Restart and Shutdown Event Logs for Windows

Published on: March 4, 2017 / Category: Windows / Comments: 0 Comments

When monitoring Windows Servers you have one monitoring tool that every System Administrator should master. This is of course is Windows Event Viewer. From personal experience this tool has been useful for monitoring outages when you are not hosting the hardware on site. In this article I shall share the particular steps I use in doing this.

Setup Application

Boot up Event Viewer by hitting start and simply searching for it (I have this app pinned to Start for easy access).

Navigate to the following directory to find the System events you want to be filtering through:

```
Event Viewer (Local) > Windows Logs > System
```

Setup Filter

Once within here, under “Actions” on the right hand pane hit “Filter Current Log…”. For this exercise we simply want to view all the useful logs that may show more information on system restarts and shutdowns. To narrow down this filter, we add the Event IDs we want to look at in the Event ID field. The particular Event IDs we want to be looking for are as follows:

Event ID: 41

The kernel power event ID 41 error occurs when the computer is shut down, or it restarts unexpectedly. Useful for identifying if a machine has uncleanly rebooted/shut down.

Event ID: 1074

Indicates that an application or a user initiated a restart or shutdown. Useful for identifying a rogue service causing these events.

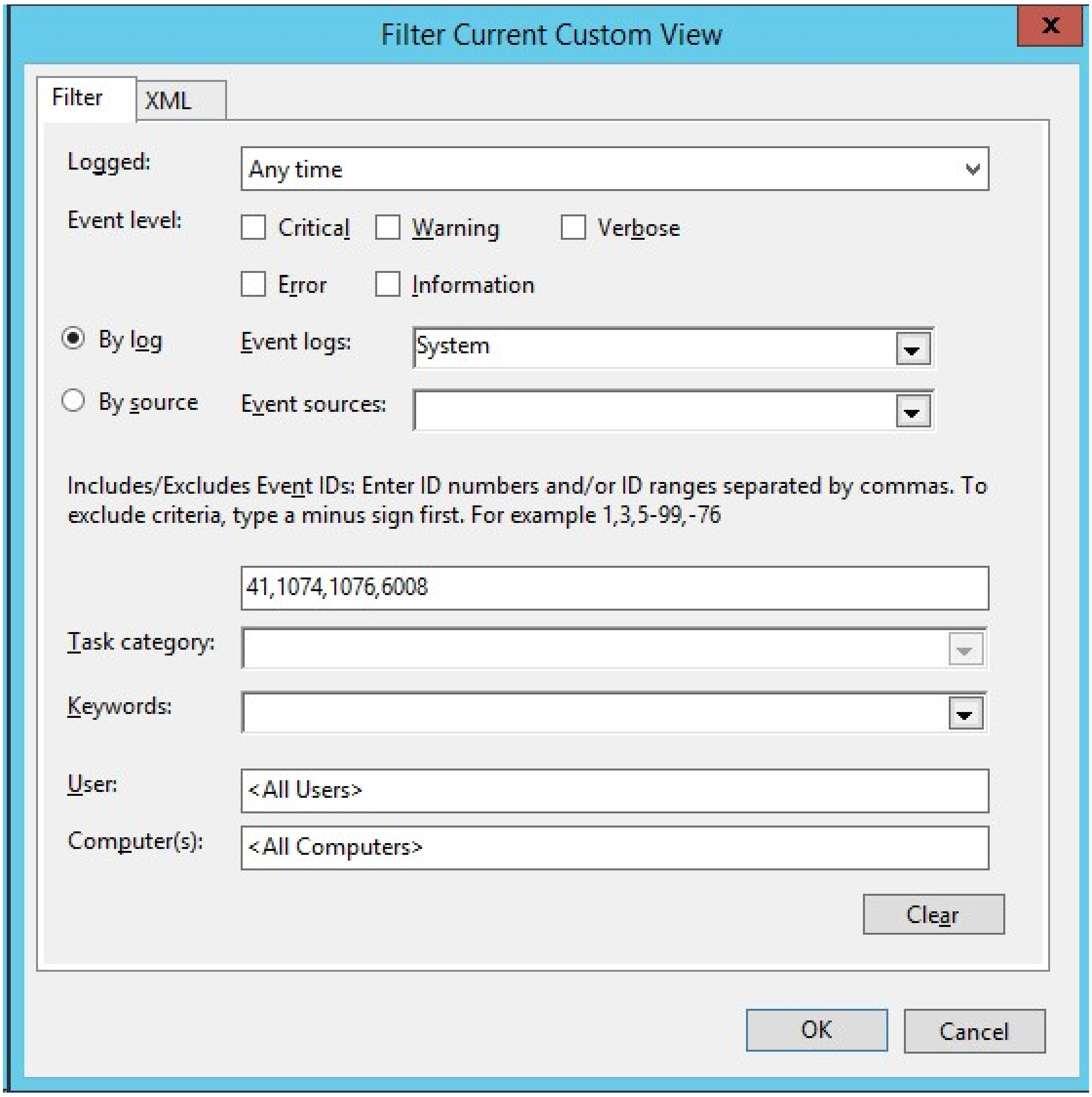
Event ID: 1076

A really useful one as this one records your notes when the system has restored after an unexpected restart/shutdown. Usually I put in a resolution not here to record what I identified the cause to be.

Event ID: 6008

Records that the system started after it was not shut down properly. May identify other things that may have been missed.

With these selected, the setup should be as follows (nothing else needs amending):



Logged: Any time

Event level: □ Critical □ Warning □ Verbose □ Error □ Information

● By log Event logs: System

○ By source Event sources:

Includes/Excludes Event IDs: Enter ID numbers and/or ID ranges separated by commas. To exclude criteria, type a minus sign first. For example 1,3,5-99,-76

41,1074,1076,6008

Task category:

Keywords:

User: <All Users>

Computer(s): <All Computers>

Summary

Using this filter will show you all the events that were captured during unscheduled restarts and shutdowns. For me this is extremely useful as when this happens it’s vital in knowing what caused it.

Download

To import this filter into your own Event Viewer you can download this already preset here:

Restart and Shutdown History.xml

Code:

```
<ViewerConfig><QueryConfig><QueryParams><Simple><Channel>System</
Channel><EventId>41,1074,1076,6008</EventId><RelativeTimeInfo>0</
RelativeTimeInfo><BySource>False</BySource></Simple></
QueryParams><QueryNode><Name>Restart &amp; Shutdown
History</Name><Description>May show what has caused an unexplained restart
or shutdown - JY</Description><SortConfig Asc="0"><Column Name="Date and
Time" Type="System.DateTime" Path="Event/System/TimeCreated/@SystemTime"
Visible="">329</Column></SortConfig><QueryList><Query Id="0"
Path="System"><Select Path="System">*[System[(EventID=41 or EventID=1074
or EventID=1076 or
EventID=6008)]]</Select></Query></QueryList></QueryNode></QueryConfig><Res
ultsConfig><Columns><Column Name="Level" Type="System.String"
Path="Event/System/Level" Visible="">279</Column><Column Name="Keywords"
Type="System.String" Path="Event/System/Keywords">70</Column><Column
Name="Date and Time" Type="System.DateTime"
Path="Event/System/TimeCreated/@SystemTime" Visible="">329</Column><Column
Name="Source" Type="System.String" Path="Event/System/Provider/@Name"
Visible="">239</Column><Column Name="Event ID" Type="System.UInt32"
Path="Event/System/EventID" Visible="">239</Column><Column Name="Task
Category" Type="System.String" Path="Event/System/Task"
Visible="">241</Column><Column Name="User" Type="System.String"
Path="Event/System/Security/@UserID">50</Column><Column Name="Operational
Code" Type="System.String" Path="Event/System/Opcode">110</Column><Column
Name="Log" Type="System.String"
Path="Event/System/Channel">80</Column><Column Name="Computer"
Type="System.String" Path="Event/System/Computer">170</Column><Column
Name="Process ID" Type="System.UInt32"
Path="Event/System/Execution/@ProcessID">70</Column><Column Name="Thread
ID" Type="System.UInt32"
Path="Event/System/Execution/@ThreadID">70</Column><Column Name="Processor
ID" Type="System.UInt32"
Path="Event/System/Execution/@ProcessorID">90</Column><Column
Name="Session ID" Type="System.UInt32"
Path="Event/System/Execution/@SessionID">70</Column><Column Name="Kernel
Time" Type="System.UInt32"
Path="Event/System/Execution/@KernelTime">80</Column><Column Name="User
Time" Type="System.UInt32"
Path="Event/System/Execution/@UserTime">70</Column><Column Name="Processor
Time" Type="System.UInt32"
Path="Event/System/Execution/@ProcessorTime">100</Column><Column
Name="Correlation Id" Type="System.Guid"
Path="Event/System/Correlation/@ActivityID">85</Column><Column
Name="Relative Correlation Id" Type="System.Guid"
Path="Event/System/Correlation/@RelatedActivityID">140</Column><Column
Name="Event Source Name" Type="System.String"
Path="Event/System/Provider/@EventSourceName">140</Column></Columns></
ResultsConfig></ViewerConfig>
```