Skaner plików *syslog*

1. Wstęp.

Celem niniejszego projektu jest wykorzystanie generatora skanerów flex do stworzenia skanera plików *syslog.*

Do zbierania informacji o działaniu systemu i umieszczania ich w plikach służy demon systemowy *syslogd*. Plikiem konfiguracyjnym *syslogd* jest `etc/syslog.conf`

Plik ten opisuje reguły systemu logowania. W pojedynczej linii pliku podane jest najpierw skąd i o jakim priorytecie informacje mają być zapisywane, po czym podana jest pełna ścieżka do pliku, w którym te informacje mają zostać zgromadzone. Zamiast ścieżki do pliku może tu być ewentualnie podany adres innego komputera lub identyfikator użytkownika, który miałby te informacje otrzymywać.

Format pliku `/etc/syslog.conf` jest następujący:

`facility.priority action`

gdzie

- facility - określa z jakiej części systemu pochodzi informacja, możliwe są następujące wpisy: auth, authpriv, cron, daemon, kern, lpr, mail, mark, news, security (to samo co auth), syslog, user, uucp i
- local0 - local7. Gwiazdka (*) zastępuje wszystkie facility.
- priority - określa priorytety logowanych wiadomości - wszystkie wiadomości o tym lub wyższym priorytecie trafiają do logu. Możliwe wartości to: debug, info, notice, warning, warn (to samo co warning), err, error (to samo co err), crit, alert, emerg, panic (to samo co emerg). Znak równości (=) przed nazwą priorytetu wskazuje, że należy zbierać wiadomości tylko o takim priorytecie, wykrzyknik (!) zaś oznacza zignoruj wyższe lub równe danemu. Gwiazdka (*) zastępuje wszystkie priorytety. Przykładowo:

  ```
  auth.debug /var/adm/log/auth
  local0.debug /var/adm/log/tcpd
  *.err;kern.debug;daemon.notice;mail.crit /var/adm/messages
  ```

- action - określa gdzie trafiają zebrane komunikaty. Może to być nazwa pliku, łącza, terminala, maszyny zdalnej (poprzedzona znakiem @, wtedy wiadomości są przesyłane do demona na tej maszynie) lub użytkownika (wiadomości trafiają do tego użytkownika). Przykładowo:

  ```
  local7.debug /var/adm/log/router.daily
  *.alert root
  *.* @logserver
  ```

Zadanie

Przykładowo, skaner dla wejścia:

```
  *.=debug /var/log/debug
*.err /var/log/syslog

  ♯Uzytkownicy ktorzy powinni ujrzec wiadomosc ze sie zalogowales.
*.=alert root,your_username
*.=emerg root,your_username

  mail.info;mail.notice /var/log/maillog
kern.* /var/log/kern.log
daemon.info;daemon.notice /var/log/daemon.log
```

```
cron.* /var/log/cron.log
mail.* /var/log/mail.log
user.* /var/log/user.log
uucp.* /var/log/uucp.log
*.*;auth,authpriv.none /var/log/syslog

  ♯Umiesc pliki z logami w dwoch miejscach
authpriv.*;auth.* /admin/auth.log
authpriv.*;auth.* /var/log/secure

  ♯Wyswietlanie wszystkiego na konsoli
*.* /dev/tty12

  ♯Logowanie na zdalnym serwerze
*.* @logserver
```

ma wypisywać na wyjściu komunikat, że format pliku jest poprawny.

W przypadku pojawienia się linii o nieprawidłowym formacie powinnien być wypisany komunikat o błędzie, wraz z numerem linii, w której błąd wystąpił. Komunikat o błędzie powinien pojawić się dla każdej niepoprawnej linii.

Dodatkowo proszę przyjąć, że nazwy plików, katalogów, poleceń, terminali itp. składają się z następujących znaków [a-zA-Z0-9._-]. Dozwolone są powtórzenia w części facility (patrz opis pliku syslog.conf), czyli przykładowo auth,auth.*.

Dokumentację do *lex*'a/*flex*'a znajdziecie tutaj:
`http://www.kompilatory.agh.edu.pl/pages/tk-laboratorium/flex.html`