

Sistem Log Dosyaları

Hangimizin hatasız gün geçiyor ki? Sabahı şyerlerimize gidip kahvelerimizi aldığımızda sunucumuzun ekranında bir hatam mesajıyla karşılaşmak artık hayatımızda "normal" ler arasında yerini alabilir. Yokhiçde öyle kötü bir şeyde değil. Dü şünün hatalar olmasa nasıl öğrenebilirdik? İstebu yüzden buseferde ço ğunlukla hepimizin bildi ğifakat detayınabelkide hiç girmedi ğibir konuyuele almak istedim. Sistemlog (günlük) dosyaları. Türkçe anlamı her ne kadargünlük bile olsabuyazıdabirayrıcalıkyapıp, tamamlamı vermesi açısından anl oğ kelimesinin günlük kelimesi yerine kullanaca ğım.

FreeBSD sisteminizde log, günlük dosyaları oldu ğunubiliyorsunuz, bu dosyaları düzenli bir şekilde okumanın çok yararlı bir şey oldu ğunuda. Veehattakullanıcıların sabit disklerini doldurup yer bırakmayan şeytanı log dosyaları hakkında birkaç hikaye bile duymu ş olabilirsiniz. Pek inasıl bulabiliriz bu mistik log dosyalarını? Hem eneski güvenilir komutlarından olan birini kullanarak FreeBSD sisteminizi genelle rleşimine bir gözatalım:

```
man hier
```

Daha sonra bu man sayfasında "log" isminin su komutla arayalım:

```
/log
```

İlk sonuç sistemde birden çok program loglarını saklamak için kullanılan /var klasörü oluyor.

```
/var/ multi-purpose log, temporary, transient, and spool files
```

Eğer aynı aramayı iki kere 'n' tu şunaba saraki nelerseniz, /var klasörünün cron ve log olmak üzere iki alt klasörü oldu ğunugörürsünüz.

```
cron/log      cron log files; see cron(8)
log/          misc. system log files
```

Eğer aramayı bir kez daha "n" tu şunaba saraki nelerseniz karşınıza "Pattern not found" şeklinde bir mesaj gelecek ve bu man sayfasında şkabir/log terimi olmadığı nı belirtecektir.

Bizim için asıl önemli olan sistem log dosyaları oldu ğu için isterseniz /var/log klasörüne bir gözatalım:

```
ls /var/log
cron          messages      setuid.today
dmesg.today  ppp.logs     setuid.yesterday
dmesg.yesterday security     slip.log
lpd-errs     sendmail.st  wtmp
maillog      sendmail.st.0
```

FreeBSD versiyonunuza, sistemde yükledi ğiniz port laraven zamandır bu klasörü kullandığınız görebüçük tıde ğerleride ğişebilmektedir. Emin immeraklı bir tip olarak bütün

bulogdosyalarınagözetipiçindeneleroldu günugörmekisteyeceksinizfakatbundanönce yaratılmışolanbudosyalarınizin`lerinebirgözatalım:

```
ls -l
total 324
drwxr-xr-x  3 root  wheel  1024 Nov  5 00:00 ./
drwxr-xr-x 18 root  wheel   512 Sep 26 10:53 ../
-rw-----  1 root  wheel 81964 Nov  5 09:15 cron
-rw-r----- 1 root  wheel  3435 Nov  3 02:06 dmesg.today
-rw-r----- 1 root  wheel  3382 Nov  2 02:06 dmesg.yesterday
-rw-rw-r--  1 root  wheel    0 Jul 28 09:10 lpd-errs
-rw-rw-r--  1 root  wheel 16821 Nov  5 08:41 maillog
-rw-rw-r--  1 root  wheel 78888 Nov  5 08:40 messages
-rw-----  1 root  wheel 80332 Oct 30 14:17 ppp.log
-rw-----  1 root  wheel    0 Jul 28 09:10 security
-rw-rw-r--  1 root  wheel   616 Nov  5 08:41 sendmail.st
-rw-rw-r--  1 root  wheel   616 Nov  4 19:33 sendmail.st.0
-rw-r----- 1 root  wheel  7791 Nov  3 02:06 setuid.today
-rw-r----- 1 root  wheel  6587 Nov  2 02:06 setuid.yesterday
-rw-----  1 root  wheel    0 Jul 28 09:10 slip.log
-rw-r--r--  1 root  wheel  2684 Nov  2 21:12 wtmp
```

Çıktıyabakılırsanormalbirkullanıcınınidosyalarınıyarısınıagöz atabilmesansıvar.Eğer kullanıcıWheelgrubununbirüyesiisebirkaçdosyayıdahaaçmaiznibulunma kta.Fakat bütüidosyalarıaçmahakkihalasüperkullanıcımızda(root).

Budosyalaragözetmadanöncesonbir şeydaha:Budosyalarısizyaratmadı ğınızagöretenur bilgiiçerdiklerindebilmiyorsunuz.Unutmayınbilmedi ğinizbirdosyayı filekomutunu kullanmadansakinaçmayın.Simdidenedosyasıolduklarınabirgözatalım :

```
file *
cron: ASCII text
dmesg.today: English text
dmesg.yesterday: English text
lpd-errs: empty
maillog: ASCII text
messages: English text
ppp.log: mail text
security: empty
sendmail.st: data
sendmail.st.0: data
setuid.today: ASCII text
setuid.yesterday: ASCII text
slip.log: empty
wtmp: data
```

Dataismindekidosyalargenellikleyazdırılmazdosyalararasınağ irmekte.Yani sendmail* veya wtmpdosyalarını moreve catkomutlarınıkullanarakterminalinizdeaçmayaçalı şmak zamankaybivesisteminiziyormaktanbasabiriseyaramayacaktı r.Çıktıyabakarsak lpd-errs, securityve slip.logdosyalarınınbosolduklarınıgörebiliriz.Di ğerdosyalar text dosyalarıve“r”(okuma)izniolankullanıcılar tarafındanaçılabilir durumdalar.Budosyalardan bazılarıbüyükolmaklaberabere ğersizengüncelolanyanıdosyanınmensonbitiniğörmek isterseniz tailkomututamsizegöre:

```
tail maillog
```

Bu komut `maillog` dosyasının en son 10 satırını listeleyecektir. Geleniğininkarı şık olması ise `maillog` dosyasının satırlarının uzun olmasından kaynaklanmaktadır.

Artık hangi dosyaları göze alabileceğinizi biliyorsunuz. Pek çok dosyaları bu kadar bilgiyi ekliyor ve bulog dosyalarından etur bilgini görmek istediğinizi nasıl belirleyeceğimizi? Olayı sık tutumasi açısından `apropos` komutunu kullanmak hiç defena olmaz:

```
apropos system log
```

Bu komut bize log dosyaları ile ilgili tüm mandosyalarını listeleyecektir. Arama sonuçlarını daha iyi alabilmek için tırnak kullanalım:

```
apropos "system log"
```

tırnak kullanmadan `apropos` komutunu yazdığımız terimlerden herhangi birini içeren man sayfa larını getirirken, tırnak şartları `apropos` programına sadece yazdığımız kiterim içeren man sayfa larını bulmasını söylemek için kullanılır. Farkedeceğimizi gibiyaptığımız sonuç arama çok daha az sonuç çıkartacaktır:

```
logger(1) - make entries in the system log
newsyslog(8) - maintain system log files to manageable sizes
syslog(3), vsyslog(3), openlog(3), closelog(3), setlogmask(3) - control
system log
```

Yaklaşıyoruz. Görünüşe göre FreeBSD sistem log ları yerine “syslog” terimini kullanmakta. Tekrardan deneyelim:

```
apropos syslog
newsyslog(8) - maintain system log files to manageable sizes
syslog(3), vsyslog(3), openlog(3), closelog(3), setlogmask(3) - control
system log
syslog.conf(5) - syslogd 8 configuration file
syslogd(8) - log systems messages
Sys::Syslog(3), openlog(3), closelog(3), setlogmask(3), syslog(3) - Perl
interface to the UNIX syslog(3) calls
```

Tamam `syslogd` bütün sistem mesajlarının yazılması ile ilgili deamon ve `syslog.conf` dosyasında onun konfigürasyonunu belirliyor.

Pek çok dosya üzerinde oynamaya hakkımız var mı?:

```
ls -l /etc/syslog.conf
-rw-r--r-- 1 root wheel 903 Jul 28 09:10 /etc/syslog.conf
```

Hiç şartı olmayan bir biçimde tüm kullanıcıların okuyabileceği fakat sadece süper kullanıcılarında değiştirebileceği bir dosya daha. Normal kullanıcı olarak `more` komutunu kullanarak bir gözatalım:

```
more /etc/syslog.conf
```

```
# $FreeBSD: src/etc/syslog.conf,v 1.13 2000/02/08 21:57:28 rwatson Exp $
#
# Spaces are NOT valid field separators in this file.
# Consult the syslog.conf(5) manpage.
```

```

*.err;kern.debug;auth.notice;mail.crit      /dev/console
*.notice;kern.debug;lpr.info;mail.crit;news.err  /var/log/messages
security.*                                    /var/log/security
mail.info                                     /var/log/maillog
lpr.info                                      /var/log/lpd-errs
cron.*                                        /var/log/cron
*.err                                         root
*.notice;news.err                            root
*.alert                                       root
*.emerg                                       *
# uncomment this to enable logging of all log messages to /var/log/all.log
#*. *                                         /var/log/all.log
# uncomment this to enable logging to a remote loghost named loghost
#*. *                                         @loghost
# uncomment these if you're running inn
# news.crit                                  /var/log/news/news.crit
# news.err                                   /var/log/news/news.err
# news.notice                                /var/log/news/news.notice
!startslip
*. *                                         /var/log/slip.log
!ppp
*. *                                         /var/log/ppp.log

```

Dosyadabelirtilenparametrelerebazılarıçokaçık şekildegörevlerinibelirtselerdebizyine desyslog.conf(5)dosyasınabakıpneyaptı ğımızibilirbir şekilde de ğışıklıyapmaya gecelim.Mandosyasındakibazıparametrelerebelirtece ğimfakattümparametlerigörmek isterseniz man 5 syslog.confkomutunugirmenizgerekecek.

Syslog.confdosyasındakihersatirikibölümdenolu şmaktamesajtipinibelirleyenselector(soltaraf),vee ğerkullandı ğımızkuralauyarsayılacakışibelirtenactionbölümü(sa ğ taraf).Selectorbölümüsizindegörebilece ğinizgibiactionbölümündenbirkaçtabileayrılmı ş durumda.

Selectorbölümüisekendiiçindenoktaileikiyeayrılmı şdurumda.

facility.level

Buradafacilitymesajıneyinyarattı ğınıvelevelisemesajınönemliliksırasını belirtmekte.Facilityveleveliçinkullanılabilecekde ğerleresyslog(3)sayfasından ulaşabilir.Aşağıdakitablolarbude ğerlerigöstermekte:

Table 1: Facilities

Facility Name	What Program It Represents
AUTH	The authorization system: login(1), su(1), getty(8), etc.
AUTHPRIV	The same as AUTH, but logged to a file readable only by selected individuals.
CRON	The cron daemon: cron(8).
DAEMON	System daemons, such as routed(8), that are not provided for explicitly by other facilities.
FTP	The file transfer protocol daemons: ftpd(8), tftpd(8).
KERN	Messages generated by the kernel. These cannot be generated by any user processes.
LPR	The line printer spooling system: lpr(1), lpc(8), lpd(8), etc.
MAIL	The mail system.

NEWS	The network news system.
SECURITY	Security subsystems.
SYSLOG	Messages generated internally by syslogd(8).
USER	Messages generated by random user processes. This is the default facility identifier if none is specified.
UUCP	The uucp system. ipfw(4).
*	Specifies all facilities or programs except mark.
MARK	A special facility used by syslogd.

Table 2: Levels

Level Name	What It Represents
EMERG	A panic condition. This is normally broadcast to all users.
ALERT	A condition that should be corrected immediately, such as a corrupted system database.
CRIT	Critical conditions, e.g., hard device errors.
ERR	Errors.
WARNING	Warning messages.
NOTICE	Conditions that are not error conditions, but should possibly be handled specially.
INFO	Informational messages.
DEBUG	Messages that contain information normally of use only when debugging a program.
NONE	Special level to disable the facility.

Butablolarihangiturmesajlarinkonsolayollandı ğınıgörmekiçin kullanabiliriz.Konsolumuzdailkgörünensubbeyazkalınyazılımesajlar inkayna ğınıbulmaya çalıştığımızda:

```
*.err;kern.debug;auth.notice;mail.crit /dev/console
```

Karsımızaçıkıyor.Buradaselectorbölümününbirbirlerineba ğlıbirçok"facility.level"dan oluştuğunadikkatedin.Soldansa ğasa ğado ğruokundu ğunda syslogd`yekonsolasu mesajlarıyollamasınısöylemekte:

- bütünprogramlardangelenhatamesajları
- kerneltarafındanyaratılandebugmesajları
- sistemegiri şvesukomutununkullanımınadairmesajlar
- kritike-postamesajları

Aynimantı ğıkullanarakhangiturmesajlarınhangilogdosyalarınagönderildi ğini girebilirsiniz:

```
*.notice;kern.debug;lpr.info;mail.crit;news.err /var/log/messages
security.* /var/log/security
mail.info /var/log/maillog
lpr.info /var/log/lpd-errs
cron.* /var/log/cron
```

Dosyanıngerisiniianlamakiçinisea şağıdakitablodayazılıolanbe şparametreyibilmek durumundayız:

Table 3: Actions

Syntax of Action	What It Does
/pathname	Messages are added to the end of the specified file.
@hostname	Messages are forwarded to the syslogd(8) program on the specified computer.
user1,user2,etc.	Messages are written to those users if they are logged in.
*	Messages are written to all logged-in users.
command	Pipes the message to the specified command.

Sizinde farkettiğiniz gibi tablodaki satırların her birinin başına bir eylem (action) ekleyebilirsiniz. Örneğin, aşağıdaki gibi bir yapıya sahip bir syslog.conf dosyasını oluşturabilirsiniz:

```
!startslip
*.*                /var/log/slip.log
!ppp
*.*                /var/log/ppp.log
```

Bu parametreler, syslog.conf dosyasındaki mesajların loglara yazılmasını kontrol eder. Bir programın /etc/syslog.conf dosyasına eklenmesi için programın çalıştırılabilir adını bir satıra, önüne ! işareti ekleyerek yazarsınız. Diğer satırlar ise normalde yapılmış gibi selector ve action ile devam eder.

Bu konudaki yardımcı olmaları açısından man 5 syslog.conf sayfasının birçok deyimini inceleyebilirsiniz. syslog.conf dosyanızın üzerinde oynamayı yaptıktan sonra yeni parametreleri kullanabilmesi için syslogd programının bir HUP sinyaliyle yeniden başlatılması gerekebilir. Bunun için:

```
more /var/run/syslog.pid
```

Komutun kullanıldığı programın PID (işlem numarası) ni öğrendikten sonra, number kelimesini syslogd'nin PID numarasıyla değiştirerek, super kullanıcı olarak:

```
kill -1 number
```

Komutun kullanabiliriz.

Buyazıda bahsettiğimiz gibi, newsyslog programı /var/log klasörüne baktığınızda bazılarını göreceksiniz. newsyslog programı .0, .1, .2 şeklinde sonlanan dosyalar oluşturur. Bunlara önce newsyslog programının birer adını verilir. Hemen man sayfasına bir göz atalım:

```
man newsyslog
```

NAME

```
newsyslog - maintain system log files to manageable sizes
```

Newsyslog is a program that should be scheduled to run periodically by cron(8). When it is executed it archives log files if necessary. If a log file is determined to require archiving, newsyslog rearranges the files so that "logfile" is empty, "logfile.0" has the last period's logs in it, "logfile.1" has the next to last period's logs in it, and so on, up to a

user-specified number of archived logs. Optionally, the archived logs can be compressed to save space.

Diğerbirde işlee gerbirlogdosyasıçokbüyükhalegelirse newsyslogonualıp .0ile sonlandırıpvemuhemelensıkı ştırıpayniisimdebirdosyaolu şturmakta.Örneğin:

- maillog.1.gzeneskimaillogdosyasıvesıkı ştırılmışhalde
- maillog.0.gzikincieneskimaillogdosyasıvebudasıkı ştırılmış
- maillogisesuandasyslogdtarafındankullanılmaktaolandosya

Eğer newsyslogprogramcı ğınınmansafyasınıokumayadevamederseniz;konfigürasyon dosyasıolan /etc/newsyslog.confdosyasınınasilde ğıştirebileceğiniziö ğrenebilirböylece dosyalarınnezamanisimlerinde ğıştirilipnezamansıkı ştırılacağımbelirleyebilirsiniz.

Newsyslogtarafındansıkı ştırılmışbirdosyanıçeri ğinigörüntülemek için zmorekomutunu kullanabilirsiniz:

```
zmore maillog.0.gz
```

/var/logklasöründekieskilog`larıılmekisterseniz, .gzveyabirnumarailebitenlerisilmek herzamandahamantıklıolacaktır.E ğerbunudaotomati ğeba ğlamakistersenizayrırcabircron jobkullanmanızagerekkalmandan newsyslogbunuotomati ğeyapmasansınısize sunmakta.Buprogramcıkistedi ğinizbüyüklyadaküçüklüklelogdosyalarııtutabileceğve bunlarızamanıgeldi ğindede ğıştirebilecektir.Buradadikkatedilmesiğerekennokta /etc/syslog.conf.dosyasındabelirti ğinizisimlerdekilogdosyalarıılmemektir.Zira syslogdbdosyalarıarayacakvebulamayıncahataverecektir.Bunagöreyukarıda verdi ğim örnektebulunan maillog.0.gzve maillog.1.gzdosyalarınınsilinmesigüvenliiken maillog dosyasıyerindekalmalıdır.

Eğeryanlı şlıklagereklibirlogdosyasınısilerseniz touchkomutunukullanarak yeni,bosbir dosyaolu şturabilirsiniz:

```
cd /var/log
rm maillog (oops)
touch maillog
```

Sistemlogdosyalarınaçokufakbirgiri şbileolsabukendileriufakfakatiçerikleriçokde ğerli olanbudosyalarınöneminibelirtmekacısındanönemlibiryazıoldusanırım.Unutmay ğnkiyen iyisistemyöneticileribulogdosyalarınıdevamlıkarı ştıranksilerdençikmakta.E ğertekte /var/logdosyasınagiripbakmakistemiyorsanızFreeBSDbütünsisteml og`larınızıtoparlayıp görmenizyarayacakde ğışikalternatiflersunmaktabunun içinFreeBSDportssayfasında bulunansysutilsbölümünebakmanızıtavsiyeediyorum.

ÖzgürÖzdemircili

<http://www.enderunix.org>

<http://news.enderunix.org>

<http://haber.enderunix.org>

Sorularınıçin: dionypheles@gmx.net

Kaynaklar

DruLavigne` in “Wherethe logsfiles live” adlı yazısından çevirilmiş tir.

Yazar`ın sayfasına <http://www.oreillynet.com/pub/au/73>, orijinal metne ise http://www.onlamp.com/pub/a/bsd/2000/11/08/FreeBSD_Basics.html?page=1 adresinden ulaşabilirsiniz.