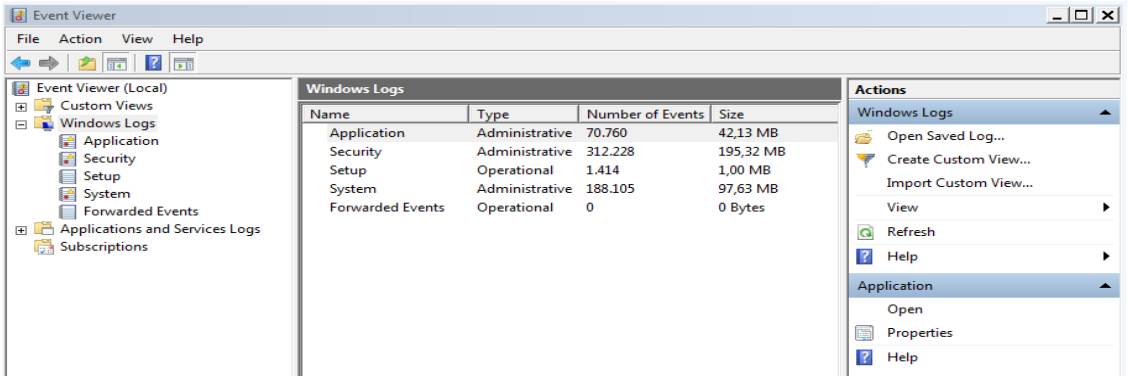
# EVENT VIEWER IN WINDOWS 7

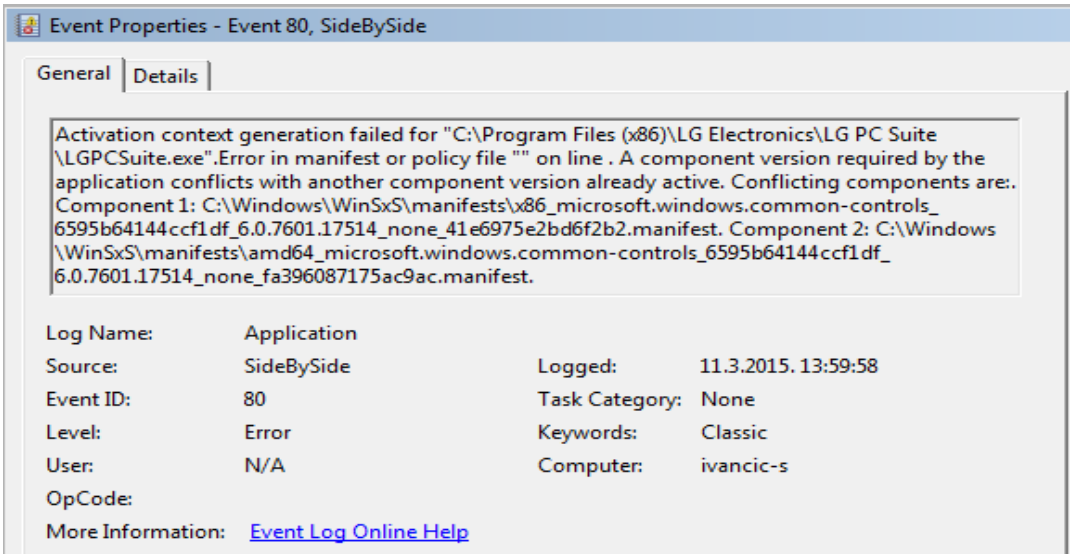
## Event Viewer

We can open Event Viewer in different ways, such as trough Computer Management and Administrative Tools. However, the easiest way is to type "eventvwr" in search box, or "eventvwr.msc" in the Run box to open the Event Viewer.




Event Viewer

The standard Windows logs are now located under Windows Logs section (Application, Security, Setup, System and Forwarded Events logs). If we select particular log, and then select some event, we will see the summary of the event at the bottom of the Viewer, in the preview pane. On the right side we have options to filter logs, to create custom logs, view properties of the event, etc. We can also see event properties by right-clicking the event, and then selecting the "Event Properties" option.

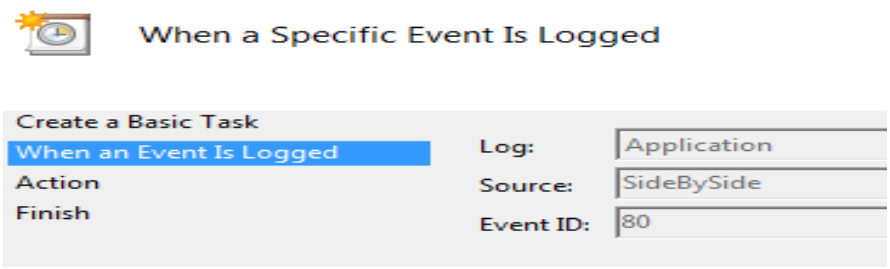



Event Properties

Event properties give us more information about the event. If we go to the Details tab we can even get an XML view if we need to save, parse it, etc. When we right-click an event, we also have an option to attach a task to event. This way, if the event occurs again, the task will run. When we select the "Attach Task To This Event" option, the Basic Task wizard will appear. The first thing we can do is give the name to the task.

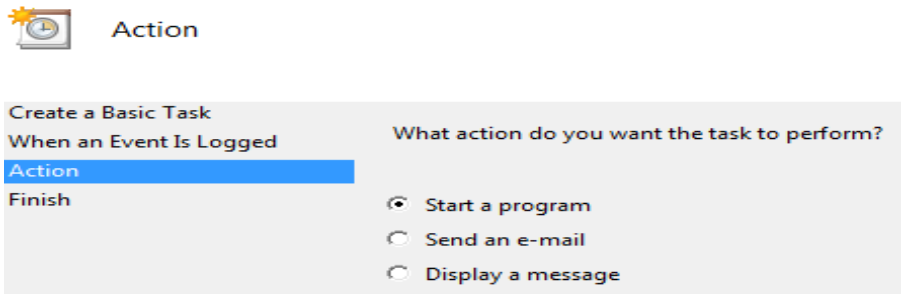

Task Name

On the next screen we can see that it will by default fill the log, source, and event ID information for us.




Event Logged

On the next screen we can specify the action we want the task to perform.




Task Action

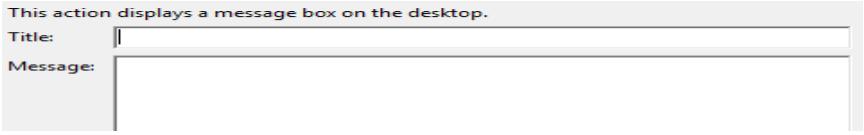
If we select a program, we will be able to select a program or script that the task will run.


Task Program or Script

If we specify to send an e-mail, we can specify from whom the e-email should come from, who will receive it, subject, text, attachment, and we need to specify the SMTP server.

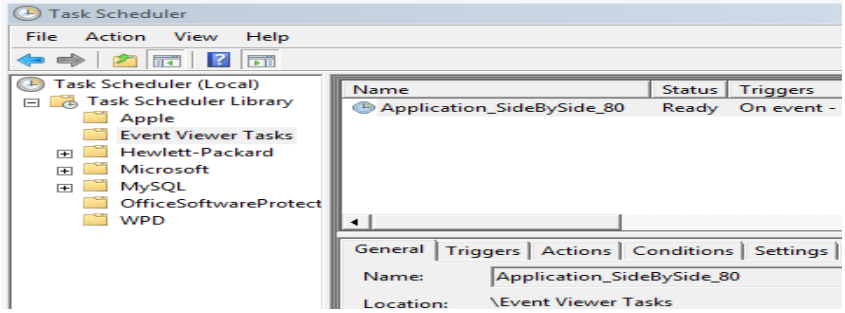

Task E-mail

If we select a "Display a message" option, we will be able to specify a message that will appear on the desktop when the event occurs.




Task Message

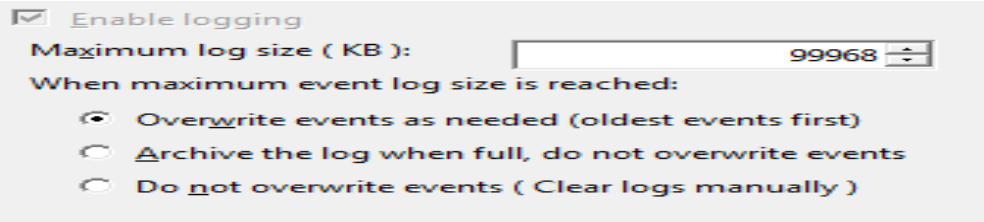
So, this wizard will create a task in the Task Scheduler, based on the trigger from our event. Task Scheduler is available in Administrative Tools. Tasks created by Event Viewer will be stored under "Task Scheduler Library" -> "Event Viewer Tasks".




Task Scheduler

Here we can see the details about our task, and even force it to run.

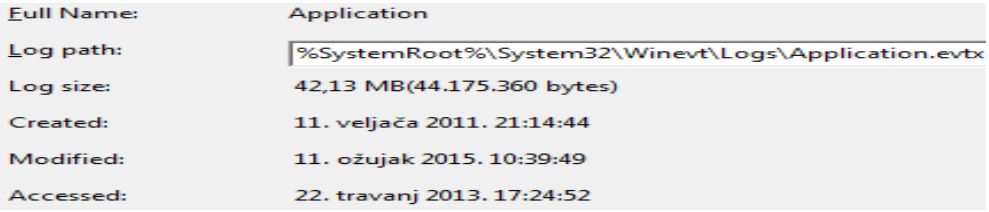
The next thing we should consider is the size of our logs. For example, if we right-click on the Application log, and select the Properties option, we will be able to select the maximum log size.




Log Options

The larger the size, the more events it can save, but at the same time, it takes up space and impacts performance. We can also specify what to do when the maximum event log size is reached. The default is to overwrite events as needed. If we specify the "Do not overwrite events" option, we will have to manually clear the log. Also, users won't be able to use the computer until the log is cleared. Only the administrator will be able to log on to the computer and clear the log.

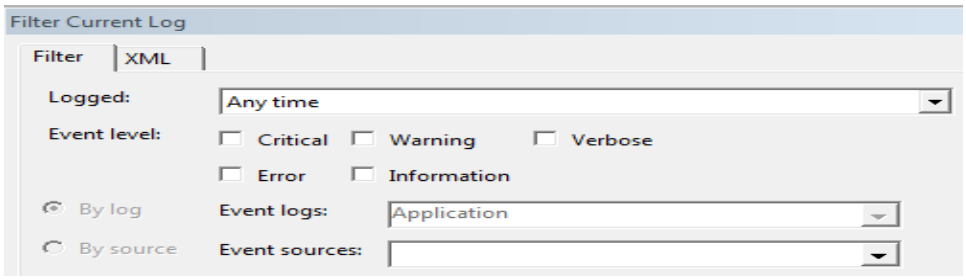
In this window we also see the actual path to the log file and the current log size.




Log Properties

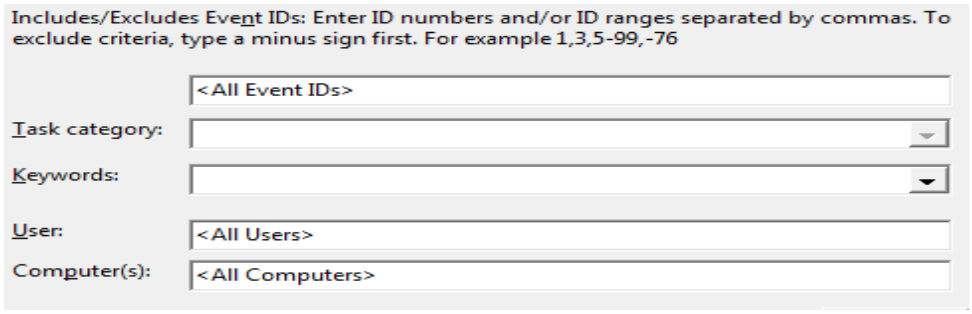
# Using Filters

We can filter our logs by choosing the Filter Current Log option from the Actions menu. In the filter we can specify the event level (critical, warning, verbose, error, information).




Filter part 1

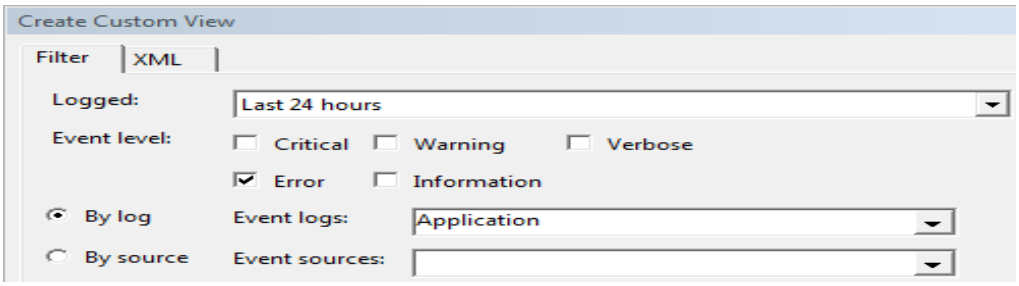
Also, we can enter IDs, task categories, keywords, users, and computer to filter using this criteria.




Filter part 2

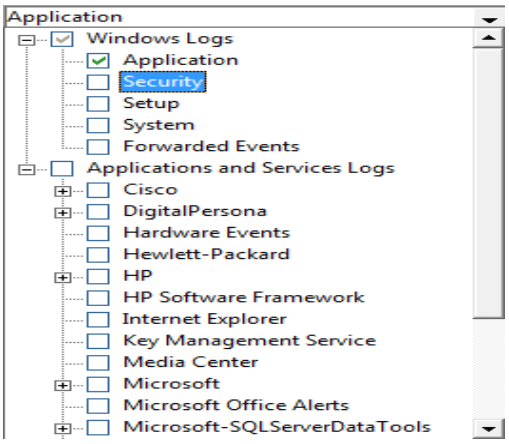
Keep in mind that filters are only active only while we stay in the current log. If we select another log, the filter will reset. If we want to define our own view with filters and preserve it, we can create a custom view from the Actions menu.

The custom view has the same options as when creating a filter. In our case we will create a view which will only show us errors that happened in the last 24 hours in the Applications log.



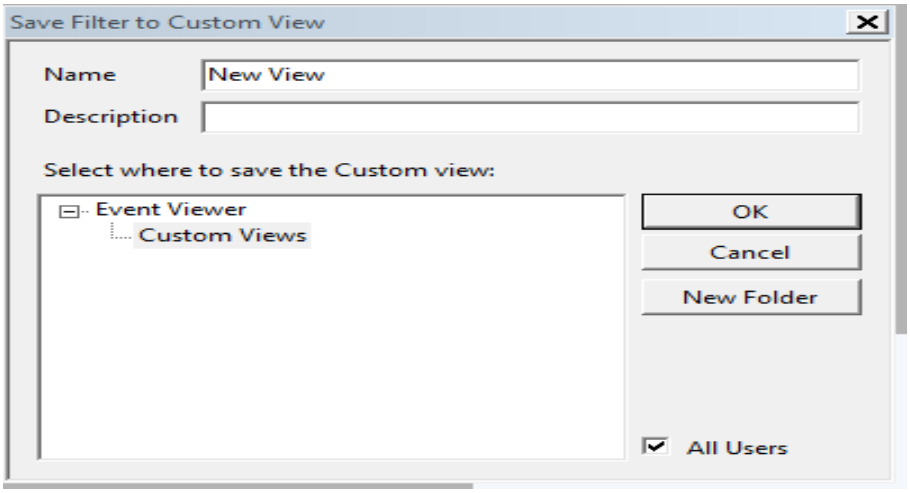

Custom View Example

Note that when we choose the log, we can combine multiple logs if we wish. We can even use the Applications and Services Logs which can show us events from hardware, Internet Explorer, and even more details events under the Microsoft section from other Windows services. Almost every major Windows service has its own log.



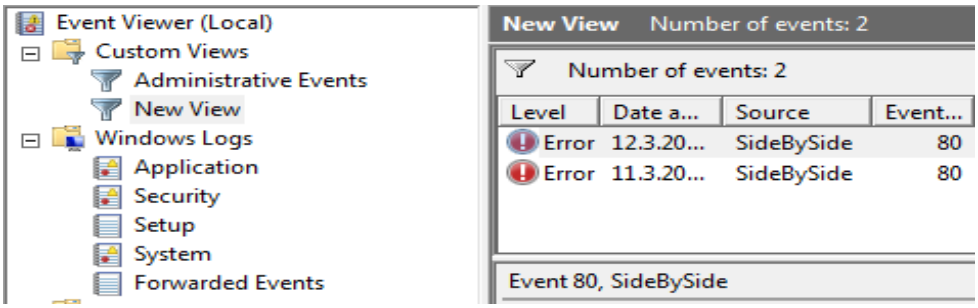

Different Logs

When we define our own view, we can name it and give it description. We can even organize our custom views in folders.




View Name and Folder

So, now when we select our custom view, only filtered events will be shown.




Custom View in Action

We can always edit our custom view by right-clicking it and choosing the appropriate option, as well as export it.

Source: http://www.utilizewindows.com/7/management/528-event-viewer-in-windows-7