also called **standby** and **battery** backup). These UPS systems are defined by how power moves through the unit.' (See also: https://www.vertiv.com/en-emea/about/news-and-insights/articles/educational-articles/what-are-the-different-types-of-ups-systems/

A quality powerboard with surge monitoring capabilities will, in turn, protect the UPS, and, anything else plugged in it. Note that **laser printers** should not be on this particular board, as they **draw a lot of power when switched on,** and should be directly plugged to the mains, via a separate circuit/oulet, if practicable, or, switch on before swithing on the ret of your systems.

2) **Re data security and The Cloud,** The Cloud also has its rackets, sadly, and cheap or no-charge sign-up soon changes....and you definitely get what you pay for. Google has 10 Gb free, which must be regularly accessed, to be 'live'. Cloud security will always be an issue online. Meanwhile, email repositories can also be useful, and/or, a personal website could suffice to store extra current files which you can retrieve as you want, ie, stored without links ..? A separate working storage partition on you main system hard-drive is a must, also, as well as any other offline storage.

Good quality portable HDDs, for main backup storage at home, cannot be bettered, especially if you have a lockable fireproof repository. Also, consider another backup set at a different location..?

If not backed up at least 3x, then not backed up at all, is the realistic motto these days.

3) **Use a separate Internet interface system,** (a reliable laptop would do), if online security is an issue, and keep your main processing system air-gapped, as much as possible, only go online for updates, when not otherwise in use, plus, usual virus-checker, et al, must be installed.

4) **Consider local wifi providers, rather than major telecom providers**. Eg, your landline number retained, and unlimited data for approx $80 pm..? Personal service, better security, and less outages..?

5) **For reliable system,** as always, buy from established, dedicated, computer businesses of good reputation. **Never trust a department store bargain, or online trading, unless you really know what you are doing...**

6) Meanwhile, a further tip for your computer security, recommend that your main Internet interface system has a Linux OS, very easy to use, (eg, Mint, being very much like XP), can read/format to NTFS, re external drives, so, passing files for uploading from your main processing computer to your Linux interface system will pose no problems, and then upload to your website with Clonezilla. Takes about 15 mins to clone any Linux OS partition to a given HDD/SSD, using live Gparted, no problems there. Also, ClamAV is a useful Open Source antivirus, compatible with Mint, that can also read Microsoft data hard drives plugged as slaves, or via USB..