COMPUTER MANAGEMENT IN "WINDOWS.."

by Francis Chao

fchao2@yahoo.com
Web location for this presentation:

http://aztcs.org

Click on “Meeting Notes”
SUMMARY

The Computer Management "Microsoft Management Console" in "Windows.." provides you with access to the "System Tools" submenu, the "Disk Management" applet, and the "Services" window. These applets allow you to perform maintenance, repairs, and modifications to a "Windows.." computer.
TOPICS

- Uses of "Computer Management"
- Starting "Computer Management"
- Submenu Items of "Computer Management"
- Task Scheduler
- Event Viewer
- Shared Folders
TOPICS (continued)

- Local Users and Groups
- Disk Management
- Services and Applications
Uses of "Computer Management"

• Problem analysis and resolution for a "Windows.."

• Key applets for speeding up a slow "Windows.." computer (as part of our "Speeding Up Windows.." procedures)
Starting "Computer Management"

• Method 1:  
Log into "Windows.." with a user account that has a "type" of "Administrator". 
Right click on "Start button".  
Use either mouse button to click on "Computer Management" in the pop-up "Power Users" menu  (Windows 8, Windows 8.1, and Windows 10)
<table>
<thead>
<tr>
<th>Disk Management</th>
</tr>
</thead>
<tbody>
<tr>
<td>Computer Management</td>
</tr>
<tr>
<td>Command Prompt</td>
</tr>
</tbody>
</table>
Method 2:
Log into "Windows.." with a user account that has a "type" of "Administrator". Inside a Search box, a Run field, or a command prompt in "Windows..", type compmgmt.msc and then hit the Enter key of the keyboard ("Windows 2000" and higher)
Run

Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: compmgmt.msc
Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: compmgmt.msc

[OK] [Cancel] [Browse...]
Starting "Computer Management" (continued)

- Method 3:
  Log into "Windows.." with a user account that has a "type" of "Administrator".
  Get into the "Control Panel". If you see "System and Security", double-click on it.
  Double-click on "Administrative Tools".
  Double-click on "Computer Management".
("Windows 2000" and higher)
Adjust your computer's settings

System and Security
- Review your computer's status
- Save backup copies of your files with File History
- Find and fix problems

Network and Internet
- View network status and tasks
- Choose homegroup and sharing options

Hardware and Sound
- View devices and printers
- Add a device

Programs
- Uninstall a program

User Accounts and Family Safety
- Change account type
- Set up Family Safety for any user

Appearance and Personalization
- Change the theme
- Change desktop background
- Adjust screen resolution

Clock, Language, and Region
- Add a language
- Change input methods
- Change date, time, or number formats

Ease of Access
- Let Windows suggest settings
- Optimize visual display
System and Security
Review your computer's status
Save backup copies of your files with File History
Find and fix problems
Administrative Tools

- Free up disk space
- Defragment and optimize your drives
- Create and format hard disk partitions
- View event logs
- Schedule tasks
Administrative Tools
Method 4:
Log into "Windows.." with a user account that has a "type" of "Administrator". Start "Windows Explorer" or "File Explorer" or the "Start menu" if your version of "Windows.." has one. Locate "Computer", "My Computer", or "This PC" and right-click on it. Select "Manage" from the pop-up utility menu.
This PC

Desktop

Documents
Expand

Manage

Pin to Start

Map network drive...
Starting "Computer Management" (continued)

Method 3:
Log into "Windows.." with a user account that has a "type" of "Administrator". Inside the "Start menu" or "Windows Explorer" or "File Explorer", right-click on "My Computer" (Windows XP) "Computer" (Windows XP, Windows Vista, Windows 7, or Windows 8) "This PC" (Windows 8.1 or Windows 10). Then double-click on "Computer Management".
Submenu Items of "Computer Management"

- System Tools
- Storage
- Services and Applications
Submenu Items of "Computer Management"

• System Tools
  = Problem resolution tools

• Storage:
  = Disk Management

• Services and Applications:
  = Services console
  = WMI Control
"Disk Management"

- "Disk Management" lets you perform higher level tasks relative to the "Tools" menu:
  Inside "Disk Management", you can install new hard drives, "initialize" (= partition) hard drives, and create new partitions on hard drives, and modify the size of existing hard drive partitions.
"Disk Management" (continued)

- Inside "Disk Management", you can all right click on an existing hard drive partition, select "Properties", select the "Tools" tab, and then perform the usual "Error checking" and "Optimize and defragment drive" functions that you are used to doing from inside the "Windows Explorer" or "File Explorer" applets.
"Disk Management" (continued)

- Operating system sees hard drive by means of "Logical Block Addressing" (LBA):

  48-bit Address:
  00000000000000000000000000000000000000000000000000000000000000000
  to
  xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
  xxxxxxxxxxxxxxxx
"Disk Management" (continued)

• Operating system sees hard drive by means of "Logical Block Addressing" (LBA):
  Topmost track (ring) to bottom-most tract (ring)
  Outermost cylinder to inner-most cylinder
"Disk Management" (continued)

- "Zone Bit Recording" so that outer-most cylinders have more bits per track (ring) relative to inner-most cylinders
"Disk Management" (continued)

- "Disk Management" lets you adjust the size of the partition non-destructively:
  Extend the partition (to make it bigger)
  and
  Shrink the partition (to make it smaller)
"Disk Management" (continued)

- "Disk Management does not let you adjust the start location of a hard drive the partition. Shifting the start location of a hard drive partition is called "moving a partition"."
A very reliable third-party disk utility to move a hard drive partition: "GParted Live" CD (Linux-based). To download a free copy, go to http://gparted.org/livecd.php
"Disk Management" (continued)

- The current version of "GParted Live" CD can boot up most Windows 8/8.1/10 computers that have "Secure Boot" enabled. If you have a "Secure Boot" computer and it does not boot, you will have to temporarily disable "Secure Boot" before booting up with the "GParted Live" CD.
"Disk Management" (continued)

- For other third-party disk management utilities that can also "move" a partition, see http://www.techsupportalert.com/best-free-partition-management-software.htm
"Disk Management" (continued)

• Right click on any drive or partition to start up "Tools" from inside "Properties":
  There are two "Tools": "Error Checking"
  and
  "Optimize and Defragment Drive"
In "Windows 8", "Windows 8.1", and "Windows 10", the "Spot Verifier" service in "Services" assists "Disk Management" and "Tools" by keeping a real-time list of possible bad locations on all hard drives.
"Disk Management" (continued)

• According to
https://www.petri.com/fix-disk-errors-windows-8-and-windows-server-2012:
"Disk Management" (continued)

- Windows 8 and Server 2012 introduce a new capability that allows the file system to verify whether an issue is caused by a transient memory error or whether there is genuine file corruption on the disk.
"Disk Management" (continued)

- When the file system driver detects corruption, it verifies whether the corruption is genuine using the new Spot Verifier service.
"Disk Management" (continued)

- If the errors are verified to be genuine, an online scan of the volume catalogs the issues so that they can be fixed at a later point without scanning the entire volume offline.
"Event Viewer"

- Let's you look at a historical record of what has happened inside the computer for problem analysis and resolution:
"Event Viewer" (continued)

• Gives you a user-friendly time-line view of the what has happened inside "Windows.." and various software application programs. Provides a permanent record of error messages that have popped up and then disappeared.
"Event Viewer" (continued)

• When something unexpected happens in your computer, you need to immediately record the time so you need to have an accurate digital watch or clock that is synchronized to the clock applet in the Notification area of your computer. This watch or clock cannot be one that is running inside your computer!
"Event Viewer" (continued)

• Details of the various "logs" that are displayed in the "Event Viewer" can be found at http://www.sevenforums.com/tutorials/226084-event-viewer-open-use-windows-7-a.html:
Application (program) - Events are classified as error, warning, or information, depending on the severity of the event. An error is a significant problem, such as loss of data. A warning is an event that isn't necessarily significant, but might indicate a possible future problem.
• An information event describes the successful operation of a program, driver, or service.
Security - These events are called audits and are described as successful or failed depending on the event, such as whether a user trying to log on to Windows was successful.
"Event Viewer" (continued)

• Setup - Computers that are configured as domain controllers will have additional logs displayed here.

• System - System events are logged by Windows and Windows system services, and are classified as error, warning, or information.
"Event Viewer" (continued)

- **Forwarded Events** - These events are forwarded to this log by other computers.
"Event Viewer" (continued)

- Applications and Services Logs:

Applications and Services Logs vary. They include separate logs about the programs that run on your computer, as well as more detailed logs that pertain to specific Windows services. This category of logs includes four subtypes: Admin, Operational, Analytic, and Debug logs.
• Admin - These events are primarily targeted at end users, administrators, and support personnel. The events that are found in the Admin channels indicate a problem and a well-defined solution that an administrator can act on. An example of an admin event is an event that occurs when an application fails to connect to a printer.
"Event Viewer" (continued)

• These events are either well documented or have a message associated with them that gives the reader direct instructions of what must be done to rectify the problem.
Operational - Operational events are used for analyzing and diagnosing a problem or occurrence. They can be used to trigger tools or tasks based on the problem or occurrence. An example of an operational event is an event that occurs when a printer is added or removed from a system.
"Event Viewer" (continued)

- Analytic - Analytic events are published in high volume. They describe program operation and indicate problems that cannot be handled by user intervention.

- Debug - Debug events are used by developers troubleshooting issues with their programs.

<end of quote>
"Example 1" Step 1: If it is not already turned on, power on the "Windows" computer.
"Example 1" Step 2:
Click on the Windows "Start" button:
"Event Viewer" (continued)

• "Example 1" Step 3: Double-click on "Control Panel" in the "Start menu":
"Event Viewer" (continued)

- "Example 1" Step 4: Double-click on "Administrative Tools" in "Control Panel" window:
Adjust your computer's settings

- Administrative Tools
- Backup and Restore
- BitLocker Drive Encryption
- Color Management
- Credential Manager
- Date and Time
- Default Programs
- Desktop Gadgets
- Device Manager
- Devices and Printers
- Display
- Ease of Access Center
- Flash Player (32-bit)
- Folder Options
"Event Viewer" (continued)

• "Example 1" Step 5: Double-click on "Computer Management" in the "Administrative Tools" window:
"Example 1" Step 6: Click on the + Plus sign to the left of "Event Viewer" in the "Computer Management" window. The + Plus sign will change to a - Minus sign and the subordinate items inside "Event Viewer" will be displayed:
<table>
<thead>
<tr>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Tools</td>
</tr>
<tr>
<td>Storage</td>
</tr>
<tr>
<td>Services and Applications</td>
</tr>
</tbody>
</table>

- System Tools
- Storage
- Services and Applications
"Example 1" Step 7: Double-click on the "System" log in the "Name" column:
### Windows Logs

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Number of Events</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application</td>
<td>Administrative</td>
<td>33,035</td>
</tr>
<tr>
<td>Security</td>
<td>Administrative</td>
<td>30,146</td>
</tr>
<tr>
<td>Setup</td>
<td>Operational</td>
<td>633</td>
</tr>
<tr>
<td>System</td>
<td>Administrative</td>
<td>56,330</td>
</tr>
<tr>
<td>Forwarded Events</td>
<td>Operational</td>
<td>0</td>
</tr>
</tbody>
</table>
"Example 1" Step 8:
Note that in our example, the "System" log reported 4 Disk Errors at the time that "Windows 7.." locked up.
<table>
<thead>
<tr>
<th></th>
<th>8/17/2011 6:09:15 PM</th>
<th>Disk</th>
<th>15</th>
<th>None</th>
</tr>
</thead>
<tbody>
<tr>
<td>Error</td>
<td>8/17/2011 6:09:15 PM</td>
<td>Disk</td>
<td>15</td>
<td>None</td>
</tr>
<tr>
<td>Error</td>
<td>8/17/2011 6:09:15 PM</td>
<td>Disk</td>
<td>15</td>
<td>None</td>
</tr>
<tr>
<td>Error</td>
<td>8/17/2011 6:09:15 PM</td>
<td>Disk</td>
<td>15</td>
<td>None</td>
</tr>
<tr>
<td>Error</td>
<td>8/17/2011 6:09:15 PM</td>
<td>Disk</td>
<td>15</td>
<td>None</td>
</tr>
</tbody>
</table>
"Example 1" Step 9: Double-click on any errors that you find to get more information about them:
The device, `\Device\Harddisk1\DR1`, is not ready for access yet.

<table>
<thead>
<tr>
<th>Log Name</th>
<th>System</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source</td>
<td>Disk</td>
</tr>
<tr>
<td>Event</td>
<td>15</td>
</tr>
<tr>
<td>Level</td>
<td>Error</td>
</tr>
<tr>
<td>User</td>
<td>N/A</td>
</tr>
<tr>
<td>OpCode</td>
<td></td>
</tr>
<tr>
<td>More Information</td>
<td>Event Loca Online</td>
</tr>
<tr>
<td>Logged</td>
<td>8/17/2011</td>
</tr>
<tr>
<td>Task Category</td>
<td>None</td>
</tr>
<tr>
<td>Keywords</td>
<td>Classic</td>
</tr>
<tr>
<td>Computer</td>
<td>e9280t</td>
</tr>
</tbody>
</table>
"Example 1" Step 10: Go to the left pane of the "Computer Management" window and click on the "Application" log to see if it shows any errors or information notices that are pertinent to the date and time when the "System" log showed disk errors:
"Event Viewer" (continued)

- "Example 1" Step 11: Go to the left pane of the "Computer Management" window and click on the "Security" log to see if shows any errors or information notices that are pertinent to the date and time when the "System" log showed disk errors.
"Event Viewer" (continued)

- "Example 1" Step 12: Close the "Computer Management" window by clicking on the "X" button in the upper right-hand corner.
"Event Viewer" (continued)

• "Example 1" Step 13: Click on "Computer" or "My Computer", or "Windows Explorer" in the "Start menu": 
"Example 1" Step 14:
A "Windows Explorer" or "File Explorer" window will be displayed:
"Event Viewer" (continued)

• "Example 1" Step 15: Use the right mouse button to click on the C: drive to highlight it

• "Example 1" Step 16: A pop-up utility menu will be displayed:
"Event Viewer" (continued)

• "Example 1" Step 17: Click on "Properties" in the pop-up utility menu:
"Event Viewer" (continued)

• "Example 1" Step 18:
  A "Properties" box will be displayed:
"Event Viewer" (continued)

- "Example 1" Step 19: Click on the "Tools" tab:
Error-checking

This option will check the drive for errors.

Check now...

Defragmentation

This option will defragment files on the drive.

Defragment now...

Backup

This option will back up files on the drive.

Back up now...
"Event Viewer" (continued)

• "Example 1" Step 20:
  Click on the "Check now.." button.
HP-ST3750528AS (C:) Properties

Error-checking
This option will check the drive for errors.

Defragmentation
This option will defragment files on the drive.

Backup
This option will back up files on the drive.

Check now...
Defragment now...
Back up now...

[OK] [Cancel] [Apply]
"Event Viewer" (continued)

- "Example 1" Step 21:
  A "Check Disk" box will be displayed:
"Example 1" Step 22: Make sure that there is a checkmark for "Automatically fix file system errors": 
Check Disk HP-ST3750528AS (C:)

Check disk options

- Automatically fix file system errors
- Scan for and attempt recovery of bad sectors

Start  Cancel
"Event Viewer" (continued)

- "Example 1" Step 23: Place a checkmark in the box to the left of "Scan for and attempt recovery of bad sectors": 
Check disk options

- Automatically fix file system errors
- Scan for and attempt recovery of bad sectors

Start  Cancel
"Event Viewer" (continued)

- "Example 1" Step 25:
  Click on the "Start" button:
Check disk options

- Automatically fix file system errors
- Scan for and attempt recovery of bad sectors

Start
Cancel
"Event Viewer" (continued)

- "Example 1" Step 26:
  Click on the "Schedule disk check" button:
Windows can't check the disk while it's in use

Do you want to check for hard disk errors the next time you start your computer?

Schedule disk check  Cancel
"Event Viewer" (continued)

• "Example 1" Step 27: Close the "Properties" box by clicking on the "X" button in its upper right-hand corner:
HP-ST3750528AS (C:) Properties

- **Error-checking**: This option will check the drive for errors.
  - **Check now...**

- **Defragmentation**: This option will defragment files on the drive.
  - **Defragment now...**

- **Backup**: This option will back up files on the drive.
  - **Back up now...**

Buttons: OK, Cancel, Apply
"Example 1" Step 28: Shutdown and restart the computer.

"Example 1" Step 29: After the "Windows.." splash screen is displayed, a disk error check will start. Note that in "Stage 4 of 5" it says that "Windows replaced bad clusters in file 15841 of name \pagefile.sys.":
• Note that in "Stage 4 of 5" it says that "Windows replaced bad clusters in file 15841 of name \pagefile.sys.":
240384 file records processed.
File verification completed.
1236 large file records processed.
0 bad file records processed.
2 EA records processed.
75 reparse records processed.
CHKDSK is verifying indexes (stage 2 of 5).
307738 index entries processed.
Index verification completed.
0 unindexed files scanned.
0 unindexed files recovered.
CHKDSK is verifying security descriptors (stage 1).
240384 file SDs/SIDs processed.
Security descriptor verification completed.
33678 data files processed.
CHKDSK is verifying Usn Journal...
33887232 USN bytes processed.

Usn Journal verification completed.
CHKDSK is verifying file data (stage 4 of 5).
Windows replaced bad clusters in file 15841 of name \pagefile.sys.
17 percent complete. (42070 of 240368 files processed.)
"Event Viewer" (continued)

• Note that in "Stage 5 of 5" it says "Adding 1 bad clusters to the Bad Clusters File. Correcting errors in the volume bitmap.":
CHKDSK is verifying free space (stage 5 of 5)...
29768490 free clusters processed.

Free space verification is complete.
Adding 1 bad clusters to the Bad Clusters File.
Correcting errors in the volume Bitmap.
Windows has made corrections to the file system.

719746044 KB total disk space.
600190672 KB in 176211 files.
116268 KB in 33679 indexes.
   4 KB in bad sectors.
 365140 KB in use by the system.
 65536 KB occupied by the log file.
119073960 KB available on disk.

4096 bytes in each allocation unit.
179936511 total allocation units on disk.
29768490 allocation units available on disk.

Windows has finished checking your disk.
Please wait while your computer restarts.
"Example 2" : Cyberlink sells great video editing software. When one of their programs crashes in a computer, here are their instructions for what they should do to send the screenshots of the "Application" Event Log to their tech support
"Event Viewer" (continued)

• Reference:
  http://www.cyberlink.com/support/faq-content.do?id=10449:
• Navigate to Windows Logs > Application, and then find the latest event with “Error” in the Level column and “Application Error” in the Source column
<table>
<thead>
<tr>
<th>Level</th>
<th>Date and Time</th>
<th>Source</th>
<th>Event ID</th>
<th>Task Category</th>
</tr>
</thead>
<tbody>
<tr>
<td>Error</td>
<td>12/31/2009 5:09:20 PM</td>
<td>VSS</td>
<td>8194</td>
<td>None</td>
</tr>
<tr>
<td>Error</td>
<td>12/24/2009 7:21:41 PM</td>
<td>VSS</td>
<td>8194</td>
<td>None</td>
</tr>
<tr>
<td>Error</td>
<td>5/18/2010 6:10:55 PM</td>
<td>Application Error</td>
<td>1000</td>
<td>(100)</td>
</tr>
<tr>
<td>Error</td>
<td>7/1/2009 3:50:29 PM</td>
<td>MsInstaller</td>
<td>10005</td>
<td>None</td>
</tr>
<tr>
<td>Error</td>
<td>5/18/2010 6:10:51 PM</td>
<td>Application Error</td>
<td>1000</td>
<td>(100)</td>
</tr>
<tr>
<td>Error</td>
<td>5/18/2010 6:11:15 PM</td>
<td>Application Error</td>
<td>1000</td>
<td>(100)</td>
</tr>
<tr>
<td>Error</td>
<td>5/18/2010 6:24:17 PM</td>
<td>Application Error</td>
<td>1000</td>
<td>(100)</td>
</tr>
</tbody>
</table>
Event 1000, Application Error

Faulting application name: PDR8.exe, version: 8.0.0.2704, time stamp: 0x4b8fbf31
Faulting module name: ntdll.dll, version: 6.1.7100.0, time stamp: 0x49eea66e
Exception code: 0xc0150010
Fault offset: 0x00082dcb
Faulting process id: 0x4f8
Faulting application start time: 0x01caf6617ba83170
Faulting application path: C:\Program Files\CyberLink\PowerDirector\PDR8.exe
Faulting module path: C:\Windows\SYSTEM32\ntdll.dll
Report Id: e1a3cb25-6254-11df-9fc5-001601946950
"Event Viewer" (continued)

• Copy the text on the General tab.
• Open Notepad, paste the text, and then save the log as .txt.
• Or you can take a snapshot of the entire screen and save as a .jpg file.
"Event Viewer" (continued)

• Steps to take a screen shot:
  a) To take a screen shot, press the "Prt Scr" key on your keyboard when you encounter this error.
  b) Then go to Start > Programs > Accessories > Paint.
  c) Paste the screen captured there by pressing "Ctrl+V" or Alt+Edit+Paste.
"Event Viewer" (continued)

• d) Save the file as a .jpeg and then send it to us for analysis.
• Send the log (.txt or .jpg) to us

<End of quote>
"Task Scheduler"

- The "Task Scheduler Library" of the "Task Scheduler" lets you look at what tasks will be run at what times by third party programs: You can sometimes remove entries that have been placed here by malware!
Computer Management

File  Action  View  Help

Computer Management (Local)
- System Tools
  - Task Scheduler
  - Task Scheduler Library
- Event Viewer
- Shared Folders
- Local Users and Groups

<table>
<thead>
<tr>
<th>Name</th>
<th>Status</th>
<th>Triggers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adobe Acrobat Update Task</td>
<td>Queued</td>
<td>At logon of any user - After trigger event.</td>
</tr>
<tr>
<td>Adobe Flash Player Updater</td>
<td>Ready</td>
<td>At 7:15 PM every day - After trigger event.</td>
</tr>
</tbody>
</table>
"Task Scheduler" (continued)

- "Microsoft" submenu of the "Task Scheduler Library" lets you look at what tasks will be run at what times by the "Windows.." operating system and "Microsoft Office" programs. Do not edit these events directly: Use the graphical "Settings" or "Properties" of "Windows.." and "..Office.." instead.
"Task Scheduler" (continued)

"Task Scheduler" (continued)

"Task Scheduler" (continued)

• The use of "Task Scheduler" as an alarm clock needs to be carefully coordinated with "Power Options" in the Windows "Control Panel" to avoid conflicts. It is easier and more reliable to run an alarm clock program that knows how to over-ride the "sleep" state of "Windows..":
"Task Scheduler" (continued)

- http://freealarmclocksoftware.com/ is a great free alarm clock for "Windows."

- (The only alarm clock that works well for my Mac is Aurora which can be purchased at https://www.oneperiodic.com/products/aurora/)
"Shared Folders"

- "Shared Folders" lets you see what other computers on your local network can see when they click on your computer inside their own "Windows Explorer" or "File Explorer" applets.
"Shared Folders" (continued)

• When you install or start up "Windows.." for the first time, it has a bad habit of sharing files from inside some or all of the "User" profiles with other computers on your local network. This is done without notifying you!
"Shared Folders" (continued)

"Shared Folders" (continued)

• According to
  http://dottech.org/11324/4-ways-to-monitor-who-is-accessing-your-shared-foldersfiles/, you do the following inside "Shared Folders":
"Shared Folders" (continued)

<start of quote:>

• See all the folders they are sharing (Computer Management -> System Tools -> Shared Folders -> Shares);
"Shared Folders" (continued)

• See who (from their network) is connected to their computer (Computer Management -> System Tools -> Shared Folders -> Sessions);
"Shared Folders" (continued)

- What shared files are opened (Computer Management -> System Tools -> Shared Folders -> Open Files).
"Shared Folders" (continued)

• You also have the ability to create new shares, stop sharing specific shares, disconnect anyone connected to your computer, or disconnect access to just the opened files.
"Shared Folders" (continued)

• If you want can also right click on “Computer Management (Local)” -> “Connect to another computer” to monitor the shares of another computer (if you have access).
"Shared Folders" (continued)

- Read more at http://dottech.org/11324/4-ways-to-monitor-who-is-accessing-your-shared-foldersfiles/#bwHzz2LALHMIcpT.99
"Services" Console

- "Services" by themselves, do not use a lot of RAM and CPU cycles

- However, when you stop or disable services, you can stop and/or disable the "processes" that depend on them and these processes can result in massive savings in RAM, CPU cycles, and network bandwidth
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Status</th>
<th>Startup Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>#Id_String1.6844F930_1628_4223_B5CC_5BB9...</td>
<td></td>
<td>Started</td>
<td>Automatic</td>
</tr>
<tr>
<td>ActiveX Installer (AxInstSV)</td>
<td>Provides User Account Co...</td>
<td>Manual</td>
<td></td>
</tr>
<tr>
<td>Adaptive Brightness</td>
<td>Monitors ambient light se...</td>
<td>Manual</td>
<td></td>
</tr>
<tr>
<td>Adobe Acrobat Update Service</td>
<td>Adobe Acrobat Updater k...</td>
<td>Started</td>
<td>Automatic</td>
</tr>
<tr>
<td>Adobe Flash Player Update Service</td>
<td>This service keeps your A...</td>
<td>Manual</td>
<td></td>
</tr>
<tr>
<td>Application Experience</td>
<td>Processes application com...</td>
<td>Manual</td>
<td></td>
</tr>
<tr>
<td>Application Identity</td>
<td>Determines and verifies t...</td>
<td>Manual</td>
<td></td>
</tr>
<tr>
<td>Application Information</td>
<td>Facilitates the running of i...</td>
<td>Manual</td>
<td></td>
</tr>
<tr>
<td>Application Layer Gateway Service</td>
<td>Provides support for 3rd ...</td>
<td>Manual</td>
<td></td>
</tr>
<tr>
<td>Application Management</td>
<td>Processes installation, re...</td>
<td>Manual</td>
<td></td>
</tr>
<tr>
<td>Background Intelligent Transfer Service</td>
<td>Transfers files in the back...</td>
<td>Started</td>
<td>Automatic(D...</td>
</tr>
<tr>
<td>Base Filtering Engine</td>
<td>The Base Filtering Engine...</td>
<td>Started</td>
<td>Automatic</td>
</tr>
<tr>
<td>BitLocker Drive Encryption Service</td>
<td>BDESVC hosts the BitLock...</td>
<td>Manual</td>
<td></td>
</tr>
<tr>
<td>Block Level Backup Engine Service</td>
<td>The WBENGINE service is ...</td>
<td>Manual</td>
<td></td>
</tr>
<tr>
<td>Bluetooth Support Service</td>
<td>The Bluetooth service sup...</td>
<td>Manual</td>
<td></td>
</tr>
<tr>
<td>BranchCache</td>
<td>This service caches netw...</td>
<td>Manual</td>
<td></td>
</tr>
<tr>
<td>Certificate Propagation</td>
<td>Copies user certificates a...</td>
<td>Manual</td>
<td></td>
</tr>
<tr>
<td>CNG Key Isolation</td>
<td>The CNG key isolation ser...</td>
<td>Manual</td>
<td></td>
</tr>
<tr>
<td>COM+ Event System</td>
<td>Supports System Event N...</td>
<td>Started</td>
<td>Automatic</td>
</tr>
<tr>
<td>COM+ System Application</td>
<td>Manages the configuration...</td>
<td>Started</td>
<td>Manual</td>
</tr>
</tbody>
</table>
"Services" Console (continued)

• In addition to accessing the "Services" Microsoft Management Console from the "Services and Applications" submenu tree of "Computer Management", you can access "Services" by running "services.msc" from any "Run" box, any command prompt, or any search box inside "Windows..":

159
"Services" Console (continued)

• Step 6a: Click on the “Start” button which is located at the left or bottom of the gray "taskbar" in “Windows 7”:
"Services" Console (continued)

- Step 6b: The Windows "Start menu" will be displayed:
Step 6c: Inside the "Search" box, type services.msc
"Services" Console (continued)

- Step 6d: Press the Enter key of the keyboard.
"Services" Console (continued)

- Step 6e: If a "User Account Control" box is displayed, click on its "Yes" button:
"Services" Console (continued)

- Step 6f: A “Services” window will be displayed:
"Services" Console (continued)
"Services" Console (continued)

- Step 6g: Click on “Action” in the Menu bar
"Services" Console (continued)

- Step 6h: Click on the “Export List” in the pull-down menu:
"Services" Console (continued)

• Step 6i: Use the "Export List.." box to save the “List Report” to a location in any hard drive, giving the report an appropriate name based on the time and date. (The comma delimited .csv opens with less problems in Microsoft Excel, compared to the other available file formats.)
"Services" Console (continued)
"Services" Console (continued)
"Services" Console (continued)

• Step 6j:
  Stop and disable “services” that you do not need.
"Services" Console (continued)

• Step 6j (continued):
(Do not make any changes to the "Volume Shadow Copy" service or the "Power Service". The "Power Service" is needed by "Windows Audio" service so disabling it will cause your sound card to fail. The "IP Helper" service is needed for conventional file and printer sharing in "Windows 7" and "Windows 8".)
"Services" Console (continued)

- Step 6j (continued): Stopping and disabling the "Themes" service disables "Aerosnap", "Snap Assist", and "Aero Peak to Preview the Desktop", which is up to the individual end user.
"Services" Console (continued)

Step 6k for "Windows 7":
For documentation on what you can stop and disable in "Windows 7" see
http://svchost-exe.net/standard-windows-7-services
and
http://www.blackviper.com/2010/12/17/black-vipers-windows-7-service-pack-1-service-configurations/
and

175
DETAILS OF STEP 6:
Use “services.msc”.. (continued)

and
and
http://oakroadsystems.com/tech/7service.htm
and
http://www.computingunleashed.com/speed-up-windows-7-ultimate-guide-to.html
and
http://windows7themes.net/windows-7-services-safe-to-disable.html
DETAILS OF STEP 6:
Use “services.msc”.. (continued)

and
and
http://www.optimizingpc.com/windows7/optimizing_windows_7_services.html
and
"Services" Console (continued)

- Step 6k for "Windows XP":
  For documentation on what you can stop and disable in "Windows XP", see
  http://www.makeuseof.com/tag/winrank-speed-up-your-computer-part-1/
  and
"Services" Console (continued)

and

http://www.techknowl.com/disable-unwanted-services-and-speed-up.html and

http://www.techduke.com/2007/06/20/windows-services-background-processes-explained/ and

and
"Services" Console (continued)

and

http://www.ss64.com/nt/syntax-services.html

and


and

http://www.blackviper.com/2008/05/19/black-vipers-windows-xp-x86-32-bit-service-pack-3-service-configurations/
"Services" Console (continued)

Step 6k for **Windows 10**: For documentation on what you can stop and disable in "Windows 10", see http://www.blackviper.com/service-configurations/black-vipers-windows-10-service-configurations/ and "Tweakhound" has not posted any services.msc tweaks at https://tweakhound.com/2015/08/10/my-windows-10-tweaks/ yet
"Services" Console (continued)

- Step 6k for "Windows Vista": For documentation on what you can stop and disable, see http://www.blackviper.com/2009/05/31/black-vipers-windows-vista-service-pack-2-service-configurations/ and
"Services" Console (continued)

and
and
and
http://www.techduke.com/2007/06/20/windows-services-background-processes-explained/
"Services" Console (continued)

and
and
http://www.optimizingpc.com/vista/optimizing_windows_services.html
and
"Services" Console (continued)

and
http://www.techrepublic.com/blog/window-on-windows/tweak-windows-vista-services-the-right-way/720
and
http://smallvoid.com/articles/windows-vista/services/
"Services" Console (continued)

Step 6k for "Windows 8" and "Windows 8.1":
For documentation on what you can stop and disable, see
http://www.blackviper.com/service-configurations/black-vipers-windows-8-service-configurations/
and
http://www.tweakhound.com/2013/10/22/tweaking-windows-8-1/10/
"Services" Console (continued)

For example, to stop and disable the "Themes" service, do the following inside the "Services" box:

Example Step 1: Locate the "Themes" service:
"Services" Console (continued)

Example Step 2: Use your RIGHT mouse button to click on the "Themes" service:
"Services" Console (continued)

Example Step 3: Click on "Properties" in the pop-up context menu:
"Services" Console (continued)

Example Step 4: A "Themes Properties" box will be displayed:
Example Step 5: Click on the "Stop" button to stop the "Themes" service:
"Services" Console (continued)

Example Step 6: Click on drop-down list button to the right of "Automatic":

![Themes Properties (Local Computer) window]
"Services" Console (continued)

Example Step 7: A drop-down list will be displayed:
"Services" Console (continued)

Example Step 8: Click on "Disabled" in the drop-down list:
"Services" Console (continued)

Example Step 9: "Startup type" will now be shown as "Disabled":

![Screenshot of Themes Properties (Local Computer) dialog box with "Disabled" selected for Startup type.](image)
"Services" Console (continued)

Example Step 10: Click on the "Apply" button:
"Services" Console (continued)

Example Step 11: Click on the "OK" button to make the "..Properties.." box disappear:
"Services" Console (continued)

- Extended view versus standard view of the services.msc "Microsoft Management Console" snap-in
  
  See
  