





LPI 108.2. LPI 108.2. Bitàcoles del sistema

Wiki:

http://acacha.org/mediawiki/index.php/LPI_108.2

Objectius

108.2. Bitàcoles del sistema	
	<ul style="list-style-type: none"> ▪ Objectiu: Els candidats han de ser capaços de configurar el dimoni syslog. Aquest objectiu també inclou configurar el dimoni de logging per tal d'enviar les bitàcoles a un servidor central o acceptar bitàcoles com servidor central de bitàcoles. ▪ Pes: 2
	<p>Àrees Clau de Coneixement:</p> <ul style="list-style-type: none"> ▪ Fitxers de configuració de syslog ▪ syslog ▪ Ajudes estàndard, prioritats i accions
	<p>La següent és una llista parcial de fitxers, termes i utilitats utilitzades:</p> <ul style="list-style-type: none"> ▪ syslog.conf ▪ syslogd ▪ klogd ▪ logger
	<p>Apunts: LPI 108.2. Bitàcoles del sistema</p>

- ♦ **Aka: fitxers de log o de fitxers de registre o registre del sistema**

- ♦ L'origen del nom està en els llibres de navegació on s'anoten tots els esdeveniments rellevants d'un viatge.



♦ **Registre del sistema (SYStem LOG)**

- ♦ Tant podem **gestionar els registres del sistema local** com podem configurar un **servidor de log** on les màquines d'una xarxa puguin centralitzar els seus fitxers de log.
- ♦ La majoria de sistemes Linux utilitzen el **dimoni syslog** per tal de gestionar el manteniments i ús dels logs del sistema d'una forma unificada.
- ♦ **Ryslog**: versió millorada de syslog que utilitzen algunes distribucions Linux com Ubuntu o Fedora
- ♦ **LPI=syslog**. De totes formes són molt similars

♦ Normalment ja està instal·lat

♦ Comprovar si està instal·lat:

Ubuntu

```
$ dpkg -l | grep syslog  
ii  rsyslog 4.2.0-2ubuntu5.1 enhanced multi-threaded syslogd
```

♦ Instal·lació:

- El paquet del syslog tradicional: syslogd

```
sudo apt-get install rsyslog
```

♦ Hi ha altres implementacions

- Syslog-ng
- Metalog
- ...

♦ Fitxers de configuració:

```
$ dpkg -L rsyslog | grep etc
/etc
/etc/rsyslog.d
/etc/logcheck
/etc/logcheck/ignore.d.server
/etc/logcheck/ignore.d.server/rsyslog
/etc/rsyslog.conf
/etc/logrotate.d
/etc/logrotate.d/rsyslog
/etc/init
/etc/init/rsyslog.conf
/etc/init/rsyslog-kmsg.conf
/etc/init/dmesg.conf
/etc/init.d
/etc/init.d/rsyslog
/etc/init.d/rsyslog-kmsg
/etc/init.d/dmesg
```

Configuració

- ♦ **Permet utilitzar un grapat predefinit de fitxers de log a on s'enregistraran la majoria d'esdeveniments del sistema.**
 - ♦ D'aquesta manera diferents serveis del sistema arriben a utilitzar el mateix fitxer de log. **Els fitxers de log es classifiquen per facilities**
 - ♦ Fitxer principal de configuració:
 - **/etc/rsyslog.conf** (rsyslog)
 - **/etc/syslog.conf** (syslog tradicional)

Configuració

Format de les línies:

```
facility.priority
```

```
action
```

- ◆ Facility: paraula clau que identifica el tipus de programa o eina que ha generat el missatge de log. Valors possibles:
 - **authpriv o auth o security**: Utilitzat per les aplicacions que gestionen les autoritzacions del sistema (PAM, login, su, sudo, etc...). Auth i security són obsoletes (deprecated)
 - **cron**: Eines de gestió automàtica de tasques com cron
 - **daemon**: **Calaix de sastre**. Servidors sense facility específica
 - **kern**: Missatges del nucli. Vegeu també ksylogd i dmesg.
 - **lpr**: Gestió de la impressió al sistema (CUPS i altres)
 - **mail**: Servidors de correu electrònic
 - **news**: Eines com servidors de notícies.
 - **syslog**: Missatges generats de forma interna per syslog
 - **user**: Aplicacions d'usuari del sistema per a missatges a mida.
 - **local0 a local7 i mark**: Reservat per a usos específics i ús intern de syslog

Configuració

♦ **Priority:** Indica la importància del missatge.

- **debug:** Mostra la màxima informació possible i només s'utilitza quan s'està provant una aplicació. No és recomanable activar-ho en un sistema en explotació ja que pot afectar al rendiment del sistema.
- **info:** Missatges d'informació.
- **notice:** no són necessàriament errors però s'haurien de tenir en compte.
- **warning o warn(obsolet):** Avisos importants que tot i no ser errors poden tenir algun tipus de repercusió.
- **error o err (obsolet):** Missatges d'error.
- **crit:** Missatges d'error importants com errors de maquinari.
- **alert:** Missatges crítics d'error que s'haurien de solucionar immediatament
- **emerg o panic (deprecated):** Missatges molts greus que normalment impliquen que la màquina deixarà de funcionar immediatament o ja ha deixat de funcionar. Mostra els missatges més importants que són els missatges relacionats amb errors molt greus. Pànic encara s'accepta però és obsolet.

♦ **action:** és un fitxer o màquina remota on es guarda el registre

Configuració

- ◆ Es poden especificar múltiples facilitats separant-les per comes (,)
- ◆ Es poden indicar múltiples selectors separant-los per punt i coma (;)
- ◆ El conjunt format per una "facility" més una acció (action) s'anomena **selector** (facility.action)
- ◆ Un asterisk (*) va referència a totes les facilities.
- ◆ Es poden fer comentaris dins el fitxer de configuració utilitzant el coixinet (#)
- ◆ Tots els missatges incorporen un codi de prioritat. Si el codi és igual o major en prioritat que el llindar especificat aleshores el missatge s'enregistra.

Configuració

- ♦ **@: Permet indicar una màquina remota**
- ♦ **/dev/console o /dev/xconsole**
 - ♦ S'utilitza com a fitxer de log d'errors crítics. Envia el missatge a totes les consoles virtuals

- ♦ **Exemple:**

```
kern.*           /var/log/kernel
kern.crit        @IP_MAUQUINA_REMOTA
kern.crit        /dev/console
```

- ♦ Envia tots els missatges de log del nucli a /var/log/kernel.
- ♦ A més els missatges crítics del nucli s'envien a una màquina_remota
- ♦ Finalment els missatges crítics es mostren per les consoles

♦ Ubuntu 9.10

```
$ cat /etc/rsyslog.conf | grep -v '^#\|^$\|^;'  
$ModLoad imuxsock # provides support for local  
system logging  
$ModLoad imklog    # provides kernel logging  
support (previously done by rklogd)  
$KLogPath /var/run/rsyslog/kmsg  
$ActionFileDefaultTemplate  
RSYSLOG_TraditionalFileFormat  
$RepeatedMsgReduction on  
$FileOwner syslog  
$FileGroup adm  
$FileCreateMode 0640  
$DirCreateMode 0755  
$Umask 0022  
$PrivDropToUser syslog  
$PrivDropToGroup syslog  
$IncludeConfig /etc/rsyslog.d/*.conf
```

♦ **/etc/rsyslog.d/*.conf**

```
$ ls -l /etc/rsyslog.d
total 24
-rw-r--r--  1 root root 1605 2009-10-15 06:27 50-default.conf
-rw-r--r--  1 root root 242 2009-09-22 15:52 postfix.conf
```

- ♦ Les aplicacions (a l'exemple postfix) poden indicar la seva pròpia configuració dels logs

♦ **Documentació. Paquet rsyslog-doc**

A `usr/share/doc/rsyslog-doc` Hi ha documentació en format web:

```
$ firefox /usr/share/doc/rsyslog-doc/html/index.html
```

I un fitxer amb exemples a:

```
/usr/share/doc/rsyslog-doc/examples/sample.conf
```

rsyslog

```
$ cat /etc/rsyslog.d/50-default.conf | grep -v '^#\|^$\|^;'
auth,authpriv.*                /var/log/auth.log
*.*;auth,authpriv.none         -/var/log/syslog
daemon.*                       -/var/log/daemon.log
kern.*                         -/var/log/kern.log
lpr.*                          -/var/log/lpr.log
mail.*                         -/var/log/mail.log
user.*                         -/var/log/user.log
mail.info                     -/var/log/mail.info
mail.warn                     -/var/log/mail.warn
mail.err                      /var/log/mail.err
news.crit                     /var/log/news/news.crit
news.err                      /var/log/news/news.err
news.notice                   -/var/log/news/news.notice
*.=debug;\
                                auth,authpriv.none;\
                                news.none;mail.none         -/var/log/debug
*.=info;*.=notice;*.=warn;\
                                auth,authpriv.none;\
                                cron,daemon.none;\
                                mail,news.none              -/var/log/messages
*.=emerg                      *
daemon.*;mail.*;\
                                news.err;\
                                *.=debug;*.=info;\
                                *.=notice;*.=warn           | /dev/xconsole
```

logger

- ♦ **La majoria de missatges de log són generats de forma automàtica per servies i dimonis del sistema**

- ♦ Tots els llenguatges de programació tenen llibreries que faciliten les tasques de logging).
- ♦ Amb l'eina logger podeu enviar un missatge de forma manual. La sintaxi és:

```
logger [-isd] [-f file] [-p pri] [-t tag] [-u socket] [message ...]
```

- ♦ Exemple:

```
$ sudo logger -i -s -p user.notice -t TAG Aturant el sistema
```


logger

◆ On:

- ◆ **-i**: Mostra el PID al fitxer de log.
- ◆ **-s**: Permet que els missatges es mostrin al fitxer de log i també a les sortides estàndard.
- ◆ **-d**: El missatge s'envia per datagrames i no pas per una connexió
- ◆ **f (file)**: Permet enviar tot un fitxer al log.
- ◆ **-p (priority)**: Permet indicar la prioritat del missatge, cal indicar-la com un selector (facility.priority). La prioritat **per defecte és user.notice**.
- ◆ **-t (tag)**: permet indicar una etiqueta extra
- ◆ **-u**: Es pot utilitzar un socket per enviar les dades al fitxer de log.
- ◆ **message**: El missatge a mostrar.

logrotate

- ♦ **Eina que s'encarrega de rotar (de rotació) fitxers**
 - ♦ Capacitat de poder "rotar" les bitàcoles de forma que no consumeixin recursos del sistema en excés.
 - ♦ **Rotar:** un cop un fitxer de log té una mida màxima (en número de línies o en bytes del fitxers) o cada x temps, aquest fitxer s'elimina i es torna a començar o es fa una còpia del fitxer (normalment s'afegeix una extensió numèrica). Sovint també es comprimeixen els fitxers de log que encara es volen mantenir i es realitzen operacions de neteja eliminant els fitxers de log més antics.

logrotate

♦ Exemple de rotació:

```
$ ls -lah /var/log/syslog*  
-rw-r----- 1 syslog adm 31K 2010-04-24 14:00 /var/log/syslog  
-rw-r----- 1 syslog adm 259K 2010-04-24 09:09 /var/log/syslog.1  
-rw-r----- 1 syslog adm 23K 2010-04-23 07:38 /var/log/syslog.2.gz  
-rw-r----- 1 syslog adm 21K 2010-04-21 05:33 /var/log/syslog.3.gz  
-rw-r----- 1 syslog adm 23K 2010-04-20 11:29 /var/log/syslog.4.gz  
-rw-r----- 1 syslog adm 5,6K 2010-04-19 07:57 /var/log/syslog.5.gz  
-rw-r----- 1 syslog adm 25K 2010-04-18 06:55 /var/log/syslog.6.gz
```

- ♦ Es mantenen 7 fitxers de log
- ♦ 5 comprimits amb gzip
- ♦ Tasques realitzades:
 - Crear un nou fitxer
 - Desplaçar tots els anteriors
 - Esborrar els més àntic dels antics fitxers de log
 - Comprimir els fitxers més antics.

logrotate

♦ Fitxers instal·lats:

```
$ dpkg -L logrotate
...
/usr/sbin/logrotate
...
/usr/share/man/man8/logrotate.8.gz
...
/usr/share/doc
...
/var/lib/logrotate
/etc
/etc/logrotate.d
/etc/logrotate.conf
/etc/cron.daily
/etc/cron.daily/logrotate
```

♦ Tasca cron diària:

```
$ cat /etc/crontab
# m h dom mon dow user  command
...
25 6   * * *   root    test -x /usr/sbin/anacron || ( cd / &&
run-parts --report /etc/cron.daily )
```

♦ Configuració

```
$ cat /etc/logrotate.conf
weekly
rotate 4
create

#compress

/var/log/wtmp {
    missingok
    monthly
    create 0664 root utmp
    rotate 1
}
...
```

logrotate

- Cada aplicació pot tenir la seva pròpia configuració:

```
$ ls /etc/logrotate.d/  
apache2          consolekit  
appport          cups  
apt              dpkg  
aptitude         jockey  
checkbox           kdm  
clamav-freshclam
```

rotate: és el nombre de fitxers a mantenir

compress: Es comprimeixen els fitxers antics (per defecte a partir del .2)

missingok: Si falta el primer fitxer s'utilitza el segon.

```
$ cat /etc/logrotate.d/rsyslog  
/var/log/syslog  
{  
    rotate 7  
    daily  
    missingok  
    notifempty  
    delaycompress  
    compress  
    postrotate  
    reload rsyslog >/dev/null 2>&1 || true  
    endscript  
}  
/var/log/mail.info  
/var/log/mail.warn  
/var/log/user.log  
/var/log/lpr.log  
/var/log/cron.log  
/var/log/debug  
/var/log/messages  
{  
    rotate 4  
    weekly  
    missingok  
    notifempty  
    compress  
    delaycompress  
    sharedscripts  
    postrotate  
    reload rsyslog >/dev/null 2>&1 || true  
    endscript  
}
```

Syslog remot

*.info @syslog.iesebre.com

♦ Client syslog:

*.info @192.168.0.9

```
$ cat /etc/services | grep  
syslog  
syslog 514/udp
```

♦ Servidor de syslog

- ♦ Pot funcionar amb TCP o **UDP**. Port 514
- ♦ Descomenteu a **/etc/rsyslog.conf**:

```
# provides UDP syslog reception  
$ModLoad imudp  
$UDPServerRun 514
```

- **\$ sudo /etc/init.d/rsyslog reload**
- **Upstart:** \$ sudo reload rsyslog



Reconeixement 3.0 Unported

Sou lliure de:



copiar, distribuir i comunicar públicament l'obra



fer-ne obres derivades

Amb les condicions següents:



Reconeixement. Heu de reconèixer els crèdits de l'obra de la manera especificada per l'autor o el llicenciador (però no d'una manera que suggereixi que us donen suport o rebeu suport per l'ús que feu l'obra).

- Quan reutilitzeu o distribuïu l'obra, heu de deixar ben clar els termes de la llicència de l'obra.
- Alguna d'aquestes condicions pot no aplicar-se si obteniu el permís del titular dels drets d'autor.
- No hi ha res en aquesta llicència que menyscabi o restringeixi els drets morals de l'autor.

Advertiment

Els drets derivats d'usos legítims o altres limitacions reconegudes per llei no queden afectats per l'anterior
Això és un resum fàcilment llegible del text legal (la llicència completa).

<http://creativecommons.org/licenses/by/3.0/deed.ca>