Event Time Record ID Event ID Level Channel Provider Description Opcode Task Keywords Process ID Thread ID Computer User

13/09/2019 17:14:06.702 492 12 Information System Microsoft-Windows-Kernel-General The operating system started at system time 2019-09-13T16:14:06.375199800Z. 0x8000000000000000 4 8 Helen-PC NT AUTHORITY\SYSTEM

13/09/2019 17:14:07.030 493 6 Information System Microsoft-Windows-FilterManager File System Filter 'FileInfo' (6.1, 2009-07-14T00:34:25.000000000Z) has successfully loaded and registered with Filter Manager. 0x8000000000000000 4 8 Helen-PC NT AUTHORITY\SYSTEM

13/09/2019 17:14:07.607 4 5 Information Microsoft-Windows-Kernel-WHEA/Operational Microsoft-Windows-Kernel-WHEA "WHEA successfully initialized.

4 error sources are active

Error record format version is 10." 0x2000000000000000 4 8 Helen-PC NT AUTHORITY\SYSTEM

13/09/2019 17:14:10.088 497 41 Critical System Microsoft-Windows-Kernel-Power The system has rebooted without cleanly shutting down first. This error could be caused if the system stopped responding, crashed, or lost power unexpectedly. 63 0x8000000000000002 4 8 Helen-PC NT AUTHORITY\SYSTEM

13/09/2019 17:14:10.212 498 89 Information System Microsoft-Windows-Kernel-Power "ACPI thermal zone ACPI\ThermalZone\THRM has been enumerated.

_PSV = 383K

_TC1 = 2

_TC2 = 5

_TSP = 30000ms

_AC0 = 343K

_AC1 = 0K

_AC2 = 0K

_AC3 = 0K

_AC4 = 0K

_AC5 = 0K

_AC6 = 0K

_AC7 = 0K

_AC8 = 0K

_AC9 = 0K

_CRT = 383K

_HOT = 0K

_PSL - see event data." 86 0x8000000000000020 4 68 Helen-PC NT AUTHORITY\SYSTEM

13/09/2019 17:14:10.400 500 26 Information System Microsoft-Windows-Kernel-Processor-Power "Processor 1 in group 0 exposes the following:

2 idle state(s)

4 performance state(s)

8 throttle state(s)" 4 0x8000000000000000 4 52 Helen-PC NT AUTHORITY\SYSTEM

13/09/2019 17:14:10.400 499 26 Information System Microsoft-Windows-Kernel-Processor-Power "Processor 0 in group 0 exposes the following:

2 idle state(s)

4 performance state(s)

8 throttle state(s)" 4 0x8000000000000000 4 52 Helen-PC NT AUTHORITY\SYSTEM

13/09/2019 17:14:13.000 496 6013 Information System EventLog The system uptime is 7 seconds. Classic Helen-PC

13/09/2019 17:14:13.000 495 6005 Information System EventLog The Event log service was started. Classic Helen-PC

13/09/2019 17:14:13.000 494 6009 Information System EventLog Microsoft (R) Windows (R) 6.01. 7601 Service Pack 1 Multiprocessor Free. Classic Helen-PC

13/09/2019 17:14:13.582 502 20010 Information System Microsoft-Windows-UserPnp "One or more of the Plug and Play service's subsystems has changed state.

PlugPlay install subsystem enabled: 'true'

PlugPlay caching subsystem enabled: 'true'

" 7010 0x8000000000000000 632 648 Helen-PC NT AUTHORITY\SYSTEM

13/09/2019 17:14:13.582 501 7036 Information System Service Control Manager The Plug and Play service entered the running state. Classic 444 624 Helen-PC

13/09/2019 17:14:13.629 503 7036 Information System Service Control Manager The Power service entered the running state. Classic 444 624 Helen-PC

13/09/2019 17:14:13.660 504 6 Information System Microsoft-Windows-FilterManager File System Filter 'luafv' (6.1, 2009-07-14T00:26:13.000000000Z) has successfully loaded and registered with Filter Manager. 0x8000000000000000 4 56 Helen-PC NT AUTHORITY\SYSTEM

13/09/2019 17:14:13.676 505 7036 Information System Service Control Manager The DCOM Server Process Launcher service entered the running state. Classic 444 624 Helen-PC

13/09/2019 17:14:13.676 506 7036 Information System Service Control Manager The RPC Endpoint Mapper service entered the running state. Classic 444 624 Helen-PC

13/09/2019 17:14:13.691 507 7036 Information System Service Control Manager The Remote Procedure Call (RPC) service entered the running state. Classic 444 624 Helen-PC

13/09/2019 17:14:13.785 508 7036 Information System Service Control Manager The Windows Event Log service entered the running state. Classic 444 608 Helen-PC

13/09/2019 17:14:13.910 509 7036 Information System Service Control

Manager The Multimedia Class Scheduler service entered the running state. Classic 444 592 Helen-PC

13/09/2019 17:14:13.941 510 7036 Information System Service Control Manager The Windows Audio Endpoint Builder service entered the running state. Classic 444 608 Helen-PC

13/09/2019 17:14:14.000 226 6000 Information Application Microsoft-Windows-Winlogon The winlogon notification subscriber <SessionEnv> was unavailable to handle a notification event. Classic Helen-PC

13/09/2019 17:14:14.000 225 4101 Information Application Microsoft-Windows-Winlogon Windows license validated. Classic Helen-PC

13/09/2019 17:14:14.000 227 9003 Information Application Desktop Window Manager The Desktop Window Manager was unable to start because a composited theme is not in use Classic Helen-PC

13/09/2019 17:14:14.000 224 4625 Information Application Microsoft-Windows-EventSystem The EventSystem sub system is suppressing duplicate event log entries for a duration of 86400 seconds. The suppression timeout can be controlled by a REG_DWORD value named SuppressDuplicateDuration under the following registry key: HKLM\Software\Microsoft\EventSystem\EventLog. Classic Helen-PC

13/09/2019 17:14:14.034 511 7036 Information System Service Control Manager The Windows Audio service entered the running state. Classic 444 608 Helen-PC

13/09/2019 17:14:14.066 228 1531 Information Application Microsoft-Windows-User Profiles Service "The User Profile Service has started successfully.

" 0x8000000000000000 896 1012 Helen-PC NT AUTHORITY\SYSTEM

13/09/2019 17:14:14.066 512 7036 Information System Service Control Manager The Themes service entered the running state. Classic 444 592 Helen-PC

13/09/2019 17:14:14.066 513 7036 Information System Service Control Manager The User Profile Service service entered the running state.

Classic 444 592 Helen-PC

13/09/2019 17:14:14.081 514 7036 Information System Service Control Manager The Group Policy Client service entered the running state.
Classic 444 608 Helen-PC

13/09/2019 17:14:14.097 515 7036 Information System Service Control Manager The COM+ Event System service entered the running state.
Classic 444 592 Helen-PC

13/09/2019 17:14:14.112 517 7036 Information System Service Control Manager The Desktop Window Manager Session Manager service entered the running state. Classic 444 592 Helen-PC

13/09/2019 17:14:14.112 518 7036 Information System Service Control Manager The Security Accounts Manager service entered the running state.
Classic 444 592 Helen-PC

13/09/2019 17:14:14.112 516 7036 Information System Service Control Manager The System Event Notification Service service entered the running state.
Classic 444 592 Helen-PC

13/09/2019 17:14:14.159 520 7036 Information System Service Control Manager The CNG Key Isolation service entered the running state.
Classic 444 624 Helen-PC

13/09/2019 17:14:14.159 521 7036 Information System Service Control Manager The Network Store Interface Service service entered the running state.
Classic 444 608 Helen-PC

13/09/2019 17:14:14.159 519 7036 Information System Service Control Manager The TCP/IP NetBIOS Helper service entered the running state.
Classic 444 608 Helen-PC

13/09/2019 17:14:14.190 522 50036 Information System Microsoft-Windows-Dhcp-Client DHCPv4 client service is started ServiceStart (68) Service State Event (4) 0x2000000000000000 772 272 Helen-PC NT AUTHORITY \LOCAL SERVICE

13/09/2019 17:14:14.206 523 51046 Information System Microsoft-Windows-DHCPv6-Client DHCPv6 client service is started ServiceStart (62)
Service State Event (4) 0x2000000000000000 772 576 Helen-PC NT AUTHORITY\LOCAL SERVICE

13/09/2019 17:14:14.206 524 7036 Information System Service Control Manager The Extensible Authentication Protocol service entered the running state.

Classic 444 608 Helen-PC

13/09/2019 17:14:14.206 525 7036 Information System Service Control Manager The DHCP Client service entered the running state.
Classic 444 608 Helen-PC

13/09/2019 17:14:14.268 526 7036 Information System Service Control Manager The DNS Client service entered the running state.
Classic 444 624 Helen-PC

13/09/2019 17:14:14.300 527 7036 Information System Service Control Manager The WLAN AutoConfig service entered the running state.
Classic 444 608 Helen-PC

13/09/2019 17:14:14.300 528 4000 Information System Microsoft-Windows-WLAN-AutoConfig "WLAN AutoConfig service has successfully started.

" Start (1) 0x4000000000000000 852 904 Helen-PC NT AUTHORITY\SYSTEM

13/09/2019 17:14:14.440 529 7036 Information System Service Control Manager The Shell Hardware Detection service entered the running state.
Classic 444 624 Helen-PC

13/09/2019 17:14:14.534 530 7001 Information System Microsoft-Windows-Winlogon User Logon Notification for Customer Experience Improvement Program 1101 0x2000000000000000 484 516 Helen-PC NT AUTHORITY\SYSTEM

13/09/2019 17:14:14.549 11 1 Information Microsoft-Windows-User Profile Service/Operational Microsoft-Windows-User Profiles Service Recieved user logon notification on session 1. 0x4000000000000000 896 264
Helen-PC Helen-PC\Helen

13/09/2019 17:14:14.565 13 5 Information Microsoft-Windows-User Profile Service/Operational Microsoft-Windows-User Profiles Service Registry file C:\Users\Helen\AppData\Local\Microsoft\Windows\\UsrClass.dat is loaded at HKU \S-1-5-21-954126658-284120372-3882474944-1000_Classes.
0x4000000000000000 896 920 Helen-PC NT AUTHORITY\SYSTEM

13/09/2019 17:14:14.565 12 5 Information Microsoft-Windows-User Profile Service/Operational Microsoft-Windows-User Profiles Service Registry file C:\Users\Helen\ntuser.dat is loaded at HKU \S-1-5-21-954126658-284120372-3882474944-1000.
0x4000000000000000 896 920 Helen-PC NT AUTHORITY\SYSTEM

13/09/2019 17:14:14.612 6 21 Information Microsoft-Windows-

TerminalServices-LocalSessionManager/Operational Microsoft-Windows-TerminalServices-LocalSessionManager "Remote Desktop Services: Session logon succeeded:

User: Helen-PC\Helen

Session ID: 1

Source Network Address: LOCAL" 0x1000000000000000 492 768 Helen-PC NT AUTHORITY\SYSTEM

13/09/2019 17:14:14.612 14 2 Information Microsoft-Windows-User Profile Service/Operational Microsoft-Windows-User Profiles Service Finished processing user logon notification on session 1. 0x4000000000000000 896 264 Helen-PC Helen-PC\Helen

13/09/2019 17:14:14.612 531 7036 Information System Service Control Manager The Task Scheduler service entered the running state. Classic 444 592 Helen-PC

13/09/2019 17:14:14.752 7 22 Information Microsoft-Windows-TerminalServices-LocalSessionManager/Operational Microsoft-Windows-TerminalServices-LocalSessionManager "Remote Desktop Services: Shell start notification received:

User: Helen-PC\Helen

Session ID: 1

Source Network Address: LOCAL" 0x1000000000000000 492 784 Helen-PC NT AUTHORITY\SYSTEM

13/09/2019 17:14:14.799 532 7036 Information System Service Control Manager The Print Spooler service entered the running state. Classic 444 624 Helen-PC

13/09/2019 17:14:15.000 229 5615 Undefined Application Microsoft-Windows-WMI Windows Management Instrumentation Service started sucessfully Classic Helen-PC

13/09/2019 17:14:15.064 533 7036 Information System Service Control Manager The Base Filtering Engine service entered the running state. Classic 444 624 Helen-PC

13/09/2019 17:14:15.298 534 7036 Information System Service Control Manager The Windows Firewall service entered the running state. Classic 444 624 Helen-PC

13/09/2019 17:14:15.314 535 7036 Information System Service Control Manager The Workstation service entered the running state. Classic 444 624 Helen-PC

13/09/2019 17:14:15.360 536 7036 Information System Service Control Manager The Cryptographic Services service entered the running state. Classic 444 624 Helen-PC

13/09/2019 17:14:15.423 537 201 Information System Microsoft-Windows-Application-Experience The Program Compatibility Assistant service started successfully. 0x8000000000000000 852 1396 Helen-PC NT AUTHORITY\SYSTEM

13/09/2019 17:14:15.438 538 7036 Information System Service Control Manager The Program Compatibility Assistant Service service entered the running state. Classic 444 624 Helen-PC

13/09/2019 17:14:15.470 539 7036 Information System Service Control Manager The Diagnostic Policy Service service entered the running state. Classic 444 624 Helen-PC

13/09/2019 17:14:15.485 540 7036 Information System Service Control Manager The Superfetch service entered the running state. Classic 444 592 Helen-PC

13/09/2019 17:14:15.563 541 7036 Information System Service Control Manager The Distributed Link Tracking Client service entered the running state. Classic 444 604 Helen-PC

13/09/2019 17:14:15.579 542 7036 Information System Service Control Manager The Windows Management Instrumentation service entered the running state. Classic 444 592 Helen-PC

13/09/2019 17:14:15.626 543 7036 Information System Service Control Manager The IP Helper service entered the running state. Classic 444 620 Helen-PC

13/09/2019 17:14:15.750 544 7036 Information System Service Control Manager The Network Location Awareness service entered the running state. Classic 444 592 Helen-PC

13/09/2019 17:14:15.844 545 7036 Information System Service Control Manager The Server service entered the running state. Classic 444

592 Helen-PC

13/09/2019 17:14:15.922 546 7036 Information System Service Control Manager The Diagnostic Service Host service entered the running state.
Classic 444 592 Helen-PC

13/09/2019 17:14:15.953 547 7036 Information System Service Control Manager The Diagnostic System Host service entered the running state.
Classic 444 604 Helen-PC

13/09/2019 17:14:15.969 548 7036 Information System Service Control Manager The Application Experience service entered the running state.
Classic 444 604 Helen-PC

13/09/2019 17:14:15.984 549 7036 Information System Service Control Manager The Network List Service service entered the running state.
Classic 444 604 Helen-PC

13/09/2019 17:14:16.000 230 5617 Undefined Application Microsoft-Windows-WMI Windows Management Instrumentation Service subsystems initialized successfully Classic Helen-PC

13/09/2019 17:14:16.062 3 1001 Information Microsoft-Windows-Resource-Exhaustion-Detector/Operational Microsoft-Windows-Resource-Exhaustion-Detector The Windows Resource Exhaustion Detector started. Events logged when the resource exhaustion detector is started. (11) Lifecycle Events (1) Events related to lifecycle of resource exhaustion detector. 1220 1592 Helen-PC NT AUTHORITY\LOCAL SERVICE

13/09/2019 17:14:16.109 550 7036 Information System Service Control Manager The Portable Device Enumerator Service service entered the running state.
Classic 444 604 Helen-PC

13/09/2019 17:14:16.780 551 20003 Information System Microsoft-Windows-UserPnp Driver Management has concluded the process to add Service tunnel for Device Instance ID ROOT*ISATAP\0001 with the following status: 0.
7005 0x8000000000000000 896 916 Helen-PC NT AUTHORITY\SYSTEM

13/09/2019 17:14:17.000 231 102 Information Application ESENT
WinMail (1924) WindowsMail0: The database engine (6.01.7601.0000) started a new instance (0). General (1) Classic Helen-PC

13/09/2019 17:14:18.000 235 223 Information Application ESENT
WinMail (1924) WindowsMail0: Starting the backup of log files (range C:\Users\Helen\AppData\Local\Microsoft\Windows Mail\edb00003.log - C:\Users\Helen\AppData

\Local\Microsoft\Windows Mail\edb00003.log). Logging/Recovery (3) Classic Helen-PC

13/09/2019 17:14:18.000 236 224 Information Application ESENT WinMail (1924) WindowsMail0: Deleting log files C:\Users\Helen\AppData\Local \Microsoft\Windows Mail\edb00002.log to C:\Users\Helen\AppData\Local\Microsoft \Windows Mail\edb00002.log. Logging/Recovery (3) Classic Helen-PC

13/09/2019 17:14:18.000 237 213 Information Application ESENT WinMail (1924) WindowsMail0: The backup procedure has been successfully completed. Logging/Recovery (3) Classic Helen-PC

13/09/2019 17:14:18.000 233 220 Information Application ESENT WinMail (1924) WindowsMail0: Beginning the backup of the file C:\Users\Helen \AppData\Local\Microsoft\Windows Mail\WindowsMail.MSMessageStore (size 2 Mb). Logging/Recovery (3) Classic Helen-PC

13/09/2019 17:14:18.000 232 210 Information Application ESENT WinMail (1924) WindowsMail0: A full backup is starting. Logging/Recovery (3) Classic Helen-PC

13/09/2019 17:14:18.000 234 221 Information Application ESENT WinMail (1924) WindowsMail0: Ending the backup of the file C:\Users\Helen \AppData\Local\Microsoft\Windows Mail\WindowsMail.MSMessageStore. Logging/Recovery (3) Classic Helen-PC

13/09/2019 17:14:18.122 552 7036 Information System Service Control Manager The Protected Storage service entered the running state. Classic 444 616 Helen-PC

13/09/2019 17:14:23.000 238 103 Information Application ESENT WinMail (1924) WindowsMail0: The database engine stopped the instance (0). General (1) Classic Helen-PC

13/09/2019 17:14:23.566 42 2011 Information Microsoft-Windows-Windows Firewall With Advanced Security/Firewall Microsoft-Windows-Windows Firewall With Advanced Security "Windows Firewall was unable to notify the user that it blocked an application from accepting incoming connections on the network.

Reason: The application is a system service

Application Path: C:\windows\system32\lsass.exe

IP Version: IPv6

Protocol: TCP

Port: 49156

Process Id: 460

User: S-1-5-18" 0x8000000000000000 1220 1344 Helen-PC NT AUTHORITY\LOCAL SERVICE

13/09/2019 17:14:24.000 239 102 Information Application ESENT Windows (888) Windows: The database engine (6.01.7601.0000) started a new instance (0). General (1) Classic Helen-PC

13/09/2019 17:14:24.000 243 1003 Information Application Microsoft-Windows-Search "The Windows Search Service started.

" Search service (1) Classic Helen-PC

13/09/2019 17:14:24.000 242 302 Information Application ESENT Windows (888) Windows: The database engine has successfully completed recovery steps. Logging/Recovery (3) Classic Helen-PC

13/09/2019 17:14:24.000 241 301 Information Application ESENT Windows (888) Windows: The database engine has begun replaying logfile C:\ProgramData\Microsoft\Search\Data\Applications\Windows\MSS.log. Logging/Recovery (3) Classic Helen-PC

13/09/2019 17:14:24.000 240 300 Information Application ESENT Windows (888) Windows: The database engine is initiating recovery steps. Logging/Recovery (3) Classic Helen-PC

13/09/2019 17:14:24.564 553 7036 Information System Service Control Manager The Windows Search service entered the running state. Classic 444 588 Helen-PC

13/09/2019 17:14:25.000 244 102 Information Application ESENT WinMail (1912) WindowsMail0: The database engine (6.01.7601.0000) started a new instance (0). General (1) Classic Helen-PC

13/09/2019 17:14:26.000 245 103 Information Application ESENT WinMail (1912) WindowsMail0: The database engine stopped the instance (0). General (1) Classic Helen-PC

13/09/2019 17:14:34.862 554 7036 Information System Service Control Manager The Network Connections service entered the running state.

Classic 444 588 Helen-PC

13/09/2019 17:14:35.000 246 3036 Warning Application Microsoft-Windows-Search "The content source <C:\ProgramData\Microsoft\Windows\Start Menu\> cannot be accessed.

Context: Application, SystemIndex Catalog

Details:

The URL was already processed during this update. If you received this message while processing alerts, then the alerts are redundant, or else Modify should be used instead of Add. (HRESULT : 0x80040d0d) (0x80040d0d)

" Gatherer (3) Classic Helen-PC

13/09/2019 17:15:07.044 4 1015 Information Microsoft-Windows-ReadyBoost/Operational Microsoft-Windows-ReadyBoost "Summary of ReadyBoot Performance:

Io Read Count: 15477

Io Read Bytes: 286008320

Cache Hit Count: 12779

Cache Hit Bytes: 206495232

Cache Hit Percentage: 0.825676810751438

Boot Prefetch Time (us): 6141029

Boot Prefetch Bytes: 631549952

Boot Prefetch Read Count: 12903

" 1016 0x8000000000002000 852 2016 Helen-PC NT AUTHORITY\SYSTEM

13/09/2019 17:15:07.481 5 1016 Information Microsoft-Windows-ReadyBoost/Operational Microsoft-Windows-ReadyBoost "Boot plan calculation completed in 1748 ms.

Boot Plan Timestamp: 2019-09-13T17:15:05.734502800Z

Reason: System boot completion

Result: 0x0" 1016 0x8000000000002000 852 2016 Helen-PC NT AUTHORITY\SYSTEM

13/09/2019 17:15:47.121 9 100 Information Microsoft-Windows-Diagnosis-DPS/Operational Microsoft-Windows-Diagnosis-DPS Diagnostic module {C8544339-5BE9-4F25-862E-485F1B1A6935} (%SystemRoot%\system32\diagperf.dll) detected a problem for scenario {86432A0B-3C7D-4DDF-A89C-172FAA90485D}, instance {7C78A59D-7E7B-4F23-8903-224B4FB3734B}, original activity ID {86432A0B-3C7D-4DDF-A89C-172FAA90485D}. A diagnostic module detected a problem (12) Scenario Lifecycle (1) Scenario lifecycle events 1220 1728 Helen-PC NT AUTHORITY\LOCAL SERVICE

13/09/2019 17:15:47.121 10 105 Information Microsoft-Windows-Diagnosis-DPS/Operational Microsoft-Windows-Diagnosis-DPS Diagnostic module {C8544339-5BE9-4F25-862E-485F1B1A6935} (%SystemRoot%\system32\diagperf.dll) started troubleshooting scenario {86432A0B-3C7D-4DDF-A89C-172FAA90485D}, instance {7C78A59D-7E7B-4F23-8903-224B4FB3734B}, original activity ID {86432A0B-3C7D-4DDF-A89C-172FAA90485D}. A scenario instance was dispatched for troubleshooting (13) Scenario Lifecycle (1) Scenario lifecycle events 1220 1728 Helen-PC NT AUTHORITY\LOCAL SERVICE

13/09/2019 17:15:47.433 11 110 Information Microsoft-Windows-Diagnosis-DPS/Operational Microsoft-Windows-Diagnosis-DPS Diagnostic module {C8544339-5BE9-4F25-862E-485F1B1A6935} (%SystemRoot%\system32\diagperf.dll) finished troubleshooting scenario {86432A0B-3C7D-4DDF-A89C-172FAA90485D}, instance {7C78A59D-7E7B-4F23-8903-224B4FB3734B}, original activity ID {86432A0B-3C7D-4DDF-A89C-172FAA90485D}. No resolution was set by the diagnostic module.A diagnostic module completed troubleshooting without setting a resolution (14) Scenario Lifecycle (1) Scenario lifecycle events 1220 1728 Helen-PC NT AUTHORITY\LOCAL SERVICE

13/09/2019 17:16:05.000 247 10 Error Application Microsoft-Windows-WMI Event filter with query "SELECT * FROM __InstanceModificationEvent WITHIN 60 WHERE TargetInstance ISA "Win32_Processor" AND TargetInstance.LoadPercentage > 99" could not be reactivated in namespace "//./root/CIMV2" because of error 0x80041003. Events cannot be delivered through this filter until the problem is corrected. Classic Helen-PC

13/09/2019 17:16:14.889 3 823 Information Microsoft-Windows-PrintService/Admin Microsoft-Windows-PrintService The default printer was changed to Microsoft XPS Document Writer,winspool,Ne00:. See the event user data for context information. Spooler Operation Succeeded (11) Changing the default printer (49) Print Spooler 1100 1188 Helen-PC NT AUTHORITY\SYSTEM

13/09/2019 17:16:15.997 555 7036 Information System Service Control Manager The Background Intelligent Transfer Service service entered the running state. Classic 444 588 Helen-PC

13/09/2019 17:16:16.000 249 1 Information Application SecurityCenter The Windows Security Center Service has started. Classic Helen-PC

13/09/2019 17:16:16.000 248 900 Information Application Microsoft-Windows-Security-SPP "The Software Protection service is starting.

" Classic Helen-PC

13/09/2019 17:16:16.199 556 7036 Information System Service Control Manager The Portable Device Enumerator Service service entered the stopped state. Classic 444 588 Helen-PC

13/09/2019 17:16:16.215 557 7036 Information System Service Control Manager The Windows Font Cache Service service entered the running state. Classic 444 588 Helen-PC

13/09/2019 17:16:16.262 558 7036 Information System Service Control Manager The SSDP Discovery service entered the running state. Classic 444 588 Helen-PC

13/09/2019 17:16:16.340 559 7036 Information System Service Control Manager The Software Protection service entered the running state. Classic 444 588 Helen-PC

13/09/2019 17:16:16.574 560 7036 Information System Service Control Manager The Windows Defender service entered the running state. Classic 444 588 Helen-PC

13/09/2019 17:16:16.589 2 306 Verbose Microsoft-Windows-Bits-Client/Operational Microsoft-Windows-Bits-Client The BITS service loaded the job list from disk. 0x4000000000000000 896 200 Helen-PC NT AUTHORITY\SYSTEM

13/09/2019 17:16:16.823 561 7036 Information System Service Control Manager The Security Center service entered the running state. Classic 444 588 Helen-PC

13/09/2019 17:16:16.964 6 101 Undefined Microsoft-Windows-Windows Defender/WHC Microsoft-Windows-Windows Defender Windows Defender state updated to 10. 0x4000000000000000 1500 1272 Helen-PC NT AUTHORITY\SYSTEM

13/09/2019 17:16:17.000 250 1066 Information Application Microsoft-Windows-Security-SPP "Initialization status for service objects.

C:\Windows\system32\sppwinob.dll, msft:spp/windowsfunctionality/agent/7.0, 0x00000000, 0x00000000

C:\Windows\system32\sppobjs.dll, msft:rm/algorithm/phone/1.0, 0x00000000, 0x00000000

C:\Windows\system32\sppobjs.dll, msft:rm/algorithm/pkey/2005, 0x00000000, 0x00000000

C:\Windows\system32\sppobjs.dll, msft:spp/TaskScheduler/1.0, 0x00000000, 0x00000000

C:\Windows\system32\sppobjs.dll, msft:spp/volume/services/kms/1.0, 0x00000000, 0x00000000

C:\Windows\system32\sppobjs.dll, msft:spp/volume/services/kms/licenserenewal/1.0, 0x00000000, 0x00000000

" Classic Helen-PC

13/09/2019 17:16:18.000 251 1003 Information Application Microsoft-Windows-Security-SPP "The Software Protection service has completed licensing status check.

Application Id=55c92734-d682-4d71-983e-d6ec3f16059f

Licensing Status=

1: 01f5fc37-a99e-45c5-b65e-d762f3518ead, 1, 0 [(0 [0xC004F014, 0, 0], [(?)(?)(?)(?)(?)(?)]) (1)(2)]

2: 2e7d060d-4714-40f2-9896-1e4f15b612ad, 1, 1 [(0)(1)(2 [0x00000000, 0, 1], [(?)(5 0x00000000 30 33480)(1 0x00000000 0 0 msft:rm/algorithm/flags/1.0 0x00000000 0)(?)(?)(?)])]

3: 3b965dfc-31d9-4903-886f-873a0382776c, 1, 0 [(0 [0xC004F014, 0, 0], [(?)(?)(?)(?)(?)(?)]) (1)(2)]

4: 586bc076-c93d-429a-afe5-a69fbc644e88, 1, 0 [(0 [0xC004F014, 0, 0], [(?)(?)(?)(?)(?)(?)]) (1)(2)]

5: 5e017a8a-f3f9-4167-b1bd-ba3e236a4d8f, 1, 0 [(0 [0xC004F014, 0, 0], [(?)(?)(?)(?)(?)(?)]) (1)(2)]

6: 5e35dc43-389b-47c5-b889-2088b06738cb, 1, 0 [(0 [0xC004F014, 0, 0], [(?)(?)(?)(?)(?)(?)]) (1)(2)]

7: 6a7d5d8a-92af-4e6a-af4b-8fddaec800e5, 1, 0 [(0 [0xC004F014, 0, 0], [(?)(?)(?)(?)(?)(?)]) (1)(2)]

8: 9ab82e0c-ffc9-4107-baa1-c65a8bd3ccc3, 1, 0 [(0 [0xC004F014, 0, 0], [(?)(?)(?)(?)(?)(?)]) (1)(2)]

9: 9f83d90f-a151-4665-ae69-30b3f63ec659, 1, 0 [(0 [0xC004F014, 0, 0], [(?)(?)(?)(?)(?)(?)]) (1)(2)]

10: a63275f4-530c-48a7-b0d3-4f00d688d151, 1, 0 [(0 [0xC004F014, 0, 0], [(?)(?)(?)(?)(?)(?)]) (1)(2)]

11: b8a4bb91-69b1-460d-93f8-40e0670af04a, 1, 0 [(0 [0xC004F014, 0, 0], [(?)(?)(?)(?)(?)(?)]) (1)(2)]

12: d2c04e90-c3dd-4260-b0f3-f845f5d27d64, 1, 0 [(0 [0xC004F014, 0, 0], [(?)(?)(?)(?)(?)(?)]) (1)(2)]

13: e68b141f-4dfa-4387-b3b7-e65c4889216e, 1, 0 [(0 [0xC004F014, 0, 0], [(?)(?)(?)(?)(?)(?)]) (1)(2)]

14: ee4e1629-bcdc-4b42-a68f-b92e135f78d7, 1, 0 [(0 [0xC004F014, 0, 0], [(?)(?)(?)(?)(?)(?)]) (1)(2)]

15: 4a8149bb-7d61-49f4-8822-82c7bf88d64b, 1, 0 [(0 [0xC004F014, 0, 0], [(?)(?)(?)(?)(?)(?)]) (1)(2)]

16: afd5f68f-b70f-4000-a21d-28dbc8be8b07, 1, 0 [(0 [0xC004F014, 0, 0], [(?)(?)(?)(?)(?)(?)]) (1)(2)]

" Classic Helen-PC

13/09/2019 17:16:18.000 252 902 Undefined Application Microsoft-Windows-Security-SPP "The Software Protection service has started.

6.1.7601.17514" Classic Helen-PC

13/09/2019 17:16:18.820 562 7036 Information System Service Control Manager The Windows Update service entered the running state.
Classic 444 612 Helen-PC

13/09/2019 17:16:21.363 7 101 Undefined Microsoft-Windows-Windows Defender/WHC Microsoft-Windows-Windows Defender Windows Defender state updated to 10. 0x4000000000000000 1500 1532 Helen-PC
NT AUTHORITY\SYSTEM

13/09/2019 17:16:28.945 1 101 Information Microsoft-Windows-

Diagnosis-Scripted/Operational Microsoft-Windows-Diagnosis-Scripted The scripted diagnostic engine started initializing a diagnostic package located at C:\Windows\diagnostics\system\networking. Lifecycle Keyword 2192 2196 Helen-PC Helen-PC\Helen

13/09/2019 17:16:29.303 2 102 Information Microsoft-Windows-Diagnosis-Scripted/Operational Microsoft-Windows-Diagnosis-Scripted The scripted diagnostic engine completed initializing a diagnostic package located at C:\Windows\diagnostics\system\networking. Lifecycle Keyword 2192 2196 Helen-PC Helen-PC\Helen

13/09/2019 17:16:29.303 1 1 Information Microsoft-Windows-Diagnosis-Scripted/Admin Microsoft-Windows-Diagnosis-Scripted The scripted diagnostic engine executed a diagnostic package located at C:\Windows\diagnostics\system\networking with ID NetworkDiagnostics. Admin Keyword2192 2196 Helen-PC Helen-PC\Helen

13/09/2019 17:16:29.350 3 103 Information Microsoft-Windows-Diagnosis-Scripted/Operational Microsoft-Windows-Diagnosis-Scripted The scripted diagnostic engine started diagnosing the diagnostic package NetworkDiagnostics. Lifecycle Keyword 2192 2208 Helen-PC Helen-PC\Helen

13/09/2019 17:16:41.113 4 201 Error Microsoft-Windows-Diagnosis-Scripted/Operational Microsoft-Windows-Diagnosis-Scripted The scripted diagnostic engine has encountered an error 0x803C0100. Lifecycle Keyword 2192 2208 Helen-PC Helen-PC\Helen

13/09/2019 17:17:09.130 4 42 Information Microsoft-Windows-WindowsUpdateClient/Operational Microsoft-Windows-WindowsUpdateClient There has been a change in the health of Windows Update. Other (18) Automatic Updates (2) State 896 2512 Helen-PC NT AUTHORITY\SYSTEM

13/09/2019 17:17:09.130 6 29 Warning Microsoft-Windows-WindowsUpdateClient/Operational Microsoft-Windows-WindowsUpdateClient Windows Update lost connectivity. State Change (17) Windows Update Agent (1) Connection 896 2512 Helen-PC NT AUTHORITY\SYSTEM

13/09/2019 17:17:09.130 5 42 Information Microsoft-Windows-WindowsUpdateClient/Operational Microsoft-Windows-WindowsUpdateClient There has been a change in the health of Windows Update. Other (18) Automatic Updates (2) State 896 2512 Helen-PC NT AUTHORITY\SYSTEM

13/09/2019 17:17:21.724 563 7036 Information System Service Control Manager The Windows Modules Installer service entered the running state.

Classic 444 612 Helen-PC

13/09/2019 17:17:27.247 12 1002 Warning Microsoft-Windows-Known Folders API Service Microsoft-Windows-KnownFolders Error 0x80070002 occurred while verifying known folder {1777F761-68AD-4D8A-87BD-30B759FA33DD} with path 'C:\Windows\system32\config\systemprofile\Favorites'.
0x8000000000000000 888 1660 Helen-PC NT AUTHORITY\SYSTEM

13/09/2019 17:17:27.247 13 1002 Warning Microsoft-Windows-Known Folders API Service Microsoft-Windows-KnownFolders Error 0x80070002 occurred while verifying known folder {625B53C3-AB48-4EC1-BA1F-A1EF4146FC19} with path 'C:\Windows\system32\config\systemprofile\AppData\Roaming\Microsoft\Windows\Start Menu'. 0x8000000000000000 888 1660 Helen-PC NT AUTHORITY\SYSTEM

13/09/2019 17:17:27.247 14 1002 Warning Microsoft-Windows-Known Folders API Service Microsoft-Windows-KnownFolders Error 0x80070002 occurred while verifying known folder {FDD39AD0-238F-46AF-ADB4-6C85480369C7} with path 'C:\Windows\system32\config\systemprofile\Documents'.
0x8000000000000000 888 1660 Helen-PC NT AUTHORITY\SYSTEM

13/09/2019 17:17:27.247 15 1002 Warning Microsoft-Windows-Known Folders API Service Microsoft-Windows-KnownFolders Error 0x80070002 occurred while verifying known folder {B4BFCC3A-DB2C-424C-B029-7FE99A87C641} with path 'C:\Windows\system32\config\systemprofile\Desktop'.
0x8000000000000000 888 1660 Helen-PC NT AUTHORITY\SYSTEM

13/09/2019 17:17:36.794 16 1002 Warning Microsoft-Windows-Known Folders API Service Microsoft-Windows-KnownFolders Error 0x80070002 occurred while verifying known folder {B4BFCC3A-DB2C-424C-B029-7FE99A87C641} with path 'C:\Windows\system32\config\systemprofile\Desktop'.
0x8000000000000000 1476 1808 Helen-PC NT AUTHORITY\SYSTEM

13/09/2019 17:17:38.557 17 1002 Warning Microsoft-Windows-Known Folders API Service Microsoft-Windows-KnownFolders Error 0x80070002 occurred while verifying known folder {AE50C081-EBD2-438A-8655-8A092E34987A} with path 'C:\Windows\system32\config\systemprofile\AppData\Roaming\Microsoft\Windows\Recent'.
0x8000000000000000 1476 1808 Helen-PC NT AUTHORITY\SYSTEM

13/09/2019 17:18:23.454 253 1001 Information Application Microsoft-Windows-LoadPerf Performance counters for the WmiApRpl (WmiApRpl) service were removed successfully. The Record Data contains the new values of the system Last Counter and Last Help registry entries. 0x8000000000000000 3068 412
Helen-PC NT AUTHORITY\SYSTEM

13/09/2019 17:18:23.532 254 1000 Information Application Microsoft-Windows-LoadPerf Performance counters for the WmiApRpl (WmiApRpl) service were loaded successfully. The Record Data in the data section contains the new index values assigned to this service. 0x8000000000000000 3068 412 Helen-PC NT AUTHORITY\SYSTEM

14/09/2019 10:28:06.702 564 12 Information System Microsoft-Windows-Kernel-General The operating system started at system time 2019-09-14T09:28:06.375199800Z. 0x8000000000000000 4 8 Helen-PC NT AUTHORITY\SYSTEM

14/09/2019 10:28:07.030 565 6 Information System Microsoft-Windows-FilterManager File System Filter 'FileInfo' (6.1, 2009-07-14T00:34:25.000000000Z) has successfully loaded and registered with Filter Manager. 0x8000000000000000 4 8 Helen-PC NT AUTHORITY\SYSTEM

14/09/2019 10:28:10.088 570 41 Critical System Microsoft-Windows-Kernel-Power The system has rebooted without cleanly shutting down first. This error could be caused if the system stopped responding, crashed, or lost power unexpectedly. 63 0x8000000000000002 4 8 Helen-PC NT AUTHORITY\SYSTEM

14/09/2019 10:28:10.322 571 26 Information System Microsoft-Windows-Kernel-Processor-Power "Processor 0 in group 0 exposes the following:

2 idle state(s)

4 performance state(s)

8 throttle state(s)" 4 0x8000000000000000 4 52 Helen-PC NT AUTHORITY\SYSTEM

14/09/2019 10:28:10.322 572 26 Information System Microsoft-Windows-Kernel-Processor-Power "Processor 1 in group 0 exposes the following:

2 idle state(s)

4 performance state(s)

8 throttle state(s)" 4 0x8000000000000000 4 52 Helen-PC NT AUTHORITY\SYSTEM

14/09/2019 10:28:10.743 573 89 Information System Microsoft-Windows-Kernel-Power "ACPI thermal zone ACPI\ThermalZone\THRM has been

enumerated.

_PSV = 383K

_TC1 = 2

_TC2 = 5

_TSP = 30000ms

_AC0 = 343K

_AC1 = 0K

_AC2 = 0K

_AC3 = 0K

_AC4 = 0K

_AC5 = 0K

_AC6 = 0K

_AC7 = 0K

_AC8 = 0K

_AC9 = 0K

_CRT = 383K

_HOT = 0K

_PSL - see event data." 86 0x8000000000000020 4 64 Helen-PC
NT AUTHORITY\SYSTEM

14/09/2019 10:28:13.000 567 6009 Information System EventLog
Microsoft (R) Windows (R) 6.01. 7601 Service Pack 1 Multiprocessor Free.
Classic Helen-PC

14/09/2019 10:28:13.000 566 6008 Error System EventLog The previous system shutdown at 17:19:10 on 13/09/2019 was unexpected.
Classic Helen-PC

14/09/2019 10:28:13.000 569 6013 Information System EventLog The system uptime is 7 seconds. Classic Helen-PC

14/09/2019 10:28:13.000 568 6005 Information System EventLog The Event log service was started. Classic Helen-PC

14/09/2019 10:28:13.551 575 20010 Information System Microsoft-Windows-UserPnp "One or more of the Plug and Play service's subsystems has changed state.

PlugPlay install subsystem enabled: 'true'

PlugPlay caching subsystem enabled: 'true'

" 7010 0x8000000000000000 600 620 Helen-PC NT AUTHORITY\SYSTEM

14/09/2019 10:28:13.551 574 7036 Information System Service Control Manager The Plug and Play service entered the running state.
Classic 440 584 Helen-PC

14/09/2019 10:28:13.613 576 7036 Information System Service Control Manager The Power service entered the running state. Classic 440
584 Helen-PC

14/09/2019 10:28:13.629 577 6 Information System Microsoft-Windows-FilterManager File System Filter 'luafv'
(6.1, 2009-07-14T00:26:13.000000000Z) has successfully loaded and registered with Filter Manager. 0x8000000000000000 4 68 Helen-PC NT AUTHORITY\SYSTEM

14/09/2019 10:28:13.644 578 7036 Information System Service Control Manager The DCOM Server Process Launcher service entered the running state.
Classic 440 584 Helen-PC

14/09/2019 10:28:13.660 579 7036 Information System Service Control Manager The RPC Endpoint Mapper service entered the running state.
Classic 440 584 Helen-PC

14/09/2019 10:28:13.676 580 7036 Information System Service Control Manager The Remote Procedure Call (RPC) service entered the running state.
Classic 440 584 Helen-PC

14/09/2019 10:28:13.754 581 7036 Information System Service Control Manager The Windows Event Log service entered the running state.
Classic 440 588 Helen-PC

14/09/2019 10:28:13.878 582 7036 Information System Service Control Manager The Multimedia Class Scheduler service entered the running state.

Classic 440 588 Helen-PC

14/09/2019 10:28:13.925 583 7036 Information System Service Control Manager The Windows Audio Endpoint Builder service entered the running state. Classic 440 724 Helen-PC

14/09/2019 10:28:14.000 255 4625 Information Application Microsoft-Windows-EventSystem The EventSystem sub system is suppressing duplicate event log entries for a duration of 86400 seconds. The suppression timeout can be controlled by a REG_DWORD value named SuppressDuplicateDuration under the following registry key: HKLM\Software\Microsoft\EventSystem\EventLog. Classic Helen-PC

14/09/2019 10:28:14.000 257 6000 Information Application Microsoft-Windows-Winlogon The winlogon notification subscriber <SessionEnv> was unavailable to handle a notification event. Classic Helen-PC

14/09/2019 10:28:14.000 256 4101 Information Application Microsoft-Windows-Winlogon Windows license validated. Classic Helen-PC

14/09/2019 10:28:14.034 585 7036 Information System Service Control Manager The Themes service entered the running state. Classic 440 588 Helen-PC

14/09/2019 10:28:14.034 584 7036 Information System Service Control Manager The Windows Audio service entered the running state. Classic 440 588 Helen-PC

14/09/2019 12:06:34.702 586 12 Information System Microsoft-Windows-Kernel-General The operating system started at system time 2019-09-14T11:06:34.375199800Z. 0x8000000000000000 4 8 Helen-PC NT AUTHORITY\SYSTEM

14/09/2019 12:06:35.030 591 6 Information System Microsoft-Windows-FilterManager File System Filter 'FileInfo' (6.1, 2009-07-14T00:34:25.000000000Z) has successfully loaded and registered with Filter Manager. 0x8000000000000000 4 8 Helen-PC NT AUTHORITY\SYSTEM

14/09/2019 12:06:35.685 5 5 Information Microsoft-Windows-Kernel-WHEA/Operational Microsoft-Windows-Kernel-WHEA "WHEA successfully initialized.

4 error sources are active

Error record format version is 10." 0x2000000000000000 4 8 Helen-PC NT AUTHORITY\SYSTEM

14/09/2019 12:06:38.150 592 41 Critical System Microsoft-Windows-Kernel-Power The system has rebooted without cleanly shutting down first. This error could be caused if the system stopped responding, crashed, or lost power unexpectedly. 63 0x8000000000000002 4 8 Helen-PC NT AUTHORITY\SYSTEM

14/09/2019 12:06:38.228 593 89 Information System Microsoft-Windows-Kernel-Power "ACPI thermal zone ACPI\ThermalZone\THRM has been enumerated.

_PSV = 383K

_TC1 = 2

_TC2 = 5

_TSP = 30000ms

_AC0 = 343K

_AC1 = 0K

_AC2 = 0K

_AC3 = 0K

_AC4 = 0K

_AC5 = 0K

_AC6 = 0K

_AC7 = 0K

_AC8 = 0K

_AC9 = 0K

_CRT = 383K

_HOT = 0K

_PSL - see event data." 86 0x8000000000000020 4 44 Helen-PC NT AUTHORITY\SYSTEM

14/09/2019 12:06:38.415 594 26 Information System Microsoft-Windows-Kernel-Processor-Power "Processor 0 in group 0 exposes the following:

2 idle state(s)

4 performance state(s)

8 throttle state(s)" 4 0x8000000000000000 4 52 Helen-PC NT AUTHORITY\SYSTEM

14/09/2019 12:06:38.431 595 26 Information System Microsoft-Windows-Kernel-Processor-Power "Processor 1 in group 0 exposes the following:

2 idle state(s)

4 performance state(s)

8 throttle state(s)" 4 0x8000000000000000 4 52 Helen-PC NT AUTHORITY\SYSTEM

14/09/2019 12:06:41.000 590 6013 Information System EventLog The system uptime is 7 seconds. Classic Helen-PC

14/09/2019 12:06:41.000 589 6005 Information System EventLog The Event log service was started. Classic Helen-PC

14/09/2019 12:06:41.000 588 6009 Information System EventLog Microsoft (R) Windows (R) 6.01. 7601 Service Pack 1 Multiprocessor Free. Classic Helen-PC

14/09/2019 12:06:41.000 587 6008 Error System EventLog The previous system shutdown at 10:28:43 on 14/09/2019 was unexpected. Classic Helen-PC

14/09/2019 12:06:41.629 597 20010 Information System Microsoft-Windows-UserPnp "One or more of the Plug and Play service's subsystems has changed state.

PlugPlay install subsystem enabled: 'true'

PlugPlay caching subsystem enabled: 'true'

" 7010 0x8000000000000000 608 628 Helen-PC NT AUTHORITY\SYSTEM

14/09/2019 12:06:41.629 596 7036 Information System Service Control Manager The Plug and Play service entered the running state. Classic 444 592 Helen-PC

14/09/2019 12:06:41.691 598 7036 Information System Service Control Manager The Power service entered the running state. Classic 444 592 Helen-PC

14/09/2019 12:06:41.722 600 7036 Information System Service Control Manager The DCOM Server Process Launcher service entered the running state. Classic 444 596 Helen-PC

14/09/2019 12:06:41.722 599 6 Information System Microsoft-Windows-FilterManager File System Filter 'luafv' (6.1, 2009-07-14T00:26:13.000000000Z) has successfully loaded and registered with Filter Manager. 0x8000000000000000 4 56 Helen-PC NT AUTHORITY\SYSTEM

14/09/2019 12:06:41.738 601 7036 Information System Service Control Manager The RPC Endpoint Mapper service entered the running state. Classic 444 596 Helen-PC

14/09/2019 12:06:41.754 602 7036 Information System Service Control Manager The Remote Procedure Call (RPC) service entered the running state. Classic 444 596 Helen-PC

14/09/2019 12:06:41.847 603 7036 Information System Service Control Manager The Windows Event Log service entered the running state. Classic 444 592 Helen-PC

14/09/2019 12:06:41.941 604 7036 Information System Service Control Manager The Multimedia Class Scheduler service entered the running state. Classic 444 592 Helen-PC

14/09/2019 12:06:42.000 258 4625 Information Application Microsoft-Windows-EventSystem The EventSystem sub system is suppressing duplicate event log entries for a duration of 86400 seconds. The suppression timeout can be controlled by a REG_DWORD value named SuppressDuplicateDuration under the following registry key: HKLM\Software\Microsoft\EventSystem\EventLog. Classic Helen-PC

14/09/2019 12:06:42.000 259 4101 Information Application Microsoft-Windows-Winlogon Windows license validated. Classic Helen-PC

14/09/2019 12:06:42.000 260 6000 Information Application Microsoft-Windows-Winlogon The winlogon notification subscriber <SessionEnv> was unavailable

to handle a notification event. Classic Helen-PC

14/09/2019 12:06:42.000 261 9003 Information Application Desktop Window Manager The Desktop Window Manager was unable to start because a composited theme is not in use Classic Helen-PC

14/09/2019 12:06:42.003 605 7036 Information System Service Control Manager The Windows Audio Endpoint Builder service entered the running state. Classic 444 820 Helen-PC

14/09/2019 12:06:42.112 606 7036 Information System Service Control Manager The Windows Audio service entered the running state. Classic 444 820 Helen-PC

14/09/2019 12:06:42.128 607 7036 Information System Service Control Manager The Themes service entered the running state. Classic 444 592 Helen-PC

14/09/2019 12:06:42.128 608 7036 Information System Service Control Manager The Group Policy Client service entered the running state. Classic 444 596 Helen-PC

14/09/2019 12:06:42.144 609 7036 Information System Service Control Manager The User Profile Service service entered the running state. Classic 444 592 Helen-PC

14/09/2019 12:06:42.144 262 1531 Information Application Microsoft-Windows-User Profiles Service "The User Profile Service has started successfully.

" 0x8000000000000000 860 996 Helen-PC NT AUTHORITY\SYSTEM

14/09/2019 12:06:42.159 610 7036 Information System Service Control Manager The COM+ Event System service entered the running state. Classic 444 596 Helen-PC

14/09/2019 12:06:42.175 612 7036 Information System Service Control Manager The Desktop Window Manager Session Manager service entered the running state. Classic 444 596 Helen-PC

14/09/2019 12:06:42.175 611 7036 Information System Service Control Manager The System Event Notification Service service entered the running state. Classic 444 596 Helen-PC

14/09/2019 12:06:42.175 613 7036 Information System Service Control Manager The Security Accounts Manager service entered the running state. Classic 444 592 Helen-PC

14/09/2019 12:06:42.222 615 7036 Information System Service Control Manager The Network Store Interface Service service entered the running state. Classic 444 592 Helen-PC

14/09/2019 12:06:42.222 614 7036 Information System Service Control Manager The TCP/IP NetBIOS Helper service entered the running state. Classic 444 592 Helen-PC

14/09/2019 12:06:42.237 616 7036 Information System Service Control Manager The CNG Key Isolation service entered the running state. Classic 444 592 Helen-PC

14/09/2019 12:06:42.237 617 50036 Information System Microsoft-Windows-Dhcp-Client DHCPv4 client service is started ServiceStart (68) Service State Event (4) 0x2000000000000000 760 348 Helen-PC NT AUTHORITY \LOCAL SERVICE

14/09/2019 12:06:42.237 618 51046 Information System Microsoft-Windows-DHCPv6-Client DHCPv6 client service is started ServiceStart (62) Service State Event (4) 0x2000000000000000 760 300 Helen-PC

14/09/2019 12:06:42.253 619 7036 Information System Service Control Manager The DHCP Client service entered the running state. Classic 444 592 Helen-PC

14/09/2019 12:06:42.284 620 7036 Information System Service Control Manager The Extensible Authentication Protocol service entered the running state. Classic 444 592 Helen-PC

14/09/2019 12:06:42.346 621 7036 Information System Service Control Manager The DNS Client service entered the running state. Classic 444 592 Helen-PC

14/09/2019 12:06:42.362 622 7036 Information System Service Control Manager The WLAN AutoConfig service entered the running state. Classic 444 820 Helen-PC

14/09/2019 12:06:42.362 623 4000 Information System Microsoft-Windows-WLAN-AutoConfig "WLAN AutoConfig service has successfully started.

" Start (1) 0x4000000000000000 832 572 Helen-PC NT

AUTHORITY\SYSTEM

14/09/2019 12:06:42.409 624 7036 Information System Service Control Manager The Shell Hardware Detection service entered the running state. Classic 444 820 Helen-PC

14/09/2019 12:06:42.487 625 7001 Information System Microsoft-Windows-Winlogon User Logon Notification for Customer Experience Improvement Program 1101 0x2000000000000000 492 512 Helen-PC NT AUTHORITY\SYSTEM

14/09/2019 12:06:42.534 15 1 Information Microsoft-Windows-User Profile Service/Operational Microsoft-Windows-User Profiles Service Recieved user logon notification on session 1. 0x4000000000000000 860 112 Helen-PC Helen-PC\Helen

14/09/2019 12:06:42.549 16 5 Information Microsoft-Windows-User Profile Service/Operational Microsoft-Windows-User Profiles Service Registry file C:\Users\Helen\ntuser.dat is loaded at HKU \S-1-5-21-954126658-284120372-3882474944-1000. 0x4000000000000000 860 900 Helen-PC NT AUTHORITY\SYSTEM

14/09/2019 12:06:42.565 17 5 Information Microsoft-Windows-User Profile Service/Operational Microsoft-Windows-User Profiles Service Registry file C:\Users\Helen\AppData\Local\Microsoft\Windows\\UsrClass.dat is loaded at HKU \S-1-5-21-954126658-284120372-3882474944-1000_Classes. 0x4000000000000000 860 900 Helen-PC NT AUTHORITY\SYSTEM

14/09/2019 12:06:42.565 626 7036 Information System Service Control Manager The Task Scheduler service entered the running state. Classic 444 592 Helen-PC

14/09/2019 12:06:42.612 8 21 Information Microsoft-Windows-TerminalServices-LocalSessionManager/Operational Microsoft-Windows-TerminalServices-LocalSessionManager "Remote Desktop Services: Session logon succeeded:

User: Helen-PC\Helen

Session ID: 1

Source Network Address: LOCAL" 0x1000000000000000 484 1012 Helen-PC NT AUTHORITY\SYSTEM

14/09/2019 12:06:42.612 627 7036 Information System Service Control

Manager The Print Spooler service entered the running state.
Classic 444 592 Helen-PC

14/09/2019 12:06:42.612 18 2 Information Microsoft-Windows-User Profile Service/Operational Microsoft-Windows-User Profiles Service Finished processing user logon notification on session 1. 0x4000000000000000 860 112 Helen-PC Helen-PC\Helen

14/09/2019 12:06:42.736 9 22 Information Microsoft-Windows-TerminalServices-LocalSessionManager/Operational Microsoft-Windows-TerminalServices-LocalSessionManager "Remote Desktop Services: Shell start notification received:

User: Helen-PC\Helen

Session ID: 1

Source Network Address: LOCAL" 0x1000000000000000 484 776 Helen-PC NT AUTHORITY\SYSTEM

14/09/2019 12:06:43.000 264 5611 Information Application Microsoft-Windows-WMI The Windows Management Instrumentation service has detected an inconsistent system shutdown. Classic Helen-PC

14/09/2019 12:06:43.000 263 5615 Undefined Application Microsoft-Windows-WMI Windows Management Instrumentation Service started sucessfully
Classic Helen-PC

14/09/2019 12:06:43.095 4 823 Information Microsoft-Windows-PrintService/Admin Microsoft-Windows-PrintService The default printer was changed to Microsoft XPS Document Writer,winspool,Ne00:. See the event user data for context information. Spooler Operation Succeeded (11) Changing the default printer (49) Print Spooler 1052 1148 Helen-PC NT AUTHORITY\SYSTEM

14/09/2019 12:06:43.189 628 7036 Information System Service Control Manager The Base Filtering Engine service entered the running state.
Classic 444 596 Helen-PC

14/09/2019 12:06:43.267 629 7036 Information System Service Control Manager The Windows Firewall service entered the running state.
Classic 444 596 Helen-PC

14/09/2019 12:06:43.298 630 7036 Information System Service Control Manager The Workstation service entered the running state.

Classic 444 820 Helen-PC

14/09/2019 12:06:43.407 631 7036 Information System Service Control Manager The Cryptographic Services service entered the running state.
Classic 444 736 Helen-PC

14/09/2019 12:06:43.423 632 201 Information System Microsoft-Windows-Application-Experience The Program Compatibility Assistant service started successfully. 0x8000000000000000 832 1452 Helen-PC NT AUTHORITY\SYSTEM

14/09/2019 12:06:43.470 633 7036 Information System Service Control Manager The Program Compatibility Assistant Service service entered the running state. Classic 444 820 Helen-PC

14/09/2019 12:06:43.501 634 7036 Information System Service Control Manager The Diagnostic Policy Service service entered the running state.
Classic 444 736 Helen-PC

14/09/2019 12:06:43.548 635 7036 Information System Service Control Manager The Superfetch service entered the running state.
Classic 444 596 Helen-PC

14/09/2019 12:06:43.594 636 7036 Information System Service Control Manager The Distributed Link Tracking Client service entered the running state.
Classic 444 736 Helen-PC

14/09/2019 12:06:43.641 637 7036 Information System Service Control Manager The Windows Management Instrumentation service entered the running state. Classic 444 1112 Helen-PC

14/09/2019 12:06:43.641 638 7036 Information System Service Control Manager The Network Location Awareness service entered the running state.
Classic 444 736 Helen-PC

14/09/2019 12:06:43.704 639 7036 Information System Service Control Manager The IP Helper service entered the running state. Classic 444 1544 Helen-PC

14/09/2019 12:06:43.969 640 7036 Information System Service Control Manager The Server service entered the running state. Classic 444 1548 Helen-PC

14/09/2019 12:06:44.031 641 7036 Information System Service Control Manager The Application Experience service entered the running state.
Classic 444 820 Helen-PC

14/09/2019 12:06:44.078 642 7036 Information System Service Control Manager The Diagnostic Service Host service entered the running state. Classic 444 1548 Helen-PC

14/09/2019 12:06:44.078 643 7036 Information System Service Control Manager The Diagnostic System Host service entered the running state. Classic 444 820 Helen-PC

14/09/2019 12:06:44.125 644 7036 Information System Service Control Manager The Network List Service service entered the running state. Classic 444 1544 Helen-PC

14/09/2019 12:06:44.140 4 1001 Information Microsoft-Windows-Resource-Exhaustion-Detector/Operational Microsoft-Windows-Resource-Exhaustion-Detector The Windows Resource Exhaustion Detector started. Events logged when the resource exhaustion detector is started. (11) Lifecycle Events (1) Events related to lifecycle of resource exhaustion detector. 1116 1440 Helen-PC NT AUTHORITY\LOCAL SERVICE

14/09/2019 12:06:44.218 645 7036 Information System Service Control Manager The Portable Device Enumerator Service service entered the running state. Classic 444 592 Helen-PC

14/09/2019 12:06:45.825 646 20003 Information System Microsoft-Windows-UserPnp Driver Management has concluded the process to add Service tunnel for Device Instance ID ROOT*ISATAP\0001 with the following status: 0. 7005 0x8000000000000000 860 112 Helen-PC NT AUTHORITY \SYSTEM

14/09/2019 12:06:46.000 271 224 Information Application ESENT WinMail (1976) WindowsMail0: Deleting log files C:\Users\Helen\AppData\Local \Microsoft\Windows Mail\edb00004.log to C:\Users\Helen\AppData\Local\Microsoft \Windows Mail\edb00004.log. Logging/Recovery (3) Classic Helen-PC

14/09/2019 12:06:46.000 272 213 Information Application ESENT WinMail (1976) WindowsMail0: The backup procedure has been successfully completed. Logging/Recovery (3) Classic Helen-PC

14/09/2019 12:06:46.000 270 223 Information Application ESENT WinMail (1976) WindowsMail0: Starting the backup of log files (range C:\Users \Helen\AppData\Local\Microsoft\Windows Mail\edb00005.log - C:\Users\Helen\AppData \Local\Microsoft\Windows Mail\edb00005.log). Logging/Recovery (3) Classic Helen-PC

14/09/2019 12:06:46.000 269 221 Information Application ESENT WinMail (1976) WindowsMail0: Ending the backup of the file C:\Users\Helen \AppData\Local\Microsoft\Windows Mail\WindowsMail.MSMessageStore. Logging/Recovery (3) Classic Helen-PC

14/09/2019 12:06:46.000 268 220 Information Application ESENT WinMail (1976) WindowsMail0: Beginning the backup of the file C:\Users\Helen \AppData\Local\Microsoft\Windows Mail\WindowsMail.MSMessageStore (size 2 Mb). Logging/Recovery (3) Classic Helen-PC

14/09/2019 12:06:46.000 267 210 Information Application ESENT WinMail (1976) WindowsMail0: A full backup is starting. Logging/Recovery (3) Classic Helen-PC

14/09/2019 12:06:46.000 266 102 Information Application ESENT WinMail (1976) WindowsMail0: The database engine (6.01.7601.0000) started a new instance (0). General (1) Classic Helen-PC

14/09/2019 12:06:46.000 265 5617 Undefined Application Microsoft-Windows-WMI Windows Management Instrumentation Service subsystems initialized successfully Classic Helen-PC

14/09/2019 12:06:46.465 647 7036 Information System Service Control Manager The Protected Storage service entered the running state. Classic 444 592 Helen-PC

14/09/2019 12:06:51.000 273 103 Information Application ESENT WinMail (1976) WindowsMail0: The database engine stopped the instance (0). General (1) Classic Helen-PC

14/09/2019 12:06:51.613 43 2011 Information Microsoft-Windows-Windows Firewall With Advanced Security/Firewall Microsoft-Windows-Windows Firewall With Advanced Security "Windows Firewall was unable to notify the user that it blocked an application from accepting incoming connections on the network.

Reason: The application is a system service

Application Path: C:\windows\system32\lsass.exe

IP Version: IPv6

Protocol: TCP

Port: 49156

Process Id: 460

User: S-1-5-18" 0x8000000000000000 1116 1388
Helen-PC NT AUTHORITY\LOCAL SERVICE

14/09/2019 12:06:52.000 277 302 Information Application ESENT
Windows (1664) Windows: The database engine has successfully completed recovery steps. Logging/Recovery (3) Classic Helen-PC

14/09/2019 12:06:52.000 276 301 Information Application ESENT
Windows (1664) Windows: The database engine has begun replaying logfile C:\ProgramData\Microsoft\Search\Data\Applications\Windows\MSS.log.
Logging/Recovery (3) Classic Helen-PC

14/09/2019 12:06:52.000 275 300 Information Application ESENT
Windows (1664) Windows: The database engine is initiating recovery steps.
Logging/Recovery (3) Classic Helen-PC

14/09/2019 12:06:52.000 274 102 Information Application ESENT
Windows (1664) Windows: The database engine (6.01.7601.0000) started a new instance (0). General (1) Classic Helen-PC

14/09/2019 12:06:53.000 278 1003 Information Application Microsoft-Windows-Search "The Windows Search Service started.

" Search service (1) Classic Helen-PC

14/09/2019 12:06:53.017 648 7036 Information System Service Control Manager The Windows Search service entered the running state.
Classic 444 580 Helen-PC

14/09/2019 12:06:54.000 280 103 Information Application ESENT
WinMail (1424) WindowsMail0: The database engine stopped the instance (0).
General (1) Classic Helen-PC

14/09/2019 12:06:54.000 279 102 Information Application ESENT
WinMail (1424) WindowsMail0: The database engine (6.01.7601.0000) started a new instance (0). General (1) Classic Helen-PC

14/09/2019 12:06:57.000 281 4121 Information Application Microsoft-Windows-Search "

A master merge has restarted for catalog SystemIndex." Search service (1)
Classic Helen-PC

14/09/2019 12:07:03.267 649 7036 Information System Service Control

Manager The Network Connections service entered the running state.
Classic 444 580 Helen-PC

14/09/2019 12:07:32.767 650 7036 Information System Service Control Manager The Application Information service entered the running state.
Classic 444 580 Helen-PC

14/09/2019 12:07:35.590 6 1015 Information Microsoft-Windows-ReadyBoost/Operational Microsoft-Windows-ReadyBoost "Summary of ReadyBoot Performance:

Io Read Count: 18251

Io Read Bytes: 319689728

Cache Hit Count: 13218

Cache Hit Bytes: 211850752

Cache Hit Percentage: 0.724234288532135

Boot Prefetch Time (us): 6040147

Boot Prefetch Bytes: 631529472

Boot Prefetch Read Count: 12902

" 1016 0x8000000000002000 832 1928 Helen-PC NT AUTHORITY\SYSTEM

14/09/2019 12:07:36.027 7 1016 Information Microsoft-Windows-ReadyBoost/Operational Microsoft-Windows-ReadyBoost "Boot plan calculation completed in 2168 ms.

Boot Plan Timestamp: 2019-09-14T12:07:33.859303000Z

Reason: System boot completion

Result: 0x0" 1016 0x8000000000002000 832 1928 Helen-PC NT AUTHORITY\SYSTEM

14/09/2019 12:08:15.246 12 100 Information Microsoft-Windows-Diagnosis-DPS/Operational Microsoft-Windows-Diagnosis-DPS Diagnostic module {C8544339-5BE9-4F25-862E-485F1B1A6935} (%SystemRoot%\system32\diagperf.dll) detected a problem for scenario {86432A0B-3C7D-4DDF-A89C-172FAA90485D}, instance {B00F84A9-E992-4BC6-A1EF-FA5035F84ABB}, original activity ID {86432A0B-3C7D-4DDF-A89C-172FAA90485D}. A diagnostic module detected a problem (12) Scenario Lifecycle (1) Scenario lifecycle events 1116 1128 Helen-PC NT AUTHORITY

\LOCAL SERVICE

14/09/2019 12:08:15.246 13 105 Information Microsoft-Windows-Diagnosis-DPS/Operational Microsoft-Windows-Diagnosis-DPS Diagnostic module {C8544339-5BE9-4F25-862E-485F1B1A6935} (%SystemRoot%\system32\diagperf.dll) started troubleshooting scenario {86432A0B-3C7D-4DDF-A89C-172FAA90485D}, instance {B00F84A9-E992-4BC6-A1EF-FA5035F84ABB}, original activity ID {86432A0B-3C7D-4DDF-A89C-172FAA90485D}. A scenario instance was dispatched for troubleshooting (13) Scenario Lifecycle (1) Scenario lifecycle events 1116 1128 Helen-PC NT AUTHORITY\LOCAL SERVICE

14/09/2019 12:08:15.651 14 110 Information Microsoft-Windows-Diagnosis-DPS/Operational Microsoft-Windows-Diagnosis-DPS Diagnostic module {C8544339-5BE9-4F25-862E-485F1B1A6935} (%SystemRoot%\system32\diagperf.dll) finished troubleshooting scenario {86432A0B-3C7D-4DDF-A89C-172FAA90485D}, instance {B00F84A9-E992-4BC6-A1EF-FA5035F84ABB}, original activity ID {86432A0B-3C7D-4DDF-A89C-172FAA90485D}. No resolution was set by the diagnostic module.A diagnostic module completed troubleshooting without setting a resolution (14) Scenario Lifecycle (1) Scenario lifecycle events 1116 1128 Helen-PC NT AUTHORITY \LOCAL SERVICE

14/09/2019 12:08:32.000 282 10 Error Application Microsoft-Windows-WMI Event filter with query "SELECT * FROM __InstanceModificationEvent WITHIN 60 WHERE TargetInstance ISA "Win32_Processor" AND TargetInstance.LoadPercentage > 99" could not be reactivated in namespace "//./root/CIMV2" because of error 0x80041003. Events cannot be delivered through this filter until the problem is corrected. Classic Helen-PC

14/09/2019 12:08:44.000 283 900 Information Application Microsoft-Windows-Security-SPP "The Software Protection service is starting.

" Classic Helen-PC

14/09/2019 12:08:44.043 651 7036 Information System Service Control Manager The Background Intelligent Transfer Service service entered the running state. Classic 444 592 Helen-PC

14/09/2019 12:08:44.277 652 7036 Information System Service Control Manager The Windows Font Cache Service service entered the running state. Classic 444 592 Helen-PC

14/09/2019 12:08:44.387 653 7036 Information System Service Control Manager The SSDP Discovery service entered the running state. Classic 444 592 Helen-PC

14/09/2019 12:08:44.402 654 7036 Information System Service Control Manager The Portable Device Enumerator Service service entered the stopped state. Classic 444 592 Helen-PC

14/09/2019 12:08:44.511 655 7036 Information System Service Control Manager The Software Protection service entered the running state. Classic 444 592 Helen-PC

14/09/2019 12:08:44.636 3 306 Verbose Microsoft-Windows-Bits-Client/Operational Microsoft-Windows-Bits-Client The BITS service loaded the job list from disk. 0x4000000000000000 860 600 Helen-PC NT AUTHORITY\SYSTEM

14/09/2019 12:08:44.855 656 7036 Information System Service Control Manager The Windows Defender service entered the running state. Classic 444 592 Helen-PC

14/09/2019 12:08:45.000 284 1 Information Application SecurityCenter The Windows Security Center Service has started. Classic Helen-PC

14/09/2019 12:08:45.057 657 7036 Information System Service Control Manager The Security Center service entered the running state. Classic 444 592 Helen-PC

14/09/2019 12:08:45.229 8 101 Undefined Microsoft-Windows-Windows Defender/WHC Microsoft-Windows-Windows Defender Windows Defender state updated to 10. 0x4000000000000000 1784 1508 Helen-PC NT AUTHORITY\SYSTEM

14/09/2019 12:08:45.962 658 7036 Information System Service Control Manager The Windows Update service entered the running state. Classic 444 592 Helen-PC

14/09/2019 12:08:46.000 287 902 Undefined Application Microsoft-Windows-Security-SPP "The Software Protection service has started.

6.1.7601.17514" Classic Helen-PC

14/09/2019 12:08:46.000 286 1003 Information Application Microsoft-Windows-Security-SPP "The Software Protection service has completed licensing status check.

Application Id=55c92734-d682-4d71-983e-d6ec3f16059f

Licensing Status=

1: 01f5fc37-a99e-45c5-b65e-d762f3518ead, 1, 0 [(0 [0xC004F014, 0, 0], [(?)(?)(?)(?)(?)(?)])

(1)(2)]

2: 2e7d060d-4714-40f2-9896-1e4f15b612ad, 1, 1 [(0)(1)(2 [0x00000000, 0, 1], [(?)(5 0x00000000 30 32340)(1 0x00000000 0 0 msft:rm/algorithm/flags/1.0 0x00000000 0)(?)(?)(?)])]

3: 3b965dfc-31d9-4903-886f-873a0382776c, 1, 0 [(0 [0xC004F014, 0, 0], [(?)(?)(?)(?)(?)(?)]) (1)(2)]

4: 586bc076-c93d-429a-afe5-a69fbc644e88, 1, 0 [(0 [0xC004F014, 0, 0], [(?)(?)(?)(?)(?)(?)]) (1)(2)]

5: 5e017a8a-f3f9-4167-b1bd-ba3e236a4d8f, 1, 0 [(0 [0xC004F014, 0, 0], [(?)(?)(?)(?)(?)(?)]) (1)(2)]

6: 5e35dc43-389b-47c5-b889-2088b06738cb, 1, 0 [(0 [0xC004F014, 0, 0], [(?)(?)(?)(?)(?)(?)]) (1)(2)]

7: 6a7d5d8a-92af-4e6a-af4b-8fddaec800e5, 1, 0 [(0 [0xC004F014, 0, 0], [(?)(?)(?)(?)(?)(?)]) (1)(2)]

8: 9ab82e0c-ffc9-4107-baa1-c65a8bd3ccc3, 1, 0 [(0 [0xC004F014, 0, 0], [(?)(?)(?)(?)(?)(?)]) (1)(2)]

9: 9f83d90f-a151-4665-ae69-30b3f63ec659, 1, 0 [(0 [0xC004F014, 0, 0], [(?)(?)(?)(?)(?)(?)]) (1)(2)]

10: a63275f4-530c-48a7-b0d3-4f00d688d151, 1, 0 [(0 [0xC004F014, 0, 0], [(?)(?)(?)(?)(?)(?)]) (1)(2)]

11: b8a4bb91-69b1-460d-93f8-40e0670af04a, 1, 0 [(0 [0xC004F014, 0, 0], [(?)(?)(?)(?)(?)(?)]) (1)(2)]

12: d2c04e90-c3dd-4260-b0f3-f845f5d27d64, 1, 0 [(0 [0xC004F014, 0, 0], [(?)(?)(?)(?)(?)(?)]) (1)(2)]

13: e68b141f-4dfa-4387-b3b7-e65c4889216e, 1, 0 [(0 [0xC004F014, 0, 0], [(?)(?)(?)(?)(?)(?)]) (1)(2)]

14: ee4e1629-bcdc-4b42-a68f-b92e135f78d7, 1, 0 [(0 [0xC004F014, 0, 0], [(?)(?)(?)(?)(?)(?)]) (1)(2)]

15: 4a8149bb-7d61-49f4-8822-82c7bf88d64b, 1, 0 [(0 [0xC004F014, 0, 0], [(?)(?)(?)(?)(?)(?)]) (1)(2)]

16: afd5f68f-b70f-4000-a21d-28dbc8be8b07, 1, 0 [(0 [0xC004F014, 0, 0], [(?)(?)(?)(?)(?)(?)]) (1)(2)]

" Classic Helen-PC

14/09/2019 12:08:46.000 285 1066 Information Application Microsoft-Windows-Security-SPP "Initialization status for service objects.

C:\Windows\system32\sppwinob.dll, msft:spp/windowsfunctionality/agent/7.0, 0x00000000, 0x00000000

C:\Windows\system32\sppobjs.dll, msft:rm/algorithm/phone/1.0, 0x00000000, 0x00000000

C:\Windows\system32\sppobjs.dll, msft:rm/algorithm/pkey/2005, 0x00000000, 0x00000000

C:\Windows\system32\sppobjs.dll, msft:spp/TaskScheduler/1.0, 0x00000000, 0x00000000

C:\Windows\system32\sppobjs.dll, msft:spp/volume/services/kms/1.0, 0x00000000, 0x00000000

C:\Windows\system32\sppobjs.dll, msft:spp/volume/services/kms/licenserenewal/1.0, 0x00000000, 0x00000000

" Classic Helen-PC

14/09/2019 12:08:47.007 9 101 Undefined Microsoft-Windows-Windows Defender/WHC Microsoft-Windows-Windows Defender Windows Defender state updated to 10. 0x4000000000000000 1784 1148 Helen-PC NT AUTHORITY\SYSTEM

14/09/2019 12:09:36.350 7 42 Information Microsoft-Windows-WindowsUpdateClient/Operational Microsoft-Windows-WindowsUpdateClient There has been a change in the health of Windows Update. Other (18) Automatic Updates (2) State 860 1620 Helen-PC NT AUTHORITY\SYSTEM

14/09/2019 12:09:36.350 8 42 Information Microsoft-Windows-WindowsUpdateClient/Operational Microsoft-Windows-WindowsUpdateClient There has been a change in the health of Windows Update. Other (18) Automatic Updates (2) State 860 1620 Helen-PC NT AUTHORITY\SYSTEM

14/09/2019 12:09:36.350 9 29 Warning Microsoft-Windows-WindowsUpdateClient/Operational Microsoft-Windows-WindowsUpdateClient Windows Update lost connectivity. State Change (17) Windows Update Agent (1) Connection 860 1620 Helen-PC NT AUTHORITY\SYSTEM

14/09/2019 12:10:02.995 18 1002 Warning Microsoft-Windows-Known Folders API Service Microsoft-Windows-KnownFolders Error 0x80070002 occurred while verifying known folder {B4BFCC3A-DB2C-424C-B029-7FE99A87C641} with path 'C:\Windows\system32\config\systemprofile\Desktop'.
0x8000000000000000 1892 1932 Helen-PC NT AUTHORITY\SYSTEM

14/09/2019 12:10:04.056 19 1002 Warning Microsoft-Windows-Known Folders API Service Microsoft-Windows-KnownFolders Error 0x80070002 occurred while verifying known folder {AE50C081-EBD2-438A-8655-8A092E34987A} with path 'C:\Windows\system32\config\systemprofile\AppData\Roaming\Microsoft\Windows\Recent'.
0x8000000000000000 1892 1932 Helen-PC NT AUTHORITY\SYSTEM

14/09/2019 12:10:56.191 289 3011 Error Application Microsoft-Windows-LoadPerf Unloading the performance counter strings for service WmiApRpl (WmiApRpl) failed. The first DWORD in the Data section contains the error code.
0x8000000000000000 1396 260 Helen-PC NT AUTHORITY\SYSTEM

14/09/2019 12:10:56.191 288 3001 Error Application Microsoft-Windows-LoadPerf The performance counter name string value in the registry is not formatted correctly. The malformed string is 6548. The first DWORD in the Data section contains the index value to the malformed string while the second and third DWORDs in the Data section contain the last valid index values. 0x8000000000000000
1396 260 Helen-PC NT AUTHORITY\SYSTEM

14/09/2019 12:10:59.218 290 2006 Warning Application Microsoft-Windows-LoadPerf The LastCounter and LastHelp values of the performance registry are corrupted and need to be updated. The first and second DWORDs in the Data Section contain the original LastCounter and LastHelp values, respectively, while the third and fourth DWORDs in the Data Section contain the updated new values.
0x8000000000000000 1396 260 Helen-PC NT AUTHORITY\SYSTEM

14/09/2019 12:10:59.264 292 1000 Information Application Microsoft-Windows-LoadPerf Performance counters for the WmiApRpl (WmiApRpl) service were loaded successfully. The Record Data in the data section contains the new index values assigned to this service. 0x8000000000000000 1396 260 Helen-PC

14/09/2019 12:10:59.264 291 3001 Error Application Microsoft-Windows-LoadPerf The performance counter name string value in the registry is not formatted correctly. The malformed string is 6548. The first DWORD in the Data section contains the index value to the malformed string while the second and third DWORDs in the Data section contain the last valid index values. 0x8000000000000000
1396 260 Helen-PC NT AUTHORITY\SYSTEM

14/09/2019 12:11:42.000 293 1005 Information Application Microsoft-Windows-CEIP Customer Experience Improvement Program data was successfully consolidated into files that will be sent to Microsoft for analysis. These files will be sent only if the user has opted to join the Windows Customer Experience Improvement Program. Classic Helen-PC

14/09/2019 12:11:43.194 2 100 Information Microsoft-Windows-WindowsBackup/ActionCenter Microsoft-Windows-WindowsBackup Windows Backup status 0x8000000000000000 888 1812 Helen-PC NT AUTHORITY\LOCAL SERVICE

14/09/2019 12:12:02.663 659 7036 Information System Service Control Manager The Multimedia Class Scheduler service entered the stopped state. Classic 444 1140 Helen-PC

14/09/2019 12:23:22.434 660 7036 Information System Service Control Manager The Multimedia Class Scheduler service entered the running state. Classic 444 1904 Helen-PC

14/09/2019 12:23:22.685 661 20003 Information System Microsoft-Windows-UserPnp Driver Management has concluded the process to add Service USBSTOR for Device Instance ID USB\VID_10D6&PID_1101\5&2C5DFB53&0&1 with the following status: 0. 7005 0x8000000000000000 620 1676 Helen-PC NT AUTHORITY\SYSTEM

14/09/2019 12:23:22.795 662 20001 Information System Microsoft-Windows-UserPnp Driver Management concluded the process to install driver FileRepository\usbstor.inf_amd64_neutral_0725c2806a159a9d\usbstor.inf for Device Instance ID USB\VID_10D6&PID_1101\5&2C5DFB53&0&1 with the following status: 0x0. 7005 0x8000000000000000 620 1676 Helen-PC NT AUTHORITY\SYSTEM

14/09/2019 12:23:23.125 663 20003 Information System Microsoft-Windows-UserPnp Driver Management has concluded the process to add Service disk for Device Instance ID USBSTOR\DISK&VEN_ACTIONS&PROD_HS_USB_FLASHDISK&REV_2.00\6&292CF7D3&0&_____&0 with the following status: 0. 7005 0x8000000000000000 2024 1080 Helen-PC NT AUTHORITY\SYSTEM

14/09/2019 12:23:23.266 664 20001 Information System Microsoft-Windows-UserPnp Driver Management concluded the process to install driver FileRepository\disk.inf_amd64_neutral_10ce25bbc5a9cc43\disk.inf for Device Instance ID USBSTOR\DISK&VEN_ACTIONS&PROD_HS_USB_FLASHDISK&REV_2.00\6&292CF7D3&0&_____&0 with the following status: 0x0. 7005 0x8000000000000000 2024 1080 Helen-PC NT AUTHORITY\SYSTEM

14/09/2019 12:23:23.312 665 7036 Information System Service Control

Manager The Portable Device Enumerator Service service entered the running state. Classic 444 1744 Helen-PC

14/09/2019 12:23:23.593 666 20003 Information System Microsoft-Windows-UserPnp Driver Management has concluded the process to add Service volsnap for Device Instance ID STORAGE\VOLUME_?? _USBSTOR#DISK&VEN_ACTIONS&PROD_HS_USB_FLASHDISK&REV_2.00#6&292CF7D3&0 &_____&0#{53F56307-B6BF-11D0-94F2-00A0C91EFB8B} with the following status: 0. 7005 0x8000000000000000 1924 200 Helen-PC NT AUTHORITY\SYSTEM

14/09/2019 12:23:23.624 667 20001 Information System Microsoft-Windows-UserPnp Driver Management concluded the process to install driver FileRepository\volume.inf_amd64_neutral_df8bea40ac96ca21\volume.inf for Device Instance ID STORAGE\VOLUME_?? _USBSTOR#DISK&VEN_ACTIONS&PROD_HS_USB_FLASHDISK&REV_2.00#6&292CF7D3&0 &_____&0#{53F56307-B6BF-11D0-94F2-00A0C91EFB8B} with the following status: 0x0. 7005 0x8000000000000000 1924 200 Helen-PC NT AUTHORITY\SYSTEM

14/09/2019 12:23:24.888 668 20003 Information System Microsoft-Windows-UserPnp Driver Management has concluded the process to add Service umbus for Device Instance ID UMB\UMB\1&841921D&0&WPDBUSENUMROOT with the following status: 0. 7005 0x8000000000000000 944 1196 Helen-PC NT AUTHORITY\SYSTEM

14/09/2019 12:23:24.997 669 20001 Information System Microsoft-Windows-UserPnp Driver Management concluded the process to install driver FileRepository\umbus.inf_amd64_neutral_2d4257afa2e35253\umbus.inf for Device Instance ID UMB\UMB\1&841921D&0&WPDBUSENUMROOT with the following status: 0x0. 7005 0x8000000000000000 944 1196 Helen-PC NT AUTHORITY\SYSTEM

14/09/2019 12:23:25.000 670 24576 Information System Microsoft-Windows-WPDClassInstaller Drivers were successfully installed for device . Driver Installation (16) Classic Helen-PC

14/09/2019 12:23:25.000 672 24579 Information System Microsoft-Windows-WPDClassInstaller Autoplay registration was skipped for device . Driver Post-Install Configuration (32) Classic Helen-PC

14/09/2019 12:23:25.000 671 24577 Information System Microsoft-Windows-WPDClassInstaller Media player and imaging program compatibility layers were successfully registered for device . Layer bits 0x00000002 were requested, layer bits 0x00000002 were registered. Driver Post-Install Configuration (32) Classic

Helen-PC

14/09/2019 12:23:25.231 20 1002 Warning Microsoft-Windows-Known Folders API Service Microsoft-Windows-KnownFolders Error 0x80070002 occurred while verifying known folder {FDD39AD0-238F-46AF-ADB4-6C85480369C7} with path 'C:\Windows\system32\config\systemprofile\Documents'.
0x8000000000000000 1988 308 Helen-PC NT AUTHORITY\SYSTEM

14/09/2019 12:23:25.309 673 10000 Information System Microsoft-Windows-DriverFrameworks-UserModeA driver package which uses user-mode driver framework version 1.9.0 is being installed on device WPDBUSENUMROOT\UMB\2&37C186B&0&STORAGE#VOLUME#_??_USBSTOR#DISK&VEN_ACTIONS&PROD_HS_USB_FLASHDISK&REV_2.00#6&292CF7D3&0&_____&0#. Start (1) Installation or update of device drivers. (48)
0x2000000000000000 1988 308 Helen-PC NT AUTHORITY\SYSTEM

14/09/2019 12:23:25.309 674 10001 Information System Microsoft-Windows-DriverFrameworks-UserModeThe UMDF service WpdFs (CLSID {112DE495-AC4C-46F8-B663-6A4266C53313}) was installed. It requires framework version 1.9.0 or higher. Installation or update of device drivers. (48) 0x2000000000000000
1988 308 Helen-PC NT AUTHORITY\SYSTEM

14/09/2019 12:23:25.325 675 7040 Information System Service Control Manager The start type of the Windows Driver Foundation - User-mode Driver Framework service was changed from demand start to auto start.
Classic 444 1744 Helen-PC NT AUTHORITY\SYSTEM

14/09/2019 12:23:25.356 1 1000 Information Microsoft-Windows-DriverFrameworks-UserMode/Operational Microsoft-Windows-DriverFrameworks-UserMode The Driver Manager service started successfully Start (1) Startup of the driver manager service. (16)0x8000000000000000 832 984 Helen-PC NT AUTHORITY\SYSTEM

14/09/2019 12:23:25.387 676 7036 Information System Service Control Manager The Windows Driver Foundation - User-mode Driver Framework service entered the running state. Classic 444 1744 Helen-PC

14/09/2019 12:23:25.465 677 10100 Information System Microsoft-Windows-DriverFrameworks-UserModeThe driver package installation has succeeded.
Stop (2) Installation or update of device drivers. (48) 0x2000000000000000
1988 308 Helen-PC NT AUTHORITY\SYSTEM

14/09/2019 12:23:25.512 678 7045 Information System Service Control Manager "A service was installed in the system.

Service Name: WUDFRd

Service File Name: system32\DRIVERS\WUDFRd.sys

Service Type: kernel mode driver

Service Start Type: demand start

Service Account: " Classic 444 1744 Helen-PC NT AUTHORITY\SYSTEM

14/09/2019 12:23:25.543 679 20003 Information System Microsoft-Windows-UserPnp Driver Management has concluded the process to add Service WUDFRd for Device Instance ID WPDBUSENUMROOT\UMB\2&37C186B&0&STORAGE#VOLUME#_??_USBSTOR#DISK&VEN_ACTIONS&PROD_HS_USB_FLASHDISK&REV_2.00#6&292CF7D3&0&_____&0# with the following status: 0. 7005 0x8000000000000000 1988 308 Helen-PC NT AUTHORITY\SYSTEM

14/09/2019 12:23:25.606 2 1003 Information Microsoft-Windows-DriverFrameworks-UserMode/Operational Microsoft-Windows-DriverFrameworks-UserMode The Driver Manager service is starting a host process for device WPDBUSENUMROOT.UMB.2&37C186B&0&STORAGE#VOLUME#_??_USBSTOR#DISK&VEN_ACTIONS&PROD_HS_USB_FLASHDISK&REV_2.00#6&292CF7D3&0&_____&0#. Start (1) Creation of a new driver host process. (17) 0x8000000000000000 832 1936 Helen-PC NT AUTHORITY\SYSTEM

14/09/2019 12:23:25.637 4 2001 Information Microsoft-Windows-DriverFrameworks-UserMode/Operational Microsoft-Windows-DriverFrameworks-UserMode The UMDF Host Process ({E6641102-6E26-40A8-8F9A-38A76AFCE39F}) started successfully. Stop (2) Startup of a new driver host process. (32) 0x8000000000000000 580 200 Helen-PC NT AUTHORITY\LOCAL SERVICE

14/09/2019 12:23:25.637 3 2000 Information Microsoft-Windows-DriverFrameworks-UserMode/Operational Microsoft-Windows-DriverFrameworks-UserMode The UMDF Host Process ({E6641102-6E26-40A8-8F9A-38A76AFCE39F}) is starting up. Start (1) Startup of a new driver host process. (32) 0x8000000000000000 580 200 Helen-PC NT AUTHORITY\LOCAL SERVICE

14/09/2019 12:23:25.668 5 1004 Information Microsoft-Windows-DriverFrameworks-UserMode/Operational Microsoft-Windows-DriverFrameworks-UserMode The host process ({E6641102-6E26-40A8-8F9A-38A76AFCE39F}) started successfully. Stop (2) Creation of a new driver host process. (17)

0x8000000000000000 832 1936 Helen-PC NT AUTHORITY\SYSTEM

14/09/2019 12:23:25.684 7 2010 Information Microsoft-Windows-DriverFrameworks-UserMode/Operational Microsoft-Windows-DriverFrameworks-UserMode The UMDF Host Process ({E6641102-6E26-40A8-8F9A-38A76AFCE39F}) has successfully loaded drivers for device WPDBUSENUMROOT\UMB\2&37C186B&0&STORAGE#VOLUME#_??_USBSTOR#DISK&VEN_ACTIONS&PROD_HS_USB_FLASHDISK&REV_2.00#6&292CF7D3&0&_____&0#. Stop (2) Loading drivers to control a newly discovered device. (33) 0x8000000000000000 580 1700 Helen-PC NT AUTHORITY\LOCAL SERVICE

14/09/2019 12:23:25.684 6 2003 Information Microsoft-Windows-DriverFrameworks-UserMode/Operational Microsoft-Windows-DriverFrameworks-UserMode The UMDF Host Process ({E6641102-6E26-40A8-8F9A-38A76AFCE39F}) has been asked to load drivers for device WPDBUSENUMROOT\UMB\2&37C186B&0&STORAGE#VOLUME#_??_USBSTOR#DISK&VEN_ACTIONS&PROD_HS_USB_FLASHDISK&REV_2.00#6&292CF7D3&0&_____&0#. Start (1) Loading drivers to control a newly discovered device. (33) 0x8000000000000000 580 1700 Helen-PC NT AUTHORITY\LOCAL SERVICE

14/09/2019 12:23:25.684 8 2004 Undefined Microsoft-Windows-DriverFrameworks-UserMode/Operational Microsoft-Windows-DriverFrameworks-UserMode The UMDF Host is loading driver WpdFs at level 0 for device WPDBUSENUMROOT\UMB\2&37C186B&0&STORAGE#VOLUME#_??_USBSTOR#DISK&VEN_ACTIONS&PROD_HS_USB_FLASHDISK&REV_2.00#6&292CF7D3&0&_____&0#. Start (1) Loading drivers to control a newly discovered device. (33) 0x8000000000000000 580 1700 Helen-PC NT AUTHORITY\LOCAL SERVICE

14/09/2019 12:23:25.699 17 2106 Information Microsoft-Windows-DriverFrameworks-UserMode/Operational Microsoft-Windows-DriverFrameworks-UserMode Received a Pnp or Power operation (27, 0) for device WPDBUSENUMROOT\UMB\2&37C186B&0&STORAGE#VOLUME#_??_USBSTOR#DISK&VEN_ACTIONS&PROD_HS_USB_FLASHDISK&REV_2.00#6&292CF7D3&0&_____&0# which was completed by the lower drivers with status 0x0 Start (1) Pnp or Power Management operation to a particular device. (37) 0x8000000000000000 580 1700 Helen-PC NT AUTHORITY\LOCAL SERVICE

14/09/2019 12:23:25.699 10 2005 Verbose Microsoft-Windows-DriverFrameworks-UserMode/Operational Microsoft-Windows-DriverFrameworks-UserMode The UMDF Host Process ({E6641102-6E26-40A8-8F9A-38A76AFCE39F}) has loaded module C:\Windows\System32\drivers\UMDF\WpdFs.dll while loading drivers for

device WPDBUSENUMROOT\UMB\2&37C186B&0&STORAGE#VOLUME#_??
_USBSTOR#DISK&VEN_ACTIONS&PROD_HS_USB_FLASHDISK&REV_2.00#6&292CF7D3&0
&_____&0#. Loading drivers to control a newly discovered device. (33)
0x8000000000000000 580 1700 Helen-PC NT AUTHORITY\LOCAL
SERVICE

14/09/2019 12:23:25.699 11 2005 Verbose Microsoft-Windows-
DriverFrameworks-UserMode/Operational Microsoft-Windows-DriverFrameworks-
UserMode The UMDF Host Process ({E6641102-6E26-40A8-8F9A-38A76AFCE39F}) has
loaded module C:\Windows\system32\wmvcore.dll while loading drivers for device
WPDBUSENUMROOT\UMB\2&37C186B&0&STORAGE#VOLUME#_??
_USBSTOR#DISK&VEN_ACTIONS&PROD_HS_USB_FLASHDISK&REV_2.00#6&292CF7D3&0
&_____&0#. Loading drivers to control a newly discovered device. (33)
0x8000000000000000 580 1700 Helen-PC NT AUTHORITY\LOCAL
SERVICE

14/09/2019 12:23:25.699 12 2005 Verbose Microsoft-Windows-
DriverFrameworks-UserMode/Operational Microsoft-Windows-DriverFrameworks-
UserMode The UMDF Host Process ({E6641102-6E26-40A8-8F9A-38A76AFCE39F}) has
loaded module C:\Windows\system32\WMASF.DLL while loading drivers for device
WPDBUSENUMROOT\UMB\2&37C186B&0&STORAGE#VOLUME#_??
_USBSTOR#DISK&VEN_ACTIONS&PROD_HS_USB_FLASHDISK&REV_2.00#6&292CF7D3&0
&_____&0#. Loading drivers to control a newly discovered device. (33)
0x8000000000000000 580 1700 Helen-PC NT AUTHORITY\LOCAL
SERVICE

14/09/2019 12:23:25.699 13 2005 Verbose Microsoft-Windows-
DriverFrameworks-UserMode/Operational Microsoft-Windows-DriverFrameworks-
UserMode The UMDF Host Process ({E6641102-6E26-40A8-8F9A-38A76AFCE39F}) has
loaded module C:\Windows\WinSxS\amd64_microsoft.windows.gdiplus_
6595b64144ccf1df_1.1.7601.17514_none_2b24536c71ed437a\gdiplus.dll while loading
drivers for device WPDBUSENUMROOT\UMB\2&37C186B&0&STORAGE#VOLUME#_??
_USBSTOR#DISK&VEN_ACTIONS&PROD_HS_USB_FLASHDISK&REV_2.00#6&292CF7D3&0
&_____&0#. Loading drivers to control a newly discovered device. (33)
0x8000000000000000 580 1700 Helen-PC NT AUTHORITY\LOCAL
SERVICE

14/09/2019 12:23:25.699 14 2006 Undefined Microsoft-Windows-
DriverFrameworks-UserMode/Operational Microsoft-Windows-DriverFrameworks-
UserMode The UMDF Host successfully loaded the driver at level 0. Stop (2)
Loading drivers to control a newly discovered device. (33)
0x8000000000000000 580 1700 Helen-PC NT AUTHORITY\LOCAL
SERVICE

14/09/2019 12:23:25.699 15 2100 Information Microsoft-Windows-

DriverFrameworks-UserMode/Operational Microsoft-Windows-DriverFrameworks-UserMode Received a Pnp or Power operation (27, 0) for device WPDBUSENUMROOT\UMB\2&37C186B&0&STORAGE#VOLUME#_??_USBSTOR#DISK&VEN_ACTIONS&PROD_HS_USB_FLASHDISK&REV_2.00#6&292CF7D3&0&_____&0#. Start (1) Pnp or Power Management operation to a particular device. (37) 0x8000000000000000 580 1700 Helen-PC NT AUTHORITY\LOCAL SERVICE

14/09/2019 12:23:25.699 16 2105 Information Microsoft-Windows-DriverFrameworks-UserMode/Operational Microsoft-Windows-DriverFrameworks-UserMode Forwarded a Pnp or Power operation (27, 0) for device WPDBUSENUMROOT\UMB\2&37C186B&0&STORAGE#VOLUME#_??_USBSTOR#DISK&VEN_ACTIONS&PROD_HS_USB_FLASHDISK&REV_2.00#6&292CF7D3&0&_____&0# to the lower driver with status 0xC00000BB Start (1) Pnp or Power Management operation to a particular device. (37) 0x8000000000000000 580 1700 Helen-PC NT AUTHORITY\LOCAL SERVICE

14/09/2019 12:23:25.699 9 2005 Verbose Microsoft-Windows-DriverFrameworks-UserMode/Operational Microsoft-Windows-DriverFrameworks-UserMode The UMDF Host Process ({E6641102-6E26-40A8-8F9A-38A76AFCE39F}) has loaded module C:\Windows\system32\WUDFx.dll while loading drivers for device WPDBUSENUMROOT\UMB\2&37C186B&0&STORAGE#VOLUME#_??_USBSTOR#DISK&VEN_ACTIONS&PROD_HS_USB_FLASHDISK&REV_2.00#6&292CF7D3&0&_____&0#. Loading drivers to control a newly discovered device. (33) 0x8000000000000000 580 1700 Helen-PC NT AUTHORITY\LOCAL SERVICE

14/09/2019 12:23:25.730 18 2101 Information Microsoft-Windows-DriverFrameworks-UserMode/Operational Microsoft-Windows-DriverFrameworks-UserMode Completed a Pnp or Power operation (27, 0) for device WPDBUSENUMROOT\UMB\2&37C186B&0&STORAGE#VOLUME#_??_USBSTOR#DISK&VEN_ACTIONS&PROD_HS_USB_FLASHDISK&REV_2.00#6&292CF7D3&0&_____&0# with status 0x0.Stop (2)Pnp or Power Management operation to a particular device. (37) 0x8000000000000000 580 1700 Helen-PC NT AUTHORITY\LOCAL SERVICE

14/09/2019 12:23:25.730 19 2100 Information Microsoft-Windows-DriverFrameworks-UserMode/Operational Microsoft-Windows-DriverFrameworks-UserMode Received a Pnp or Power operation (27, 9) for device WPDBUSENUMROOT\UMB\2&37C186B&0&STORAGE#VOLUME#_??_USBSTOR#DISK&VEN_ACTIONS&PROD_HS_USB_FLASHDISK&REV_2.00#6&292CF7D3&0&_____&0#. Start (1) Pnp or Power Management operation to a particular device. (37) 0x8000000000000000 580 1972 Helen-PC NT AUTHORITY\LOCAL SERVICE

14/09/2019 12:23:25.730 20 2105 Information Microsoft-Windows-DriverFrameworks-UserMode/Operational Microsoft-Windows-DriverFrameworks-UserMode Forwarded a Pnp or Power operation (27, 9) for device WPDBUSENUMROOT\UMB\2&37C186B&0&STORAGE#VOLUME#_??_USBSTOR#DISK&VEN_ACTIONS&PROD_HS_USB_FLASHDISK&REV_2.00#6&292CF7D3&0&_____&0# to the lower driver with status 0xC00000BB Start (1) Pnp or Power Management operation to a particular device. (37) 0x8000000000000000 580 1972 Helen-PC NT AUTHORITY\LOCAL SERVICE

14/09/2019 12:23:25.730 21 2106 Information Microsoft-Windows-DriverFrameworks-UserMode/Operational Microsoft-Windows-DriverFrameworks-UserMode Received a Pnp or Power operation (27, 9) for device WPDBUSENUMROOT\UMB\2&37C186B&0&STORAGE#VOLUME#_??_USBSTOR#DISK&VEN_ACTIONS&PROD_HS_USB_FLASHDISK&REV_2.00#6&292CF7D3&0&_____&0# which was completed by the lower drivers with status 0x0 Start (1) Pnp or Power Management operation to a particular device. (37) 0x8000000000000000 580 1972 Helen-PC NT AUTHORITY\LOCAL SERVICE

14/09/2019 12:23:25.730 22 2101 Information Microsoft-Windows-DriverFrameworks-UserMode/Operational Microsoft-Windows-DriverFrameworks-UserMode Completed a Pnp or Power operation (27, 9) for device WPDBUSENUMROOT\UMB\2&37C186B&0&STORAGE#VOLUME#_??_USBSTOR#DISK&VEN_ACTIONS&PROD_HS_USB_FLASHDISK&REV_2.00#6&292CF7D3&0&_____&0# with status 0x0.Stop (2)Pnp or Power Management operation to a particular device. (37) 0x8000000000000000 580 1972 Helen-PC NT AUTHORITY\LOCAL SERVICE

14/09/2019 12:23:25.730 23 2100 Information Microsoft-Windows-DriverFrameworks-UserMode/Operational Microsoft-Windows-DriverFrameworks-UserMode Received a Pnp or Power operation (27, 20) for device WPDBUSENUMROOT\UMB\2&37C186B&0&STORAGE#VOLUME#_??_USBSTOR#DISK&VEN_ACTIONS&PROD_HS_USB_FLASHDISK&REV_2.00#6&292CF7D3&0&_____&0#. Start (1) Pnp or Power Management operation to a particular device. (37) 0x8000000000000000 580 1700 Helen-PC NT AUTHORITY\LOCAL SERVICE

14/09/2019 12:23:25.730 24 2105 Information Microsoft-Windows-DriverFrameworks-UserMode/Operational Microsoft-Windows-DriverFrameworks-UserMode Forwarded a Pnp or Power operation (27, 20) for device WPDBUSENUMROOT\UMB\2&37C186B&0&STORAGE#VOLUME#_??_USBSTOR#DISK&VEN_ACTIONS&PROD_HS_USB_FLASHDISK&REV_2.00#6&292CF7D3&0&_____&0# to the lower driver with status 0xC00000BB Start (1) Pnp or Power Management operation to a particular device. (37) 0x8000000000000000 580

1700 Helen-PC NT AUTHORITY\LOCAL SERVICE

14/09/2019 12:23:25.730 26 2101 Information Microsoft-Windows-DriverFrameworks-UserMode/Operational Microsoft-Windows-DriverFrameworks-UserMode Completed a Pnp or Power operation (27, 20) for device WPDBUSENUMROOT\UMB\2&37C186B&0&STORAGE#VOLUME#_??_USBSTOR#DISK&VEN_ACTIONS&PROD_HS_USB_FLASHDISK&REV_2.00#6&292CF7D3&0&_____&0# with status 0x0.Stop (2)Pnp or Power Management operation to a particular device. (37) 0x8000000000000000 580 1700 Helen-PC NT AUTHORITY\LOCAL SERVICE

14/09/2019 12:23:25.730 25 2106 Information Microsoft-Windows-DriverFrameworks-UserMode/Operational Microsoft-Windows-DriverFrameworks-UserMode Received a Pnp or Power operation (27, 20) for device WPDBUSENUMROOT\UMB\2&37C186B&0&STORAGE#VOLUME#_??_USBSTOR#DISK&VEN_ACTIONS&PROD_HS_USB_FLASHDISK&REV_2.00#6&292CF7D3&0&_____&0# which was completed by the lower drivers with status 0x0 Start (1) Pnp or Power Management operation to a particular device. (37) 0x8000000000000000 580 1700 Helen-PC NT AUTHORITY\LOCAL SERVICE

14/09/2019 12:23:25.871 680 20001 Information System Microsoft-Windows-UserPnp Driver Management concluded the process to install driver FileRepository\wpdfs.inf_amd64_neutral_fc4ebadff3a40ae4\wpdfs.inf for Device Instance ID WPDBUSENUMROOT\UMB\2&37C186B&0&STORAGE#VOLUME#_??_USBSTOR#DISK&VEN_ACTIONS&PROD_HS_USB_FLASHDISK&REV_2.00#6&292CF7D3&0&_____&0# with the following status: 0x0. 7005 0x8000000000000000 1988 308 Helen-PC NT AUTHORITY\SYSTEM