Loggerythm Systems

Loggerythm Log Analyser

Getting it to work - Documentation Home

For reverse proxy reporting you MUST be logging the Service name (s-svcname) **field OR set your inside IP's, one or the other or both.**

	The name of the service that is logged. Which can be :
Service name (s-svcname)	- **w3proxy** indicates outgoing Web requests to the Web Proxy service. - **fwsrv** indicates Firewall service. - **w3reverseproxy** indicates incoming Web requests to the Web Proxy service.

Then to set up Loggerythm, follow these steps.

1) Edit the conf file with a text editor, Notepad will do, set up a profile, you can just modify the existing one called **[isaweb_server1]** if you want. Looking at this below the only things you will need to change are the **db_path** and **html_path** to point to where your logs are for db_path and where you want your output to go for html_path, html_path must be a valid existing path, the program will not create directories if they don't exist. **NO TRAILING BACKSLASHES PLEASE.**

2) Optional - Then add your inside IP address ranges following the example given, the only wild card character you can use is the star * . If you really don't care about the program NOT counting activity inside the firewall then just leave this blank.

3) For GMT hours, take your time zone, be it plus or minus GMT / UTC, work out the difference in seconds, i.e. for me it UTC +11 so its 11 x 60 x 60 = 39600. You need this because ISA logs in GMT Time, if we don't correct then your usage peaks show up in the wrong place, in my case at mid-evening instead of mid-morning.

4) A valid report period, can be lastday, lastweek, last2weeks, last3weeks, lastmonth, all

```
[isaweb]
logtype=isawebext
filespec=webextd*.log
db_path=d:\logs\isalogs
html_path=C:\Output\ISAWeb
dolookups=0
cost_kb=0
tablerows=25
insideips=172.17.*,172.18.*,192.168.*
DateSeparator=-
LogDateFormat=yyyy/mm/dd
defaultfilename=index.html
```

```
GMThours=39600
ReportPeriod=lastweek
iptowatch=
usertowatch=
ignore_anon=
userdetail=1
userdetailrows=10
```

**Do not change Date Separator, log date format will be correct in 99% of default setups.

5) Test it, open a DOS prompt and go to the Loggerythm Directory, Win2K and NT ? try this

C:\>cd\program*\logg*) , Just a bit quicker :)

C:\Program Files\Loggerythm Log Analyser>

Then run the program giving the name of your profile created above as a parameter, ie for the above profile we would type , **loggerythm isaweb**

C:\Program Files\Loggerythm Log Analyser>**loggerythm isaweb**

If all is OK a dialog box will come up which will show the progress, when you have it running OK like this you can then add this to the Scheduler service, you need to enter the path to the file like this

"C:\Program Files\Loggerythm Log Analyser\Loggerythm.exe" isaweb

An easy way to do this is to open s DOS box and "drag" loggerythm.exe into it from Windows explorer.

Documentation Home

Last Revised 15/03/2004

http://www.loggerythm.com/
mailto:info@Loggerythm.com

info@loggerythm.com Phone & Fax +1 (603) 299-5640