Sistem Log Dosyaları

Hangimizin hatasız günü geçiyor ki? Sabah işyerlerimize gidip kahvelerimizi aldığımızda sunucumuzun ekranında bir hata mesajıyla karsılaşmak artık hayatımızda “normal”`ler arasında yerini aldı bile.Yok hiç de öyle kötü bir şey değil bu.Düşünün hatalar olmasa nasıl öğrenebilirdik ki? İste bu yüzden bu seferde çoğunlukla hepimizin bildiği fakat detayına belkide hiç girmediği bir konuyu ele almak istedim. Sistem log (günlük) dosyaları. Türkçe anlamı her ne kadar günlük bile olsa bu yazıda bir ayrıcalık yapıp, tam anlamı vermesi açısından log kelimesini günlük kelimesi yerine kullanacağım.

FreeBSD sisteminizde log, günlük dosyaları olduğunu biliyorsunuz, bu dosyaları düzenli bir şekilde okumanın çok yararlı bir şey olduğunu da .Ve hatta kullanıcıların sabit disklerini doldurup yer bırakmayan şeytani log dosyaları hakkında birkaç hikaye bile duymuş olabilirsiniz.Peki nasıl bulabiliriz bu mistik log dosyacıklarını?Hemen eski güvenilir komutlarından olan birini kullanarak FreeBSD sistemimizin genel yerleşimine bir göz atalım:

```
man hier
```

Daha sonra bu man sayfası içinde “log” ismini 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 ayni aramayı iki kere ‘n’ tuşuna basarak yinelerseniz, `/var` klasörünün `cron` ve `log` olmak üzere iki alt klasörü olduğunu görürsünüz.

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

Eğer aramayı bir kez daha “n” tuşuna basarak yinelerseniz karsınıza "Pattern not found" seklinde bir mesaj gelecek ve bu man sayfası içinde başka bir /log terimi olmadığını belirtecektir.

Bizim için asil önemli olan sistem log dosyaları olduğu için isterseniz `/var/log` klasörüne bir göz atalım:

```
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 yüklediğiniz port`lara ve ne zamandır bu klasörü kullandığınıza göre bu çıktı değerleri değişebilmektedir.Eminim meraklı bir tip olarak bütün

bu log dosyalarına göz atıp içinde neler olduğunu görmek isteyeceksiniz fakat bundan önce yaratılmış olan bu dosyaların izin`lerine bir göz atalım:

```
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
```

Çıktıya bakılırsa normal bir kullanıcının dosyaların yarısına gözatabilme sansı var.Eğer kullanıcı Wheel grubunun bir üyesiyse birkaç dosyayı daha açma izni bulunmakta.Fakat bütün dosyaları açma hakki hala süper kullanıcımızda (root).

Bu dosyalara gözatmadan önce son bir şey daha: Bu dosyaları siz yaratmadığınıza göre ne tur bilgi içerdiklerini de bilmiyorsunuz.Unutmayın bilmediğiniz bir dosyayı `file` komutunu kullanmadan sakin açmayın.Simdi de ne dosyası olduklarına bir göz atalım:

```
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
```

`Data` ismindeki dosyalar genellikle yazdırılamaz dosyalar arasına girmekte.Yani `sendmail*` veya `wtmp` dosyalarını `more` ve `cat` komutlarını kullanarak terminalinizde açmaya çalışmak zaman kaybı ve sisteminizi yormaktan basa bir ise yaramayacaktır.Çıktıya bakarsak `lpd-errs, security` ve `slip.log` dosyalarının bos olduklarını görebiliriz.Diğer dosyalar text dosyaları ve “r”(okuma) izni olan kullanıcılar tarafından açılabilir durumdalar.Bu dosyalardan bazıları büyük olmakla beraber eğer siz en güncel olan yani dosyanın en son bitini görmek isterseniz `tail` komutu tam size göre:

```
tail maillog
```

Bu komut `maillog` dosyasının en son 10 satirini listeleyecektir.Gelen çıktının karışık olması ise maillog dosyasının satırlarının uzun olmasından kaynaklanmakta.

Artık hangi dosyalara göz atabileceğinizi biliyorsunuz.Peki bu dosyalara bu kadar bilgiyi kim ekliyor ve bu log dosyalarında ne tur bilgi görmek istediğinizi nasıl belirleyeceğiz?Olaya ışık tutum asi acısından `apropos` komutunu kullanmak hiç de fena olmaz:

```
apropos system log
```

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

```
apropos "system log"
```

tırnak kullanmadan `apropos` komutu bize yazdığımız terimlerden herhangi birini içeren man sayfalarını getirirken, tırnak işaretleri `apropos` programına sadece yazdığımız iki terimi içeren man sayfalarını bulmasını söylemek için kullanılır.Fark edeceğiniz gibi bu yaptığımız son 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 logları yerine “syslog” terimini kullanmakta.Tekrar 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
```

Tam isabet `syslogd` bütün sistem mesajlarının yazılması ile ilgilenen deamon ve `syslog.conf` dosyası da onun konfigürasyonunu belirliyor.

Peki bu dosya üzerinde oynama yapma hakkimiz var mi?:

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

Hiç şaşırtıcı olmayan bir biçimde tüm kullanıcıların okuyabileceği fakat sadece süper kullanıcının değiştirebileceği bir dosya daha.Normal kullanıcı olarak `more` komutunu kullanarak bir göz atalım:

```
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
```

Dosyada belirtilen parametlerelerin bazıları çok açık şekilde görevlerini belirtseler de biz yine de syslog.conf(5) dosyasına bakıp ne yaptığımızı bilir bir şekilde değişiklik yapmaya gecelim.Man dosyasındaki bazı parametleri belirteceğim fakat tüm parametleri görmek isterseniz `man 5 syslog.conf` komutunu girmeniz gerekecek.

`Syslog.conf` dosyasındaki her satir iki bolümden oluşmakta: mesaj tipini belirleyen selector (sol taraf), ve eğer kullandığımız kurala uyarsa yapılacak işi belirten action bolumu (sağ taraf).Selector bolumu sizinde görebileceğiniz gibi action bölümünden birkaç tab ile ayrılmış durumda.

Selector bolumu ise kendi içinde nokta ile ikiye ayrılmış durumda.

```
facility.level
```

Burada facility mesajı neyin yarattığını ve level ise mesajın önemlilik sırasını belirtmekte.Facility ve level için kullanılabilecek değerlere syslog(3) sayfasından ulaşabilir.Aşağıdaki tablolar bu değerleri göstermekte:

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.

Bu tabloları hangi tur mesajların konsola yollandığını görmek için kullanabiliriz.Konsolumuzda ilk görünen su beyaz kalın yazılı mesajların kaynağını bulmaya çalıştığımızda:

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

Karsımıza çıkıyor.Burada selector bölümünün birbirlerine bağlı birçok "facility.level"`dan oluştuğuna dikkat edin.Soldan sağa sağa doğru okunduğunda `syslogd` `ye konsola su mesajları yollamasını söylemekte:

- bütün programlardan gelen hata mesajları
- kernel tarafından yaratılan debug mesajları
- sisteme giriş ve su komutunun kullanımına dair mesajlar
- kritik e-posta mesajları

Ayni mantığı kullanarak hangi tur mesajların hangi log dosyalarına gönderildiğini 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
```

Dosyanın gerisini anlamak için ise aşağıdaki tabloda yazılı olan beş parametreyi bilmek 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 fark ettiğiniz gibi tabloda bulunan iki satir ünlem işareti ile başlamakta ve action bolumu bulunmamakta:

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

Bulunan parametreler dışında başka programların mesajlarını log olarak tutmak isteyebilirsiniz. Bir programı `/etc/syslog.conf` dosyasına ekleyebilmek için programın çalıştırılabilir adını ayrı bir satıra, önüne `!` işareti ekleyerek yerleştirin.Diğer satirda ise normalde yaptığınız gibi selector ve action değerlerini girin.

Bu konuda yardımcı olması acısından `man 5 syslog.conf` sayfasının birçok değişik senaryo için, birçok örnek içerdiğini göreceksiniz.`Syslog.conf` dosyanız üzerinde oynama yaptıktan sonra yeni parametleri kullanabilmesi için `syslogd` programına bir HUP sinyali yollayarak tekrar başlatılmasını sağlamanız gerekmekte.Bunun için:

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

Komutunu kullanıp programın PID (işlem numarası)`ni öğrendikten sonra, number kelimesini syslogd`nin PID numarası ile değiştirerek, süper kullanıcı olarak:

```
kill -1 number
```

Komutunu kullanabiliriz.

Bu yazıda bahsetmek istediğim son şey ise `newsyslog` programcığı. `/var/log` klasörüne baktığınızda bazıları sıkıştırılmış ve sonu .gz ile biten, bazıları ise `.0`, `.1`, seklinde sonlanan dosyalar olduğunu göreceksiniz.Bunlar daha önce `newsyslog` programcığının birer urunu.Hemen man safyasına 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.
```

Diğer bir değişle eğer bir log dosyası çok büyük hale gelirse `newsyslog` onu alıp `.0` ile sonlandırıp ve muhtemelen sıkıştırıp ayni isimde bir dosya oluşturmakta.Örneğin:

- `maillog.1.gz` en eski maillog dosyası ve sıkıştırılmış halde
- `maillog.0.gz` ikinci en eski maillog dosyası ve bu da sıkıştırılmış
- `maillog` ise su anda syslogd tarafından kullanılmakta olan dosya

Eğer `newsyslog` programcığının man safyasını okumaya devam ederseniz; konfigürasyon dosyası olan `/etc/newsyslog.conf` dosyasını nasıl değiştirebileceğinizi öğrenebilir böylece dosyaların ne zaman isimlerinin değiştirilip ne zaman sıkıştırılacağını belirleyebilirsiniz.

`Newsyslog` tarafından sıkıştırılmış bir dosyanın içeriğini görüntülemek için `zmore` komutunu kullanabilirsiniz:

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

`/var/log` klasöründeki eski log`ları silmek isterseniz,`.gz` veya bir numara ile bitenleri silmek her zaman daha mantıklı olacaktır.Eğer bunu da otomatiğe bağlamak isterseniz ayrıca bir cron job kullanmanıza gerek kalmadan `newsyslog` bunu otomatiğe yapma sansını size sunmakta.Bu programcık istediğiniz büyüklük yada küçüklükle log dosyaları tutabilecek ve bunları zamanı geldiğinde değiştirebilecektir.Burada dikkat edilmesi gereken nokta `/etc/syslog.conf`. dosyasında belirttiğiniz isimlerdeki log dosyalarını silmemektir.Zira `syslogd` bu dosyaları arayacak ve bulamayınca hata verecektir.Buna göre yukarıda verdiğim örnekte bulunan `maillog.0.gz` ve `maillog.1.gz` dosyalarının silinmesi güvenli iken `maillog` dosyası yerinde kalmalıdır.

Eğer yanlışlıkla gerekli bir log dosyasını silerseniz `touch` komutunu kullanarak yeni, bos bir dosya oluşturabilirsiniz:

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

Sistem log dosyalarına çok ufak bir giriş bile olsa bu kendileri ufak fakat içerikleri çok değerli olan bu dosyaların önemini belirtmek acısından önemli bir yazı oldu sanırım.Unutmayın ki en iyi sistem yöneticileri bu log dosyalarını devamlı karıştıran kişilerden çıkmakta.Eğer tek tek /var/log dosyasına girip bakmak istemiyorsanız FreeBSD bütün sistem log`larınızı toparlayıp görmeniz yarayacak değişik alternatifler sunmakta bunun için FreeBSD ports sayfasında bulunan sysutils bölümüne bakmanızı tavsiye ediyorum.

Özgür Özdemircili
http://www.enderunix.org
http://news.enderunix.org
http://haber.enderunix.org

Sorularınız için : dionypheles@gmx.net

Kaynaklar

Dru Lavigne`in “Where the logs files live” adlı yazısından çevirilmiştir.

Yazar`in 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.