Awstats cannot process /var/log/apache2/access.log file by default / Awstats cannot open Apache server log file on Debian by default and how to fix that

Author : admin

By default the permissions of **/var/log/apache2/** are as shown below:

drwxr-x--- 2 root adm 4096 Mar 21 14:18 /var/log/apache2/

This is quite restrictive, awstats runs by default with the www-data user which is actually the user name used by Apache webserver on Debian platform.
Therefore **Awstats** cannot swith to the **/var/log/apache2/** directory and consequently cannot process the apache **access.log file** which by the way again has restrictive permissions as you can see below:

-rw-r----- 1 root adm 0 Sep 23 2009 access.log

Thus itâ€™s necessery to work out the default Debian restrictive permissions to the Apache webserver logs to â€œallowâ€• Awstats to be able to access the log files and consequently generate itâ€™s statistics.

To do that you have to allow all users to have a read access over both **/var/log/apache2/access.log** and **/var/log/apache2/error.log** otherwise you will receiver errors like:

debian:~# sudo -u www-data /usr/bin/perl /usr/lib/cgi-bin/awstats.pl -update -config=mydomain.org

Create/Update database for config "/etc/awstats/awstats.mydomain.org.conf" by AWStats version 6.7 (build 1.892)
From data in log file "/var/log/apache2/access.log"...
Error: Couldn't open server log file "/var/log/apache2/access.log" : Permission denied
Setup ('/etc/awstats/awstats.mydomain.org.conf' file web server or permissions) may be wrong.
Check config file permissions and AWStats documentation (in 'docs' directory).
debian:~#

So now to letâ€™s set some permissions to allow the www-data user to be able to access /var/log/apache2.
First way to do that is via executing:

debian:~# chmod 755 -R /var/log/apache2/*

This however from a security stand point is a complete bull-shit, that way everybody that has a physical ssh account on the server will be able to read your /var/log/apache2/.
Therefore you might try something else like for example:

debian:~# chown 754 /var/log/apache2
After which you have to change the permissions for /var/log/apache2/access.log and

/var/log/apache2/error.log to:
debian:~# chown 644 /var/log/apache2/access.log /var/log/apache2/error.log

Even if you do that, if /var/log/apache2/access.log and /var/log/apache2/error.log is the only log files on your webserver soon the permissions will broke once again, after the periodical logrotate is executed via the cron daemon.
To get around this annoyance you have to edit your **/etc/logrotate.d/apache2** conf file and change substitute:

create 640 root adm
with
create 644 root adm

Well thatâ€™s all, all left is to wait that the awstats is executed one more time through crond.
If you want to modify something to the way awstats is invoked via cron you have to edit:

/etc/cron.d/awstats

Now hopefully your awstats should work just perfectly fine :)