Kiwi Harvester

A Freeware Serial Port to Syslog Converter for Windows

by SolarWinds, Inc.

Kiwi Harvester listens for data via the computer's serial interface and converts the data received into standard UDP syslog messages. The messages are then forwarded via the syslog protocol to a central logging server such as Kiwi Syslog Server.

This allows you to integrate non-ethernet enabled devices into your central logging system. Such devices include: PBX call logging systems, main frame computers, remote sensing devices and router console ports.

Table of Contents

1 Introduction

1.1 Kiwi Harvester

A Freeware Serial Port to Syslog converter for Windows.

Copyright 2003-2009 SolarWinds, Inc.

Latest version available from: http://www.kiwisyslog.com

Kiwi Harvester listens for data via the computer's serial interface and converts the data received into standard syslog messages. The messages are then forwarded via the UDP protocol to a central logging server such as Kiwi Syslog Server.

The Harvester allows you to integrate non-ethernet enabled devices into your central logging system. Such devices include: PBX call logging systems, main frame computers, remote sensing devices and router console ports.

Kiwi Harvester is installed as a system service and runs on Windows 2000 or later.

The application has a small footprint and is easily and quickly configured via an ini text file.

Features

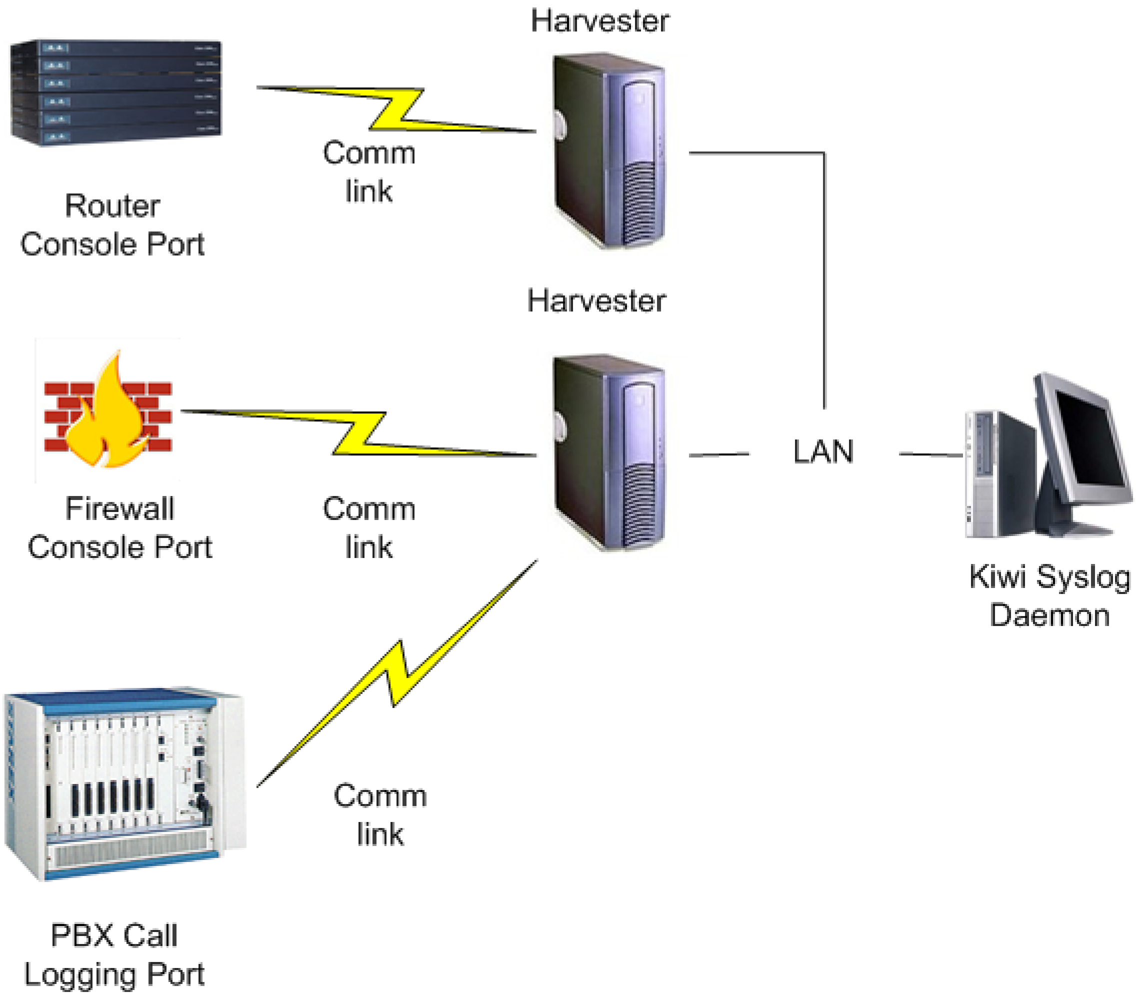
- Accepts input from network devices via a comm port
- Forwards messages via UDP
- Configurable via ini file
- Runs as service
- Supports comm port speeds from 300 to 115200 bps
- Allows a unique ID to be added to messages for identification
- Freeware

Typical uses:

- Forwarding of router console messages for out of band notification.
- Forwarding of PBX call records for billing purposes.
- Forwarding of messages from a remote sensing device or PLC device.
- Out of band messaging for a secure firewall. (Redirect the logging output to the

serial port)
- Capturing of redirected printer output. (Printer port set to Com1)

Example Usage:



2 Harvester Service

2.1 Getting Started

The Kiwi Harvester installer will place all the required files into the specified folder. A default ini file is created, this will need to be modified to suit your system settings (Comm port number and speed settings).

The installer will create shortcuts under the Start Menu | Programs | SolarWinds | Kiwi Harvester menu.

These shortcuts will allow you to configure, install and start the program without having to use the command line options. However, you may use the following command line options to control the service.

If the Harvester is manually run without a command switch it will start up but will perform no function. You will not be able to stop it again without using the task manager to kill the process. The Harvester program is called Kiwi_Harvester.exe.

The command line switches are:

```
      -install
      -uninstall
```

To install the service, run the Harvester program with the -install switch. This registers the service with the operating system, but does not start it immediately. The service is set to start automatically when the operating system starts. The command might look like:

```
      C:\Program Files\KiwiHarvester\Kiwi_Harvester.exe -install
```

The service can be manually started in a number of ways. You can use the standard Windows administration services dialogue to start or stop the service. You can also use the 'net start' or 'net stop' command from the command prompt. The service name by default is Syslog Harvester and is set by the entry in the configuration ini file.

To use the 'net' command, first run a command prompt session. At the prompt type

```
      'net start "Kiwi_Harvester"'      to start the service, or
      'net stop "Kiwi_Harvester"'       to stop the service.
```

Note the name should match the entry for the servicename setting. If the name has spaces in it, the name should be enclosed by quotes.

To uninstall the service. first make sure the service is not running. Then manually run the Harvester programs with the -uninstall switch. The command might look like:

```
      C:\Program Files\KiwiHarvester\Kiwi_Harvester.exe -uninstall
```

2.2 Configuring

The Harvester service is configured via a text ini file. To change the configuration simply edit the ini file, Kiwi_Harvester.ini in the install folder, and restart the service.

The default ini file looks like this:

```
[Kiwi_Harvester]
commport=1
commini=9600,N,8,1
flowcontrol=1
udpport=514
udptarget=localhost
msgformat=1
crsend=1
servicename=Kiwi_Harvester
facility=23
level=6
buffermax=4096
sendcommmess=1
checkseq=0
OriginalAddress=
KiwiHarvesterID=
EnableStatusTimer=
StatusTimerPeriod=
```

If the ini file does not exist when the Harvester is started, it is created with the default settings.

If any required settings are not found, the defaults are used and then written back to the ini file.

2.2.1 commport

The **commport** setting may be any valid comm port from 1 to 255.

By default, comm port 1 is used.

2.2.2 commini

The **commini** setting sets the characteristics of the comm port. The settings are in a comma separated sequence and refer to the port speed, parity, data bits, stop bits.

For example, a **commini** setting of '9600,N,8,1' means a speed of 9600bps, no parity, 8 data bits, 1 stop bit.

Cisco router consoles are configured to use 9600,N,8,1 by default. Some PBX equipment may only support 1200 bps with 7 bit even parity, so the **commini** setting of 1200,E,7,1 should be used.

2.2.3 flowcontrol

The **flowcontrol** setting specifies the flow control to use.

0 = None
1 = Xon/Xoff
2 = RTS
3 = RTS/Xon/Xoff

The default is 1 (Xon/Xoff)

2.2.4 udpport

The **udpport** setting specifies the UDP port to send the syslog messages to. By default this is port 514. Valid port numbers are 1 to 65535.

2.2.5 udptarget

The **udptarget** setting specifies the logging server which the message should be forwarded to. This value can be an IP address or host name.

For example: 192.168.1.1, or kiwi-syslog-server

2.2.6 msgformat

The **msgformat** setting determines the format of the forwarded syslog messages.

The following message formats are available:
1 - Kiwi Syslog Server message format. (Just a priority code added)
2 - RFC 3164 message format (Adds date, time, host etc)
3 - Raw data (No reformatting, no priority code added to the message)

By default, the option is set to 1.

2.2.7 crsend

The **crsend** setting determines how many carriage returns (ASCII chr 13) are sent to the comm port when it is first activated. It may be any number from 0 to 10. This can be used to "wake up" the comm port when the program is first started.

The default value is 1.

2.2.8 servicename

The **servicename** entry is used to uniquely identify the service to the operating system. By default a service name of "Kiwi_Harvester" is used. If you install more than one instance of the Harvester on a system, make sure each has a unique **servicename**. The service name is used by the system services controller to stop and start the service.

2.2.9 facility

Each Syslog message includes a priority value at the beginning of the text. The priority value ranges from 0 to 191 and is made up of a Facility value and a Level value.

The Facility value is a way of determining which process of the machine created the message. Since the Syslog protocol was originally written on BSD Unix, the Facilities reflect the names of Unix processes and Daemons.

The priority value is calculated using the following formula:
Priority = Facility * 8 + Level

The list of Facilities available:

0	kernel
1	user
2	mail
3	daemon
4	authorization
5	syslogd
6	line printer subsystem
7	news
8	UUCP
9	cron
10	security
11	FTP
12	NTP
13	log audit
14	log alert
15	clock daemon

16	local use 0	(local0)
17	local use 1	(local1)
18	local use 2	(local2)
19	local use 3	(local3)
20	local use 4	(local4)
21	local use 5	(local5)
22	local use 6	(local6)
23	local use 7	(local7)

By default, this value is set to 23 (Local7).

2.2.10 level

Each Syslog message includes a priority value at the beginning of the text. The priority value ranges from 0 to 191 and is made up of a Facility value and a Level value.

The priority value is calculated using the following formula:
Priority = Facility * 8 + Level

The list of severity Levels:

0	Emergency: system is unusable
1	Alert: action must be taken immediately
2	Critical: critical conditions
3	Error: error conditions
4	Warning: warning conditions
5	Notice: normal but significant condition
6	Informational: informational messages
7	Debug: debug-level messages

By default, this value is set to 6 (info).

2.2.11 buffermax

The **buffermax** setting tells the Harvester when to send a message if no message delimiter is found. The setting of 4096 would tell Harvester to forward the data buffer as a syslog message when data in the buffer exceeds 4096 bytes and a CR or LF has not been found in the buffer.

2.2.12 sendcommmess

If this value is set to 1, any change in comm port interface status will generate a syslog message. For example, if DSR or CD change state, a syslog message is generated so that the time and date of the event can be logged remotely. A change in interface state could mean that the monitored device has rebooted or gone offline.

The values may be:
0 - do not send interface changed messages
1 - send interface changed messages

2.2.13 checkseq

This setting determines if the Harvester will check sequenced messages for missing numbers. The Kiwi HarvesterGen can create sequenced messages in the form: "This is HarvesterGen message #####". A sequential number replaces the hashes. If this value is set to 1, any missing messages will generate an error in the log file.

The values may be:
 0 - do not sequence check
 1 - sequence check

This value is set to 0 by default to improve performance.

2.2.14 OriginalAddress

This setting allows you to add a unique identifier to all messages in the form of an IP address. It is valid for msgformats 1 and 2, but is not added to 3 which is raw message format.

If the setting value is blank or the setting not found, no identifier is added to messages.

The identifier is in the form:
 OriginalAddress=192.168.0.0

The address must be a valid IP address format.

This identifier is known to Kiwi Syslog Server and may be used as an auto split value when logging.

2.2.15 KiwiHarvesterID

This setting allows you to add a unique identifier to all messages in the form of a 1 to 12 character string. It is valid for msgformats 1 and 2, but is not added to 3 which is raw message format.

If the setting value is blank or the setting not found, no identifier is added to messages.

The identifier is in the form:
 KiwiHarvesterID=uniquestring

The default value for this setting is:
 KiwiHarvesterID=Harvester

This identifier may be used to uniquely identify records when an IP address may not be unique. It might be used by a Kiwi Syslog Server script to filter for records coming from specific devices.

2.2.16 EnableStatusTimer

This setting allows you to enable a timer that when fired will send a message to the port specified by udpport.

The timer is only enabled if the setting value is set to 1.

Possible values are 0 or 1. The default value is 0.

This can be useful to confirm that your configuration is correctly set up.

2.2.17 StatusTimerPeriod

If you have enabled the status timer (EnableStatusTimer) then this value sets how often, in seconds, the timer is fired.

The default value is 30.

2.3 Running

The Harvester normally runs as a service. You can check the service status from the Control Panel | Services applet, or look for the process named "Kiwi_Harverster.exe" in the task manager.

The Harvester creates a log file when it runs called `Kiwi_Harvester.log` situated in the install folder. Check the log file for any messages that might indicate that there is a problem.

To run the program interactively instead of as a service, use the `-interact` command line option.

```
C:\Program Files\KiwiHarvester\Kiwi_Harvester.exe -interact
```

2.4 Troubleshooting

The Harvester has been tested at speeds from 1200bps to 115200bps. Should the data appear to be garbled, the speed may have been set incorrectly. Always ensure that both ends of the comm link are deactivated before changing the link speed. Failure to do this has been known to totally confuse the comm ports.

Ensure you have only one device running against a physical comm port. The results of running active devices on say both comm 1 and comm 3 are unpredictable.

To help with the setting up and testing of the Harvester, SolarWinds offer a small tool called HarvesterGen. This application sends messages to a comm port and when used in conjunction with the Harvester should help confirm that the Harvester is working correctly on your system. This can be obtained from: www.kiwisyslog.com