Vino's Event Viewer v01c run on Windows 2008 in English
Report run at 11/04/2014 9:47:01 PM

Note: All dates below are in the format dd/mm/yyyy

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
'Application' Log - Critical Type
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
'Application' Log - Error Type
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
Log: 'Application' Date/Time: 09/04/2014 9:02:13 AM
Type: Error Category: 0
Event: 1026 Source: .NET Runtime
Application: Launchpad.exe
Framework Version: v4.0.30319
Description: The process was terminated due to an unhandled exception.
Exception Info: System.ObjectDisposedException
Stack:
   at System.IO.FileStream.get_Length()
   at
Microsoft.WindowsServerSolutions.Diagnostics.Logging.TraceListeners.RotatingLogTrace
Listener.UpdateWriter(System.String)
   at
Microsoft.WindowsServerSolutions.Diagnostics.Logging.TraceListeners.LogTraceListener
.Write(System.String)
   at
Microsoft.WindowsServerSolutions.Diagnostics.Logging.TraceListeners.LogTraceListener
.TraceData(System.Diagnostics.TraceEventCache, System.String,
System.Diagnostics.TraceEventType, Int32, System.Object)
   at
Microsoft.WindowsServerSolutions.Diagnostics.Logging.LogTraceSource.TraceData(System
.Diagnostics.TraceEventType, Int32,
Microsoft.WindowsServerSolutions.Diagnostics.Logging.LogEventInfo)
   at
Microsoft.WindowsServerSolutions.Diagnostics.Logging.LogOrchestrator.Write(Microsoft
.WindowsServerSolutions.Diagnostics.Logging.LogEventInfo)
   at Microsoft.WindowsServerSolutions.Diagnostics.Logging.Log.Write(System.Object,
System.Collections.Generic.IEnumerable`1<System.String>, Int32, Int32,
System.Diagnostics.TraceEventType, System.String)
   at
Microsoft.WindowsServerSolutions.Diagnostics.Logging.Log.WriteInfo(System.Object,
System.String)
   at
Microsoft.WindowsServerSolutions.Administration.Controls.AlertsView.AlertsViewer.Dis
pose(Boolean)
   at System.ComponentModel.Component.Dispose()
   at System.Windows.Forms.Control.Dispose(Boolean)
   at System.Windows.Forms.ContainerControl.Dispose(Boolean)
   at System.Windows.Forms.Form.Dispose(Boolean)
   at System.ComponentModel.Component.Dispose()
   at
Microsoft.WindowsServerSolutions.LaunchPad.MainWindow.alertsViewDialog_FormClosed(Sy
stem.Object, System.Windows.Forms.FormClosedEventArgs)
   at System.Windows.Forms.Form.WmClose(System.Windows.Forms.Message ByRef)
   at System.Windows.Forms.Form.WndProc(System.Windows.Forms.Message ByRef)
   at System.Windows.Forms.NativeWindow.DebuggableCallback(IntPtr, Int32, IntPtr,
IntPtr)
   at System.Windows.Forms.UnsafeNativeMethods.CallWindowProc(IntPtr, IntPtr, Int32,
IntPtr, IntPtr)
   at System.Windows.Forms.UnsafeNativeMethods.CallWindowProc(IntPtr, IntPtr, Int32,
IntPtr, IntPtr)
   at System.Windows.Forms.NativeWindow.DefWndProc(System.Windows.Forms.Message

```
ByRef)
   at System.Windows.Forms.Form.DefWndProc(System.Windows.Forms.Message ByRef)
   at System.Windows.Forms.Control.WndProc(System.Windows.Forms.Message ByRef)
   at System.Windows.Forms.Form.WndProc(System.Windows.Forms.Message ByRef)
   at System.Windows.Forms.NativeWindow.DebuggableCallback(IntPtr, Int32, IntPtr,
IntPtr)


Log: 'Application' Date/Time: 07/04/2014 12:15:42 AM
Type: Error Category: 0
Event: 8206 Source: System Restore
The restore point selected was damaged or deleted during the restore (Scheduled
Checkpoint).

Log: 'Application' Date/Time: 06/04/2014 1:37:11 PM
Type: Error Category: 0
Event: 1026 Source: .NET Runtime
Application: Launchpad.exe
Framework Version: v4.0.30319
Description: The process was terminated due to an unhandled exception.
Exception Info: System.ObjectDisposedException
Stack:
   at System.IO.FileStream.get_Length()
   at
Microsoft.WindowsServerSolutions.Diagnostics.Logging.TraceListeners.RotatingLogTrace
Listener.UpdateWriter(System.String)
   at
Microsoft.WindowsServerSolutions.Diagnostics.Logging.TraceListeners.LogTraceListener
.Write(System.String)
   at
Microsoft.WindowsServerSolutions.Diagnostics.Logging.TraceListeners.LogTraceListener
.TraceData(System.Diagnostics.TraceEventCache, System.String,
System.Diagnostics.TraceEventType, Int32, System.Object)
   at
Microsoft.WindowsServerSolutions.Diagnostics.Logging.LogTraceSource.TraceData(System
.Diagnostics.TraceEventType, Int32,
Microsoft.WindowsServerSolutions.Diagnostics.Logging.LogEventInfo)
   at
Microsoft.WindowsServerSolutions.Diagnostics.Logging.LogOrchestrator.Write(Microsoft
.WindowsServerSolutions.Diagnostics.Logging.LogEventInfo)
   at Microsoft.WindowsServerSolutions.Diagnostics.Logging.Log.Write(System.Object,
System.Collections.Generic.IEnumerable`1<System.String>, Int32, Int32,
System.Diagnostics.TraceEventType, System.String)
   at
Microsoft.WindowsServerSolutions.Diagnostics.Logging.Log.WriteInfo(System.Object,
System.String)
   at
Microsoft.WindowsServerSolutions.Administration.Controls.AlertsView.AlertsViewer.Dis
pose(Boolean)
   at System.ComponentModel.Component.Dispose()
   at System.Windows.Forms.Control.Dispose(Boolean)
   at System.Windows.Forms.ContainerControl.Dispose(Boolean)
   at System.Windows.Forms.Form.Dispose(Boolean)
   at System.ComponentModel.Component.Dispose()
   at
Microsoft.WindowsServerSolutions.LaunchPad.MainWindow.alertsViewDialog_FormClosed(Sy
stem.Object, System.Windows.Forms.FormClosedEventArgs)
   at System.Windows.Forms.Form.WmClose(System.Windows.Forms.Message ByRef)
   at System.Windows.Forms.Form.WndProc(System.Windows.Forms.Message ByRef)
   at System.Windows.Forms.NativeWindow.DebuggableCallback(IntPtr, Int32, IntPtr,
IntPtr)
   at System.Windows.Forms.UnsafeNativeMethods.CallWindowProc(IntPtr, IntPtr, Int32,
IntPtr, IntPtr)
```

```
   at System.Windows.Forms.UnsafeNativeMethods.CallWindowProc(IntPtr, IntPtr, Int32,
IntPtr, IntPtr)
   at System.Windows.Forms.NativeWindow.DefWndProc(System.Windows.Forms.Message
ByRef)
   at System.Windows.Forms.Form.DefWndProc(System.Windows.Forms.Message ByRef)
   at System.Windows.Forms.Control.WndProc(System.Windows.Forms.Message ByRef)
   at System.Windows.Forms.Form.WndProc(System.Windows.Forms.Message ByRef)
   at System.Windows.Forms.NativeWindow.DebuggableCallback(IntPtr, Int32, IntPtr,
IntPtr)


Log: 'Application' Date/Time: 06/04/2014 8:05:13 AM
Type: Error Category: 0
Event: 1026 Source: .NET Runtime
Application: Launchpad.exe
Framework Version: v4.0.30319
Description: The process was terminated due to an unhandled exception.
Exception Info: System.NullReferenceException
Stack:
   at System.Windows.Forms.ListView+ListViewNativeItemCollection.get_Item(Int32)
   at System.Windows.Forms.ListView+ListViewItemCollection.get_Item(Int32)
   at System.Windows.Forms.ListView+ListViewNativeItemCollection.Clear()
   at System.Windows.Forms.ListView.Dispose(Boolean)
   at System.ComponentModel.Component.Dispose()
   at System.Windows.Forms.Control.Dispose(Boolean)
   at System.ComponentModel.Component.Dispose()
   at System.Windows.Forms.Control.Dispose(Boolean)
   at System.Windows.Forms.ContainerControl.Dispose(Boolean)
   at System.ComponentModel.Component.Dispose()
   at System.Windows.Forms.Control.Dispose(Boolean)
   at System.Windows.Forms.ContainerControl.Dispose(Boolean)
   at
Microsoft.WindowsServerSolutions.Administration.Controls.AlertsView.AlertsViewer.Dis
pose(Boolean)
   at System.ComponentModel.Component.Dispose()
   at System.Windows.Forms.Control.Dispose(Boolean)
   at System.Windows.Forms.ContainerControl.Dispose(Boolean)
   at System.Windows.Forms.Form.Dispose(Boolean)
   at System.ComponentModel.Component.Dispose()
   at
Microsoft.WindowsServerSolutions.LaunchPad.MainWindow.alertsViewDialog_FormClosed(Sy
stem.Object, System.Windows.Forms.FormClosedEventArgs)
   at System.Windows.Forms.Form.WmClose(System.Windows.Forms.Message ByRef)
   at System.Windows.Forms.Form.WndProc(System.Windows.Forms.Message ByRef)
   at System.Windows.Forms.NativeWindow.DebuggableCallback(IntPtr, Int32, IntPtr,
IntPtr)


Log: 'Application' Date/Time: 19/03/2014 5:49:04 AM
Type: Error Category: 0
Event: 8194 Source: VSS
Volume Shadow Copy Service error: Unexpected error querying for the
IVssWriterCallback interface.  hr = 0x80070005, Access is denied. . This is often
caused by incorrect security settings in either the writer or requestor process.

Operation:
   Gathering Writer Data

Context:
   Writer Class Id: {e8132975-6f93-4464-a53e-1050253ae220}
   Writer Name: System Writer
   Writer Instance ID: {dc4596fd-8f1b-4130-922c-dcb215ee4e32}
```

Log: 'Application' Date/Time: 19/03/2014 1:42:35 AM
Type: Error Category: 0
Event: 8193 Source: System Restore
Failed to create restore point (Process = C:\Windows\system32\svchost.exe -k netsvcs; Description = Windows Update; Error = 0x81000101).

Log: 'Application' Date/Time: 18/03/2014 6:01:03 AM
Type: Error Category: 0
Event: 8194 Source: VSS
Volume Shadow Copy Service error: Unexpected error querying for the IVssWriterCallback interface. hr = 0x80070005, Access is denied. . This is often caused by incorrect security settings in either the writer or requestor process.

Operation:
Gathering Writer Data

Context:
Writer Class Id: {e8132975-6f93-4464-a53e-1050253ae220}
Writer Name: System Writer
Writer Instance ID: {dc4596fd-8f1b-4130-922c-dcb215ee4e32}

Log: 'Application' Date/Time: 17/03/2014 5:22:02 AM
Type: Error Category: 0
Event: 8194 Source: VSS
Volume Shadow Copy Service error: Unexpected error querying for the IVssWriterCallback interface. hr = 0x80070005, Access is denied. . This is often caused by incorrect security settings in either the writer or requestor process.

Operation:
Gathering Writer Data

Context:
Writer Class Id: {e8132975-6f93-4464-a53e-1050253ae220}
Writer Name: System Writer
Writer Instance ID: {dc4596fd-8f1b-4130-922c-dcb215ee4e32}

Log: 'Application' Date/Time: 16/03/2014 5:04:16 AM
Type: Error Category: 0
Event: 8194 Source: VSS
Volume Shadow Copy Service error: Unexpected error querying for the IVssWriterCallback interface. hr = 0x80070005, Access is denied. . This is often caused by incorrect security settings in either the writer or requestor process.

Operation:
Gathering Writer Data

Context:
Writer Class Id: {e8132975-6f93-4464-a53e-1050253ae220}
Writer Name: System Writer
Writer Instance ID: {dc4596fd-8f1b-4130-922c-dcb215ee4e32}

Log: 'Application' Date/Time: 15/03/2014 6:36:02 AM
Type: Error Category: 0
Event: 8194 Source: VSS
Volume Shadow Copy Service error: Unexpected error querying for the IVssWriterCallback interface. hr = 0x80070005, Access is denied. . This is often caused by incorrect security settings in either the writer or requestor process.

Operation:
Gathering Writer Data

Context:
Writer Class Id: {e8132975-6f93-4464-a53e-1050253ae220}

```
   Writer Name: System Writer
   Writer Instance ID: {dc4596fd-8f1b-4130-922c-dcb215ee4e32}

Log: 'Application' Date/Time: 14/03/2014 5:32:03 AM
Type: Error Category: 0
Event: 8194 Source: VSS
Volume Shadow Copy Service error: Unexpected error querying for the
IVssWriterCallback interface.  hr = 0x80070005, Access is denied. . This is often
caused by incorrect security settings in either the writer or requestor process.

Operation:
   Gathering Writer Data

Context:
   Writer Class Id: {e8132975-6f93-4464-a53e-1050253ae220}
   Writer Name: System Writer
   Writer Instance ID: {dc4596fd-8f1b-4130-922c-dcb215ee4e32}

Log: 'Application' Date/Time: 13/03/2014 5:05:05 AM
Type: Error Category: 0
Event: 8194 Source: VSS
Volume Shadow Copy Service error: Unexpected error querying for the
IVssWriterCallback interface.  hr = 0x80070005, Access is denied. . This is often
caused by incorrect security settings in either the writer or requestor process.

Operation:
   Gathering Writer Data

Context:
   Writer Class Id: {e8132975-6f93-4464-a53e-1050253ae220}
   Writer Name: System Writer
   Writer Instance ID: {dc4596fd-8f1b-4130-922c-dcb215ee4e32}

Log: 'Application' Date/Time: 04/03/2014 6:27:43 AM
Type: Error Category: 100
Event: 1000 Source: Application Error
Faulting application name: dragon_updater.exe, version: 0.0.0.0, time stamp:
0x51a5da71 Faulting module name: unknown, version: 0.0.0.0, time stamp: 0x00000000
Exception code: 0xc0000005 Fault offset: 0x00000000 Faulting process id: 0x6f0
Faulting application start time: 0x01cf28953af8fec4 Faulting application path:
C:\Program Files (x86)\Comodo\Dragon\dragon_updater.exe Faulting module path:
unknown Report Id: 17533237-a366-11e3-9a63-78acc0bed4a8

Log: 'Application' Date/Time: 16/02/2014 6:40:04 AM
Type: Error Category: 0
Event: 8194 Source: VSS
Volume Shadow Copy Service error: Unexpected error querying for the
IVssWriterCallback interface.  hr = 0x80070005, Access is denied. . This is often
caused by incorrect security settings in either the writer or requestor process.

Operation:
   Gathering Writer Data

Context:
   Writer Class Id: {e8132975-6f93-4464-a53e-1050253ae220}
   Writer Name: System Writer
   Writer Instance ID: {38154832-8764-405b-b72b-cf67667fb791}

Log: 'Application' Date/Time: 15/02/2014 5:59:10 AM
Type: Error Category: 0
Event: 8194 Source: VSS
Volume Shadow Copy Service error: Unexpected error querying for the
IVssWriterCallback interface.  hr = 0x80070005, Access is denied. . This is often
```

caused by incorrect security settings in either the writer or requestor process.

Operation:
   Gathering Writer Data

Context:
   Writer Class Id: {e8132975-6f93-4464-a53e-1050253ae220}
   Writer Name: System Writer
   Writer Instance ID: {38154832-8764-405b-b72b-cf67667fb791}

Log: 'Application' Date/Time: 14/02/2014 6:30:05 AM
Type: Error Category: 0
Event: 8194 Source: VSS
Volume Shadow Copy Service error: Unexpected error querying for the
IVssWriterCallback interface. hr = 0x80070005, Access is denied. . This is often
caused by incorrect security settings in either the writer or requestor process.

Operation:
   Gathering Writer Data

Context:
   Writer Class Id: {e8132975-6f93-4464-a53e-1050253ae220}
   Writer Name: System Writer
   Writer Instance ID: {38154832-8764-405b-b72b-cf67667fb791}

Log: 'Application' Date/Time: 21/01/2014 7:00:50 AM
Type: Error Category: 0
Event: 8194 Source: VSS
Volume Shadow Copy Service error: Unexpected error querying for the
IVssWriterCallback interface. hr = 0x80070005, Access is denied. . This is often
caused by incorrect security settings in either the writer or requestor process.

Operation:
   Gathering Writer Data

Context:
   Writer Class Id: {e8132975-6f93-4464-a53e-1050253ae220}
   Writer Name: System Writer
   Writer Instance ID: {d123063a-1b87-47ed-af08-81b0a56382e4}

Log: 'Application' Date/Time: 20/01/2014 7:28:10 AM
Type: Error Category: 0
Event: 8194 Source: VSS
Volume Shadow Copy Service error: Unexpected error querying for the
IVssWriterCallback interface. hr = 0x80070005, Access is denied. . This is often
caused by incorrect security settings in either the writer or requestor process.

Operation:
   Gathering Writer Data

Context:
   Writer Class Id: {e8132975-6f93-4464-a53e-1050253ae220}
   Writer Name: System Writer
   Writer Instance ID: {d123063a-1b87-47ed-af08-81b0a56382e4}

Log: 'Application' Date/Time: 19/01/2014 6:55:27 AM
Type: Error Category: 0
Event: 8194 Source: VSS
Volume Shadow Copy Service error: Unexpected error querying for the
IVssWriterCallback interface. hr = 0x80070005, Access is denied. . This is often
caused by incorrect security settings in either the writer or requestor process.

Operation:

```
   Gathering Writer Data

Context:
   Writer Class Id: {e8132975-6f93-4464-a53e-1050253ae220}
   Writer Name: System Writer
   Writer Instance ID: {d123063a-1b87-47ed-af08-81b0a56382e4}

Log: 'Application' Date/Time: 18/01/2014 5:55:03 AM
Type: Error Category: 0
Event: 8194 Source: VSS
Volume Shadow Copy Service error: Unexpected error querying for the
IVssWriterCallback interface.  hr = 0x80070005, Access is denied. . This is often
caused by incorrect security settings in either the writer or requestor process.

Operation:
   Gathering Writer Data

Context:
   Writer Class Id: {e8132975-6f93-4464-a53e-1050253ae220}
   Writer Name: System Writer
   Writer Instance ID: {d123063a-1b87-47ed-af08-81b0a56382e4}

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
'Application' Log - Warning Type
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
Log: 'Application' Date/Time: 08/04/2014 5:33:54 AM
Type: Warning Category: 0
Event: 1530 Source: Microsoft-Windows-User Profiles Service
Windows detected your registry file is still in use by other applications or
services. The file will be unloaded now. The applications or services that hold your
registry file may not function properly afterwards.     DETAIL -   1 user registry
handles leaked from \Registry\User\S-1-5-21-3455503661-4230816971-2044476751-1022:
Process 5568 (\Device\HarddiskVolume2\Windows\System32\msiexec.exe) has opened key
\REGISTRY\USER\S-1-5-21-3455503661-4230816971-2044476751-1022\Software\Microsoft\Win
dows\CurrentVersion\Explorer\FileExts


Log: 'Application' Date/Time: 06/04/2014 9:09:39 AM
Type: Warning Category: 0
Event: 1530 Source: Microsoft-Windows-User Profiles Service
Windows detected your registry file is still in use by other applications or
services. The file will be unloaded now. The applications or services that hold your
registry file may not function properly afterwards.     DETAIL -   5 user registry
handles leaked from \Registry\User\S-1-5-21-3455503661-4230816971-2044476751-1022:
Process 696 (\Device\HarddiskVolume2\Windows\System32\lsass.exe) has opened key
\REGISTRY\USER\S-1-5-21-3455503661-4230816971-2044476751-1022
Process 696 (\Device\HarddiskVolume2\Windows\System32\lsass.exe) has opened key
\REGISTRY\USER\S-1-5-21-3455503661-4230816971-2044476751-1022
Process 696 (\Device\HarddiskVolume2\Windows\System32\lsass.exe) has opened key
\REGISTRY\USER\S-1-5-21-3455503661-4230816971-2044476751-1022\Software\Microsoft\Sys
temCertificates\Disallowed
Process 696 (\Device\HarddiskVolume2\Windows\System32\lsass.exe) has opened key
\REGISTRY\USER\S-1-5-21-3455503661-4230816971-2044476751-1022\Software\Microsoft\Sys
temCertificates\My
Process 696 (\Device\HarddiskVolume2\Windows\System32\lsass.exe) has opened key
\REGISTRY\USER\S-1-5-21-3455503661-4230816971-2044476751-1022\Software\Microsoft\Sys
temCertificates\CA


Log: 'Application' Date/Time: 13/02/2014 8:05:45 AM
Type: Warning Category: 0
Event: 10010 Source: Microsoft-Windows-RestartManager
Application 'C:\Program Files\Windows Server\Bin\Launchpad.exe' (pid 4328) cannot be
```

restarted - Application SID does not match Conductor SID..

Log: 'Application' Date/Time: 13/02/2014 8:05:45 AM
Type: Warning Category: 0
Event: 10010 Source: Microsoft-Windows-RestartManager
Application 'C:\Program Files\Windows Server\Bin\Launchpad.exe' (pid 4328) cannot be restarted - Application SID does not match Conductor SID..

Log: 'Application' Date/Time: 13/02/2014 8:03:55 AM
Type: Warning Category: 1
Event: 1020 Source: ASP.NET 4.0.30319.0
Updates to the IIS metabase were aborted because IIS is either not installed or is disabled on this machine. To configure ASP.NET to run in IIS, please install or enable IIS and re-register ASP.NET using aspnet_regiis.exe /i.

Log: 'Application' Date/Time: 13/02/2014 8:03:48 AM
Type: Warning Category: 1
Event: 1020 Source: ASP.NET 4.0.30319.0
Updates to the IIS metabase were aborted because IIS is either not installed or is disabled on this machine. To configure ASP.NET to run in IIS, please install or enable IIS and re-register ASP.NET using aspnet_regiis.exe /i.

Log: 'Application' Date/Time: 15/01/2014 8:22:52 AM
Type: Warning Category: 0
Event: 6004 Source: Microsoft-Windows-Winlogon
The winlogon notification subscriber <TrustedInstaller> failed a critical notification event.

Log: 'Application' Date/Time: 15/01/2014 8:22:52 AM
Type: Warning Category: 0
Event: 6006 Source: Microsoft-Windows-Winlogon
The winlogon notification subscriber <TrustedInstaller> took 108 second(s) to handle the notification event (CreateSession).

Log: 'Application' Date/Time: 15/01/2014 8:22:03 AM
Type: Warning Category: 0
Event: 6005 Source: Microsoft-Windows-Winlogon
The winlogon notification subscriber <TrustedInstaller> is taking long time to handle the notification event (CreateSession).

Log: 'Application' Date/Time: 15/01/2014 8:17:28 AM
Type: Warning Category: 0
Event: 1530 Source: Microsoft-Windows-User Profiles Service
Windows detected your registry file is still in use by other applications or services. The file will be unloaded now. The applications or services that hold your registry file may not function properly afterwards. DETAIL - 5 user registry handles leaked from \Registry\User\S-1-5-21-3455503661-4230816971-2044476751-1022:
Process 740 (\Device\HarddiskVolume2\Windows\System32\lsass.exe) has opened key \REGISTRY\USER\S-1-5-21-3455503661-4230816971-2044476751-1022
Process 740 (\Device\HarddiskVolume2\Windows\System32\lsass.exe) has opened key \REGISTRY\USER\S-1-5-21-3455503661-4230816971-2044476751-1022
Process 740 (\Device\HarddiskVolume2\Windows\System32\lsass.exe) has opened key \REGISTRY\USER\S-1-5-21-3455503661-4230816971-2044476751-1022\Software\Microsoft\SystemCertificates\Disallowed
Process 740 (\Device\HarddiskVolume2\Windows\System32\lsass.exe) has opened key \REGISTRY\USER\S-1-5-21-3455503661-4230816971-2044476751-1022\Software\Microsoft\SystemCertificates\My
Process 740 (\Device\HarddiskVolume2\Windows\System32\lsass.exe) has opened key \REGISTRY\USER\S-1-5-21-3455503661-4230816971-2044476751-1022\Software\Microsoft\SystemCertificates\CA

Log: 'Application' Date/Time: 11/01/2014 11:49:06 PM

Type: Warning Category: 0
Event: 1015 Source: MsiInstaller
Failed to connect to server. Error: 0x800401F0

Log: 'Application' Date/Time: 11/01/2014 11:49:06 PM
Type: Warning Category: 0
Event: 1015 Source: MsiInstaller
Failed to connect to server. Error: 0x800401F0

Log: 'Application' Date/Time: 11/01/2014 11:49:06 PM
Type: Warning Category: 0
Event: 1015 Source: MsiInstaller
Failed to connect to server. Error: 0x800401F0

Log: 'Application' Date/Time: 11/01/2014 11:49:06 PM
Type: Warning Category: 0
Event: 1015 Source: MsiInstaller
Failed to connect to server. Error: 0x800401F0

Log: 'Application' Date/Time: 11/01/2014 11:49:06 PM
Type: Warning Category: 0
Event: 1015 Source: MsiInstaller
Failed to connect to server. Error: 0x800401F0

Log: 'Application' Date/Time: 11/01/2014 11:49:04 PM
Type: Warning Category: 0
Event: 1015 Source: MsiInstaller
Failed to connect to server. Error: 0x800401F0

Log: 'Application' Date/Time: 11/01/2014 11:49:04 PM
Type: Warning Category: 0
Event: 1015 Source: MsiInstaller
Failed to connect to server. Error: 0x800401F0

Log: 'Application' Date/Time: 11/01/2014 11:48:59 PM
Type: Warning Category: 0
Event: 1015 Source: MsiInstaller
Failed to connect to server. Error: 0x800401F0

Log: 'Application' Date/Time: 11/01/2014 9:53:41 PM
Type: Warning Category: 0
Event: 1530 Source: Microsoft-Windows-User Profiles Service
Windows detected your registry file is still in use by other applications or services. The file will be unloaded now. The applications or services that hold your registry file may not function properly afterwards.   DETAIL -   5 user registry handles leaked from \Registry\User\S-1-5-21-3455503661-4230816971-2044476751-1022:
Process 648 (\Device\HarddiskVolume2\Windows\System32\lsass.exe) has opened key \REGISTRY\USER\S-1-5-21-3455503661-4230816971-2044476751-1022
Process 648 (\Device\HarddiskVolume2\Windows\System32\lsass.exe) has opened key \REGISTRY\USER\S-1-5-21-3455503661-4230816971-2044476751-1022
Process 648 (\Device\HarddiskVolume2\Windows\System32\lsass.exe) has opened key \REGISTRY\USER\S-1-5-21-3455503661-4230816971-2044476751-1022\Software\Microsoft\SystemCertificates\Disallowed
Process 648 (\Device\HarddiskVolume2\Windows\System32\lsass.exe) has opened key \REGISTRY\USER\S-1-5-21-3455503661-4230816971-2044476751-1022\Software\Microsoft\SystemCertificates\My
Process 648 (\Device\HarddiskVolume2\Windows\System32\lsass.exe) has opened key \REGISTRY\USER\S-1-5-21-3455503661-4230816971-2044476751-1022\Software\Microsoft\SystemCertificates\CA

Log: 'Application' Date/Time: 25/12/2013 4:16:43 AM
Type: Warning Category: 0

VEW

Event: 1530 Source: Microsoft-Windows-User Profiles Service
Windows detected your registry file is still in use by other applications or services. The file will be unloaded now. The applications or services that hold your registry file may not function properly afterwards. DETAIL - 1 user registry handles leaked from
\Registry\User\S-1-5-21-3455503661-4230816971-2044476751-1022_Classes:
Process 1728 (\Device\HarddiskVolume2\Program Files\SUPERAntiSpyware\SASCore64.exe) has opened key \REGISTRY\USER\S-1-5-21-3455503661-4230816971-2044476751-1022_CLASSES

Vino's Event Viewer v01c run on Windows 2008 in English
Report run at 11/04/2014 9:45:34 PM

Note: All dates below are in the format dd/mm/yyyy

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
'Application' Log - Critical Type
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
'Application' Log - Error Type
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
Log: 'Application' Date/Time: 09/04/2014 9:02:13 AM
Type: Error Category: 0
Event: 1026 Source: .NET Runtime
Application: Launchpad.exe
Framework Version: v4.0.30319
Description: The process was terminated due to an unhandled exception.
Exception Info: System.ObjectDisposedException
Stack:
   at System.IO.FileStream.get_Length()
   at
Microsoft.WindowsServerSolutions.Diagnostics.Logging.TraceListeners.RotatingLogTrace
Listener.UpdateWriter(System.String)
   at
Microsoft.WindowsServerSolutions.Diagnostics.Logging.TraceListeners.LogTraceListener
.Write(System.String)
   at
Microsoft.WindowsServerSolutions.Diagnostics.Logging.TraceListeners.LogTraceListener
.TraceData(System.Diagnostics.TraceEventCache, System.String,
System.Diagnostics.TraceEventType, Int32, System.Object)
   at
Microsoft.WindowsServerSolutions.Diagnostics.Logging.LogTraceSource.TraceData(System
.Diagnostics.TraceEventType, Int32,
Microsoft.WindowsServerSolutions.Diagnostics.Logging.LogEventInfo)
   at
Microsoft.WindowsServerSolutions.Diagnostics.Logging.LogOrchestrator.Write(Microsoft
.WindowsServerSolutions.Diagnostics.Logging.LogEventInfo)
   at Microsoft.WindowsServerSolutions.Diagnostics.Logging.Log.Write(System.Object,
System.Collections.Generic.IEnumerable`1<System.String>, Int32, Int32,
System.Diagnostics.TraceEventType, System.String)
   at
Microsoft.WindowsServerSolutions.Diagnostics.Logging.Log.WriteInfo(System.Object,
System.String)
   at
Microsoft.WindowsServerSolutions.Administration.Controls.AlertsView.AlertsViewer.Dis
pose(Boolean)
   at System.ComponentModel.Component.Dispose()
   at System.Windows.Forms.Control.Dispose(Boolean)
   at System.Windows.Forms.ContainerControl.Dispose(Boolean)
   at System.Windows.Forms.Form.Dispose(Boolean)
   at System.ComponentModel.Component.Dispose()
   at
Microsoft.WindowsServerSolutions.LaunchPad.MainWindow.alertsViewDialog_FormClosed(Sy
stem.Object, System.Windows.Forms.FormClosedEventArgs)
   at System.Windows.Forms.Form.WmClose(System.Windows.Forms.Message ByRef)
   at System.Windows.Forms.Form.WndProc(System.Windows.Forms.Message ByRef)
   at System.Windows.Forms.NativeWindow.DebuggableCallback(IntPtr, Int32, IntPtr,
IntPtr)
   at System.Windows.Forms.UnsafeNativeMethods.CallWindowProc(IntPtr, IntPtr, Int32,
IntPtr, IntPtr)
   at System.Windows.Forms.UnsafeNativeMethods.CallWindowProc(IntPtr, IntPtr, Int32,
IntPtr, IntPtr)
   at System.Windows.Forms.NativeWindow.DefWndProc(System.Windows.Forms.Message

```
ByRef)
   at System.Windows.Forms.Form.DefWndProc(System.Windows.Forms.Message ByRef)
   at System.Windows.Forms.Control.WndProc(System.Windows.Forms.Message ByRef)
   at System.Windows.Forms.Form.WndProc(System.Windows.Forms.Message ByRef)
   at System.Windows.Forms.NativeWindow.DebuggableCallback(IntPtr, Int32, IntPtr,
IntPtr)


Log: 'Application' Date/Time: 07/04/2014 12:15:42 AM
Type: Error Category: 0
Event: 8206 Source: System Restore
The restore point selected was damaged or deleted during the restore (Scheduled
Checkpoint).

Log: 'Application' Date/Time: 06/04/2014 1:37:11 PM
Type: Error Category: 0
Event: 1026 Source: .NET Runtime
Application: Launchpad.exe
Framework Version: v4.0.30319
Description: The process was terminated due to an unhandled exception.
Exception Info: System.ObjectDisposedException
Stack:
   at System.IO.FileStream.get_Length()
   at
Microsoft.WindowsServerSolutions.Diagnostics.Logging.TraceListeners.RotatingLogTrace
Listener.UpdateWriter(System.String)
   at
Microsoft.WindowsServerSolutions.Diagnostics.Logging.TraceListeners.LogTraceListener
.Write(System.String)
   at
Microsoft.WindowsServerSolutions.Diagnostics.Logging.TraceListeners.LogTraceListener
.TraceData(System.Diagnostics.TraceEventCache, System.String,
System.Diagnostics.TraceEventType, Int32, System.Object)
   at
Microsoft.WindowsServerSolutions.Diagnostics.Logging.LogTraceSource.TraceData(System
.Diagnostics.TraceEventType, Int32,
Microsoft.WindowsServerSolutions.Diagnostics.Logging.LogEventInfo)
   at
Microsoft.WindowsServerSolutions.Diagnostics.Logging.LogOrchestrator.Write(Microsoft
.WindowsServerSolutions.Diagnostics.Logging.LogEventInfo)
   at Microsoft.WindowsServerSolutions.Diagnostics.Logging.Log.Write(System.Object,
System.Collections.Generic.IEnumerable`1<System.String>, Int32, Int32,
System.Diagnostics.TraceEventType, System.String)
   at
Microsoft.WindowsServerSolutions.Diagnostics.Logging.Log.WriteInfo(System.Object,
System.String)
   at
Microsoft.WindowsServerSolutions.Administration.Controls.AlertsView.AlertsViewer.Dis
pose(Boolean)
   at System.ComponentModel.Component.Dispose()
   at System.Windows.Forms.Control.Dispose(Boolean)
   at System.Windows.Forms.ContainerControl.Dispose(Boolean)
   at System.Windows.Forms.Form.Dispose(Boolean)
   at System.ComponentModel.Component.Dispose()
   at
Microsoft.WindowsServerSolutions.LaunchPad.MainWindow.alertsViewDialog_FormClosed(Sy
stem.Object, System.Windows.Forms.FormClosedEventArgs)
   at System.Windows.Forms.Form.WmClose(System.Windows.Forms.Message ByRef)
   at System.Windows.Forms.Form.WndProc(System.Windows.Forms.Message ByRef)
   at System.Windows.Forms.NativeWindow.DebuggableCallback(IntPtr, Int32, IntPtr,
IntPtr)
   at System.Windows.Forms.UnsafeNativeMethods.CallWindowProc(IntPtr, IntPtr, Int32,
IntPtr, IntPtr)
```

```
   at System.Windows.Forms.UnsafeNativeMethods.CallWindowProc(IntPtr, IntPtr, Int32,
IntPtr, IntPtr)
   at System.Windows.Forms.NativeWindow.DefWndProc(System.Windows.Forms.Message
ByRef)
   at System.Windows.Forms.Form.DefWndProc(System.Windows.Forms.Message ByRef)
   at System.Windows.Forms.Control.WndProc(System.Windows.Forms.Message ByRef)
   at System.Windows.Forms.Form.WndProc(System.Windows.Forms.Message ByRef)
   at System.Windows.Forms.NativeWindow.DebuggableCallback(IntPtr, Int32, IntPtr,
IntPtr)
```

```
Log: 'Application' Date/Time: 06/04/2014 8:05:13 AM
Type: Error Category: 0
Event: 1026 Source: .NET Runtime
Application: Launchpad.exe
Framework Version: v4.0.30319
Description: The process was terminated due to an unhandled exception.
Exception Info: System.NullReferenceException
Stack:
   at System.Windows.Forms.ListView+ListViewNativeItemCollection.get_Item(Int32)
   at System.Windows.Forms.ListView+ListViewItemCollection.get_Item(Int32)
   at System.Windows.Forms.ListView+ListViewNativeItemCollection.Clear()
   at System.Windows.Forms.ListView.Dispose(Boolean)
   at System.ComponentModel.Component.Dispose()
   at System.Windows.Forms.Control.Dispose(Boolean)
   at System.ComponentModel.Component.Dispose()
   at System.Windows.Forms.Control.Dispose(Boolean)
   at System.Windows.Forms.ContainerControl.Dispose(Boolean)
   at System.ComponentModel.Component.Dispose()
   at System.Windows.Forms.Control.Dispose(Boolean)
   at System.Windows.Forms.ContainerControl.Dispose(Boolean)
   at
Microsoft.WindowsServerSolutions.Administration.Controls.AlertsView.AlertsViewer.Dis
pose(Boolean)
   at System.ComponentModel.Component.Dispose()
   at System.Windows.Forms.Control.Dispose(Boolean)
   at System.Windows.Forms.ContainerControl.Dispose(Boolean)
   at System.Windows.Forms.Form.Dispose(Boolean)
   at System.ComponentModel.Component.Dispose()
   at
Microsoft.WindowsServerSolutions.LaunchPad.MainWindow.alertsViewDialog_FormClosed(Sy
stem.Object, System.Windows.Forms.FormClosedEventArgs)
   at System.Windows.Forms.Form.WmClose(System.Windows.Forms.Message ByRef)
   at System.Windows.Forms.Form.WndProc(System.Windows.Forms.Message ByRef)
   at System.Windows.Forms.NativeWindow.DebuggableCallback(IntPtr, Int32, IntPtr,
IntPtr)
```

```
Log: 'Application' Date/Time: 19/03/2014 5:49:04 AM
Type: Error Category: 0
Event: 8194 Source: VSS
Volume Shadow Copy Service error: Unexpected error querying for the
IVssWriterCallback interface.  hr = 0x80070005, Access is denied. . This is often
caused by incorrect security settings in either the writer or requestor process.

Operation:
   Gathering Writer Data

Context:
   Writer Class Id: {e8132975-6f93-4464-a53e-1050253ae220}
   Writer Name: System Writer
   Writer Instance ID: {dc4596fd-8f1b-4130-922c-dcb215ee4e32}
```

Log: 'Application' Date/Time: 19/03/2014 1:42:35 AM
Type: Error Category: 0
Event: 8193 Source: System Restore
Failed to create restore point (Process = C:\Windows\system32\svchost.exe -k netsvcs; Description = Windows Update; Error = 0x81000101).

Log: 'Application' Date/Time: 18/03/2014 6:01:03 AM
Type: Error Category: 0
Event: 8194 Source: VSS
Volume Shadow Copy Service error: Unexpected error querying for the IVssWriterCallback interface. hr = 0x80070005, Access is denied. . This is often caused by incorrect security settings in either the writer or requestor process.

Operation:
   Gathering Writer Data

Context:
   Writer Class Id: {e8132975-6f93-4464-a53e-1050253ae220}
   Writer Name: System Writer
   Writer Instance ID: {dc4596fd-8f1b-4130-922c-dcb215ee4e32}

Log: 'Application' Date/Time: 17/03/2014 5:22:02 AM
Type: Error Category: 0
Event: 8194 Source: VSS
Volume Shadow Copy Service error: Unexpected error querying for the IVssWriterCallback interface. hr = 0x80070005, Access is denied. . This is often caused by incorrect security settings in either the writer or requestor process.

Operation:
   Gathering Writer Data

Context:
   Writer Class Id: {e8132975-6f93-4464-a53e-1050253ae220}
   Writer Name: System Writer
   Writer Instance ID: {dc4596fd-8f1b-4130-922c-dcb215ee4e32}

Log: 'Application' Date/Time: 16/03/2014 5:04:16 AM
Type: Error Category: 0
Event: 8194 Source: VSS
Volume Shadow Copy Service error: Unexpected error querying for the IVssWriterCallback interface. hr = 0x80070005, Access is denied. . This is often caused by incorrect security settings in either the writer or requestor process.

Operation:
   Gathering Writer Data

Context:
   Writer Class Id: {e8132975-6f93-4464-a53e-1050253ae220}
   Writer Name: System Writer
   Writer Instance ID: {dc4596fd-8f1b-4130-922c-dcb215ee4e32}

Log: 'Application' Date/Time: 15/03/2014 6:36:02 AM
Type: Error Category: 0
Event: 8194 Source: VSS
Volume Shadow Copy Service error: Unexpected error querying for the IVssWriterCallback interface. hr = 0x80070005, Access is denied. . This is often caused by incorrect security settings in either the writer or requestor process.

Operation:
   Gathering Writer Data

Context:
   Writer Class Id: {e8132975-6f93-4464-a53e-1050253ae220}

```
   Writer Name: System Writer
   Writer Instance ID: {dc4596fd-8f1b-4130-922c-dcb215ee4e32}

Log: 'Application' Date/Time: 14/03/2014 5:32:03 AM
Type: Error Category: 0
Event: 8194 Source: VSS
Volume Shadow Copy Service error: Unexpected error querying for the
IVssWriterCallback interface.  hr = 0x80070005, Access is denied. . This is often
caused by incorrect security settings in either the writer or requestor process.

Operation:
   Gathering Writer Data

Context:
   Writer Class Id: {e8132975-6f93-4464-a53e-1050253ae220}
   Writer Name: System Writer
   Writer Instance ID: {dc4596fd-8f1b-4130-922c-dcb215ee4e32}

Log: 'Application' Date/Time: 13/03/2014 5:05:05 AM
Type: Error Category: 0
Event: 8194 Source: VSS
Volume Shadow Copy Service error: Unexpected error querying for the
IVssWriterCallback interface.  hr = 0x80070005, Access is denied. . This is often
caused by incorrect security settings in either the writer or requestor process.

Operation:
   Gathering Writer Data

Context:
   Writer Class Id: {e8132975-6f93-4464-a53e-1050253ae220}
   Writer Name: System Writer
   Writer Instance ID: {dc4596fd-8f1b-4130-922c-dcb215ee4e32}

Log: 'Application' Date/Time: 04/03/2014 6:27:43 AM
Type: Error Category: 100
Event: 1000 Source: Application Error
Faulting application name: dragon_updater.exe, version: 0.0.0.0, time stamp:
0x51a5da71 Faulting module name: unknown, version: 0.0.0.0, time stamp: 0x00000000
Exception code: 0xc0000005 Fault offset: 0x00000000 Faulting process id: 0x6f0
Faulting application start time: 0x01cf28953af8fec4 Faulting application path:
C:\Program Files (x86)\Comodo\Dragon\dragon_updater.exe Faulting module path:
unknown Report Id: 17533237-a366-11e3-9a63-78acc0bed4a8

Log: 'Application' Date/Time: 16/02/2014 6:40:04 AM
Type: Error Category: 0
Event: 8194 Source: VSS
Volume Shadow Copy Service error: Unexpected error querying for the
IVssWriterCallback interface.  hr = 0x80070005, Access is denied. . This is often
caused by incorrect security settings in either the writer or requestor process.

Operation:
   Gathering Writer Data

Context:
   Writer Class Id: {e8132975-6f93-4464-a53e-1050253ae220}
   Writer Name: System Writer
   Writer Instance ID: {38154832-8764-405b-b72b-cf67667fb791}

Log: 'Application' Date/Time: 15/02/2014 5:59:10 AM
Type: Error Category: 0
Event: 8194 Source: VSS
Volume Shadow Copy Service error: Unexpected error querying for the
IVssWriterCallback interface.  hr = 0x80070005, Access is denied. . This is often
```

caused by incorrect security settings in either the writer or requestor process.

Operation:
   Gathering Writer Data

Context:
   Writer Class Id: {e8132975-6f93-4464-a53e-1050253ae220}
   Writer Name: System Writer
   Writer Instance ID: {38154832-8764-405b-b72b-cf67667fb791}

Log: 'Application' Date/Time: 14/02/2014 6:30:05 AM
Type: Error Category: 0
Event: 8194 Source: VSS
Volume Shadow Copy Service error: Unexpected error querying for the
IVssWriterCallback interface. hr = 0x80070005, Access is denied. . This is often
caused by incorrect security settings in either the writer or requestor process.

Operation:
   Gathering Writer Data

Context:
   Writer Class Id: {e8132975-6f93-4464-a53e-1050253ae220}
   Writer Name: System Writer
   Writer Instance ID: {38154832-8764-405b-b72b-cf67667fb791}

Log: 'Application' Date/Time: 21/01/2014 7:00:50 AM
Type: Error Category: 0
Event: 8194 Source: VSS
Volume Shadow Copy Service error: Unexpected error querying for the
IVssWriterCallback interface. hr = 0x80070005, Access is denied. . This is often
caused by incorrect security settings in either the writer or requestor process.

Operation:
   Gathering Writer Data

Context:
   Writer Class Id: {e8132975-6f93-4464-a53e-1050253ae220}
   Writer Name: System Writer
   Writer Instance ID: {d123063a-1b87-47ed-af08-81b0a56382e4}

Log: 'Application' Date/Time: 20/01/2014 7:28:10 AM
Type: Error Category: 0
Event: 8194 Source: VSS
Volume Shadow Copy Service error: Unexpected error querying for the
IVssWriterCallback interface. hr = 0x80070005, Access is denied. . This is often
caused by incorrect security settings in either the writer or requestor process.

Operation:
   Gathering Writer Data

Context:
   Writer Class Id: {e8132975-6f93-4464-a53e-1050253ae220}
   Writer Name: System Writer
   Writer Instance ID: {d123063a-1b87-47ed-af08-81b0a56382e4}

Log: 'Application' Date/Time: 19/01/2014 6:55:27 AM
Type: Error Category: 0
Event: 8194 Source: VSS
Volume Shadow Copy Service error: Unexpected error querying for the
IVssWriterCallback interface. hr = 0x80070005, Access is denied. . This is often
caused by incorrect security settings in either the writer or requestor process.

Operation:

```
   Gathering Writer Data

Context:
   Writer Class Id: {e8132975-6f93-4464-a53e-1050253ae220}
   Writer Name: System Writer
   Writer Instance ID: {d123063a-1b87-47ed-af08-81b0a56382e4}

Log: 'Application' Date/Time: 18/01/2014 5:55:03 AM
Type: Error Category: 0
Event: 8194 Source: VSS
Volume Shadow Copy Service error: Unexpected error querying for the
IVssWriterCallback interface.  hr = 0x80070005, Access is denied. . This is often
caused by incorrect security settings in either the writer or requestor process.

Operation:
   Gathering Writer Data

Context:
   Writer Class Id: {e8132975-6f93-4464-a53e-1050253ae220}
   Writer Name: System Writer
   Writer Instance ID: {d123063a-1b87-47ed-af08-81b0a56382e4}

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
'Application' Log - Warning Type
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
Log: 'Application' Date/Time: 08/04/2014 5:33:54 AM
Type: Warning Category: 0
Event: 1530 Source: Microsoft-Windows-User Profiles Service
Windows detected your registry file is still in use by other applications or
services. The file will be unloaded now. The applications or services that hold your
registry file may not function properly afterwards.     DETAIL -   1 user registry
handles leaked from \Registry\User\S-1-5-21-3455503661-4230816971-2044476751-1022:
Process 5568 (\Device\HarddiskVolume2\Windows\System32\msiexec.exe) has opened key
\REGISTRY\USER\S-1-5-21-3455503661-4230816971-2044476751-1022\Software\Microsoft\Win
dows\CurrentVersion\Explorer\FileExts


Log: 'Application' Date/Time: 06/04/2014 9:09:39 AM
Type: Warning Category: 0
Event: 1530 Source: Microsoft-Windows-User Profiles Service
Windows detected your registry file is still in use by other applications or
services. The file will be unloaded now. The applications or services that hold your
registry file may not function properly afterwards.     DETAIL -   5 user registry
handles leaked from \Registry\User\S-1-5-21-3455503661-4230816971-2044476751-1022:
Process 696 (\Device\HarddiskVolume2\Windows\System32\lsass.exe) has opened key
\REGISTRY\USER\S-1-5-21-3455503661-4230816971-2044476751-1022
Process 696 (\Device\HarddiskVolume2\Windows\System32\lsass.exe) has opened key
\REGISTRY\USER\S-1-5-21-3455503661-4230816971-2044476751-1022
Process 696 (\Device\HarddiskVolume2\Windows\System32\lsass.exe) has opened key
\REGISTRY\USER\S-1-5-21-3455503661-4230816971-2044476751-1022\Software\Microsoft\Sys
temCertificates\Disallowed
Process 696 (\Device\HarddiskVolume2\Windows\System32\lsass.exe) has opened key
\REGISTRY\USER\S-1-5-21-3455503661-4230816971-2044476751-1022\Software\Microsoft\Sys
temCertificates\My
Process 696 (\Device\HarddiskVolume2\Windows\System32\lsass.exe) has opened key
\REGISTRY\USER\S-1-5-21-3455503661-4230816971-2044476751-1022\Software\Microsoft\Sys
temCertificates\CA


Log: 'Application' Date/Time: 13/02/2014 8:05:45 AM
Type: Warning Category: 0
Event: 10010 Source: Microsoft-Windows-RestartManager
Application 'C:\Program Files\Windows Server\Bin\Launchpad.exe' (pid 4328) cannot be
```

restarted - Application SID does not match Conductor SID..

Log: 'Application' Date/Time: 13/02/2014 8:05:45 AM
Type: Warning Category: 0
Event: 10010 Source: Microsoft-Windows-RestartManager
Application 'C:\Program Files\Windows Server\Bin\Launchpad.exe' (pid 4328) cannot be restarted - Application SID does not match Conductor SID..

Log: 'Application' Date/Time: 13/02/2014 8:03:55 AM
Type: Warning Category: 1
Event: 1020 Source: ASP.NET 4.0.30319.0
Updates to the IIS metabase were aborted because IIS is either not installed or is disabled on this machine. To configure ASP.NET to run in IIS, please install or enable IIS and re-register ASP.NET using aspnet_regiis.exe /i.

Log: 'Application' Date/Time: 13/02/2014 8:03:48 AM
Type: Warning Category: 1
Event: 1020 Source: ASP.NET 4.0.30319.0
Updates to the IIS metabase were aborted because IIS is either not installed or is disabled on this machine. To configure ASP.NET to run in IIS, please install or enable IIS and re-register ASP.NET using aspnet_regiis.exe /i.

Log: 'Application' Date/Time: 15/01/2014 8:22:52 AM
Type: Warning Category: 0
Event: 6004 Source: Microsoft-Windows-Winlogon
The winlogon notification subscriber <TrustedInstaller> failed a critical notification event.

Log: 'Application' Date/Time: 15/01/2014 8:22:52 AM
Type: Warning Category: 0
Event: 6006 Source: Microsoft-Windows-Winlogon
The winlogon notification subscriber <TrustedInstaller> took 108 second(s) to handle the notification event (CreateSession).

Log: 'Application' Date/Time: 15/01/2014 8:22:03 AM
Type: Warning Category: 0
Event: 6005 Source: Microsoft-Windows-Winlogon
The winlogon notification subscriber <TrustedInstaller> is taking long time to handle the notification event (CreateSession).

Log: 'Application' Date/Time: 15/01/2014 8:17:28 AM
Type: Warning Category: 0
Event: 1530 Source: Microsoft-Windows-User Profiles Service
Windows detected your registry file is still in use by other applications or services. The file will be unloaded now. The applications or services that hold your registry file may not function properly afterwards. DETAIL - 5 user registry handles leaked from \Registry\User\S-1-5-21-3455503661-4230816971-2044476751-1022:
Process 740 (\Device\HarddiskVolume2\Windows\System32\lsass.exe) has opened key \REGISTRY\USER\S-1-5-21-3455503661-4230816971-2044476751-1022
Process 740 (\Device\HarddiskVolume2\Windows\System32\lsass.exe) has opened key \REGISTRY\USER\S-1-5-21-3455503661-4230816971-2044476751-1022
Process 740 (\Device\HarddiskVolume2\Windows\System32\lsass.exe) has opened key \REGISTRY\USER\S-1-5-21-3455503661-4230816971-2044476751-1022\Software\Microsoft\SystemCertificates\Disallowed
Process 740 (\Device\HarddiskVolume2\Windows\System32\lsass.exe) has opened key \REGISTRY\USER\S-1-5-21-3455503661-4230816971-2044476751-1022\Software\Microsoft\SystemCertificates\My
Process 740 (\Device\HarddiskVolume2\Windows\System32\lsass.exe) has opened key \REGISTRY\USER\S-1-5-21-3455503661-4230816971-2044476751-1022\Software\Microsoft\SystemCertificates\CA

Log: 'Application' Date/Time: 11/01/2014 11:49:06 PM

Type: Warning Category: 0
Event: 1015 Source: MsiInstaller
Failed to connect to server. Error: 0x800401F0

Log: 'Application' Date/Time: 11/01/2014 11:49:06 PM
Type: Warning Category: 0
Event: 1015 Source: MsiInstaller
Failed to connect to server. Error: 0x800401F0

Log: 'Application' Date/Time: 11/01/2014 11:49:06 PM
Type: Warning Category: 0
Event: 1015 Source: MsiInstaller
Failed to connect to server. Error: 0x800401F0

Log: 'Application' Date/Time: 11/01/2014 11:49:06 PM
Type: Warning Category: 0
Event: 1015 Source: MsiInstaller
Failed to connect to server. Error: 0x800401F0

Log: 'Application' Date/Time: 11/01/2014 11:49:06 PM
Type: Warning Category: 0
Event: 1015 Source: MsiInstaller
Failed to connect to server. Error: 0x800401F0

Log: 'Application' Date/Time: 11/01/2014 11:49:04 PM
Type: Warning Category: 0
Event: 1015 Source: MsiInstaller
Failed to connect to server. Error: 0x800401F0

Log: 'Application' Date/Time: 11/01/2014 11:49:04 PM
Type: Warning Category: 0
Event: 1015 Source: MsiInstaller
Failed to connect to server. Error: 0x800401F0

Log: 'Application' Date/Time: 11/01/2014 11:48:59 PM
Type: Warning Category: 0
Event: 1015 Source: MsiInstaller
Failed to connect to server. Error: 0x800401F0

Log: 'Application' Date/Time: 11/01/2014 9:53:41 PM
Type: Warning Category: 0
Event: 1530 Source: Microsoft-Windows-User Profiles Service
Windows detected your registry file is still in use by other applications or services. The file will be unloaded now. The applications or services that hold your registry file may not function properly afterwards.   DETAIL -   5 user registry handles leaked from \Registry\User\S-1-5-21-3455503661-4230816971-2044476751-1022:
Process 648 (\Device\HarddiskVolume2\Windows\System32\lsass.exe) has opened key \REGISTRY\USER\S-1-5-21-3455503661-4230816971-2044476751-1022
Process 648 (\Device\HarddiskVolume2\Windows\System32\lsass.exe) has opened key \REGISTRY\USER\S-1-5-21-3455503661-4230816971-2044476751-1022
Process 648 (\Device\HarddiskVolume2\Windows\System32\lsass.exe) has opened key \REGISTRY\USER\S-1-5-21-3455503661-4230816971-2044476751-1022\Software\Microsoft\SystemCertificates\Disallowed
Process 648 (\Device\HarddiskVolume2\Windows\System32\lsass.exe) has opened key \REGISTRY\USER\S-1-5-21-3455503661-4230816971-2044476751-1022\Software\Microsoft\SystemCertificates\My
Process 648 (\Device\HarddiskVolume2\Windows\System32\lsass.exe) has opened key \REGISTRY\USER\S-1-5-21-3455503661-4230816971-2044476751-1022\Software\Microsoft\SystemCertificates\CA

Log: 'Application' Date/Time: 25/12/2013 4:16:43 AM
Type: Warning Category: 0

VEW

Event: 1530 Source: Microsoft-Windows-User Profiles Service
Windows detected your registry file is still in use by other applications or services. The file will be unloaded now. The applications or services that hold your registry file may not function properly afterwards. DETAIL - 1 user registry handles leaked from
\Registry\User\S-1-5-21-3455503661-4230816971-2044476751-1022_Classes:
Process 1728 (\Device\HarddiskVolume2\Program Files\SUPERAntiSpyware\SASCore64.exe) has opened key \REGISTRY\USER\S-1-5-21-3455503661-4230816971-2044476751-1022_CLASSES

Vino's Event Viewer v01c run on Windows 2008 in English
Report run at 11/04/2014 9:44:13 PM

Note: All dates below are in the format dd/mm/yyyy

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
'System' Log - Critical Type
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
Log: 'System' Date/Time: 08/04/2014 5:13:52 AM
Type: Critical Category: 63
Event: 41 Source: 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.

Log: 'System' Date/Time: 25/12/2013 3:11:49 AM
Type: Critical Category: 63
Event: 41 Source: 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.

Log: 'System' Date/Time: 01/11/2013 11:08:42 PM
Type: Critical Category: 63
Event: 41 Source: 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.

Log: 'System' Date/Time: 23/07/2013 4:02:44 AM
Type: Critical Category: 63
Event: 41 Source: 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.

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
'System' Log - Error Type
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
Log: 'System' Date/Time: 12/04/2014 1:38:10 AM
Type: Error Category: 0
Event: 10010 Source: Microsoft-Windows-DistributedCOM
The server {995C996E-D918-4A8C-A302-45719A6F4EA7} did not register with DCOM within the required timeout.

Log: 'System' Date/Time: 10/04/2014 2:22:08 PM
Type: Error Category: 0
Event: 10010 Source: Microsoft-Windows-DistributedCOM
The server {995C996E-D918-4A8C-A302-45719A6F4EA7} did not register with DCOM within the required timeout.

Log: 'System' Date/Time: 10/04/2014 7:14:41 AM
Type: Error Category: 0
Event: 7030 Source: Service Control Manager
The PEVSystemStart service is marked as an interactive service. However, the system is configured to not allow interactive services. This service may not function properly.

Log: 'System' Date/Time: 10/04/2014 7:14:08 AM
Type: Error Category: 0
Event: 1060 Source: Application Popup
\??\C:\ComboFix\catchme.sys has been blocked from loading due to incompatibility with this system. Please contact your software vendor for a compatible version of the driver.

Log: 'System' Date/Time: 10/04/2014 7:12:12 AM
Type: Error Category: 0

Event: 7030 Source: Service Control Manager
The PEVSystemStart service is marked as an interactive service. However, the system is configured to not allow interactive services. This service may not function properly.

Log: 'System' Date/Time: 09/04/2014 9:04:34 AM
Type: Error Category: 0
Event: 10016 Source: Microsoft-Windows-DistributedCOM
The application-specific permission settings do not grant Local Launch permission for the COM Server application with CLSID {C97FCC79-E628-407D-AE68-A06AD6D8B4D1} and APPID {344ED43D-D086-4961-86A6-1106F4ACAD9B} to the user NT AUTHORITY\SYSTEM SID (S-1-5-18) from address LocalHost (Using LRPC). This security permission can be modified using the Component Services administrative tool.

Log: 'System' Date/Time: 09/04/2014 9:02:13 AM
Type: Error Category: 0
Event: 10010 Source: Microsoft-Windows-DistributedCOM
The server {E10F6C3A-F1AE-4ADC-AA9D-2FE65525666E} did not register with DCOM within the required timeout.

Log: 'System' Date/Time: 09/04/2014 8:50:56 AM
Type: Error Category: 0
Event: 10016 Source: Microsoft-Windows-DistributedCOM
The application-specific permission settings do not grant Local Launch permission for the COM Server application with CLSID {C97FCC79-E628-407D-AE68-A06AD6D8B4D1} and APPID {344ED43D-D086-4961-86A6-1106F4ACAD9B} to the user NT AUTHORITY\SYSTEM SID (S-1-5-18) from address LocalHost (Using LRPC). This security permission can be modified using the Component Services administrative tool.

Log: 'System' Date/Time: 09/04/2014 8:48:26 AM
Type: Error Category: 0
Event: 10010 Source: Microsoft-Windows-DistributedCOM
The server {E10F6C3A-F1AE-4ADC-AA9D-2FE65525666E} did not register with DCOM within the required timeout.

Log: 'System' Date/Time: 08/04/2014 11:28:48 AM
Type: Error Category: 0
Event: 10010 Source: Microsoft-Windows-DistributedCOM
The server {E10F6C3A-F1AE-4ADC-AA9D-2FE65525666E} did not register with DCOM within the required timeout.

Log: 'System' Date/Time: 08/04/2014 5:56:22 AM
Type: Error Category: 0
Event: 10010 Source: Microsoft-Windows-DistributedCOM
The server {E10F6C3A-F1AE-4ADC-AA9D-2FE65525666E} did not register with DCOM within the required timeout.

Log: 'System' Date/Time: 08/04/2014 5:44:01 AM
Type: Error Category: 0
Event: 10010 Source: Microsoft-Windows-DistributedCOM
The server {E10F6C3A-F1AE-4ADC-AA9D-2FE65525666E} did not register with DCOM within the required timeout.

Log: 'System' Date/Time: 08/04/2014 5:35:50 AM
Type: Error Category: 0
Event: 10016 Source: Microsoft-Windows-DistributedCOM
The application-specific permission settings do not grant Local Launch permission for the COM Server application with CLSID {C97FCC79-E628-407D-AE68-A06AD6D8B4D1} and APPID {344ED43D-D086-4961-86A6-1106F4ACAD9B} to the user NT AUTHORITY\SYSTEM SID (S-1-5-18) from address LocalHost (Using LRPC). This security permission can be modified using the Component Services administrative tool.

Log: 'System' Date/Time: 08/04/2014 5:35:21 AM

Type: Error Category: 0
Event: 7001 Source: Service Control Manager
The Windows Server Download Service service depends on the Windows Server Service Provider Registry service which failed to start because of the following error: The service did not respond to the start or control request in a timely fashion.

Log: 'System' Date/Time: 08/04/2014 5:35:21 AM
Type: Error Category: 0
Event: 7001 Source: Service Control Manager
The Windows Server Notifications Provider Service service depends on the Windows Server Service Provider Registry service which failed to start because of the following error: The service did not respond to the start or control request in a timely fashion.

Log: 'System' Date/Time: 08/04/2014 5:35:21 AM
Type: Error Category: 0
Event: 7001 Source: Service Control Manager
The Windows Server Health Service service depends on the Windows Server Service Provider Registry service which failed to start because of the following error: The service did not respond to the start or control request in a timely fashion.

Log: 'System' Date/Time: 08/04/2014 5:35:21 AM
Type: Error Category: 0
Event: 7001 Source: Service Control Manager
The Windows Server Client Computer Backup Provider Service service depends on the Windows Server Service Provider Registry service which failed to start because of the following error: The service did not respond to the start or control request in a timely fashion.

Log: 'System' Date/Time: 08/04/2014 5:35:21 AM
Type: Error Category: 0
Event: 7001 Source: Service Control Manager
The Windows Server SQM Service service depends on the Windows Server Service Provider Registry service which failed to start because of the following error: The service did not respond to the start or control request in a timely fashion.

Log: 'System' Date/Time: 08/04/2014 5:35:21 AM
Type: Error Category: 0
Event: 7000 Source: Service Control Manager
The Windows Server Service Provider Registry service failed to start due to the following error: The service did not respond to the start or control request in a timely fashion.

Log: 'System' Date/Time: 08/04/2014 5:35:21 AM
Type: Error Category: 0
Event: 7009 Source: Service Control Manager
A timeout was reached (30000 milliseconds) while waiting for the Windows Server Service Provider Registry service to connect.

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
'System' Log - Warning Type
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
Log: 'System' Date/Time: 11/04/2014 4:54:43 AM
Type: Warning Category: 0
Event: 1014 Source: Microsoft-Windows-DNS-Client
Name resolution for the name auth.ff.avast.com timed out after none of the configured DNS servers responded.

Log: 'System' Date/Time: 11/04/2014 4:54:40 AM
Type: Warning Category: 2
Event: 16 Source: Microsoft-Windows-WindowsUpdateClient
Unable to Connect: Windows is unable to connect to the automatic updates service and therefore cannot download and install updates according to the set schedule. Windows

will continue to try to establish a connection.

Log: 'System' Date/Time: 09/04/2014 9:29:58 AM
Type: Warning Category: 0
Event: 1014 Source: Microsoft-Windows-DNS-Client
Name resolution for the name su.ff.avast.com timed out after none of the configured DNS servers responded.

Log: 'System' Date/Time: 09/04/2014 9:14:41 AM
Type: Warning Category: 0
Event: 1014 Source: Microsoft-Windows-DNS-Client
Name resolution for the name www.msftncsi.com timed out after none of the configured DNS servers responded.

Log: 'System' Date/Time: 09/04/2014 9:03:31 AM
Type: Warning Category: 212
Event: 219 Source: Microsoft-Windows-Kernel-PnP
The driver \Driver\WUDFRd failed to load for the device WpdBusEnumRoot\UMB\2&37c186b&0&STORAGE#VOLUME#_??_USBSTOR#DISK&VEN_GENERIC-&PROD_COMPACT_FLASH&REV_1.01#18E391066476&1#.

Log: 'System' Date/Time: 09/04/2014 9:03:15 AM
Type: Warning Category: 0
Event: 11 Source: Microsoft-Windows-Wininit
Custom dynamic link libraries are being loaded for every application. The system administrator should review the list of libraries to ensure they are related to trusted applications.

Log: 'System' Date/Time: 09/04/2014 9:01:46 AM
Type: Warning Category: 0
Event: 1014 Source: Microsoft-Windows-DNS-Client
Name resolution for the name www.update.microsoft.com timed out after none of the configured DNS servers responded.

Log: 'System' Date/Time: 09/04/2014 8:59:19 AM
Type: Warning Category: 0
Event: 1014 Source: Microsoft-Windows-DNS-Client
Name resolution for the name slcw.ff.avast.com timed out after none of the configured DNS servers responded.

Log: 'System' Date/Time: 09/04/2014 8:49:56 AM
Type: Warning Category: 212
Event: 219 Source: Microsoft-Windows-Kernel-PnP
The driver \Driver\WUDFRd failed to load for the device WpdBusEnumRoot\UMB\2&37c186b&0&STORAGE#VOLUME#_??_USBSTOR#DISK&VEN_GENERIC-&PROD_COMPACT_FLASH&REV_1.01#18E391066476&1#.

Log: 'System' Date/Time: 09/04/2014 8:49:48 AM
Type: Warning Category: 0
Event: 11 Source: Microsoft-Windows-Wininit
Custom dynamic link libraries are being loaded for every application. The system administrator should review the list of libraries to ensure they are related to trusted applications.

Log: 'System' Date/Time: 09/04/2014 4:35:40 AM
Type: Warning Category: 2
Event: 16 Source: Microsoft-Windows-WindowsUpdateClient
Unable to Connect: Windows is unable to connect to the automatic updates service and therefore cannot download and install updates according to the set schedule. Windows will continue to try to establish a connection.

Log: 'System' Date/Time: 08/04/2014 12:20:30 PM
Type: Warning Category: 212

Event: 219 Source: Microsoft-Windows-Kernel-PnP
The driver \Driver\WUDFRd failed to load for the device
WpdBusEnumRoot\UMB\2&37c186b&0&STORAGE#VOLUME#_??_USBSTOR#DISK&VEN_GENERIC-&PROD_COM
PACT_FLASH&REV_1.01#18E391066476&1#.

Log: 'System' Date/Time: 08/04/2014 12:20:05 PM
Type: Warning Category: 0
Event: 11 Source: Microsoft-Windows-Wininit
Custom dynamic link libraries are being loaded for every application. The system
administrator should review the list of libraries to ensure they are related to
trusted applications.

Log: 'System' Date/Time: 08/04/2014 6:49:15 AM
Type: Warning Category: 212
Event: 219 Source: Microsoft-Windows-Kernel-PnP
The driver \Driver\WUDFRd failed to load for the device
WpdBusEnumRoot\UMB\2&37c186b&0&STORAGE#VOLUME#_??_USBSTOR#DISK&VEN_GENERIC-&PROD_COM
PACT_FLASH&REV_1.01#18E391066476&1#.

Log: 'System' Date/Time: 08/04/2014 6:48:50 AM
Type: Warning Category: 0
Event: 11 Source: Microsoft-Windows-Wininit
Custom dynamic link libraries are being loaded for every application. The system
administrator should review the list of libraries to ensure they are related to
trusted applications.

Log: 'System' Date/Time: 08/04/2014 5:45:10 AM
Type: Warning Category: 212
Event: 219 Source: Microsoft-Windows-Kernel-PnP
The driver \Driver\WUDFRd failed to load for the device
WpdBusEnumRoot\UMB\2&37c186b&0&STORAGE#VOLUME#_??_USBSTOR#DISK&VEN_GENERIC-&PROD_COM
PACT_FLASH&REV_1.01#18E391066476&1#.

Log: 'System' Date/Time: 08/04/2014 5:44:58 AM
Type: Warning Category: 0
Event: 11 Source: Microsoft-Windows-Wininit
Custom dynamic link libraries are being loaded for every application. The system
administrator should review the list of libraries to ensure they are related to
trusted applications.

Log: 'System' Date/Time: 08/04/2014 5:35:24 AM
Type: Warning Category: 212
Event: 219 Source: Microsoft-Windows-Kernel-PnP
The driver \Driver\WUDFRd failed to load for the device
WpdBusEnumRoot\UMB\2&37c186b&0&STORAGE#VOLUME#_??_USBSTOR#DISK&VEN_GENERIC-&PROD_COM
PACT_FLASH&REV_1.01#18E391066476&1#.

Log: 'System' Date/Time: 08/04/2014 5:34:42 AM
Type: Warning Category: 0
Event: 11 Source: Microsoft-Windows-Wininit
Custom dynamic link libraries are being loaded for every application. The system
administrator should review the list of libraries to ensure they are related to
trusted applications.

Log: 'System' Date/Time: 08/04/2014 5:14:32 AM
Type: Warning Category: 212
Event: 219 Source: Microsoft-Windows-Kernel-PnP
The driver \Driver\WUDFRd failed to load for the device
WpdBusEnumRoot\UMB\2&37c186b&0&STORAGE#VOLUME#_??_USBSTOR#DISK&VEN_GENERIC-&PROD_COM
PACT_FLASH&REV_1.01#18E391066476&1#.