Loggerythm Systems

Loggerythm Log Analyser

Fixes and Updates Page

---

17 August 2003 Freeware Version 1.6.0.24

- Added webdetails.html page, when userdetail=1 in the config file then an extra page will be created, this will link from the list of top HTTP users (coming for other protocols) so you can see the top x sites visited by each EACH user, this is what everyone has been asking for, it's a bit rough at the moment but it works well. There is ZERO overhead running this, i.e. whether you have it on or not Loggerythm will still run at the same speed. This has now become the Freeware version and this feature is limited to 5 rows for each user, there will be a very very cheap commercial version shortly where this can be unlimited rows, again no extra overhead no matter how many rows you set it to, the more rows the bigger the file, that's the only tradeoff.
- Various bug fixes.

17 June 2003 1.6.0.10 quick fix for no reporting in Exchange 2000, more later when I return to base as I am on the road at the moment :)

6 June 2003 Version 1.6.0.7

- Added Firewall log analysis, this is Beta, don't pay too much attention to the data, really I am looking for feedback on what you want to see here. The file protocols.ini can be edited to add your own protocol definitions should one not exist for something you use, if you send me additions I can add them to the distribution. Amongst things this will give you that the MS reports do not is bandwidth by rule which I find really handy.
- Added IP Packet filter log analysis, this is very basic but will give you data MS does not give you by breaking up BLOCKED events into UDP, ICMP and TCP, again this is Beta but the data should be good.
- Added basic Exchange server 2000 log analysis and fixed some Exchange 5.5 stuff like the name of the server etc.
- ANY feedback will be read, I am looking to expand features now in a big way, first up will be to stop the program re-reading logs it has already read, then go from there.

x January 2003 1.5.1.x

- Fixed divide by 1000 and not 1024 when calculating Kb, this would have caused the program to show more than the actually used bandwidth by a factor of about 2.4 %
- Fixed errors page to distinguish between information entries and actual errors, information lines now start with Information -

10 September 2002 Version 151.1.54

- Fixed date routines for ISA Standard logs, should fix invalid date errors ?
- Added VERY basic support for Exchange 5.5 Tracking Logs, will give a very rough report of Mail to and from the Internet, this will be expanded over the coming months now that the basics are in place.

Conf File Changes : LogDateFormat

LogDateFormat should ALWAYS use the forward slash as separator regardless of what is in the log file. Also day and month and years should always be dd mm yyyy

ISA Web Proxy Extended Log Files = LogDateFormat=yyyy/mm/dd

ISA Web Proxy Standard Format Log Files = LogDateFormat=mm/dd/yyyy

MS Exchange Tracking Logs (Exchange 5.5) = LogDateFormat=yyyy/mm/dd

8 September 2002 Version 1.5.1.139

New Features (for both Extended and Standard Web Proxy Logs)

- New - UserToWatch field in conf file, you can now add a comma delimited list of user names to watch for, can be none, one or lots, no spaces, case not important, i.e. usertowatch=domain\user1,domain\user2,domain\user3 etc
- New - IP to watch field in conf file will now accept a comma delimited list of IP's to watch, as many as you want. i.e iptowatch=172.17.1.2,172.17.1.3,192.168.0.2 etc
- New Field in conf file ignore_anon= set this to 1 i.e ignore_anon=1 and all anonymous connections will be ignored, these will increment the ignored events counter on the main page once for each event encountered.
- New - Malformed lines in the log file are ignored and increment the ignored events counter, it might surprise you how many lines ISA can drop in a log, don't ask me why it does this but it does it a lot :) By a malformed line I mean any line that does not have the proper number of fields as specified in the #Fields line, if there are more than one #Fields line in a single file I check it each time it shows up, this can happen if you restart the web proxy, changed logged fields etc, the program will adjust to these changes automatically.

Bug Fixes (for both Extended and Standard Web Proxy Logs)

- Fixed label error of FTP External Destinations table
- Fixed Labeling error for Outgoing and Incoming bandwidth tables on Bandwidth Trends page to properly reflect what these are showing, i.e. Total Mb used by Reverse Proxy and Total Mb used by Web proxy
- Now using the cs_uri field to get the domain rather than r_host, this should fix a problem where people with chained proxies were not seeing the final destination, can someone let me know if this actually works ?

3 September 2002 Version 1.5.1.133

- Added support for ISA Standard logs, same output as ISA Extended Logs
- Combined *.hotmail.msn.com into just hotmail.msn.com so your top 100 list is not littered with a million Hotmail servers but just one :) Makes it much easier to see how much bandwidth is being used for Hotmail
- Combined *.mail.yahoo.com into mail.yaho.com
- Combined *.yimg.com into yimg.com (image source for Yahoo Web Mail)
- Fixed error on minimise and maxmise.

25 August 2002 Version 1.5.1.121

- Fixed bug where a "x,xxx,xxx,xxx is not a valid integer" error was given at 40% mark while creating output HTML, this was only where daily average bytes exceeded 2Gb
- Minor bug fixes
- Added better error reporting into error file, if reporting any bugs please send me a copy of errors.html

6 June 2002 Version 1.5.1.101

- Fixed bug where more than 2Gb of log files caused an error. Should now handle 2,000,000 Gb of log files OK :)

20 May 2002 Version 1.5.1.91

- Fixed bug where negative values for GMThours gave a range check error.
- Fixed bad memory leak when doing runs on just lastday or lastweek when you had a large number of log files.
- Tightened up date time routines even further.
- Day of week graph now is in order of days and not by Mb.
- Fixed error where difference from GMT was not taken into account for the Summary of Activity by day table.
- General bug fixes, now tested under Win2K, Nt4 and Windows Xp. Does not run on my copy of .Net WebServer Beta 3
- Added Mb a minute stats, you should get about 30-40Mb a minute processing on a PII - PIII class PC.
- Cleaned up code a lot, result = smaller exe :)
- Install file reduced to 750Kb from over 1Mb.

16 April 2002 Version 1.5.1.67

- Added iptowatch= option, where you can specify a report to run against a few specific IP's, this can be about two times faster then a normal report for one or two ip's as very little processing takes place on average. Example usage would be iptowatch=172.17.1.2,172.17.1.5 , i.e this is a comma delimited list of IP numbers to look at .
- Moved ALL DateTime routines out of Delphi DateTime functions and into SysTools4 DateTime Functions to get away from the "flakiness" of the generic Delphi routines (faster too)
- Minor bug fixes.

9 April 2002 Version 1.5.1.56

- Made it so the program decides whether an entry is incoming or outgoing by looking at what is defined in insideips in the conf file, for example, this

insideips=172.17.*,172.18.*,192.168.* would achieve the following :

- Anything from one of these IP's **to** one of these IP's would be ignored (inside to inside)
- Anything from NOT one of these IP's **to** one of these IP's would be counted as incoming and lumped with the reverse proxy stuff (outside to inside)
- Anything left will be inside to outside (easy to check but if it's outside to outside then you have got a big problem, better to leave it in :) and logged normally.

- This checking slows down things somewhat but not enough to worry about.

8 April 2002 Version 1.5.1.53

- Total rewrite of file reading routine, should now read open files OK.
- Total rewrite of line parser, now nearly two times as fast.
- Added exception logging, if it hits an unknown exception it will write debugging info to loggerythm.rip
- Was going to add NT event logging ? anybody think that would be useful ?
- Added more exception handlers.
- Added reverse proxy counters, tell me what you want here ? this was just to get the ball rolling
- On my machine I can get about 3600 lines a second, before was averaging around 2200 LPS.

2 April 2002 Version 1.5.1.23

- Unknown logtype entry in conf file caused hang - fixed
- Response Codes and object source codes updated.
- Better checking for null values when writing main.html

2 April 2002 Version 1.5.1.x

- Added proper versioning etc with 1.5
- Added Object Source counting, i.e. cache performance graph and table
  - Need to make this show a PIE graph as bar graph is a bit useless
- Added HTTP Response counting, am counting ALL responses unlike MS who only give you 5.
  - Need to make this show a PIE graph as bar graph is a bit useless
- Added listing of Object Source Codes.
- Added listing of HTTP Response Codes.
- Cache Performance Graph now a pie graph, easier to read.
- Made Conf File overwrite users choice as it's not really needed to overwrite it at this stage as there are no changes.

1 April 2001 Version 1.4.2002.

- Modified Setup to NOT overwrite existing loggerythm.conf file
- Disable cancel button after already cancelled (i.e. waiting to exit)
- Added link to error file from main page
- Added user name gathering.

31 March 2002 Version 1.4.2002.3103

- Modules working :

- ISA Server Web Proxy, conf file LogFormat ID = isaweb1
- Cancel button now exits program nicely. Before it didn't do anything.
- On Exit it shut downs everything orderly and still creates output based on info gathered to the point where it was stopped.
- Fixed left hand menu in ISAWEB module so bookmarks work, can now go straight to graph or graphic.
- Added Analysing file x of y to dialog
- Minor bug fixes here and there.

Last Revised 15/03/2004

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

Loggerythm Systems

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