/var/log/auth.log??????????????

??

????????????

`/var/auth.log` ??????????????????????????????????????

- ????

```
sudo awk '/Disconnected from invalid user/ {print $(NF-4)}' /var/log/auth.log | sort | uniq -c | sort -nr
```

- ????

```
43 root
36 ubuntu
24 user
20 test
13 admin
8 deploy
6 guest
6 ftpuser
5 oracle
5 hadoop
5 dev
5 debian
4 user1
4 sysadmin
4 samba
3 test1
3 mysql
3 max
3 kafka
```

??????????????????????????????

??????????????????????????

`/var/auth.log` ??????????????????????

- ????

```
sudo awk '/Accepted/ {split($1, date, "T"); split(date[2], time, "."); gsub("-", "/", date[1]); print date[1] " " substr(time[1], 1, 5) " " $7}' /var/log/auth.log | sort | uniq -c | sort -nr
```

??? `2024-11-25T16:21:14.772402+09:00` ???????? `2024/11/25 14:38` ?????????

- ????

```
1 2024/11/25 14:38 hoge
```

??????????????????

Revision #1
Created 25 November 2024 07:30:57 by manualmaton
Updated 25 November 2024 07:31:51 by manualmaton