Curs 2
Server basics

Gestiunea serviciilor de rețea (GSR)
13 octombrie 2016

Departamentul de Calculatoare, Comunitatea RLUG

Cuprins

Procese standard

- Un proces standard este un program interactiv cu utilizatorul
- Este de obicei rulat de utilizator din shell, are acces la stdin/stdout/stderr
- Poate fi oprit cu o comandă internă specifică (exit/quit) sau de către utilizator folosind Ctrl-C

Daemon

- Un sistem modern trebuie să poată realiza mai multe `task`-uri neinteractive în același timp
- Aceste `task`-uri sunt realizate prin daemons
- Un daemon este un proces care rulează în background (decuplat de la terminal, având uzual stdin și stdout legate la `/dev/null`) al cărui părinte este în mod uzual init
- Daemonii sunt porniți de către sistemul de operare prin intermediul script-urilor de start-up (SysV/systemd/upstart)

Interacțiunea cu un daemon

- Fișiere de configurare
- UNIX sockets / TCP sockets
- `script` de start-up (... stop/start/restart/reload/status)

Cuprins

Ce este un server?

În mod uzual termenul de server paote face referință la oricare din următoarele concepte:

- Un computer fizic, care rulează un sistem de operare adecvat pentru servere
- Un daemon care servește răspunsuri la cererile venite (de obicei) peste rețea

Servicii

- Un serviciu, în terminologie *NIX, reprezintă un daemon care implementează o anume funcționalitate (HTTP/SMTP/DNS/...)
- Un serviciu are ca și componente auxiliare:
  - Un utilizator/grup dedicat
  - Un port TCP/UDP dedicat
- `do one thing well`

Utilizatori dedicați pentru servicii

- Un utilizator poate avea acces numai la fișierele `deținute` de el sau de grupul/grupurile din care face parte
- Serviciile au fiecare unul sau mai mulți utilizatori dedicați.
- Motivele pentru care se face acest lucru sunt:
  - separare de privilegii
  - asignarea de resurse separate
  - prevenirea atacurilor informatice

Demo

Cuprins

Depanarea serviciilor - fișiere configurare și jurnalizare

- Fiecare serviciu are un fișier de configurare și un fișier de jurnalizare
- Pentru configurare
  - `httpd.conf`
  - `rsyslog.conf`
  - `sshd_config`
- Pentru jurnalizare
  - `/var/log/apache/error_log`
  - `/var/log/{messages,syslog}`
  - `/var/log/{messages,secure}`

Depanarea serviciilor - unelte

- În cazul serviciilor de rețea: ascultă pe portul care trebuie?
  - `netstat -antplu`
- Ce fișiere deschise are un serviciu?
  - `lsof -p $PID | less`
- Ce încearcă să facă un daemon?
  - `strace`

Demo

Cuprins

Rularea periodică de comenzi/programe

- `crond` se ocupă de programarea rulării la anumite intervale a unor comenzi sau programe
- Programarea se poate face din minut în minut, la o anumită oră, o dată pe zi/săptămână/lună sau orice alt tip de interval
- Programarea se poate face per user
- Editarea configurației se face folosind comanda `crontab -e`

Formatul fișierului de configurare

/etc/crontab

```
# Minute Hour Day of Month Month Day of Week Command
# (0-59) (0-23) (1-31) (1-12 or Jan-Dec) (0-6 or Sun-Sat)
0 2 12 * * /usr/bin/echo "middle of the night"
```

Cuprins

Nevoia de jurnalizare

- Pentru daemoni/servicii
- Configurarea jurnalizării
- Jurnalizare directă sau printr-un serviciu de jurnalizare
- Serviciul de jurnalizare/logging pe Unix: `syslog`

Mesajele de jurnalizare

Formatul general al unui mesaj de jurnalizare:

- timestamp, metadate, mesajul efectiv

Exemplu /var/log/auth.log

```
Oct 12 21:14:44 dr0fw0 sshd[8835]: Accepted publickey
for eugen from 192.168.10.254 port 17855 ssh2: ED25519
2e:7e:72:c2:75:15:54:e8:10:60:e0:da:6a:c7:b7:4
```

Configurarea syslog

- `/etc/*syslog.conf`
- Fișierul de configurare al daemonului de syslog constă în definiții de tip Parametru-Valoare
  - `mail.*  -/var/log/maillog`
  - `-` înseamnă că mesajele primite cu `facility mail` pot fi `buffered`
  - în mod uzual, mesajele primite de daemonul de syslog sunt scrise imediat pe disc folosind O_FSYNC

Demo: Verificarea jurnalizării folosind comanda logger

Logger command

logger -p local0.notice -t console-log "look ma, i'm in syslog"

syslog output

/var/log/messages: Aug 12 09:56:44 ve1 console-log: look ma, i'm in syslog

Remote logging

- Serviciu central de jurnalizare și servicii `agent`
- UDP vs TCP
  - UDP: Fire and Forget. Mărimea maximă a unui mesaj de syslog este de 1460-1482 bytes
    - Workaround pentru a transmite un mesaj mai lung peste UDP este adăugarea unui index de secvență la începutul mesajului: [1], [2] etc.
  - TCP: Presupune o metodă sigură de a transmite un mesaj în cealaltă parte până la o lungime de aproximativ 1MB per mesaj

Cuprins

Despre NTP

- De ce e necesar
- Mecanism de funcționare
- Surse de timp
- Clock strata
- Utilitare de verificare a stării

Mecanism de funcționare

- Clientul interoghează unul sau mai multe servere de timp
- Calculează delay-ul (round trip time) între el și server(e)
- Ceasul sistemului este ajustat treptat până este sincronizat la câteva milisecunde față de serverele de timp

Stratum

- Serverele NTP sunt "organizate" ierarhic în funcție de acuratețea lor
  - Stratum 0: ceasul atomic (sursa exactă de timp)
  - Stratum 1: ceasurile sincronizate direct cu Stratum 0
  - Stratum 2: ceasurile sincronizate direct cu Stratum 1
  - ...
  - Stratum 16: ceasul nu este sincronizat

Configurarea NTP

/etc/ntp.conf

```
server 0.centos.pool.ntp.org
server ntp2.usv.ro
```

Unelte

- `ntpstat`
- `ntpq`
- `ntpdate`

Cuprins

Resurse utile

- https://en.wikipedia.org/wiki/Daemon_(computing)
- https://tools.ietf.org/html/rfc3164 și https://tools.ietf.org/html/rfc5424
- https://en.wikipedia.org/wiki/Cron
- https://en.wikipedia.org/wiki/Network_Time_Protocol
- https://en.wikipedia.org/wiki/Ntpdate și https://en.wikipedia.org/wiki/Ntpd
- http://www.ecoca.ro/ntponeusvro/