MyLast

Documentație

Gaitur Ruslan

December 14, 2025

Cuprins

1 Prezentare Generală **3**

2 Caracteristici Principale **3**

3 Instalare și Cerințe **3**

3.1 Dependințe 3

3.2 Permisiuni 3

4 Utilizare **4**

4.1 Sintaxă 4

4.2 Moduri de Apel `<mod>` 4

4.3 Opțiuni de Filtrare `[flag_filtrare]` 4

4.4 Parametri de Filtrare `[valoare_filtrare]` 4

5 Arhitectura de Baza **5**

5.1 Argumentul Fundamental al Tuturor Functiilor 5

5.2 `mylast` 5

5.3 `mylastb` 6

6 Arhitectura Filtrelor **6**

6.1 `-n, -s, -t, -p` 6

7 Arhitectura Ajutatoare **6**

7.1 `get_len` 6

7.2 `get_time` 6

7.3 `get_date` 6

7.4 `get_duration` 7

1 Prezentare Generală

MyLast este un script Bash conceput pentru a analiza jurnalele de autentificare ale sistemului situate în `/var/log/`. Acesta reproduce funcționalitatea comenzilor Linux standard `last` și `lastb`.

Scriptul ia date din fișierele `auth.log.x` (inclusiv cele comprimate cu gzip) pentru a reconstrui istoricul sesiunilor utilizatorilor fizici și a identifica încercările de autentificare eșuate.

2 Caracteristici Principale

- **Procesare Jurnale:** Citește și concatenează `auth.log`, `auth.log.1`, etc.
- **Reconstruirea Sesiunii:** Reconstruieste exact firul de autentificare, deconectare al userului si shutdown al sistemului.
- **Reconstruirea Esecurilor de Logare:** Determina sesiunile in care au avut loc esecuri de autentificare.
- **Filtrare:** Permite filtrarea rezultatelor după constrângeri de timp specifice (De la, Până la, Prezent), dar la fel și după numărul de afișări.

3 Instalare și Cerințe

3.1 Dependințe

Asigurați-vă că următoarele sunt instalate:

- `bash` (Mediul Shell)
- `less` (Citirea fișierelor text și, in special, gzip)
- `awk`, `cut`, `grep` (Procesare text)

3.2 Permisiuni

Deoarece scriptul citește din `/var/log/auth.log`, necesită de obicei privilegii **root**.

```
sudo ./mylast.sh [...]
```

4 Utilizare

Scriptul acceptă argumente în linia de comandă pentru a determina modul de operare și logica de filtrare.

4.1 Sintaxă

```
./mylast.sh <mod> [flag\_filtrare] [valoare\_filtrare]
```

4.2 Moduri de Apel `<mod>`

Determină modul de analiză:

Flag	Descriere
`-l`	**Ultimile Logări:** Analizează sesiunile reușite.
`-lb`	**Logări Eșuate:** Analizează încercările eșuate.

Tabel 1: Moduri Principale de Execuție

4.3 Opțiuni de Filtrare `[flag_filtrare]`

Acești parametri sunt valabili doar pentru modul `-l` de rulare al scriptului.

Flag	Format
`-n`	Afișează ultimele N intrări.
`-s`	Arată sesiunile **de la** data specificată.
`-t`	Arată sesiunile **până la** data specificată.
`-p`	Arată sesiunile **active** la timpul specificat.

Tabel 2: Optiuni de Filtrare

4.4 Parametri de Filtrare `[valoare_filtrare]`

Reprezinta valoarea ce tine de filtrare. Fiecare flag de filtru are un format unic pentru propria valoare.

Flag	Format
`-n`	**<INT>** Accepta un Integer.
`-s`	**<YYYY-MM-DD-HH:mm>** Accepta format tipic date-time.
`-t`	**<YYYY-MM-DD-HH:mm>** Accepta format tipic date-time.
`-p`	**<YYYY-MM-DD-HH:mm>** Accepta formate tipic date-time.

Tabel 3: Format Acceptat Pentru Parametrii Filtrarii

5 Arhitectura de Baza

5.1 Argumentul Fundamental al Tuturor Functiilor

Scriptul definește o variabilă `SYSLOG` (`/var/log`) ce stocheaza locatia syslog-urilor. In continuare, următoarele fișiere sunt concatenate într-un singur string, care este redirectat spre funcțiile de baza `mylast/mylastb`:

```
LOG1="$SYSLOG/auth.log"
LOG2="$SYSLOG/auth.log.1"
LOG3="$SYSLOG/auth.log.2.gz"
LOG4="$SYSLOG/auth.log.3.gz"
LOG5="$SYSLOG/auth.log.4.gz"
```

5.2 `mylast`

Funcția `mylast` implementează o mașină de stări pentru a urmări sesiunile utilizatorilor.

1. **Detectare Autentificare:** Scanează după “new session”.
2. **Deconectare/Eliminare:** Scanează după “removed session” sau “logged out”.
3. **Oprire Sistem:** Dacă este detectat “system is powering down”, toate sesiunile active sunt închise.

Aceasta masina de stari este construita pe baza a 2 variabile:

Queue coada - salveaza utilizatorii autentificati dar care inca nu au fost deconectati
Session sesiunea - salveaza utilizatorii conectati si deconectati ulterior.

Scriptul parcurge syslog-urile linie dupa linie. Daca observa un nou utilizator, atunci acesta este salvat in queue. Daca acest utilizator este deconectat, atunci acesta este scos din queue si este salvat in session.

5.3 `mylastb`

Funcția `mylastb` proceseaza sesiunile in care utilizatorul a gresit parola. Cauta trivial linia, folosind `grep`, dupa sirul de caractere: "password check failed".

6 Arhitectura Filtrelor

6.1 `-n, -s, -t, -p`

Aceste filtre au o structura triviala, folosind totalitatea sesiunilor deja procesate de functia `mylast`. Se impart sesiunile distincte folosind de delimitatorul spatiu `(" ")` si verifica daca data si timpul corespund cerintelor filtrului `(s, t, p)`, inclusiv si numarul de sesiuni ce necesita afisate `(n)`.

7 Arhitectura Ajutatoare

7.1 `get_len`

Foloseste comanda built-in "for" pentru a determina numarul de linii intr-un string delimitat prin spatii.
Foloseste la parcurgerea variabilelor **Queue** si **Session**.

7.2 `get_time`

Parseaza linia de syslog si returneaza timpul in care s-a inregistrat linia respectiva de jurnal.
Foloseste la obtinerea timpului de autentificare al utilizatorului.

7.3 `get_date`

Parseaza linia de syslog si returneaza data la care s-a inregistrat linia respectiva de jurnal.
Foloseste la obtinerea datii de autentificare a utlizatorului

7.4 `get_duration`

Calculează diferența dintre timpul de început (T_s) și timpul de sfârșit (T_e).
Foloseste la formatarea finala a datelor despre timp pentru o sesiune incheiata a unui utilizator