Lucrarea de laborator nr. 9

Monitorizarea sistemului

Curs: Utilizarea Sistemelor de Operare

Autor: Gabriel Noaje

syslogd - log system messages

Notiuni introductive

- stocheaza mesajele sistemului intr-un set de fisier specificate in fisierul de config (/etc/syslog.conf) [**NU** genereaza mesajele !]
- locatia fisierelor de log (/var/log/)
- tipuri de fisiere de log
- fiecare mesaj reprezinta o linie
- fiecare mesaj poate contine un cod de prioritate la inceputul liniei
- structura fisierului */etc/ syslog.conf* si conceptele de Facility, Level, Selector, Action
- log rotate

Task-uri

- fisiere de log

Fisier log	Descriere
daemon.log	Contine mesaje ce indica care servicii au fost pornite sau oprite cu succes si care nu
dmesg	Mesaje afisate de kernel in timpul secventei de boot
httpd/access_log	Informatii despre cererile primite de serverul Apache
httpd/error_log	Erori intalnite in procesarea cererilor clientilor de catre serverul Apache
syslog	Fisier general in care e inregistrata activitatea sistemului

- Exemplu de fisier log

```
Feb 25 11:04:32 toys network: Bringing up loopback interface:
succeeded
Feb 25 11:04:35 toys network: Bringing up interface eth0: succeeded
Feb 25 13:01:14 toys vsftpd(pam_unix)[10565]: authentication
failure;logname= uid=0 euid=0 tty= ruser= rhost=10.0.0.5 user=chris
Feb 25 14:44:24 toys su(pam_unix)[11439]: session opened for user
root by chris(uid=500)
```

Fiecare linie reprezinta un mesaj care are in principal 5 parti:

```
Date time hostname process[pid]:action:version
```

1. Data si ora la care a fost inregistrat mesajul
2. Numele statie de unde a venit mesajul
3. Programul sau serviciul cauruia ii apartine mesajul
4. PID programului care a trimis mesajul (intre paranteze patrate)
5. textul propriu-zis al mesajului

- Fisierul /etc/syslog.conf

Exista 4 termeni legati de loguri

- Facility - identificatorul folosit pt a descrie aplicatia sau procesul care e emis mesajul (mail, kernel, ftp)
- Level - indicator pt importanta mesajului (debugging → critical)
- Selector - combinatie de facility si level. Ajuta la sortarea mesajelor
- Actiunea - ceea ce se intampla cu mesajul primit ce s-a potrivit cu un anumit selector

```
netinfo.err     /var/log/netinfo.log
install.*       /var/log/install.log
install.*       @192.168.1.50:32376
```

Prima coloana reprezinta selectorul in formatul *facility.level*. A 2-a coloana reprezinta actiunea asociata selectorului. Un selector poate aparea de mai multe ori dar sa fie asociat unor actiuni diferite (un mesaj poate fi scris intr-un fisier sau trimis catre o alta statie in retea - vezi ultimele 2 linii din exemplu)

Facility	Descriere
auth	Activitati legate de autentificare - introducerea userului si a parolei (getty, su, login)
authpriv	Identic cu auth, dar logarea se face intr-un fisier acesibil doar unui grup restrans de utilizatori
console	Utilizat pentru capturarea mesajelor care sunt redirectate in general catre consola
cron	Mesaje provenite de la planificatorul de sistem cron
daemon	Mesaje provenite de la toti daemonii de pe sistem
ftp	Mesaje provenite de la daemonul de ftp
kern	Mesaje provenite de la kernel
lpr	Mesaje provenite de la sistemul de printare
mail	Mesaje referitoare la sistemul de e-mail
mark	Pseudo evenimente utilizate pentru generarea de marci temporale in fisierele de log
news	Mesaje provenite de la provenite de la protocolul de stiri (network news protocol - nntp)
ntp	Mesaje provenite de la protocolul de timp al retelei (network time protocol)
local0–local7	Facilitati locale definite de utilizator

Level	Descriere
emerg	Sistemul este inutilizabil. Mesajele sunt trimise catre toti userii logati pe toate terminalele
alert	Necesita o interventie imediata
crit	Conditii critice

err	Conditii de eroare
warning	Conditii de avertizare
notice	Conditii normale, dar semnificative
info	Mesaje informative
debug	Mesaje de nivel debugging. In mod normal trebuie dezactivate, datorita informatiilor detaliate pe care le genereaza si care pot duce la umplerea rapida a spatiului pe disc
none	Pseudo nivel utilizat pentru a specifica faptul ca nu se doreste inregistrarea de mesaje

- Log rotate

Consta in mentinerea unor fisiere log de dimensiuni rezonabile si informatia recenta sa fie cat mai accesibila. Astfel se poate ca dupa un anumit timp fisierul actual de log sa fie salvat sub un alt nume si sa fie inceput un nou fisier de log.

netstat - display active network connections

Notiuni introductive

- afiseaza urmatoarele informatii:
  - Network connections
  - Routing tables
  - Interface statistics
  - Masquerade connections
  - Multicast memberships
- afiseaza o lista a conexiunilor deschise identificate fie prin nr portului fie prin serviciul asociat acelui port conform listei din /etc/services
- importanta cunoasterii informatiilor despre porturile deschise si urmarirea serviciilor care au deschis conexiuni pe un anumit port (securizarea statiei)
- exista si pe Windows
- nu poate fi folosit pentru detectarea unui sistem compromis.

Task-uri

- sintaxa comenzii

- Afisarea de tabelei de routare

```
# netstat –nr
Kernel IP routing table
Destination Gateway Genmask Flags MSS Window irtt Iface
127.0.0.1 * 255.255.255.255 UH 0 0 0 lo
172.16.1.0 * 255.255.255.0 U 0 0 0 eth0
172.16.2.0 172.16.1.1 255.255.255.0 UG 0 0 0 eth0
```

Parametrul **-r** afiseaza tabela de routare Parametrul **-n** afiseaza IP in forma cu punct in loc de host name

Coloana 1: destinatia

Coloana 2: gateway; daca nu se foloseste nici un gateway se pune *

Coloana 3: netmask

Coloana 4: flag care descrie ruta

- G - ruta foloseste un gateway
- U - interfata care trebuie folosita este activa
- H - un singur host poate fi accesat folosind ruta respectiva (de ex. 127.0.0.1 in exemplul dat)
- D - ruta este creata dinamic de catre un daemon
- M - ruta este activata daca tabelul a fost modificat de un mesaj de redirectare ICMP
- ! - ruta de respingere

Coloana 5: MMS (Maximum Segment Size) dimensiunea celei mai mari datagrame (pachet folosit in conexiunile UDP) pe care kernelul o va forma pentru transmisia pe ruta respectiva

Coloana 6: Window cantitatea maxima de date pe care sistemul o va accepta intr-un pachet

Coloana 7: irtt (inital round-trip time) timpul pe care trebuie sa-l astepte host-ul pana cand sa retransmita datagrama catre server

Coloana 8: interfata pe care o utilizeaza ruta

- Afisarea statisticilor pentru o interfata

```
# netstat –i
Kernel Interface table
Iface MTU Met RX-OK RX-ERR RX-DRP RX-OVR TX-OK TX-ERR TX-DRP TX-OVR
Flags
lo 0 0 3185 0 0 0 3185 0 0 0 BLRU
eth0 1500 0 972633 17 20 120 628711 217 0 0 BRU
```

Primele 2 coloane reprezinta MTU (Maximum Transfer Unit) [Dimensiunea maxima a unei datagrame] si Met (Metric values) pentru interfata

Coloanele RX si TX arata cate pachete au fost receptionate/transmise fara erori (RX-OK/TX-OK) sau cu erori (RX-ERR/TX-ERR); la cate pachete s-a facut drop (RX-DRP/TX-DRP); cate pachete sau pierdut datorita overrun (RX-OVR/TX-OVR)

Ultima coloana afiseaza flagurile care au fost setate pentru interfata

- B - a fost configurata o adresa de broadcast
- L - interfata loopback
- M - toate pachetele sunt primite
- 0 - ARP este dezactivat pt interfata

- P - conexiunea peer-to-peer
- R - interfata ruland
- U - interfata activa

- Afisarea conexiunilor

Comanda netstat are posibilitatea afisarii socket-urilor active si pasive. Optiunile **-t**, **-u**, **-w** si **-x** afiseaza conexiunile TCP, UDP, RAW si Unix socket Optiunea **-a** afiseaza atat conexiunile ESTABLISHED cat si cele LISTENING

Optiunea **-l** afiseaza doar conexiunile LISTENING.

Default sunt afisate doar cele ESTABLISHED.

top - display top CPU processes

Notiuni introductive

- ofera informatii in timp real despre procesele care ruleaza
- ofera o lista a proceselor si a gradului de utilizare a resursele sistemului
- ofera posibilitati (destul de reduse) de manipulare proceselor

Task-uri

- sintaxa comenzii
- tipurile de informatii oferite (semnificatia fiecarei coloane)
- comenzi (o singura tasta) suportate in timpul rularii utilitarului
- monitorizarea incarcarii sistemului: cpu, memory

Descrierea programului:

- Ecranul programului este impartit in 4 zone:
    1. Summary Area
    2. Message/Prompt Line
    3. Columns Header
    4. Task Area
- Descrierea zonelor si elementele fiecarei zone
    1. Summary Area
        - **uptime** aceasta linie este identica cu cea afisata de comanda **uptime** si poate fi afisata sau nu prin apasarea tastei **l**
            - ora curenta
            - timpul cat calculatorul a fost pornit
            - mediile in ultimele 1,5,15 minute de incarcare a sistemului Detalii despre "load averages" (http://www.teamquest.com/resources/gunther/ldavg1.shtml)
        - **processes** afiseaza numarul total de procese care ruleaza la momentul respectiv si poate fi afisat sau nu prin apasarea tastei **t**

        - numar total de procese
        - numar de procese active
        - numar de procese inactive
        - numar de procese oprite
        - numar de procese zombi (*proces zombie* = proces care si-a terminat executia, dar se afla inca in tabelul de procese, permitand procesului care l-a pornit sa citeasca statusul terminarii lui)
        - Tutorial despre Ciclul de viata al unui proces (http://www.linux-tutorial.info/modules.php?name=Tutorial&pageid=84)
    - **CPU** afiseaza informatii despre incarcarea procesorului
        - user mode
        - system mode
        - niced tasks
        - idle
    - **memory** afiseaza statistici referitaore la utilizarea memoriei si poate fi afisat sau nu prin apasarea tastei **m**
        - memorie totala disponibila
        - memorie libera
        - memorie utilizata
        - memorie partajata
        - memorie utilizata pentru buffer-e
2. Message/Prompt Line
    - pot fi introduse comenzi interactive
3. Columns Header
    - a: PID Process ID
    - b: PPID - Parent Process PID ~ process ID-ul parintelui unui task
    - c: RUSER - Real User Name ~ numele real al owner-ului taskului
    - d: UID - User Id ~ user ID owner-ului taskului
    - e: USER - User Name ~ numele efectiv al ownerului taskului
    - f: GROUP - Group Name ~ numele efectiv al grupului din care face parte ownerul taskului
    - g: TTY - Controlling Tty ~ deviceul de un a fost pornit taskul (port, consola) [nu trebuie ca orice task sa aiba asociat un device, caz in care va fi afisat “?”]
    - k: %CPU - CPU usage ~ procentul din timpul total al procesorului alocat taskului (de la ultimul refreh al ecranului)
    - l: TIME - CPU Time ~ timpul total al procesorului folosit de catre task de la inceperea sa
    - m: TIME+ - CPU Time, hundredths ~ idem TIME cu deosebirea ca arata si sutimile de secunda
    - n: %MEM - Memory usage (RES) ~ partea din memorie fizica disponibila utilizata de task
    - o: VIRT – Virtual Image (kb) ~ totalul de memorie virtuala utilizat de task (include codul, datele si librariile partajate) [SWAP+RES]

        - p: SWAP – Swapped size (kb) ~ portiunea din totalul memoriei virtuale utilizate de task
        - q: RES – Resident size (kb) ~ memoria fizica non-swap utilizata de task
        - w: S – Process Status ~ Statusul poate fi:
            - 'D' = uninterruptible sleep
            - 'R' = running
            - 'S' = sleeping
            - 'T' = traced or stopped
            - 'Z' = zombie
        - x: Command – Command line or Program name ~ afiseaza linia de comanda utilizata pt pornirea taskului sau numele asociat programului (se utlizeaza tasta **c** pentru a comuta intre cele 2 moduri) [pentru procesele care nu au o linie de comanda cum ar fi threadurile kernelului numele programului este afisar intre paranteze rotunde]
- **Comenzi intereactive:**

1. Selectarea si ordonarea coloanelor

Se utilizeaza tastele **f** [Field select] sau **o** [Order fields]. Este afisat un ecran cu stringul campurilot actuale, urmat de o descriere a fiecarui camp. Un exemplu de string:

```
ANOPQRSTUVXbcdefgjlmyzWHIK
```

Campurile sunt afisate exact in ordinea specificata de string. Descrierea campurilor:

```
    k: %CPU = CPU usage
    l: TIME = CPU Time
    m: TIME+= CPU Time, hundredths
* N: %MEM = Memory usage (RES)
* O: VIRT = Virtual Image (kb)
```

Fiecare camp are asociata o litera. Daca litera este mare inseamna ca acel camp este vizibil (acest lucru este marcat si prin asteriscul din fata literei).

Selectarea unui camp se face apasand tasta **f** apoi litera corecpunzatoare din lista afisata.

Ordonarea se face apasand tasta **o** apoi litera mare corespunzatoare pentru a muta campul la stanga sau litera mica corespunzatoare pentru a muta campul la dreapta.

Se pot folosi si urmatoarele comenzi rapide pentru sortare:

- N sorteaza taskurile dupa pid (numeric)
- A sorteaza taskurile dupa varsta (cele mai noi la inceput)
- P sorteaza taskurile dupa utilizarea CPU (default)
- M sorteaza taskurile dupa utilizarea memoriei rezidente
- T sorteaza taskurile dupa timp

1. Ordonarea crescatoare sau descrescatoare intr-o coloana se realizeaza utilizand tasta **R**
2. Coloana dupa care se face sortarea se alege utilizand tastele < si >
3. Afisarea taskurilor pentru un anumit utilizator se face realizeaza utilizand tasta **u**
4. Oprirea unui proces se poate face utilizand tasta **k** si specificand apoi PID-ul procesului
5. Activarea schemei de culori se realizeaza utilizand tastele **z** (automat) sau **Z** (interactiv)
6. Crearea fisierului de configurare se raelizeaza utilizand tasta **w** (/etc/toprc sau ~/.toprc)
7. Afisarea help-ului se realizeaza utilizand tastele **?** sau **h**
8. Iesirea din program se realizeaza utilizand tastele **q**