LINUX SERVER ADMINISTRATION

DOCUMENTATIE CURS

Sarcini administrative

Dintre sarcinile oricarui admin referitoare la loguri cele mai importante sunt:

1. Rotirea acestora

Pe langa beneficiile pe care le aduce logarea informatiilor importante din sistem, exista si dezavantaje majore ce trebuie evitate pe cat posibil de catre admin.

Dimensiunea fisierelor log creste in timp astfel incat acestea pot ocupa intreg spatiul de pe hard disk. Pe un server in productie pe care exista cateva sute de conturi doar fisierul log al serverului de email poate creste cu peste 100MB pe zi.
In plus scrierea in fisierele log de catre syslog are efecte negative in ceea ce priveste performantele generale ale intregului sistem. Un server in productie trimite informatii la cateva secunde sau chiar de mai multe ori pe secunda catre syslogd. Acesta trebuie sa deschida fisierul, sa scrie in el si sa-l inchida. Daca fisierul este de dimensiune foarte mare (sute MB) operatia poate scadea performatele sistemului astfel incat acesta sa nu mai fie utilizabil.

Administratorul trebuie sa roteasca logurile constant (zilnic, saptamanal sau lunar in functie de cantitatea de informatie salvata in acestea).

Rotirea logurilor presupune crearea unui fisier nou si pastrarea de versiuni a fisierelor log mai vechi.

Exemplu: rotirea fisierului /var/log/messages inseamna redenumirea acestuia in /var/log/messages.1 si crearea unui fiser nou numit /var/log/messages. Pastrarea a 10 versiuni presupune existenta fisierelor /var/log/messages.1 pana la /var/log/meesages.10. Programul care realizeaza automat rotirea logurilor este logrotate cu fisierul de configurare /etc/logrotate.conf

Adminul trebuie sa ruleze in fiecare seara comanda logrotate /etc/logrotate.conf folosind cron.

Exemplu logrotate.conf:

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

# keep 4 weeks worth of backlogs
rotate 4

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

# use date as a suffix of the rotated file
dateext

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

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

Detalii:

- logrotate.conf este format dintr-o sectiune globala de optiuni care se refera la optiunile nespecificate in mod express pentru fisierele log in sectiunea fiecaruia
  Exemplu:
  ```
  # rotate log files weekly
  weekly

  # keep 4 weeks worth of backlogs. Numarul de versiuni pastrate
  rotate 4
  ```
- pe langa optiunile globale pentru fiecare fisier log exista o sectiune care specifica optiunele de rotire pentru respectivul fisier. Aceasta sectiune se poate gasi in /etc/logrotate.conf sau intr-un fisier separat in directorul /etc/logrotate.d. Toate fisierele din directorul /etc/logrotate.d sunt incluse in logrotate.conf

Exemplu:

```
/var/log/httpd/access.log {
        rotate 5
        mail www@my.org
        size=100k
              create 0660 wwwuser wwwuser
        postrotate
           /sbin/killall -HUP httpd
        endscript
    }
```

Detalii:

- rotate 5 - se pastreaza 5 versiuni ale lui access.log si anume access.log.1 pana la access.log.5;
- mail www@my.org - inainte de rotire sunt trimise pe email la adresa specificata;
- size=100k - fisierul este rotit in momentul in care dimensiunea sa depaseste 100k;
- create 0660 wwwuser wwwgroup - imediat dupa rotire se creaza un nou fisier cu acelasi nume cu permisiunile 0660 si avand owner si group owner pe wwwuser respectiv wwwgroup;
- postrotate - scripturile care apar intre postrotate si endscript se executa automat dupa rotirea logurilor. In general acestea sunt scripturi care restarteaza serverul respectiv pentru a loga in noul fisier creat;

In linux un fisier se identifica dupa numarul de inode. Dupa rotire, noul fisier creat care reprezinta o versiune a vechiului fisier are acelasi inode number, iar serverul va continua sa salveze informatii in el (Exemplu: access.log.1)

Alte optiuni ce pot aparea in logrotate.conf

- daily, weekly sau monthly - fisierul este rotit zilnic, saptamanal sau lunar indiferent de dimensiune;
- missingok - daca fisierul nu exista nu se raporteaza eroare;
- ifempty/notifempty - roteste/nu roteste fisierul daca acesta este gol;
- compress/nocompress - comprima/nu comprima fisierul de tip log;

2. Verificarea constanta a logurilor

Fiindca forma in care multe servere logheaza informatia nu este "prietenoasa" si pentru ca volumul de informatie este extrem de mare, verificare manuala a logurilor are loc doar in momentul in care a avut loc un eveniment deosebit sau cand informatia cautata este de detaliu.

In general se folosesc programe numite "System log analyzers and reporters" care genereaza un rezumat al logurilor si pe care-l formateaza intr-un mod usor de urmarit.

Logwatch este unul dintre cele mai folosite programe pentru generarea de rezumate a logurilor.

Printre optiunile sale se afla:

- trimiterea automata a rezumatului pe e-mail;
- generarea de fisere raport comprimate sau nu;
- flexibilitate maxima in ceea ce priveste informatiile din raport;

Nota

Logwatch este un script scris in Perl care parseaza fisierele din /var/log.

Commanda logwatch foloseste fisierul de configurare /usr/share/logwatch/default.conf/logwatch.conf.
Optiunile din fisier pot fi suprascrise ruland logwatch cu diferite optiuni.

Printre cele mai importante optiuni sunt:

- --detail -> indica gradul de detalii din raport
- --logfile file -> proceseaza doar fisierul indicat (Exemplu: /var/log/messages)
- --service name -> numele serviciului ale carui loguri creaza raportul (Exemplu: sshd, httpd, all)
- --output -> output este directionat la consola(stdout), mail sau fisier
- --mailto address -> trimite raportul automat pe e-mail la adresa specificata
- --range <yesterday|today|all> -> perioada care contine logurile ce creaza raportul
- --logdir dir -> cauta in directorul specificat si subdirectoarele sale, fisierele log pentru generarea raportului. Default este

/var/log

Resurse

- Logrotate man page
- CLI Magic: Logrotate
- Logwatch man page

Logwatch

Durata: 3.25 min
Marime: 2.43MB