Table Of Contents

nixCraft: Linux Tips, Hacks, Tutorials, And Ideas In Blog Format
http://www.cyberciti.biz/

FreeBSD Install Logwatch Tool For Log Analysis and Monitoring

Posted by Vivek Gite <vivek@nixcraft.com>

[1]

Q. How do I watch, monitor system log under FreeBSD systems and generate summery of critical UNIX log files via email?

A. You can use log analysis tool called Logwatch which is a customizable, pluggable log-monitoring system. It will go through your logs stored at /var/log/ directory for a given period of time and make a report in the areas that you wish with the detail that you wish. Logwatch is very powerful system log analyzer and reporter for UNIX like systems.

Install Logwatch Tool

Type the following commands as root user:

```
# portsnap fetch update
# /usr/ports/sysutils/logwatch
# make install clean
```

Configure logwatch log analyzer

The default configuration file located at /usr/local/etc/logwatch/defaults/logwatch.conf. Open text editor to configure logwatch, enter:

```
# vi /usr/local/etc/logwatch/defaults/logwatch.conf
```

You need to setup MailTo variable to get reports summery via email, enter:

```
MailTo = vivek@nixcraft.in, admin@example.com
```

Set Print to No:

```
Print = No
```

If set to 'Yes', the report will be sent to screen instead of being mailed to above person(s). Save and close the file. Configure rest of the parameters as per your requirements.

Install cronjob

Install cronjob as follows, to run report, enter

```
# vi /etc/crontab
```

OR

```
# crontab -e
```

Append following code:

```
### Logwatch cron job ###
@daily /usr/local/sbin/logwatch.pl
```

Save and close the file. Now you should get daily emails. Sample logwatch report:

```
 ################### Logwatch 7.3.6 (05/19/07) ####################
        Processing Initiated: Tue Jul  8 06:25:03 2008
        Date Range Processed: yesterday
                              ( 2008-Jul-07 )
```

```
                           Period is day.
     Detail Level of Output: 5
             Type of Output: unformatted
          Logfiles for Host: freebsd.nixcraft.in
 ##################################################################

--------------------- Cron Begin ------------------------

Commands Run:
   User root:
         /usr/bin/rsnapshot daily: 1 Time(s)
         /usr/bin/rsnapshot hourly: 6 Time(s)
      if [ -x /usr/bin/vnstat ] && [ `ls /var/lib/vnstat/ | wc -l` -ge 1 ]; then /usr/bin/

---------------------- Cron End ------------------------

--------------------- Named Begin ------------------------

**Unmatched Entries**
   client 122.167.76.117 notify question section contains no SOA: 2 Time(s)

---------------------- Named End ------------------------

--------------------- pam_unix Begin ------------------------

cron:
   Sessions Opened:
      root: 2240 Time(s)

sshd:
   Sessions Opened:
      payal: 545 Time(s)
      payal by payal: 8 Time(s)

su:
   Sessions Opened:
      root -> nobody: 3 Time(s)

---------------------- pam_unix End -------------------------

--------------------- postfix Begin ------------------------

77502 bytes transferred
14 messages sent
14 messages removed from queue

Top ten local senders:
   14 messages sent by:
      root (uid=0):

---------------------- postfix End -------------------------

--------------------- SSHD Begin ------------------------

Users logging in through sshd:
   payal:
      192.168.0.5 (laptop.nixcraft.in): 460 times
      192.168.0.7 (desktop.nixcraft.in): 93 times

---------------------- SSHD End -------------------------

--------------------- Disk Space Begin ------------------------

Filesystem  1K-blocks     Used     Avail Capacity  Mounted on
/dev/ad4s1a    507630   384080     82940    82%    /
devfs               1        1         0   100%    /dev
/dev/ad6s1d 237397844 17597052 200808966     8%    /disk1
/dev/ad4s1d    507630       14    467006     0%    /tmp
/dev/ad4s1f 224192598  3170358 203086834     2%    /usr
/dev/ad4s1e  10154158    93652   9248174     1%    /var
```

```
procfs               4         4         0   100%    /proc
devfs                1         1         0   100%    /var/named/dev

devfs => 100% Used. Warning. Disk Filling up.
procfs => 100% Used. Warning. Disk Filling up.
devfs => 100% Used. Warning. Disk Filling up.

---------------------- Disk Space End ------------------------

####################### Logwatch End #########################
```