SYSLOG ve SİSTEM KAYITLARI

Hasan Ümit Ezerçe
humit@tr.net
Sistem Yöneticisi

KONULAR

- sysklogd paketi
- logger uygulaması
- syslog-ng (yeni nesil syslogd)
- sistem loglarının incelenmesi

GİRİŞ

- Bir linux sistemde hem o anda neler olup bittiğini bilmek, hem de geriye dönük kayıtlara ulaşabilmek büyük önem taşır.
- Bu iş için en yaygın kullanılan paket hemen hemen bütün linux dağıtımlarıyla birlikte gelen sysklogd paketidir.
- Sysklogd paketi, sistem kayıtlarını tutan ve çekirdek mesajlarını yakalayan iki uygulama içerir: `syslogd(8)` ve `klogd(8)`.

Syslogd

- Çalışan programlardan gelen mesajları dinler,
- Unix domain socket'lerinden veri okuyabilir, dolayısıyla uzak bilgisayarlardan kayıt alabilir,
- öntanımlı olarak `/etc/syslog.conf` dosyasını kullanır.

```
Dec 24 16:26:11 infinity shutdown: shutting down for system halt
Dec 24 16:26:11 infinity init: Switching to runlevel: 0
Dec 24 16:26:12 infinity gconfd (root-1040): Received signal 1, shutting down cleanly
Dec 24 16:26:12 infinity login(pam_unix)[942]: session closed for user root
```

syslogd çalıştırma parametreleri

`-a soket`

- `/dev/log` dışında başka soketler dinleyebilir,
- bir programı `chroot()`olarak çalıştırdığınızda gerekli olacaktır,
- örneğin:

```
#syslogd -a /chroot/named/dev/log
```

syslogd çalıştırma parametreleri

`-d`

- Debug moduna geçirir.

`-f dosya_adı`

- `/etc/syslog.conf` dışında bir dosya belirtir.

`-h`

- Dışarıdan gelen mesajları yine tanımlanmış başka bir uzak bilgisayara aktarır.

syslogd çalıştırma parametreleri

`-m zaman aralığı`

- `-- MARK --` işaretini yazma sıklığı. 0 değeri bu özelliği kapatır.

`-n`

- Otomatik olarak geri planda çalışmasını önler.

syslogd çalıştırma parametreleri

`-r`

- Uzak bilgisayarlardan mesaj almasını sağlar.
- `/etc/services` dosyasında

`syslog 514/udp`

satırının bulunması gerekir.

syslogd çalıştırma parametreleri

-v

- Syslogd'nin sürüm bilgisini yazar,

-x

- Başka makinalardan gelen mesajlar için DNS sorgusu yapmasını engeller.

klogd

İşletim sistemi çekirdeği (`kernel`)tarafından verilen mesajları syslogd'ye veya `-f` parametresi ile belirlenen bir dosyaya yazar.

Syslog.conf

- Boş satırlar ve # ile başlayanlar yorumlanmaz.
- Bu dosyadaki her bir satır bir kuraldır ve her kural iki bölümden oluşur:

SEÇİM	EYLEM
`(selector)`	`(action)`
`mail.notice`	`/var/log/mail_notice`

Syslog.conf
seçim (selector)

seçim	***eylem***
`mail.notice`	`/var/log/mail_notice`

seçim ifadesi (`mail.notice`) iki bölümden oluşur:

`tür.öncelik`

`(facility.priority)`

ilk bölüm mesajın kaynağını ya da türünü/sınıfını

ikinci bölüm ise önceliğini belirtir.

tür (facility)	***Açıklama***
auth	sistem güvenliği ve giriş izin mesajları (bunun yerine `authpriv` tipinin kullanılması önerilir).
authpriv	sistem güvenliği ile ilgili mesajlar. Bu mesaj türü "özel" olarak belirlenmiştir ve bu mesajların yazıldığı dosya'nın izinleri kısıtlanmıştır.
cron	at ve cron programları
daemon	ayrıca bir mesaj türü bulunmayan sistem `daemon`'ları için.
ftp	ftp, dosya transfer protokolu
kern	kernel (işletim sistemi çekirdeği)
local0-7	yerel kullanım için ayrılmışlardır. `local7` açılış (`boot`) mesajlarını ifade eder.
lpr	yerel yazıcı servisi
mail	mail sistemi
news	USENET haber sistemi
syslog	syslogd'nin kendi ürettiği mesajlar
user	genel kullanıcı düzeyi mesajları, bir programda veya `syslog.conf` dosyasındaki bir seçici (`selector`) satırında hiçbir tür belirtilmemişse mesaj türü user olarak kabul edilecektir.
uucp	uucp alt sistemi
mark	syslogd'nin kayıt dosyasına zaman bilgisi yazmak için

Syslog.conf
seçim (selector)

öncelik (priority)	açıklama
emerg	Sistem kullanılamaz durumda.
alert	Hemen müdahale edilmeli.
crit	Kritik durum.
err	Hata durumu.
warn	Uyarı.
notice	Normal ancak, bildirilmesi gereken durum.
info	Bilgilendirme amaçlı.
debug	Hata ayıklama mesajı.
none	Hiçbiri.

Syslog.conf seçim (selector)

- '*' işareti hem mesaj türü hem de öncelik için “hepsi” anlamına gelir.

```
*.warn;auth.none;authpriv.none
/var/log/kritik
```

- *.warn ifadesi bütün mesajlardaki warn önceliğine sahip mesajlar ve üzerindekiler anlamına gelir. auth.none ve authpriv.none ifadeleri ise auth ve authpriv türündeki mesajlardan hiçbir önceliğe ait mesajların kaydedilmeyeceğini belirtir.

Syslog.conf seçim (selector)

'=' işareti yalnızca tek bir öncelik değerini belirtmek için kullanılır.

```
ftp.=err
```

ifadesi yalnızca err önceliğine sahip mesajları işaret eder.

Syslog.conf
seçim (selector)

'!' işareti bir öncelik seviyesinin ve daha yüksek öncelik seviyelerinin devre dışı bırakılması için kullanılır.

```
kern.debug;kern.!warn
/var/log/kernel.watch
```

kern.!warn ifadesi warn ve daha yukarıdaki (err, crit, alert, emerg) öncelik seviyelerini dışarıda bırakarak geri kalan mesajları kernel.watch dosyasına yazar. (debug, info, notice)

Syslog.conf seçim (selector)

uucp.none

uucp.!*

uucp.!debug

aynı anlama gelir

Syslog.conf seçim (selector)

Aralarına ',' konarak birden fazla mesaj türü belirtilebilir.

```
news,mail.*
/var/log/mail_and_news.log
veya
news.*;mail.*
/var/log/mail_and_news.log
```

Syslog.conf
eylem (action)

- `EYLEM (action)` bölümü, seçim kısmına uyan mesajların gideceği yeri bildirir.
  - Normal Dosyai /var/log/kayit.txt
  - Named Pipe |/dev/xconsole
  - Terminal ve Konsol /dev/tty12
  - Başka Bir Bilgisayar @logserver
  - Belirli Kullanıcılar root,logguard
  - HERKES *

LOGGER

- `logger(1)` uygulamasi sayesinde `syslogd` için istediğimiz türde ve öncelikte mesaj üretebiliriz.
- `syslog.conf` dosyasına girdiğimiz bir kuralın istediğimiz gibi çalışıp çalışmadığını test etmek,
- Yazdığımız `shell script`'lere `syslogd`'ye yazma yeteneği kazandırmak.

logger -p <tür.öncelik> -t <isim> <mesaj>

LOGGER
syslog.conf test

- syslog.conf:

```
cron,mail.crit     /var/log/cron_mail.crit
```

- Aşağıdaki komutları komut satırında yazdığımızda:

```
logger -p cron.crit -t "deneme" "cron.crit mesajı..."
logger -p mail.emerg -t "deneme" "mail.emerg mesajı..."
```

- /var/log/cron_mail.crit dosyasına aşağıdakine benzer satırlar eklenecektir:

```
Jan  5 22:55:30 nevershire deneme: cron.crit mesajı...
Jan  5 22:56:11 nevershire deneme: mail.emerg mesajı...
```

LOGGER
shell script

```
/usr/local/bin/dfchk:

--

#!/bin/sh
dfull=`df -k /|grep dev|awk '{print ($5)}'|awk -F%
   '{print $1}'`
warn=95
if [ $dfull -ge $warn ]
 then
   case $dfull in
    99|100) logger -p local3.emerg -t "Disk!" "/ %$dfull
  dolu";;
    *)      logger -p local3.warn -t "Disk!" "/ %$dfull
  dolu";;
   esac
fi
--
```

LOGGER
shell script

Syslog.conf dosyasında:

```
local3.=emerg          /var/log/disk.emerg
local3.=warn           /var/log/disk.warn
--
```

%95 doluluk oranına ulaşıldığında `/var/log/disk.warn` dosyasına şöyle bir kayıt girilecektir:

```
Jan  1 00:55:24 nevershire Disk!: / %95
  dolu
```

- **ftp://ftp.win.tue.nl/pub/linux-local/utils/util-linux/**

syslog-ng giriş

- Syslog-ng (next generation):
- sadece öncelik ve mesaj kaynağı değil, mesajın içeriğine göre de filtreleme yapılabilmek,
- birbirine mesaj gönderen değişik sunucuların log dosyalarında kolayca ayırdedebilmek,
- daha güçlü ve düzgün bir dosya formatı ile çalışmak.

http://www.balabit.hu/en/downloads/syslog-ng

syslog-ng

FİLTRE (Filter)

- 'and', 'or' ve 'not' operatörleri
- Facility() level() program() host() match() fonksiyonlarını

HEDEF (Destination)

- Mesajların yazılacağı dosya veya diğer yerler

KAYNAK (Source)

- dosya, tcp veya udp portu

MESAJ YOLLARI (Message Paths/Routes)

- filtre, kaynak ve hedef'lerin birleşimi

Syslog-ng

```
Source kaynak {
unix-stream("/dev/log")
tcp(ip("10.0.1.10") port(1269));};

destination uzak { file ("/var/log/uzak.log");};
destination yerel {file ("/var/log/yerel.log");};

filter internet {from("10.0.1.10");};
filter local {from("localhost");}

log {source(kaynak); filter(internet);
  destination(uzak);};
log {source(kaynak); filter(local);
  destination(yerel);};
```

SİSTEM KAYITLARININ İNCELENMESİ

- syslog.conf dosyası incelenmelidir.

```
*.info;auth.none;privauth.none /var/log/messages
mail.*                         /var/log/maillog
authpriv.*
 /var/log/secure
local7.*                       /var/log/boot.log
```

- kayit formati:

```
Jan 6 19:21:52 nevershire sendmail[556]: alias
  database /etc/aliases rebuilt by root
```

- **Ay Gün Saat:Dakika:Saniye MakineAdı Program[pid] mesaj**

SİSTEM KAYITLARININ İNCELENMESİ

- syslog.conf'da belirtilmeyen dosyalar:

• Xfree86*.log	X Window tarafından verilen mesajları içerir.
• dmesg	Sistem açılırken ekranınızdan akan mesajları içerir, genellikle donanımınız ile ilgili bilgilerdir. (diskleriniz, seri port bilgileri, cpu, ram vs.)
• httpd/*.log	bu dizin altında bulunan dosyalar apache tarafından yaratılır. Formatları ve isimleri httpd.conf dosyasında belirtilir.
• Lastlog	login(1) tarafindan sisteme giriş bilgileri tutulur. last(1) komutu ile bu dosyadaki kayıtlara ulaşılabilir.

SİSTEM KAYITLARININ İNCELENMESİ


```
Dec 10 12:07:55 infinity login[874]: FAILED LOGIN 1 FROM
(null) FOR root, Authentication failure

Dec 10 12:08:02 infinity login[874]: FAILED LOGIN 2 FROM
(null) FOR root, Authentication failure

Dec 10 12:08:14 infinity login[874]: FAILED LOGIN 3 FROM
(null) FOR root, Authentication failure

Dec 10 12:08:29 infinity login[874]: FAILED LOGIN SESSION
FROM (null) FOR root, Authentication failure

Dec 10 12:08:29 infinity login(pam_unix)[874]: 3 more
authentication failures; logname=LOGIN uid=0 euid=0
tty=tty1 ruser= rhost=  user=root

Dec 10 12:08:29 infinity login(pam_unix)[874]:
service(login) ignoring max retries; 4 > 3

Dec 10 12:08:53 infinity login(pam_unix)[942]: session
opened for user root by LOGIN(uid=0)

Dec 10 12:08:53 infinity root[942]: ROOT LOGIN ON tty1
```

SİSTEM KAYITLARININ İNCELENMESİ


```
Dec 10 12:09:07 infinity kernel: hda: ATAPI 40X CD-ROM
drive, 128kB Cache
Dec 10 12:09:07 infinity kernel: Uniform CD-ROM driver
Revision: 3.12
Dec 10 12:09:08 infinity kernel: cdrom: This disc doesn't
have any tracks I recognize!
```

SİSTEM KAYITLARININ İNCELENMESİ


```
Jan  8 15:52:22 infinity kernel: Soundblaster audio driver
Copyright (C) by Hannu Savolainen 1993-1996
Jan  8 15:52:22 infinity kernel: sb: No ISAPnP cards found,
trying standard ones...
Jan  8 15:52:22 infinity kernel: sb: dsp reset failed.
Jan  8 15:52:32 infinity kernel: Soundblaster audio driver
Copyright (C) by Hannu Savolainen 1993-1996
Jan  8 15:52:32 infinity kernel: sb: No ISAPnP cards found,
trying standard ones...
Jan  8 15:52:32 infinity kernel: sb: dsp reset failed.
```

YARDIMCI PROGRAMLAR
logrotate

- **LOGROTATE**
- ftp://ftp.redhat.com/pub/redhat/linux/code/logrotate
- günlük, haftalık, aylık olarak veya boyuta göre
- dönüşüm, sıkıştırma, silme ve mail ile gönderme
- http://www.topology.org/linux/logrotate.html sayfasında logrotate kullanımı ile ilgili bilgi bulabilirsiniz.

YARDIMCI PROGRAMLAR
logrotate

```
#logrotate.conf
compress            # dosyalar sıkıştırılsın
 /var/log/messages {
    rotate 5        # her eski dosya 5
    weekly          # hafta silinmeden tutulacak
    postrotate              # kayıt dosyası
  değiştirildikten sonra
/sbin/killall --HUP syslogd     # syslogd yeniden
  başlatılacak
    endscript               #bu kayıt dosyası için
  işlemlerin sonu.
}
```

YARDIMCI PROGRAMLAR
logrotate

```
"/var/log/httpd/access.log" /var/log/httpd/error.log {
rotate 5                    # eski dosyalar 5 rotate işleminden
mail webmaster@my.org       # sonra mail ile gönderilecek
size=10000k                 # bu işlemler eğer dosyalar 10000k
                            # üzerine çıkarsa yapılacak
sharedscripts               #postrotate işlemleri her dosya için
postrotate                  #ayrı ayrı yapılmayacak.
/sbin/killall --HUP httpd   # httpd yeniden başlatılıyor.
Endscript
  }
```

YARDIMCI PROGRAMLAR
swatch

- **SWATCH**
- http://www.oit.ucsb.edu/~eta/swatch
- Çalıştıran kullanıcının home dizininde bulunan .swatchrc dosyasında yazan kurallara göre sistemde gerçekleşen olayları anında izler ve bunlara göre hareket eder.
- Komut satırından çalıştırılarak bir süre önce yazılmış olan kayıtlar da incelenebilir.

YARDIMCI PROGRAMLAR
swatch

- hatalı giriş yapıldığında verilen "FAILED LOGIN" mesajını takip etmek için .swatchrc dosyasına şu satırlar girilebilir:

```
watchfor /FAILED LOGIN/
 mail address=security@mydomain.org,
subject="FAILED LOGIN!"
 exec "/root/bin/send_sms"
```

- /var/log/messages dosyasına "/" işaretleri arasındaki kelime grubu yazıldığı anda belirtilen adrese bu satırları mail ile gönderecek ve exec bölümünde verilen dış programı çalıştıracaktır.

YARDIMCI PROGRAMLAR
logcolorize

- **LOGCOLORIZE**
- http://www.linuxsupportline.com/~pgp/linux
- önemli kelimelerin dikkat edilecek renklerle görüntülenmesini sağlar.
- Dilediğiniz başka anahtar kelimeleri de programın içine ekleyebilirsiniz.

```
cat /var/log/messages|logcolorize.pl|
  more
```

YARDIMCI PROGRAMLAR
freq

- **FREQ**
- http://www.bangmoney.org/projects/freq
- lastlog kayıt dosyasını inceler
- Giriş bilgilerini görmek için şu komut verilebilir.

```
# freq -a -g
Name       Logins   Graph
========== ======== ============================
oya        2        ###
humit      5        ########
root       14       ##############################
```

YARDIMCI PROGRAMLAR
isoqlog

- **ISOQLOG**
- http://www.enderunix.org/isoqlog/indextr.php
- Bir MTA log analiz programıdır.
- Qmail, Postfix, Senmail log dosyalarını tarayarak HTML formatında istatistik çıkarır.
- Gönderici, Alıcı, Toplam gönderilen mail ve büyüklüğü ve sayısı.
- Günlük, aylık ve yıllık en çok kullanılan email ve domain bilgisi.

YARDIMCI PROGRAMLAR
diğer kaynaklar

- apache, squid gibi programların kayıtlarını analiz ederek web trafiği hakkında bilgi verenler,
- firewall kayıtlarından saldırı tespit edenler,
- router'lardan gelen kayıtlara göre ağ trafiği bilgisi verenler de vardır. Geniş bilgiye:
- http://www.linux.org/apps/all/Administration/Log_Analyzers.
- http://www.counterpane.com/log-analysis.html
- http://freshmeat.net/browse/245
- Adreslerinden ulaşılabilir.

SYSLOG ve SİSTEM KAYITLARI

Hasan Ümit Ezerçe
humit@tr.net
Sistem Yöneticisi