1 SYSLOG Servisi

Linux sistemin log servisi sistemin önemli bir parçasıdır. Sistem sorunlarını önlemek ve çözmek için bir sistem yöneticisi bu logları analize edebilmelidir. Sistem loglarını konfigüre etmek ve log dosyalarını yönetebilinmelidir, özellikle sistem çok yüklenmeli çalışıyor ise bu dosyalar çok büyümektedir. Bu dosyalar sadece makul bir zaman için tutulmalıdır, bu da dosyaları incelemekte yardımcı olacaktır.

Red Hat Linux sisteminde iki sistem log süreci bulunmaktadır:

- **syslogd** – Sistemin temel log süreci
- **klogd** – Çekirdek loglarını tutan süreç

Aşağıdaki bölümlerde bu süreçler ele alınmaktadır.

1.1 syslogd Süreci

Belirtilmiş olduğu gibi **syslogd** sistemin temel loglarını tutan bir süreçtir. Bu süreç sistem açılışında ***/etc/rc.d/init.d/syslog*** scripti çalıştırılarak başlatılır.

Önemli bir olay meydana geldiğinde ve yazılım bu olay hakkında log tutmak istediğinde, mesajını **syslogd** sürecine gönderir. Genel olarak loglar ***/var/log/messages*** dosyasına yazılır. Bunun dışında **syslogd** sürecin çeşitli log işlemleri vardır. Örneğin **syslogd** olay loglarını farklı dosyalara yazabilmektedir, ya da sistem konsoluna gönderir, ya da o an sistemde bulunan kullanıcılara vb. ***/etc/syslog.conf*** dosyası **syslogd** sürecin konfigürasyon dosyasıdır.

1.2 klogd Süreci

Çekirdek mesajlarını tutan diğer onemli süreç **klogd**'dir. Genel olarak bu süreç gelen mesajları direk **syslogd** sürecine aktarır. Ama istenildiğinde bu süreç komut satırından çalıştırılarak çekirdek mesajları belirtilmiş dosyaya yazdırılabilinmektedir.

1.3 Syslog Konfigürasyonu

Sistem log servisinin konfigürasyonu ***/etc/syslog.conf*** dosyasında yer almaktadır. Bu dosyadaki her satır log türünü ve yapılacak log işlemini belirtir. Genel olarak satır yapısı şu şekildedir:

tip.öncelik[; tip.öncelik ...] işlem

Burada:

- ***tip*** – log yazdıran uygulamaların türünü belirtir. Bir kaç tip virgül ile ayırılarak beraber tanımlanabilir.
- ***öncelik*** – mesajın önemini belirtir.
- ***işlem*** – tanımlanmış tip ve önceliğe uygun bir mesaja uygulanacak işlemi belirler.

Tipler, öncelikler ve işlemler aşağıdaki tablolarda tanımlanmıştır.

Tipler ve Tanımları

Tip (Facility)	**Tanım**

belirteci	
auth	Kullanıcı tanıma mesajları.
authpriv	Özel kullanıcı tanıma mesajları. Sıradan kullanılar bu mesajları görmemelidir.
cron	Cron uygulamasının mesajları
daemon	Sunucu süreçlerin ve TCP servisinin mesajları
kern	Çekirdek mesajları
lpr	Yazıcı süreçlerin mesajları
mail	E-posta süreçlerin mesajları
news	Haber grupların mesajları
syslog	Sistem mesaj servisin mesajları
user	Kullanıcılar ile ilgili süreçlerin mesajları
uucp	Unix-to-Unix Copy Program (UUCP) mesajları
local0-local7	Makinada tanımlanmış süreçlerin mesajları
*	Tüm süreçlerin mesajları

Mesajların Öncelik Tanımları

Öncelik (priority) ifadesi	**Öncelik**	**Tanım**
debug	1	Hata ayıklama için kullanılan mesajlar
info	2	Bilgilendirme mesajlar
notice	3	Önemli durumlar için kullanılan mesajlar
warning	4	Uyarı mesajları
err	5	Hata mesajları
crit	6	Ciddi, kritik hatalar
alert	7	Acil durum mesajları
emerg	8	Sistem devre dışı
*		Tüm mesajlar
=öncelik		Sadece belirtilmiş öncelikli loglar tutulsun
! öncelik		Belirtilmiş öncelikli loglar dikkate alınmasın
!=öncelik		Belirtilmiş öncelikli loglar dışındaki tüm loglar.

Log İşlemlerin Tanımları

İşlem belirteci	**Açıklama**
tam yol	Mesajlar tam yolu ve adı verilen dosyaya yazılır
/dev/console veya /dev/ttyN	Mesajlar belirtilmiş terminale gönderilir
@host	Mesajlar uzaktaki bilgisayara gönderilir
Kullanıcı kimlik numarası	Mesaj kimlik numarası verilen kullanıcıya, o anda sistemde bulunuyor ise, gönderilir. Mesajı bir kaç kullanıcıya göndermek için kullanıcı numaralar bir virgül ile ayırılarak beraber yazılır.
*	Mesaj o an sistemde bulunan tüm kullanıcılara gönderilir

Örnek:

kern.* ***/dev/console***
.info;mail.none;authpriv.none;cron.none** ***/var/log/messages
authpriv.* ***/var/log/secure***
mail.* ***/var/log/maillog***
cron.* ***/var/log/cron***

***.emerg**	*****
***uucp,news.crit**	***/var/log/spooler**
local7.	***/var/log/boot.log**

1.4 Sistem Log Dosyası

Bu bölümde sistemin logları yazılan dosyasının yapısı ele alınmaktadır. Her mesaj bir satıra yazılır. Mesajın genel yapısı şu şekildedir:

zaman konak uygulama[süreç_kimlik_numarası]: mesaj

burada:

- *zaman* – mesajın yazılma tarihi ve saati
- *konak* – mesajı gönderen bilgisayar adı
- *uygulama* – mesajı gönderen uygulamanın ismi
- *süreç_kimlik_numarası* – mesajı gönderen uygulamanın süreç numarası
- *mesaj* – yazdırılan mesajın içeriği

Örnek:

```
Jan 29 12:46:04 cvs postgresql: Starting postgresql service:  succeeded
Jan 29 12:46:05 cvs sendmail: sendmail startup succeeded
Jan 29 12:46:06 cvs httpd: httpd startup succeeded
Jan 29 12:46:07 cvs crond: crond startup succeeded
Jan 29 12:46:07 cvs anacron: anacron startup succeeded
Jan 30 15:08:14 cvs sshd(pam_unix)[25035]: session opened for user root by (uid=0)
Jan 30 15:09:00 cvs named[25095]: starting BIND 9.1.0 -u named
Jan 30 15:09:00 cvs named: named startup succeeded
Jan 30 15:09:00 cvs named[25099]: loading configuration from '/etc/named.conf'
Jan 30 15:09:00 cvs named[25099]: listening on IPv4 interface eth0,
160.75.5.142#53
Jan 30 15:09:00 cvs named[25099]: running
```

1.5 Logların uzaktaki sunucuya gönderilmesi

Konfigürasyon bölümünde logların uzaktaki sunucuya gönderilmesi için yapılması gerekenler anlatılmıştı. Bu bölümde uzaktaki sunucu üzerinde diğer bilgisayarlardan gelen mesajları kabul etmesi için yapılması gereken ayarlar ele alınacaktır.

Uzaktaki bilgisayarlardan logları alabilmek için yerel sunucuda **syslogd** süreci "**-r**" parametresi ile çalıştırılmalıdır.

Bu değişikler süreci başlatan scriptin içinde yapılabilinmektedir, ***/etc/rc.d/init.d/syslog*** dosyası bir metin editörü ile açılıp

SYSLOGD_OPTIONS="-m 0"

değişkenine “-r” parametresi eklenmelidir:

SYSLOGD_OPTIONS="-m 0 -r"

Veya ***/etc/sysconfig/syslog*** dosyası tanımlanmış ise bu dosyada aynı değişkenin üzerinde değişiklikler yapılabilir.

1.6 Açılış Logları

Linux sistemi açılış sırasında ekrana açılış notlarını göndermektedir. Bu loglar çekirdek log tamponuna yazılmaktadır. Çekirdek log tamponunu listelemek için

dmesg

komutu kullanılır. Çok önemli olan bu logların kaybını önlemek için açılış scripti bu logları ***/var/log/dmesg*** dosyasına yazmaktadır.

Örnek bir *dmesg* dosyasının içeriği

```
Linux version 2.4.2-2 (root@porky.devel.redhat.com) (gcc version 2.96 20000731
(Red Hat Linux 7.1 2.96-79)) #1 Sun Apr 8 20:41:30 EDT 2001
BIOS-provided physical RAM map:
 BIOS-e820: 000000000009fc00 @ 0000000000000000 (usable)
 BIOS-e820: 0000000000000400 @ 000000000009fc00 (reserved)
 BIOS-e820: 0000000000020000 @ 00000000000e0000 (reserved)
 BIOS-e820: 000000000fee0000 @ 0000000000100000 (usable)
 BIOS-e820: 0000000000010000 @ 000000000ffe0000 (ACPI data)
 BIOS-e820: 0000000000010000 @ 000000000fff0000 (ACPI NVS)
 BIOS-e820: 0000000000080000 @ 00000000fff80000 (reserved)
On node 0 totalpages: 65504
zone(0): 4096 pages.
zone DMA has max 32 cached pages.
zone(1): 61408 pages.
zone Normal has max 479 cached pages.
zone(2): 0 pages.
zone HighMem has max 1 cached pages.
Kernel command line: auto BOOT_IMAGE=linux ro root=305
BOOT_FILE=/boot/vmlinuz-2.4.2-2
Initializing CPU#0
Detected 935.473 MHz processor.
Console: colour VGA+ 80x25
Calibrating delay loop... 1867.77 BogoMIPS
Memory: 255228k/262016k available (1365k kernel code, 6400k reserved, 92k data,
236k init, 0k highmem)
Dentry-cache hash table entries: 32768 (order: 6, 262144 bytes)
Buffer-cache hash table entries: 16384 (order: 4, 65536 bytes)
```

```
Page-cache hash table entries: 65536 (order: 7, 524288 bytes)
Inode-cache hash table entries: 16384 (order: 5, 131072 bytes)
VFS: Diskquotas version dquot_6.5.0 initialized
CPU: Before vendor init, caps: 0387f9ff 00000000 00000000, vendor = 0
CPU: L1 I cache: 16K, L1 D cache: 16K
CPU: L2 cache: 256K
Intel machine check architecture supported.
Intel machine check reporting enabled on CPU#0.
CPU: After vendor init, caps: 0387f9ff 00000000 00000000 00000000
CPU serial number disabled.
CPU: After generic, caps: 0383f9ff 00000000 00000000 00000000
CPU: Common caps: 0383f9ff 00000000 00000000 00000000
CPU: Intel Pentium III (Coppermine) stepping 06
Enabling fast FPU save and restore... done.
Enabling unmasked SIMD FPU exception support... done.
Checking 'hlt' instruction... OK.
POSIX conformance testing by UNIFIX
mtrr: v1.37 (20001109) Richard Gooch (rgooch@atnf.csiro.au)
mtrr: detected mtrr type: Intel
PCI: PCI BIOS revision 2.10 entry at 0xfdb21, last bus=2
PCI: Using configuration type 1
PCI: Probing PCI hardware
PCI: Using IRQ router default [8086/2410] at 00:1f.0
isapnp: Scanning for PnP cards...
isapnp: No Plug & Play device found
Linux NET4.0 for Linux 2.4
Based upon Swansea University Computer Society NET3.039
Initializing RT netlink socket
apm: BIOS not found.
Starting kswapd v1.8
pty: 256 Unix98 ptys configured
block: queued sectors max/low 169421kB/56473kB, 512 slots per queue
RAMDISK driver initialized: 16 RAM disks of 4096K size 1024 blocksize
Uniform Multi-Platform E-IDE driver Revision: 6.31
ide: Assuming 33MHz system bus speed for PIO modes; override with idebus=xx
PIIX4: IDE controller on PCI bus 00 dev f9
PIIX4: chipset revision 2
PIIX4: not 100% native mode: will probe irqs later
    ide0: BM-DMA at 0xffa0-0xffa7, BIOS settings: hda:DMA, hdb:pio
    ide1: BM-DMA at 0xffa8-0xffaf, BIOS settings: hdc:DMA, hdd:pio
```

```
hda: ST320413A, ATA DISK drive
hdc: SS06 SAMSUNG DVD-ROM SD-612S, ATAPI CD/DVD-ROM drive
ide0 at 0x1f0-0x1f7,0x3f6 on irq 14
ide1 at 0x170-0x177,0x376 on irq 15
hda: 39102336 sectors (20020 MB) w/512KiB Cache, CHS=2434/255/63, UDMA(66)
Partition check:
 hda: hda1 hda2 < hda5 hda6 >
Floppy drive(s): fd0 is 1.44M
FDC 0 is a post-1991 82077
Serial driver version 5.02 (2000-08-09) with MANY_PORTS MULTIPORT SHARE_IRQ
SERIAL_PCI ISAPNP enabled
ttyS00 at 0x03f8 (irq = 4) is a 16550A
ttyS01 at 0x02f8 (irq = 3) is a 16550A
Real Time Clock Driver v1.10d
md driver 0.90.0 MAX_MD_DEVS=256, MD_SB_DISKS=27
md.c: sizeof(mdp_super_t) = 4096
autodetecting RAID arrays
autorun ...
... autorun DONE.
NET4: Linux TCP/IP 1.0 for NET4.0
IP Protocols: ICMP, UDP, TCP, IGMP
IP: routing cache hash table of 2048 buckets, 16Kbytes
TCP: Hash tables configured (established 16384 bind 16384)
Linux IP multicast router 0.06 plus PIM-SM
NET4: Unix domain sockets 1.0/SMP for Linux NET4.0.
VFS: Mounted root (ext2 filesystem) readonly.
Freeing unused kernel memory: 236k freed
Adding Swap: 530104k swap-space (priority -1)
usb.c: registered new driver usbdevfs
usb.c: registered new driver hub
usb-uhci.c: $Revision: 1.251 $ time 20:53:29 Apr  8 2001
usb-uhci.c: High bandwidth mode enabled
PCI: Setting latency timer of device 00:1f.2 to 64
usb-uhci.c: USB UHCI at I/O 0xd000, IRQ 10
usb-uhci.c: Detected 2 ports
usb.c: new USB bus registered, assigned bus number 1
hub.c: USB hub found
hub.c: 2 ports detected
```

1.7 Log Dönüşümü

Büyük sistemlerde log dosyaları çok hızlı büyümektedir, bu sebepten dolayı dosyalar kullanışsız hale geliyorlar. Bu dosyaların boyutlarını kontrol etmek *cron* servisi her gün log dosyaların dönüşümünü yapan */etc/cron.daiyi/logrotate* scriptini çalıştırmaktadır. Red Hat linux dağıtımında mevcut olan *logrotate* scripti şu şekildedir:

#!/bin/sh

/usr/sbin/logrotate /etc/logrotate.conf

Scriptte kullanılan ***logrotate*** komutu log dosyaları üzerinde bir kaç farklı işlem uygulayabilmektedir:

- Dosyaların dönüşümü
- Log dosyaların sıkıştırılması
- Log dosyalarını özel kullanıcıları gönderilmesi

Dönüşüm bir dosyayı sıra içine sokmaktadır. Yani bir dosyayı belli bir zamanda silmek yerine ismini değiştirerek saklanmaktadır ve böylece mevcut log dosyası her zaman çalışılabilenecek boyuttadır. Log dönüşümün konfigürasyon scripti */etc/logrotate.conf*'tur. Varsayılan özellikleri ile log dosyaların dönüşümü haftada bir kez yapılamktadır. Tipik bir ***/etc/logrotate.conf*** dosyasını içeriği:

```
# see "man logrotate" for details
# rotate log files weekly
weekly

# keep 4 weeks worth of backlogs
rotate 4

# send errors to root
errors root

# create new (empty) log files after rotating old ones
create

# uncomment this if you want your log files compressed
#compress

# RPM packages drop log rotation information into this directory
include /etc/logrotate.d

# no packages own lastlog or wtmp -- we'll rotate them here
/var/log/wtmp {
    monthly
    create 0664 root utmp
    rotate 1
}

# system-specific logs may be configured here
```

Bu dosyada görülen ***/etc/logrotate.d*** dizini özel log dosyaları için dönüşüm kurallarını içermektedir.