lastb

列出登入系统失败的用户相关信息

补充说明

lastb命令 用于显示用户错误的登录列表，此指令可以发现系统的登录异常。单独执行lastb命令，它会读取位于/var/log目录下，名称为btmp的文件，并把该文件内容记录的登入失败的用户名单，全部显示出来。

语法

```
lastb(选项)(参数)
```

选项

```
-a□把从何处登入系统的主机名称或ip地址显示在最后一行；
-d□将IP地址转换成主机名称；
-f<记录文件>：指定记录文件；
-n<显示列数>或-<显示列数>：设置列出名单的显示列数；
-R□不显示登入系统的主机名称或IP地址；
-x□显示系统关机，重新开机，以及执行等级的改变等信息。
```

参数

- 用户名：显示中的用户的登录列表；
- 终端：显示从指定终端的登录列表。

实例

首次运行lastb命令会报下的错误：

```
lastb: /var/log/btmp: No such file or directory
Perhaps this file was removed by the operator to prevent logging lastb info.
```

只需建立这个不存在的文件即可。

```
touch /var/log/btmp
```

使用ssh的登录失败不会记录在btmp文件中。

```
lastb | head
root     ssh:notty    110.84.129.3     Tue Dec 17 06:19 - 06:19  (00:00)
root     ssh:notty    110.84.129.3     Tue Dec 17 04:05 - 04:05  (00:00)
root     ssh:notty    110.84.129.3     Tue Dec 17 01:52 - 01:52  (00:00)
root     ssh:notty    110.84.129.3     Mon Dec 16 23:38 - 23:38  (00:00)
leonob   ssh:notty    222.211.85.18    Mon Dec 16 22:18 - 22:18  (00:00)
leonob   ssh:notty    222.211.85.18    Mon Dec 16 22:18 - 22:18  (00:00)
root     ssh:notty    110.84.129.3     Mon Dec 16 21:25 - 21:25  (00:00)
root     ssh:notty    110.84.129.3     Mon Dec 16 19:12 - 19:12  (00:00)
root     ssh:notty    110.84.129.3     Mon Dec 16 17:00 - 17:00  (00:00)
```

```
admin    ssh:notty    129.171.193.99   Mon Dec 16 16:52 - 16:52  (00:00)
```