

MyLast

Documentație

Gaitur Ruslan

December 16, 2025

Cuprins

1	Prezentare Generală	3
2	Caracteristici Principale	3
3	Instalare și Cerințe	3
3.1	Dependințe	3
3.2	Permisii	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
4.5	Interfata Grafică	5
4.5.1	Arhitectura Interfetei	5
4.5.2	Diagrama de Afișare	5

4.6	Exemple	5
4.6.1	Utilizare de Baza (Modul -l, -lb)	5
4.6.2	Utilizare cu Filtre (Modul -l)	6
5	Arhitectura Functionalitatii	6
5.1	Arhitectura Functiilor de Baza	6
5.1.1	Argumentul Fundamental al Functiilor	6
5.1.2	mylast	7
5.1.3	mylastb	7
5.2	Arhitectura Functiilor de Filtrare	7
5.2.1	-n, -s, -t, -p	7
5.3	Arhitectura Functiilor Ajutatoare	7
5.3.1	get_len	7
5.3.2	get_time	8
5.3.3	get_date	8
5.3.4	get_duration	8

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 și shutdown al sistemului.
- **Reconstruirea Esecurilor de Logare:** Determina sesiunile în 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, în special, `gzip`)
- `awk`, `cut`, `grep` (Procesare text)

3.2 Permisii

Deoarece scriptul citește din `/var/log/auth.log`, necesită de obicei privilegiile **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: Opțiuni de Filtrare

4.4 Parametri de Filtrare [valoare_filtrare]

Reprezintă valoarea ce ține de filtrare. Fiecare flag de filtru are un format unic pentru propria valoare.

Flag	Format	Descriere
-n	INT	Numar intreg
-s	YYYY-MM-DD-HH:mm	Data si timp
-t	YYYY-MM-DD-HH:mm	Data si timp
-p	YYYY-MM-DD-HH:mm	Data si timp

Tabel 3: Format Acceptat Pentru Parametrii Filtrarii

4.5 Interfata Grafica

Deși **MyLast** este o aplicație bazată pe linia de comandă, interfața sa vizuală este definită de formatarea strictă a datelor returnate la *Standard Output*. Interacțiunea grafică are loc exclusiv în cadrul terminalului.

4.5.1 Arhitectura Interfetei

Scriptul utilizează un *layout tabular bazat pe text* pentru a reprezenta datele. Structura vizuală este proiectată pentru lizibilitate maximă, asemenea comenzilor `last`, `lastb`.

Fiecare linie afișată reprezintă o entitate distinctă și este împărțită în coloane vizuale delimitate prin spațiere dinamică:

4.5.2 Diagrama de Afișare

Fluxul vizual al datelor urmează o structura tabelara, pentru fiecare obiect de date:

```
|-----|
|Utilizator|Sesiune|  Data   |Ore de Inceput si Sfarsit|Durată|
|-----|-----|-----|-----|-----|
| student1 |  c2   |2025-12-01|      12:30-14:49      |(2:19)|
| student2 |  c3   |2025-12-01|      12:12-14:30      |(2:18)|
|-----|
```

4.6 Exemple

4.6.1 Utilizare de Baza (Modul -l , -lb)

Afișarea tuturor sesiunilor reușite (-l)

```
sudo ./mylast.sh -l
```

Afișarea încercărilor de autentificare eșuate (-lb)

```
sudo ./mylast.sh -lb
```

4.6.2 Utilizare cu Filtre (Modul -l)

Limitarea numărului de intrări (-n)

```
sudo ./mylast.sh -l -n 5
```

Filtrare după data de început (-s)

```
sudo ./mylast.sh -l -s 2023-12-01-12:00
```

Filtrare după data de sfârșit (-t)

```
sudo ./mylast.sh -l -t 2024-01-15-23:59
```

Verificarea prezenței la un moment dat (-p)

```
sudo ./mylast.sh -l -p 2023-12-25-14:30
```

5 Arhitectura Functionalitatii

5.1 Arhitectura Functiilor de Baza

5.1.1 Argumentul Fundamental al Functiilor

Scriptul definește o variabilă SYSLOG (/var/log) ce stocheaza locatia system log-urile. 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"
```

5.1.2 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 system log-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.

5.1.3 mylastb

Funcția mylastb procesează sesiunile în care utilizatorul a gresit parola. Functionalitatea de baza este asigurata de grep dupa sirul de caractere: "password check failed".

5.2 Arhitectura Functiilor de Filtrare

5.2.1 -n, -s, -t, -p

Folosind totalitatea sesiunilor deja procesate de functia mylast, verifica daca data si timpul corespund cerintelor filtrului (s, t, p), inclusiv si numarul de sesiuni ce necesita afisate (n).

5.3 Arhitectura Functiilor Ajutatoare

5.3.1 get_len

Determina numarul de linii intr-un string delimitat prin spatii. Foloseste la parcurgerea variabilelor **Queue** si **Session**.

5.3.2 `get_time`

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

5.3.3 `get_date`

Parseaza linia de system log si returneaza data la care s-a înregistrat linia respectiva de jurnal. Foloseste la obtinerea datii de autentificare a utlizatorului

5.3.4 `get_duration`

Calculează diferența dintre timpul de început (T_s) și timpul de sfârșit (T_e) al unei sesiuni. Folos-este la formatarea finala a datelor despre timp pentru o sesiune incheiata a unui utilizator.