Last updated: 2/22/08 by Mark Lachniet

Using an external batch script to ZIP Kiwi log files hourly:

Problem: Sometimes Kiwi may fail to create zip archive files. If you check the event viewer, you may see an error such as:

inter top.	erties					?			
Event									
D <u>a</u> te: Ti <u>m</u> e: Typ <u>e</u> : <u>U</u> ser: C <u>o</u> mputer	2/22/2 8:31:43 Informa N/A r: ISAPPS	3 AM I Ition I	<u>S</u> ource: Catego <u>r</u> y: Event <u>I</u> D:		ion Error	↑			
Description: Reporting queued error: faulting application syslogd_service.exe, version									
8.2.0.18, faulting module DartZip.dll, version 1.8.3.0, fault address 0x0001cc36. For more information, see Help and Support Center at <u>http://go.microsoft.com/fwlink/events.asp</u> .									
Da <u>t</u> a: @) <u>B</u> ytes () <u>W</u> or	ds						
0000:	41 70 7	70 6c	69 63		Applicat				
0000:		 70 6c 6e 20	69 63 46 61	69 6c	Applicat ion Fail ure sys	 			

Solution:

- Review Kiwi's suggestions at <u>http://www.kiwisyslog.com/kb/how-to:-use-an-alternative-compression-method-for-log-archiving/</u> (but don't follow them entirely)
- Set up Kiwi as follows (note that in our case the data log root directory is d:\logdata\asa and you'll need to change that for your own install). Note that you have to manually type in the hour and minute stuff in the appropriate box – there is no dropdown for it.

Archive time: Hourly		JTC SM	ז עד קעקק	s च				
Source folder: d:\logdata\asa	d	estination folder :\logdata\asa\						
Matching file mask: *.txt	With file		0 Byti	es 💌				
Dated files/folders options: C Use dated folder names O Use dated file names		Date format: YYYYY-MM-D 20	D-HH-SS 08-02-22-09-1	2				
2DateStamp	 ble options	Zip options: Zip files after archiving All files into single zip Protect file with a password: Notify options: Notify by e-mail						
Perform Archive Now								
	<u>H</u> elp	<u>0</u> K	<u>C</u> ancel	Apply				

3) create a batch file called d:\logdata\asa\zipscript.bat and include the following contents:

md "d:\logdata\asa\archived\%Date:/=%"

"C:\Program files\7-zip\7z.exe" a -tzip "d:\logdata\asa\archived\%Date:/=%\LogFiles-%1.zip" "d:\logdata\asa\prezip*.txt"

If Not ErrorLevel 1 Goto DeleteFiles: Echo ***SERIOUS ERROR DETECTED*** Goto Exit:

:DeleteFiles Del /S /Q "d:\logdata\asa\prezip*.*" :Exit