

SysLog Server

By Philippe & Guillaume Huysmans
January 2007

TABLE OF CONTENT

1. [What is Syslog Server](#)
2. [How to install the application](#)
3. [How to use the application](#)
4. [Configuration](#)
5. [Macros](#)

DOCUMENTATION

1. What is Syslog Server

A simple yet powerful Syslog protocol Server & Analyzer. Can be tuned to only log events under a threshold, or to directly mail and admin when another threshold value is reached. The events can be viewed by hosts, by severity, or by facility. You can also define (up to 100) macros (regexes) which will automatically trigger an action when an event raised.

It can be useful to monitor devices and workstations into a lan. Note that MsWindows cannot natively report its eventlogs to the syslog protocol but this can be easily achieved by installing [Eventlog to Syslog Utility](#), a free tools provided by the department Engineering of the Purdue University.

How EvtSys works : once you have properly installed the EvtSys service, it will begin to report all windows events to the specified server (port 514 udp).

Please note that *I do not recommend to use this feature through internet* (LAN -> WAN -> LAN) because the syslog protocol is basically unsafe : all messages are sent in clear, and a hacker could easily intercept messages containing sensitive information simply by monitoring the TCPIP traffic (with EtherReal, by example).

2. How to install the application

Unfortunately, the lazy guys from Ms did not include any way to make an application run as service in vb6, so we have to use a little trick here.

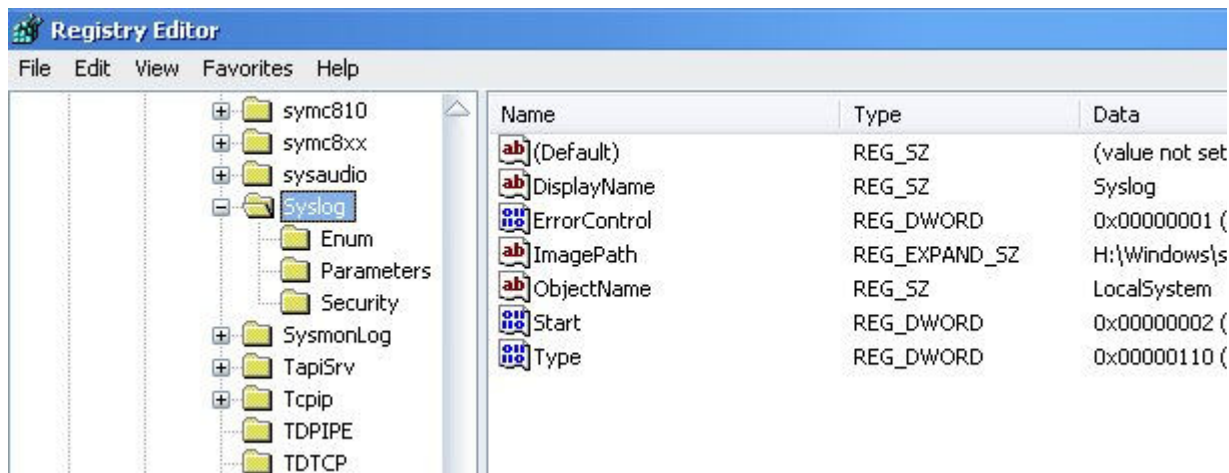
Microsoft provide a "free" utility (SrvAny.exe as part of the Windows Server Ressource Kit Tools , 12 MB.) which make possible to run any program as service. But as you know Microsoft, it would have been reeeeeeally to easy to simply release the program as free to distribute along with the applications. So you have to [download the Ressource Kit Tools](#) by yourself.

How to Install Syslog Server as Service

- Install the Syslog Server application ;-)
- Place SrvAny.exe and InstSrv.exe (from the Ressource Kit Tools) into your system directory (C:\Windows\system32)
- Click Start menu, Run, then type cmd. Then add the service by using InstSrv
---> InstSrv.exe Syslog C:\Windows\system32\srvany.exe (or whatever the actual path to srvany into your system32 directory)
- Now, you must tell to srvany that it must start your program when starting service. To do that, you must edit the registry and add a key under
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Syslog

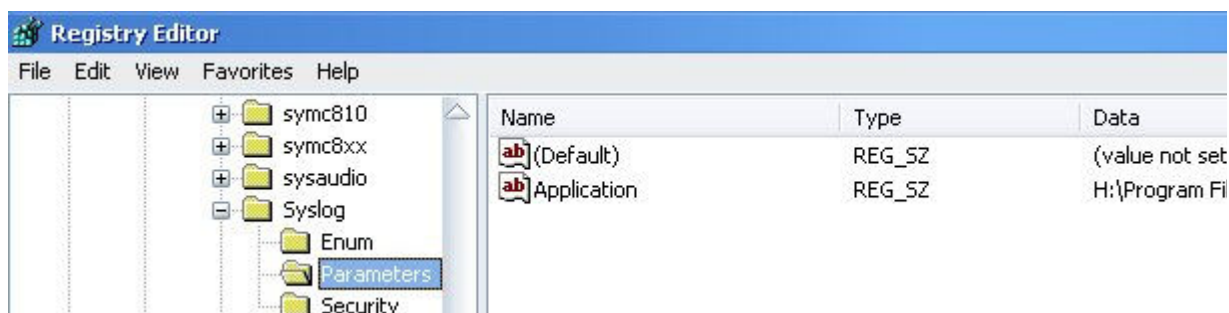
click START, then type Regedit, then choose

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Syslog.

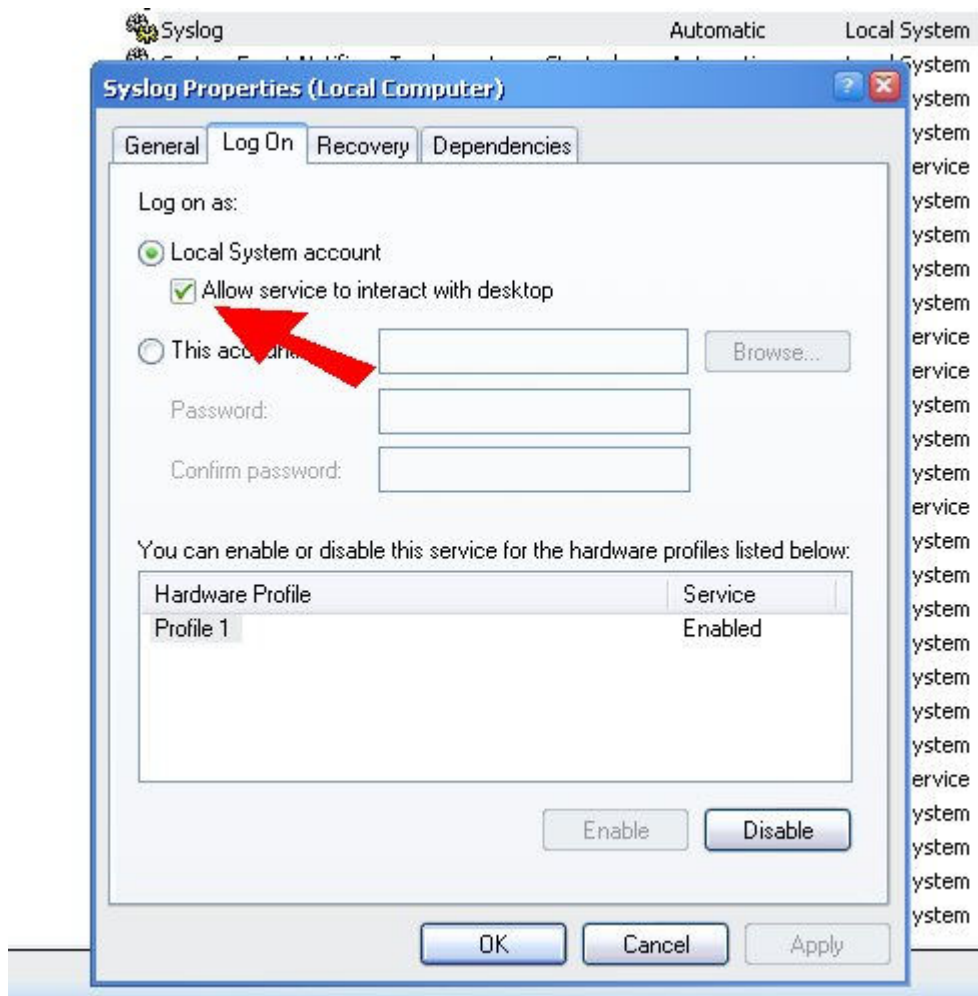



Under Syslog, add a new key named Parameters

Under Parameters, add a new string value named "Application", and as value, give the actual path of syslog.exe in your configuration (-s indicates that the program must start in minimized state)



Make sure that the service run in interactive mode : click start, Settings, Control panel, Administrative Tools, Services. Look for the Syslog service in the list and check the "allow service to interact with desktop"



- Restart your computer : the service should start, and you should see the  (Syslog) icon in the tray.

3. How to use Syslog

As soon as the program start it binds to the port 514 (udp), and wait for syslog messages to come. Basically, you can choose between three view modes :

- [By hosts](#)
- [By Facility](#)
- [By Severity](#)

In the "view by hosts" tree, by example, if you click on the root (syslog), you will see all events, in the list (datagrid). If you click on 127.0.0.1, you will see only event reported locally (EvtSys, if you have installed it).

To see the details regarding a given event, simply click on the line in the datagrid. The Event Detail form will be populated with the details regarding the event.

The screenshot shows the SysLog Server 0.9.5 application window. The title bar reads "SysLog Server 0.9.5". The menu bar includes "App", "View", "Action", "Settings", "Macros", and "Help".

The main area is divided into two sections:

- Hosts:** A tree view under "SysLog (View by Hosts)" showing three hosts: "pc-philippe [0.0.0.0]", "localhost [127.0.0.1]", and "Router [192.168.0.254]".
- Events:** A table with columns: EventIdx, Facility, Severity, Message, and TimeStamp.

EventIdx	Facility	Severity	Message	TimeStamp
40	5	5	Starting SysLog Server 0.9.5	7/01/2007 10:43:41
19	5	5	A Scheduled selective flushing has been triggered by the app.	7/01/2007 0:00:48
7	5	5	Starting SysLog Server 0.9.5	6/01/2007 17:49:59
5	5	5	Starting SysLog Server 0.9.5	6/01/2007 17:43:11
1	5	5	Starting SysLog Server 0.9.5	6/01/2007 16:29:44

Below the events table is the "Event detail" section, which contains input fields for the selected event (EventIdx: 19, TimeStamp: 7/01/2007 0:00:48, HostName: pc-philippe, HostIp: 0.0.0.0, Facility: Messages generated internally by syslogd, Severity: Notice: normal but significant condition). Below these fields is a text area containing the message: "A Scheduled selective flushing has been triggered by the app."

The status bar at the bottom displays: "[DATA] from 127.0.0.1 -- <28>MrxSmb: N/A: The redirector failed to determine the connection type."

The status bar shows all received messages, and also internal log messages, by example : [DATA] from 127.0.0.1 -- <28> MrxSmb ...

Hints :

- In View by Hosts mode, right-click on an host to get contextual menu (VNC, Ping, ...)
- Use F5 to refresh the screen
- Use CTRL-F to set a filter on the events
- Use CTRL-G to reset the current filter
- Use Action, Flush log to flush the logs (based on a given severity)
- Use Action, Export logs to export the logs into a txt file

4. Configuration

To configure the program, go to SETTINGS menu. From there you can set the select the current threshold, the alert threshold, the email address of the admin (where to send administrative alerts), the path to your favorite VNC client (see contextual menu in view by hosts mode). You can also define a conservation policy for every severity category. A value set to 0 means that the messages will never be automatically deleted.

The current threshold is the level under which the messages are not logged. The Email threshold is the level which triggers an administrative alert.

Settings

Conservation

Emergency: system is unusable : days

Alert: action must be taken immediately : days

Critical: Critical conditions : days

Error: Error conditions : days

Warning: Warning conditions : days

Notice: normal but significant condition : days

Informational: Informational messages : days

Debug: debug-level messages : days

Severity threshold

Debug: debug-level messages

Email threshold

Emergency: system is unusable

Email alert to :

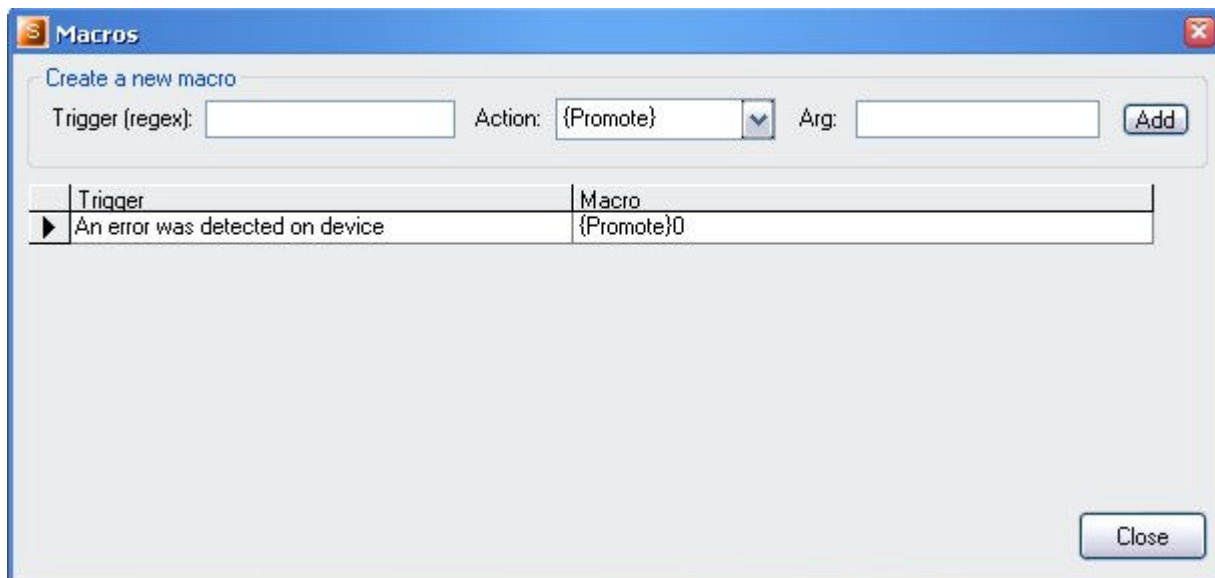
Remote Program Path

example : C:\Program Files\UltraVnc\VncViewer.exe {host}

Note : An automated selective flushing based on the settings policy is launched every time the current date changes (every day). In the example above, the logs with "error condition" severity will be automatically deleted 7 days after they occurred.

5. Macros

The way some peripherals (printers, routers, ...) and workstations report events may considerably vary. A printer may issue an error simply when the cover is open ! And windows will report a critical failure (disk error) as a simple "An error was detected on device". So you may wish to tune your syslog server in a way that major events will automatically trigger an action... And yes, it is possible.



In the Macros menu, you can insert up to 100 regexes (trigger). The possible actions are Promote, MailTo, Run, Discard. In the given example, an event containing "An error was detected on device" will promote the event to level 0 (Emergency), which will trigger an administrative alert, since the alert threshold was currently set on "Emergency".

- Promote : change the severity of the event to the specified value (0-7)
- Mailto : will simply send an administrative alert to the given address
- Run : Run the application you want
- Discard : simply discard the message