addcount

20

delcount

13

difhost-add

andrew

claire

hostname

wilsonwu

judy

kingsley

server

judy-VirtualBox
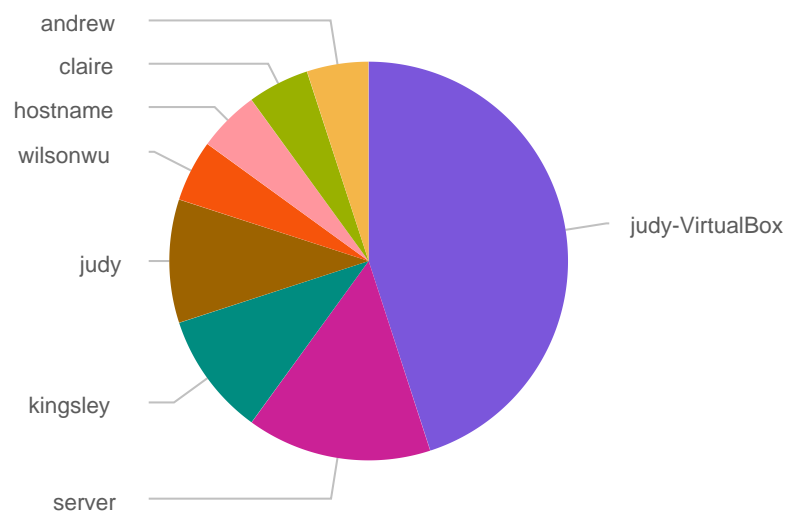
difhost-del
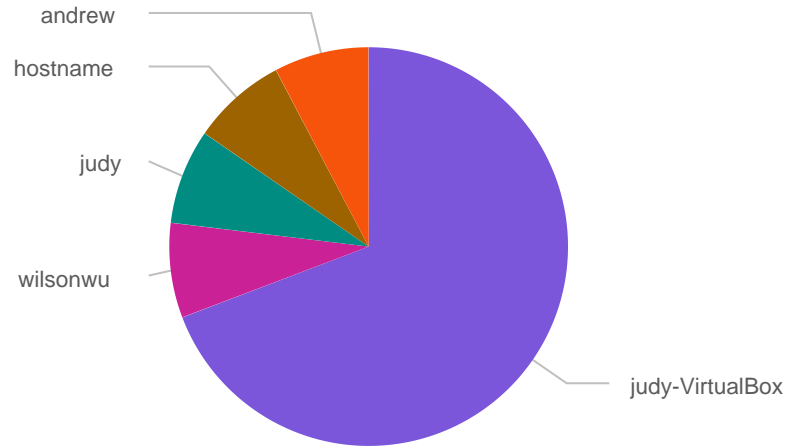
authlog

Time	Event
2025-03-04T15:55:01+0800	2025-03-04T15:55:01.812595+08:00 kingsley CRON[20069]: pam_unix(cron:session): session closed for user root
2025-03-04T15:55:01+0800	2025-03-04T15:55:01.811240+08:00 kingsley CRON[20069]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
2025-03-04T15:55:01+0800	2025-03-04T15:55:01.759027+08:00 judy-VirtualBox CRON[86875]: pam_unix(cron:session): session closed for user root
2025-03-04T15:55:01+0800	2025-03-04T15:55:01.757318+08:00 judy-VirtualBox CRON[86875]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
2025-03-04T15:55:01+0800	2025-03-04T15:55:01.406924+08:00 server CRON[13704]: pam_unix(cron:session): session closed for user root
2025-03-04T15:55:01+0800	2025-03-04T15:55:01.384713+08:00 server CRON[13704]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
2025-03-04T15:55:01+0800	2025-03-04T15:55:01.282381+08:00 hostname CRON[21679]: pam_unix(cron:session): session closed for user root
2025-03-04T15:55:01+0800	2025-03-04T15:55:01.252403+08:00 hostname CRON[21679]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
2025-03-04T15:55:01+0800	2025-03-04T15:55:01.200336+08:00 andrew CRON[10226]: pam_unix(cron:session): session closed for user root
2025-03-04T15:55:01+0800	2025-03-04T15:55:01.198480+08:00 andrew CRON[10226]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
2025-03-04T15:55:01+0800	2025-03-04T15:55:01.154945+08:00 kelly CRON[34203]: pam_unix(cron:session): session closed for user root
2025-03-04T15:55:01+0800	2025-03-04T15:55:01.127567+08:00 kelly CRON[34203]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
2025-03-04T15:55:01+0800	2025-03-04T15:55:01.097201+08:00 claire CRON[28118]: pam_unix(cron:session): session closed for user root
2025-03-04T15:55:01+0800	2025-03-04T15:55:01.089955+08:00 claire CRON[28118]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
2025-03-04T15:45:01+0800	2025-03-04T15:45:01.995815+08:00 claire CRON[27478]: pam_unix(cron:session): session closed for user root
2025-03-04T15:45:01+0800	2025-03-04T15:45:01.988906+08:00 claire CRON[27478]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
2025-03-04T15:45:01+0800	2025-03-04T15:45:01.705525+08:00 judy-VirtualBox CRON[80028]: pam_unix(cron:session): session closed for user root
2025-03-04T15:45:01+0800	2025-03-04T15:45:01.703706+08:00 judy-VirtualBox CRON[80028]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
2025-03-04T15:45:01+0800	2025-03-04T15:45:01.658018+08:00 kingsley CRON[19881]: pam_unix(cron:session): session closed for user root
2025-03-04T15:45:01+0800	2025-03-04T15:45:01.656516+08:00 kingsley CRON[19881]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
2025-03-04T15:45:01+0800	2025-03-04T15:45:01.397934+08:00 server CRON[12834]: pam_unix(cron:session): session closed for user root

splunk>

Time	Event
2025-03-04T15:45:01+0800	2025-03-04T15:45:01.362555+08:00 server CRON[12834]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
2025-03-04T15:45:01+0800	2025-03-04T15:45:01.240846+08:00 hostname CRON[21044]: pam_unix(cron:session): session closed for user root
2025-03-04T15:45:01+0800	2025-03-04T15:45:01.235077+08:00 hostname CRON[21044]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
2025-03-04T15:45:01+0800	2025-03-04T15:45:01.123934+08:00 andrew CRON[9516]: pam_unix(cron:session): session closed for user root
2025-03-04T15:45:01+0800	2025-03-04T15:45:01.103509+08:00 andrew CRON[9516]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
2025-03-04T15:45:01+0800	2025-03-04T15:45:01.029462+08:00 kelly CRON[33557]: pam_unix(cron:session): session closed for user root
2025-03-04T15:45:01+0800	2025-03-04T15:45:01.026606+08:00 kelly CRON[33557]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
2025-03-04T15:39:01+0800	2025-03-04T15:39:01.069330+08:00 andrew CRON[9062]: pam_unix(cron:session): session closed for user root
2025-03-04T15:39:01+0800	2025-03-04T15:39:01.043042+08:00 andrew CRON[9062]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
2025-03-04T15:35:01+0800	2025-03-04T15:35:01.897873+08:00 kelly CRON[32900]: pam_unix(cron:session): session closed for user root
2025-03-04T15:35:01+0800	2025-03-04T15:35:01.896102+08:00 kelly CRON[32900]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
2025-03-04T15:35:01+0800	2025-03-04T15:35:01.889068+08:00 claire CRON[26902]: pam_unix(cron:session): session closed for user root
2025-03-04T15:35:01+0800	2025-03-04T15:35:01.884887+08:00 claire CRON[26902]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
2025-03-04T15:35:01+0800	2025-03-04T15:35:01.696558+08:00 judy-VirtualBox CRON[62966]: pam_unix(cron:session): session closed for user root
2025-03-04T15:35:01+0800	2025-03-04T15:35:01.673824+08:00 judy-VirtualBox CRON[62966]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
2025-03-04T15:35:01+0800	2025-03-04T15:35:01.502558+08:00 kingsley CRON[19767]: pam_unix(cron:session): session closed for user root
2025-03-04T15:35:01+0800	2025-03-04T15:35:01.497065+08:00 kingsley CRON[19767]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
2025-03-04T15:35:01+0800	2025-03-04T15:35:01.370287+08:00 server CRON[12044]: pam_unix(cron:session): session closed for user root
2025-03-04T15:35:01+0800	2025-03-04T15:35:01.342098+08:00 server CRON[12044]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
2025-03-04T15:35:01+0800	2025-03-04T15:35:01.220553+08:00 hostname CRON[20440]: pam_unix(cron:session): session closed for user root
2025-03-04T15:35:01+0800	2025-03-04T15:35:01.216791+08:00 hostname CRON[20440]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
2025-03-04T15:35:01+0800	2025-03-04T15:35:01.021735+08:00 andrew CRON[8812]: pam_unix(cron:session): session closed for user root
2025-03-04T15:35:01+0800	2025-03-04T15:35:01.020075+08:00 andrew CRON[8812]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
2025-03-04T15:31:50+0800	2025-03-04T15:31:50.373223+08:00 server pkexec[11773]: byron: Executing command [USER=root] [TTY=unknown] [CWD=/home/byron] [COMMAND=/usr/lib/update-notifier/package-system-locked]
2025-03-04T15:31:50+0800	2025-03-04T15:31:50.372357+08:00 server pkexec: pam_unix(polkit-1:session): session opened for user root(uid=0) by byron(uid=1000)
2025-03-04T15:30:01+0800	2025-03-04T15:30:01.636452+08:00 judy-VirtualBox CRON[56944]: pam_unix(cron:session): session closed for user root
2025-03-04T15:30:01+0800	2025-03-04T15:30:01.631771+08:00 judy-VirtualBox CRON[56944]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
2025-03-04T15:30:01+0800	2025-03-04T15:30:01.345136+08:00 server CRON[11619]: pam_unix(cron:session): session closed for user root
2025-03-04T15:30:01+0800	2025-03-04T15:30:01.321670+08:00 server CRON[11619]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
2025-03-04T15:25:01+0800	2025-03-04T15:25:01.985730+08:00 andrew CRON[8214]: pam_unix(cron:session): session closed for user root
2025-03-04T15:25:01+0800	2025-03-04T15:25:01.945095+08:00 andrew CRON[8214]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
2025-03-04T15:25:01+0800	2025-03-04T15:25:01.791926+08:00 claire CRON[26336]: pam_unix(cron:session): session closed for user root
2025-03-04T15:25:01+0800	2025-03-04T15:25:01.764794+08:00 claire CRON[26336]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
2025-03-04T15:25:01+0800	2025-03-04T15:25:01.725439+08:00 kelly CRON[32170]: pam_unix(cron:session): session closed for user root
2025-03-04T15:25:01+0800	2025-03-04T15:25:01.708132+08:00 kelly CRON[32170]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
2025-03-04T15:25:01+0800	2025-03-04T15:25:01.612792+08:00 judy-VirtualBox CRON[52562]: pam_unix(cron:session): session closed for user root
2025-03-04T15:25:01+0800	2025-03-04T15:25:01.608469+08:00 judy-VirtualBox CRON[52562]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
2025-03-04T15:25:01+0800	2025-03-04T15:25:01.422756+08:00 kingsley CRON[19660]: pam_unix(cron:session): session closed for user root
2025-03-04T15:25:01+0800	2025-03-04T15:25:01.421239+08:00 kingsley CRON[19660]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
2025-03-04T15:25:01+0800	2025-03-04T15:25:01.270564+08:00 server CRON[10742]: pam_unix(cron:session): session closed for user root
2025-03-04T15:25:01+0800	2025-03-04T15:25:01.267582+08:00 server CRON[10742]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
2025-03-04T15:25:01+0800	2025-03-04T15:25:01.220526+08:00 hostname CRON[19786]: pam_unix(cron:session): session closed for user root
2025-03-04T15:25:01+0800	2025-03-04T15:25:01.203230+08:00 hostname CRON[19786]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
2025-03-04T15:17:01+0800	2025-03-04T15:17:01.887459+08:00 andrew CRON[7638]: pam_unix(cron:session): session closed for user root
2025-03-04T15:17:01+0800	2025-03-04T15:17:01.869348+08:00 andrew CRON[7638]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
2025-03-04T15:17:01+0800	2025-03-04T15:17:01.664305+08:00 claire CRON[25804]: pam_unix(cron:session): session closed for user root
2025-03-04T15:17:01+0800	2025-03-04T15:17:01.632889+08:00 claire CRON[25804]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
2025-03-04T15:17:01+0800	2025-03-04T15:17:01.611014+08:00 kelly CRON[31670]: pam_unix(cron:session): session closed for user root
2025-03-04T15:17:01+0800	2025-03-04T15:17:01.609589+08:00 kelly CRON[31670]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
2025-03-04T15:17:01+0800	2025-03-04T15:17:01.574867+08:00 judy-VirtualBox CRON[48316]: pam_unix(cron:session): session closed for user root

Time	Event
2025-03-04T15:17:01+0800	2025-03-04T15:17:01.572610+08:00 judy-VirtualBox CRON[48316]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
2025-03-04T15:17:01+0800	2025-03-04T15:17:01.287494+08:00 kingsley CRON[19551]: pam_unix(cron:session): session closed for user root
2025-03-04T15:17:01+0800	2025-03-04T15:17:01.283345+08:00 kingsley CRON[19551]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
2025-03-04T15:17:01+0800	2025-03-04T15:17:01.254377+08:00 server CRON[9992]: pam_unix(cron:session): session closed for user root
2025-03-04T15:17:01+0800	2025-03-04T15:17:01.252473+08:00 server CRON[9992]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
2025-03-04T15:17:01+0800	2025-03-04T15:17:01.198281+08:00 hostname CRON[19301]: pam_unix(cron:session): session closed for user root
2025-03-04T15:17:01+0800	2025-03-04T15:17:01.194099+08:00 hostname CRON[19301]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
2025-03-04T15:15:01+0800	2025-03-04T15:15:01.858320+08:00 andrew CRON[7446]: pam_unix(cron:session): session closed for user root
2025-03-04T15:15:01+0800	2025-03-04T15:15:01.856552+08:00 andrew CRON[7446]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
2025-03-04T15:15:01+0800	2025-03-04T15:15:01.617649+08:00 claire CRON[25613]: pam_unix(cron:session): session closed for user root
2025-03-04T15:15:01+0800	2025-03-04T15:15:01.609089+08:00 claire CRON[25613]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
2025-03-04T15:15:01+0800	2025-03-04T15:15:01.602542+08:00 judy-VirtualBox CRON[46492]: pam_unix(cron:session): session closed for user root
2025-03-04T15:15:01+0800	2025-03-04T15:15:01.579232+08:00 kelly CRON[31481]: pam_unix(cron:session): session closed for user root
2025-03-04T15:15:01+0800	2025-03-04T15:15:01.577582+08:00 kelly CRON[31481]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
2025-03-04T15:15:01+0800	2025-03-04T15:15:01.557968+08:00 judy-VirtualBox CRON[46492]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
2025-03-04T15:15:01+0800	2025-03-04T15:15:01.294689+08:00 kingsley CRON[19389]: pam_unix(cron:session): session closed for user root
2025-03-04T15:15:01+0800	2025-03-04T15:15:01.264667+08:00 kingsley CRON[19389]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
2025-03-04T15:15:01+0800	2025-03-04T15:15:01.248472+08:00 server CRON[9788]: pam_unix(cron:session): session closed for user root
2025-03-04T15:15:01+0800	2025-03-04T15:15:01.245692+08:00 server CRON[9788]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
2025-03-04T15:15:01+0800	2025-03-04T15:15:01.185231+08:00 hostname CRON[19102]: pam_unix(cron:session): session closed for user root
2025-03-04T15:15:01+0800	2025-03-04T15:15:01.182380+08:00 hostname CRON[19102]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
2025-03-04T15:10:00+0800	2025-03-04T15:10:00.689110+08:00 kingsley sudo: pam_unix(sudo:session): session closed for user root
2025-03-04T15:10:00+0800	2025-03-04T15:10:00.688547+08:00 kingsley passwd[19327]: pam_unix(passwd:chauthtok): password changed for ariana
2025-03-04T15:09:54+0800	2025-03-04T15:09:54.707077+08:00 kingsley sudo: pam_unix(sudo:session): session opened for user root(uid=0) by kingsley(uid=1000)
2025-03-04T15:09:54+0800	2025-03-04T15:09:54.706645+08:00 kingsley sudo: kingsley : TTY=pts/0 ; PWD=/opt/splunk/bin ; USER= root ; COMMAND=/usr/bin/passwd ariana
2025-03-04T15:09:40+0800	2025-03-04T15:09:40.393404+08:00 kingsley sudo: pam_unix(sudo:session): session closed for user root
2025-03-04T15:09:40+0800	2025-03-04T15:09:40.390512+08:00 kingsley passwd[19318]: pam_unix(passwd:chauthtok): password changed for poter
2025-03-04T15:09:35+0800	2025-03-04T15:09:35.963347+08:00 kingsley sudo: pam_unix(sudo:session): session opened for user root(uid=0) by kingsley(uid=1000)
2025-03-04T15:09:35+0800	2025-03-04T15:09:35.962864+08:00 kingsley sudo: kingsley : TTY=pts/0 ; PWD=/opt/splunk/bin ; USER= root ; COMMAND=/usr/bin/passwd poter
2025-03-04T15:09:30+0800	2025-03-04T15:09:30.178292+08:00 kingsley sudo: pam_unix(sudo:auth): authentication failure; logname=kingsley uid=1000 euid=0 tty=/dev/pts/0 ruser=kingsley rhost= user=kingsley
2025-03-04T15:09:01+0800	2025-03-04T15:09:01.825430+08:00 andrew CRON[7006]: pam_unix(cron:session): session closed for user root
2025-03-04T15:09:01+0800	2025-03-04T15:09:01.824232+08:00 andrew CRON[7006]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
2025-03-04T15:08:02+0800	2025-03-04T15:08:02.424777+08:00 judy-VirtualBox sudo: pam_unix(sudo:session): session closed for user root
2025-03-04T15:08:02+0800	2025-03-04T15:08:02.396781+08:00 judy-VirtualBox userdel[37316]: delete 'kkday' from shadow group 'users'
2025-03-04T15:08:02+0800	2025-03-04T15:08:02.396757+08:00 judy-VirtualBox userdel[37316]: removed shadow group 'kkday' owned by 'kkday'
2025-03-04T15:08:02+0800	2025-03-04T15:08:02.396721+08:00 judy-VirtualBox userdel[37316]: removed group 'kkday' owned by 'kkday'
2025-03-04T15:08:02+0800	2025-03-04T15:08:02.394207+08:00 judy-VirtualBox userdel[37316]: delete 'kkday' from group 'users'
2025-03-04T15:08:02+0800	2025-03-04T15:08:02.393534+08:00 judy-VirtualBox userdel[37316]: delete user 'kkday'
2025-03-04T15:08:02+0800	2025-03-04T15:08:02.091627+08:00 judy-VirtualBox sudo: pam_unix(sudo:session): session opened for user root(uid=0) by judy(uid=1000)
2025-03-04T15:08:02+0800	2025-03-04T15:08:02.090988+08:00 judy-VirtualBox sudo: judy : TTY=pts/1 ; PWD=/home/judy ; USER=root ; COMMAND=/usr/sbin/deluser kkday
2025-03-04T15:07:43+0800	2025-03-04T15:07:43.327587+08:00 judy-VirtualBox sudo: pam_unix(sudo:session): session closed for user root
2025-03-04T15:07:43+0800	2025-03-04T15:07:43.324930+08:00 judy-VirtualBox gpasswd[36554]: members of group users set by root to judy,ziven,kkday
2025-03-04T15:07:42+0800	2025-03-04T15:07:42.454847+08:00 judy-VirtualBox chfn[36454]: changed user 'kkday' information
2025-03-04T15:07:40+0800	2025-03-04T15:07:40.868212+08:00 judy-VirtualBox passwd[36217]: gkr-pam: couldn't update the login keyring password: no old password was entered
2025-03-04T15:07:40+0800	2025-03-04T15:07:40.867670+08:00 judy-VirtualBox passwd[36217]: pam_unix(passwd:chauthtok): password changed for kkday
2025-03-04T15:07:35+0800	2025-03-04T15:07:35.687177+08:00 judy-VirtualBox useradd[36204]: new user: name=kkday, UID=1002, GID= 1002, home=/home/kkday, shell=/bin/bash, from=/dev/pts/2
2025-03-04T15:07:35+0800	2025-03-04T15:07:35.644395+08:00 judy-VirtualBox groupadd[36197]: new group: name=kkday, GID=1002

Time	Event
2025-03-04T15:07:35+0800	2025-03-04T15:07:35.643314+08:00 judy-VirtualBox groupadd[36197]: group added to /etc/gshadow: name=kkday
2025-03-04T15:07:35+0800	2025-03-04T15:07:35.640705+08:00 judy-VirtualBox groupadd[36197]: group added to /etc/group: name=kkday, GID=1002
2025-03-04T15:07:35+0800	2025-03-04T15:07:35.548207+08:00 judy-VirtualBox sudo: pam_unix(sudo:session): session opened for user root(uid=0) by judy(uid=1000)
2025-03-04T15:07:35+0800	2025-03-04T15:07:35.547888+08:00 judy-VirtualBox sudo: judy : TTY=pts/1 ; PWD=/home/judy ; USER=root ; COMMAND=/usr/sbin/adduser kkday
2025-03-04T15:05:57+0800	2025-03-04T15:05:57.259758+08:00 judy-VirtualBox sudo: pam_unix(sudo:session): session closed for user root
2025-03-04T15:05:57+0800	2025-03-04T15:05:57.258880+08:00 judy-VirtualBox passwd[32938]: gkr-pam: couldn't update the login keyring password: no old password was entered
2025-03-04T15:05:57+0800	2025-03-04T15:05:57.258783+08:00 judy-VirtualBox passwd[32938]: pam_unix(passwd:chauthtok): password changed for ziven
2025-03-04T15:05:47+0800	2025-03-04T15:05:47.971658+08:00 andrew sudo: pam_unix(sudo:session): session closed for user root
2025-03-04T15:05:47+0800	2025-03-04T15:05:47.948675+08:00 andrew userdel[6798]: delete 'bob' from shadow group 'users'
2025-03-04T15:05:47+0800	2025-03-04T15:05:47.948657+08:00 andrew userdel[6798]: removed shadow group 'bob' owned by 'bob'
2025-03-04T15:05:47+0800	2025-03-04T15:05:47.948639+08:00 andrew userdel[6798]: removed group 'bob' owned by 'bob'
2025-03-04T15:05:47+0800	2025-03-04T15:05:47.948607+08:00 andrew userdel[6798]: delete 'bob' from group 'users'
2025-03-04T15:05:47+0800	2025-03-04T15:05:47.933492+08:00 andrew userdel[6798]: delete user 'bob'
2025-03-04T15:05:47+0800	2025-03-04T15:05:47.715870+08:00 andrew sudo: pam_unix(sudo:session): session opened for user root(uid=0) by andrew(uid=1000)
2025-03-04T15:05:47+0800	2025-03-04T15:05:47.673977+08:00 andrew sudo: andrew : TTY=pts/0 ; PWD=/home/andrew ; USER=root ; COMMAND=/usr/sbin/deluser bob
2025-03-04T15:05:44+0800	2025-03-04T15:05:44.799572+08:00 judy-VirtualBox sudo: pam_unix(sudo:session): session opened for user root(uid=0) by judy(uid=1000)
2025-03-04T15:05:44+0800	2025-03-04T15:05:44.780955+08:00 judy-VirtualBox sudo: judy : TTY=pts/1 ; PWD=/home/judy ; USER=root ; COMMAND=/usr/bin/passwd ziven
2025-03-04T15:05:01+0800	2025-03-04T15:05:01.877980+08:00 andrew CRON[6751]: pam_unix(cron:session): session closed for user root
2025-03-04T15:05:01+0800	2025-03-04T15:05:01.796063+08:00 andrew CRON[6751]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
2025-03-04T15:05:01+0800	2025-03-04T15:05:01.544751+08:00 judy-VirtualBox CRON[31407]: pam_unix(cron:session): session closed for user root
2025-03-04T15:05:01+0800	2025-03-04T15:05:01.504767+08:00 judy-VirtualBox CRON[31407]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
2025-03-04T15:05:01+0800	2025-03-04T15:05:01.461930+08:00 kelly CRON[30833]: pam_unix(cron:session): session closed for user root
2025-03-04T15:05:01+0800	2025-03-04T15:05:01.456424+08:00 claire CRON[24609]: pam_unix(cron:session): session closed for user root
2025-03-04T15:05:01+0800	2025-03-04T15:05:01.454401+08:00 claire CRON[24609]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
2025-03-04T15:05:01+0800	2025-03-04T15:05:01.441453+08:00 kelly CRON[30833]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
2025-03-04T15:05:01+0800	2025-03-04T15:05:01.231098+08:00 server CRON[8985]: pam_unix(cron:session): session closed for user root
2025-03-04T15:05:01+0800	2025-03-04T15:05:01.225606+08:00 server CRON[8985]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
2025-03-04T15:05:01+0800	2025-03-04T15:05:01.165964+08:00 hostname CRON[18490]: pam_unix(cron:session): session closed for user root
2025-03-04T15:05:01+0800	2025-03-04T15:05:01.164511+08:00 hostname CRON[18490]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
2025-03-04T15:05:01+0800	2025-03-04T15:05:01.156134+08:00 kingsley CRON[19276]: pam_unix(cron:session): session closed for user root
2025-03-04T15:05:01+0800	2025-03-04T15:05:01.146698+08:00 kingsley CRON[19276]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
2025-03-04T15:03:46+0800	2025-03-04T15:03:46.131021+08:00 hostname sudo: pam_unix(sudo:session): session closed for user root
2025-03-04T15:03:46+0800	2025-03-04T15:03:46.107111+08:00 hostname userdel[18402]: delete 'alice' from shadow group 'users'
2025-03-04T15:03:46+0800	2025-03-04T15:03:46.107087+08:00 hostname userdel[18402]: removed shadow group 'alice' owned by 'alice'
2025-03-04T15:03:46+0800	2025-03-04T15:03:46.107061+08:00 hostname userdel[18402]: removed group 'alice' owned by 'alice'
2025-03-04T15:03:46+0800	2025-03-04T15:03:46.106814+08:00 hostname userdel[18402]: delete 'alice' from group 'users'
2025-03-04T15:03:46+0800	2025-03-04T15:03:46.106752+08:00 hostname userdel[18402]: delete user 'alice'
2025-03-04T15:03:45+0800	2025-03-04T15:03:45.911827+08:00 hostname sudo: pam_unix(sudo:session): session opened for user root(uid=0) by sam(uid=1000)
2025-03-04T15:03:45+0800	2025-03-04T15:03:45.911411+08:00 hostname sudo: sam : TTY=pts/0 ; PWD=/home/sam ; USER=root ; COMMAND=/usr/sbin/deluser alice
2025-03-04T15:01:19+0800	2025-03-04T15:01:19.000519+08:00 hostname sudo: pam_unix(sudo:session): session closed for user root
2025-03-04T15:01:18+0800	2025-03-04T15:01:18.998711+08:00 hostname gpasswd[18153]: members of group users set by root to alice,bob,john,steve
2025-03-04T15:01:17+0800	2025-03-04T15:01:17.909439+08:00 hostname chfn[18145]: changed user 'steve' information
2025-03-04T15:01:16+0800	2025-03-04T15:01:16.280656+08:00 hostname passwd[18136]: pam_unix(passwd:chauthtok): password changed for steve
2025-03-04T15:01:10+0800	2025-03-04T15:01:10.118625+08:00 hostname useradd[18123]: new user: name=steve, UID=1005, GID=1005, home=/home/steve, shell=/bin/bash, from=/dev/pts/1
2025-03-04T15:01:10+0800	2025-03-04T15:01:10.091181+08:00 hostname groupadd[18116]: new group: name=steve, GID=1005
2025-03-04T15:01:10+0800	2025-03-04T15:01:10.090364+08:00 hostname groupadd[18116]: group added to /etc/gshadow: name=steve
2025-03-04T15:01:10+0800	2025-03-04T15:01:10.087336+08:00 hostname groupadd[18116]: group added to /etc/group: name=steve, GID=1005
2025-03-04T15:01:10+0800	2025-03-04T15:01:10.008255+08:00 hostname sudo: pam_unix(sudo:session): session opened for user root(uid=0) by sam(uid=1000)

Time	Event
2025-03-04T15:01:10+0800	2025-03-04T15:01:10.007836+08:00 hostname sudo: sam : TTY=pts/0 ; PWD=/home/sam ; USER= root ; COMMAND=/usr/sbin/adduser steve
2025-03-04T15:00:50+0800	2025-03-04T15:00:50.028638+08:00 kelly sudo: pam_unix(sudo:session): session closed for user root
2025-03-04T15:00:50+0800	2025-03-04T15:00:50.027790+08:00 kelly passwd[30220]: pam_unix(passwd:chauthtok): password changed for doremi
2025-03-04T15:00:46+0800	2025-03-04T15:00:46.336744+08:00 hostname sudo: pam_unix(sudo-i:session): session closed for user root
2025-03-04T15:00:43+0800	2025-03-04T15:00:43.984588+08:00 kelly sudo: pam_unix(sudo:session): session opened for user root(uid=0) by kelly(uid=1000)
2025-03-04T15:00:43+0800	2025-03-04T15:00:43.984220+08:00 kelly sudo: kelly : TTY=pts/0 ; PWD=/home/kelly ; USER=root ; COMMAND=/usr/bin/passwd doremi
2025-03-04T15:00:18+0800	2025-03-04T15:00:18.911737+08:00 kelly sudo: pam_unix(sudo:session): session closed for user root
2025-03-04T15:00:18+0800	2025-03-04T15:00:18.809603+08:00 kelly userdel[30187]: removed shadow group 'dodo' owned by 'dodo'
2025-03-04T15:00:18+0800	2025-03-04T15:00:18.809572+08:00 kelly userdel[30187]: removed group 'dodo' owned by 'dodo'
2025-03-04T15:00:18+0800	2025-03-04T15:00:18.809205+08:00 kelly userdel[30187]: delete user 'dodo'
2025-03-04T15:00:18+0800	2025-03-04T15:00:18.777335+08:00 kelly sudo: pam_unix(sudo:session): session opened for user root(uid=0) by kelly(uid=1000)
2025-03-04T15:00:18+0800	2025-03-04T15:00:18.776995+08:00 kelly sudo: kelly : TTY=pts/0 ; PWD=/home/kelly ; USER=root ; COMMAND=/usr/sbin/userdel -r dodo
2025-03-04T15:00:05+0800	2025-03-04T15:00:05.560690+08:00 kelly sudo: pam_unix(sudo:session): session closed for user root
2025-03-04T15:00:05+0800	2025-03-04T15:00:05.529201+08:00 kelly useradd[30160]: new user: name=faso, UID=1009, GID=1009, home =/home/faso, shell=/bin/sh, from=/dev/pts/1
2025-03-04T15:00:05+0800	2025-03-04T15:00:05.529133+08:00 kelly useradd[30160]: new group: name=faso, GID=1009
2025-03-04T15:00:05+0800	2025-03-04T15:00:05.490562+08:00 kelly sudo: pam_unix(sudo:session): session opened for user root(uid=0) by kelly(uid=1000)
2025-03-04T15:00:05+0800	2025-03-04T15:00:05.490184+08:00 kelly sudo: kelly : TTY=pts/0 ; PWD=/home/kelly ; USER=root ; COMMAND=/usr/sbin/useradd -m faso
2025-03-04T15:00:02+0800	2025-03-04T15:00:02.964788+08:00 wilsonwu sudo: pam_unix(sudo:session): session closed for user root
2025-03-04T15:00:02+0800	2025-03-04T15:00:02.942082+08:00 wilsonwu userdel[6652]: delete 'plankton' from shadow group 'users'
2025-03-04T15:00:02+0800	2025-03-04T15:00:02.942010+08:00 wilsonwu userdel[6652]: removed shadow group 'plankton' owned by 'plankton'
2025-03-04T15:00:02+0800	2025-03-04T15:00:02.941938+08:00 wilsonwu userdel[6652]: removed group 'plankton' owned by 'plankton'
2025-03-04T15:00:02+0800	2025-03-04T15:00:02.941714+08:00 wilsonwu userdel[6652]: delete 'plankton' from group 'users'
2025-03-04T15:00:02+0800	2025-03-04T15:00:02.941203+08:00 wilsonwu userdel[6652]: delete user 'plankton'
2025-03-04T15:00:02+0800	2025-03-04T15:00:02.743106+08:00 wilsonwu sudo: pam_unix(sudo:session): session opened for user root(uid=0) by wilson(uid=1000)
2025-03-04T15:00:02+0800	2025-03-04T15:00:02.742555+08:00 wilsonwu sudo: wilson : TTY=tty1 ; PWD=/home/wilson ; USER=root ; COMMAND=/usr/sbin/deluser plankton
2025-03-04T14:59:59+0800	2025-03-04T14:59:59.560201+08:00 kelly sudo: pam_unix(sudo:session): session closed for user root
2025-03-04T14:59:59+0800	2025-03-04T14:59:59.538596+08:00 kelly useradd[30140]: new user: name=doremi, UID=1008, GID=1008, home=/home/doremi, shell=/bin/sh, from=/dev/pts/1
2025-03-04T14:59:59+0800	2025-03-04T14:59:59.538372+08:00 kelly useradd[30140]: new group: name=doremi, GID=1008
2025-03-04T14:59:59+0800	2025-03-04T14:59:59.506189+08:00 kelly sudo: pam_unix(sudo:session): session opened for user root(uid=0) by kelly(uid=1000)
2025-03-04T14:59:59+0800	2025-03-04T14:59:59.505825+08:00 kelly sudo: kelly : TTY=pts/0 ; PWD=/home/kelly ; USER=root ; COMMAND=/usr/sbin/useradd -m doremi
2025-03-04T14:59:49+0800	2025-03-04T14:59:49.688356+08:00 wilsonwu sudo: pam_unix(sudo:session): session closed for user root
2025-03-04T14:59:49+0800	2025-03-04T14:59:49.686665+08:00 wilsonwu gpasswd[6609]: members of group users set by root to sam,ben,patrick,bob,plankton
2025-03-04T14:59:48+0800	2025-03-04T14:59:48.308073+08:00 wilsonwu chfn[6600]: changed user 'plankton' information
2025-03-04T14:59:46+0800	2025-03-04T14:59:46.492995+08:00 wilsonwu passwd[6593]: pam_unix(passwd:chauthtok): password changed for plankton
2025-03-04T14:59:42+0800	2025-03-04T14:59:42.313239+08:00 wilsonwu useradd[6580]: new user: name=plankton, UID=1006, GID=1006, home=/home/plankton, shell=/bin/bash, from=/dev/pts/4
2025-03-04T14:59:42+0800	2025-03-04T14:59:42.298926+08:00 wilsonwu groupadd[6573]: new group: name=plankton, GID=1006
2025-03-04T14:59:42+0800	2025-03-04T14:59:42.298016+08:00 wilsonwu groupadd[6573]: group added to /etc/gshadow: name=plankton
2025-03-04T14:59:42+0800	2025-03-04T14:59:42.294956+08:00 wilsonwu groupadd[6573]: group added to /etc/group: name=plankton, GID=1006
2025-03-04T14:59:42+0800	2025-03-04T14:59:42.250184+08:00 wilsonwu sudo: pam_unix(sudo:session): session opened for user root(uid=0) by wilson(uid=1000)
2025-03-04T14:59:42+0800	2025-03-04T14:59:42.250004+08:00 wilsonwu sudo: wilson : TTY=tty1 ; PWD=/home/wilson ; USER=root ; COMMAND=/usr/sbin/adduser plankton
2025-03-04T14:59:34+0800	2025-03-04T14:59:34.374090+08:00 kelly sudo: pam_unix(sudo:session): session closed for user root
2025-03-04T14:59:34+0800	2025-03-04T14:59:34.351949+08:00 kelly useradd[30110]: new user: name=dodo, UID=1007, GID=1007, home=/home/dodo, shell=/bin/sh, from=/dev/pts/1
2025-03-04T14:59:34+0800	2025-03-04T14:59:34.351878+08:00 kelly useradd[30110]: new group: name=dodo, GID=1007
2025-03-04T14:59:34+0800	2025-03-04T14:59:34.341287+08:00 kelly sudo: pam_unix(sudo:session): session opened for user root(uid=0) by kelly(uid=1000)
2025-03-04T14:59:34+0800	2025-03-04T14:59:34.337246+08:00 kelly sudo: kelly : TTY=pts/0 ; PWD=/home/kelly ; USER=root ; COMMAND=/usr/sbin/useradd -m dodo
2025-03-04T14:59:25+0800	2025-03-04T14:59:25.171887+08:00 wilsonwu sudo: pam_unix(sudo:session): session closed for user root
2025-03-04T14:59:25+0800	2025-03-04T14:59:25.170111+08:00 wilsonwu gpasswd[6541]: members of group users set by root to sam,ben,patrick,bob

Time	Event
2025-03-04T14:59:24+0800	2025-03-04T14:59:24.955465+08:00 andrew sudo: pam_unix(sudo:session): session closed for user root
2025-03-04T14:59:24+0800	2025-03-04T14:59:24.944367+08:00 andrew gpasswd[6388]: members of group users set by root to bob
2025-03-04T14:59:24+0800	2025-03-04T14:59:24.065231+08:00 andrew chfn[6376]: changed user 'bob' information
2025-03-04T14:59:22+0800	2025-03-04T14:59:22.383312+08:00 andrew passwd[6368]: pam_unix(passwd:chauthtok): password changed for bob
2025-03-04T14:59:14+0800	2025-03-04T14:59:14.701594+08:00 andrew useradd[6360]: new user: name=bob, UID=1002, GID=1002, home=/home/bob, shell=/bin/bash, from=/dev/pts/1
2025-03-04T14:59:14+0800	2025-03-04T14:59:14.605115+08:00 andrew groupadd[6353]: new group: name=bob, GID=1002
2025-03-04T14:59:14+0800	2025-03-04T14:59:14.604085+08:00 andrew groupadd[6353]: group added to /etc/gshadow: name=bob
2025-03-04T14:59:14+0800	2025-03-04T14:59:14.600532+08:00 andrew groupadd[6353]: group added to /etc/group: name=bob, GID=1002
2025-03-04T14:59:14+0800	2025-03-04T14:59:14.185882+08:00 andrew sudo: pam_unix(sudo:session): session opened for user root(uid=0) by andrew(uid=1000)
2025-03-04T14:59:14+0800	2025-03-04T14:59:14.013653+08:00 andrew sudo: andrew : TTY=pts/0 ; PWD=/home/andrew ; USER= root ; COMMAND=/usr/sbin/adduser bob
2025-03-04T14:58:56+0800	2025-03-04T14:58:56.914776+08:00 server sudo: pam_unix(sudo:session): session closed for user root
2025-03-04T14:58:56+0800	2025-03-04T14:58:56.912631+08:00 server gpasswd[8431]: members of group users set by root to byron,alice,jordan,maybe,bob,jacky
2025-03-04T14:58:55+0800	2025-03-04T14:58:55.913819+08:00 server chfn[8420]: changed user 'jacky' information
2025-03-04T14:58:55+0800	2025-03-04T14:58:55.355793+08:00 server passwd[8419]: gkr-pam: couldn't update the login keyring password: no old password was entered
2025-03-04T14:58:55+0800	2025-03-04T14:58:55.355676+08:00 server passwd[8419]: pam_unix(passwd:chauthtok): password changed for jacky
2025-03-04T14:58:51+0800	2025-03-04T14:58:51.606261+08:00 server useradd[8406]: new user: name=jacky, UID=1006, GID=1006, home=/home/jacky, shell=/bin/bash, from=/dev/pts/2
2025-03-04T14:58:51+0800	2025-03-04T14:58:51.591030+08:00 server groupadd[8399]: new group: name=jacky, GID=1006
2025-03-04T14:58:51+0800	2025-03-04T14:58:51.589930+08:00 server groupadd[8399]: group added to /etc/gshadow: name=jacky
2025-03-04T14:58:51+0800	2025-03-04T14:58:51.587171+08:00 server groupadd[8399]: group added to /etc/group: name=jacky, GID=1006
2025-03-04T14:58:51+0800	2025-03-04T14:58:51.518595+08:00 server sudo: pam_unix(sudo:session): session opened for user root(uid=0) by byron(uid=1000)
2025-03-04T14:58:51+0800	2025-03-04T14:58:51.518243+08:00 server sudo: byron : TTY=pts/0 ; PWD=/home/byron ; USER=root ; COMMAND=/usr/sbin/adduser jacky
2025-03-04T14:58:45+0800	2025-03-04T14:58:45.003000+08:00 server sudo: pam_unix(sudo:session): session closed for user root
2025-03-04T14:58:44+0800	2025-03-04T14:58:44.975918+08:00 server sudo: pam_unix(sudo:session): session opened for user root(uid=0) by byron(uid=1000)
2025-03-04T14:58:44+0800	2025-03-04T14:58:44.975551+08:00 server sudo: byron : TTY=pts/0 ; PWD=/home/byron ; USER=root ; COMMAND=/usr/sbin/adduser bob
2025-03-04T14:58:23+0800	2025-03-04T14:58:23.335553+08:00 kelly mongod: looking for plugins in '/home/build/build-home/opt/mongo/lib/ sasl2', failed to open directory, error: No such file or directory
2025-03-04T14:58:23+0800	2025-03-04T14:58:23.309428+08:00 kelly mongod: looking for plugins in '/home/build/build-home/opt/mongo/lib/ sasl2', failed to open directory, error: No such file or directory
2025-03-04T14:57:10+0800	2025-03-04T14:57:10.112006+08:00 server sudo: pam_unix(sudo:session): session closed for user root
2025-03-04T14:57:10+0800	2025-03-04T14:57:10.109899+08:00 server gpasswd[8248]: members of group users set by root to byron,alice,jordan,maybe,bob
2025-03-04T14:57:09+0800	2025-03-04T14:57:09.905235+08:00 server chfn[8238]: changed user 'bob' information
2025-03-04T14:57:08+0800	2025-03-04T14:57:08.564007+08:00 server passwd[8228]: gkr-pam: couldn't update the login keyring password: no old password was entered
2025-03-04T14:57:08+0800	2025-03-04T14:57:08.563931+08:00 server passwd[8228]: pam_unix(passwd:chauthtok): password changed for bob
2025-03-04T14:57:04+0800	2025-03-04T14:57:04.146989+08:00 server useradd[8214]: new user: name=bob, UID=1003, GID=1003, home =/home/bob, shell=/bin/bash, from=/dev/pts/2
2025-03-04T14:57:04+0800	2025-03-04T14:57:04.094495+08:00 server groupadd[8207]: new group: name=bob, GID=1003
2025-03-04T14:57:04+0800	2025-03-04T14:57:04.093296+08:00 server groupadd[8207]: group added to /etc/gshadow: name=bob
2025-03-04T14:57:04+0800	2025-03-04T14:57:04.089514+08:00 server groupadd[8207]: group added to /etc/group: name=bob, GID=1003
2025-03-04T14:57:04+0800	2025-03-04T14:57:04.022072+08:00 server sudo: pam_unix(sudo:session): session opened for user root(uid=0) by byron(uid=1000)
2025-03-04T14:57:04+0800	2025-03-04T14:57:04.021254+08:00 server sudo: byron : TTY=pts/0 ; PWD=/home/byron ; USER=root ; COMMAND=/usr/sbin/adduser bob
2025-03-04T14:56:36+0800	2025-03-04T14:56:36.875946+08:00 judy-VirtualBox sudo: pam_unix(sudo:session): session closed for user root
2025-03-04T14:56:36+0800	2025-03-04T14:56:36.873971+08:00 judy-VirtualBox gpasswd[20774]: members of group users set by root to judy,ziven
2025-03-04T14:56:35+0800	2025-03-04T14:56:35.889557+08:00 judy-VirtualBox chfn[20702]: changed user 'ziven' information
2025-03-04T14:56:34+0800	2025-03-04T14:56:34.287759+08:00 judy-VirtualBox passwd[20695]: gkr-pam: couldn't update the login keyring password: no old password was entered
2025-03-04T14:56:34+0800	2025-03-04T14:56:34.287263+08:00 judy-VirtualBox passwd[20695]: pam_unix(passwd:chauthtok): password changed for ziven
2025-03-04T14:56:29+0800	2025-03-04T14:56:29.109559+08:00 judy-VirtualBox useradd[20687]: new user: name=ziven, UID=1001, GID= 1001, home=/home/ziven, shell=/bin/bash, from=/dev/pts/2
2025-03-04T14:56:29+0800	2025-03-04T14:56:29.057736+08:00 judy-VirtualBox groupadd[20680]: new group: name=ziven, GID=1001
2025-03-04T14:56:29+0800	2025-03-04T14:56:29.056644+08:00 judy-VirtualBox groupadd[20680]: group added to /etc/gshadow: name=ziven
2025-03-04T14:56:29+0800	2025-03-04T14:56:29.054018+08:00 judy-VirtualBox groupadd[20680]: group added to /etc/group: name=ziven, GID=1001

Time	Event
2025-03-04T14:56:28+0800	2025-03-04T14:56:28.671019+08:00 judy-VirtualBox sudo: pam_unix(sudo:session): session opened for user root(uid=0) by judy(uid=1000)
2025-03-04T14:56:28+0800	2025-03-04T14:56:28.667477+08:00 judy-VirtualBox sudo: judy : TTY=pts/1 ; PWD=/home/judy ; USER=root ; COMMAND=/usr/sbin/adduser ziven
2025-03-04T14:55:31+0800	2025-03-04T14:55:31.271827+08:00 wilsonwu sudo: pam_unix(sudo:session): session closed for user root
2025-03-04T14:55:20+0800	2025-03-04T14:55:20.608800+08:00 wilsonwu sudo: pam_unix(sudo:session): session opened for user root(uid=0) by wilson(uid=1000)
2025-03-04T14:55:20+0800	2025-03-04T14:55:20.607433+08:00 wilsonwu sudo: wilson : TTY=pts/0 ; PWD=/etc ; USER=root ; COMMAND=/usr/bin/apt install unzip
2025-03-04T14:55:01+0800	2025-03-04T14:55:01.797888+08:00 wilsonwu CRON[6187]: pam_unix(cron:session): session closed for user root
2025-03-04T14:55:01+0800	2025-03-04T14:55:01.794864+08:00 wilsonwu CRON[6187]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
2025-03-04T14:55:01+0800	2025-03-04T14:55:01.778573+08:00 andrew CRON[6170]: pam_unix(cron:session): session closed for user root
2025-03-04T14:55:01+0800	2025-03-04T14:55:01.689432+08:00 andrew CRON[6170]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
2025-03-04T14:55:01+0800	2025-03-04T14:55:01.441448+08:00 judy-VirtualBox CRON[18460]: pam_unix(cron:session): session closed for user root
2025-03-04T14:55:01+0800	2025-03-04T14:55:01.438882+08:00 judy-VirtualBox CRON[18460]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
2025-03-04T14:55:01+0800	2025-03-04T14:55:01.383679+08:00 claire CRON[23993]: pam_unix(cron:session): session closed for user root
2025-03-04T14:55:01+0800	2025-03-04T14:55:01.379644+08:00 claire CRON[23993]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
2025-03-04T14:55:01+0800	2025-03-04T14:55:01.223274+08:00 server CRON[8128]: pam_unix(cron:session): session closed for user root
2025-03-04T14:55:01+0800	2025-03-04T14:55:01.204568+08:00 server CRON[8128]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
2025-03-04T14:55:01+0800	2025-03-04T14:55:01.173084+08:00 hostname CRON[17754]: pam_unix(cron:session): session closed for user root
2025-03-04T14:55:01+0800	2025-03-04T14:55:01.149118+08:00 hostname CRON[17754]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
2025-03-04T14:55:01+0800	2025-03-04T14:55:01.079129+08:00 kingsley CRON[18725]: pam_unix(cron:session): session closed for user root
2025-03-04T14:55:01+0800	2025-03-04T14:55:01.077722+08:00 kingsley CRON[18725]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
2025-03-04T14:54:40+0800	2025-03-04T14:54:40.175297+08:00 hostname sudo: pam_unix(sudo-i:session): session opened for user root(uid=0) by sam(uid=1000)
2025-03-04T14:54:40+0800	2025-03-04T14:54:40.174688+08:00 hostname sudo: sam : TTY=pts/0 ; PWD=/root ; USER=root ; COMMAND=/bin/bash
2025-03-04T14:54:32+0800	2025-03-04T14:54:32.227899+08:00 judy-VirtualBox gdm-password]: gkr-pam: unlocked login keyring
2025-03-04T14:54:02+0800	2025-03-04T14:54:02.971748+08:00 wilsonwu sudo: pam_unix(sudo:session): session closed for user root
2025-03-04T14:54:02+0800	2025-03-04T14:54:02.949516+08:00 wilsonwu sudo: pam_unix(sudo:session): session opened for user root(uid=0) by wilson(uid=1000)
2025-03-04T14:54:02+0800	2025-03-04T14:54:02.915745+08:00 wilsonwu sudo: wilson : TTY=pts/0 ; PWD=/usr/share ; USER=root ; COMMAND=/usr/bin/cp /usr/share/elasticsearch/elastic-stack-ca.zip /etc/kibana
2025-03-04T14:53:51+0800	2025-03-04T14:53:51.245645+08:00 hostname sudo: pam_unix(sudo:session): session closed for user root
2025-03-04T14:53:51+0800	2025-03-04T14:53:51.245588+08:00 hostname sudo: pam_unix(sudo:session): session opened for user root(uid=0) by sam(uid=1000)
2025-03-04T14:53:51+0800	2025-03-04T14:53:51.218820+08:00 hostname sudo: sam : TTY=pts/0 ; PWD=/home/sam ; USER=root ; COMMAND=/usr/bin/cat /etc/shadow
2025-03-04T14:50:02+0800	2025-03-04T14:50:02.309475+08:00 kingsley sudo: pam_unix(sudo:session): session closed for user root
2025-03-04T14:50:02+0800	2025-03-04T14:50:02.307601+08:00 kingsley gpasswd[18662]: members of group users set by root to kartrina,ariana,poter
2025-03-04T14:50:02+0800	2025-03-04T14:50:02.147616+08:00 kingsley chfn[18652]: changed user 'poter' information
2025-03-04T14:50:00+0800	2025-03-04T14:50:00.222668+08:00 kingsley passwd[18647]: pam_unix(passwd:chauthtok): password changed for poter
2025-03-04T14:49:55+0800	2025-03-04T14:49:55.123642+08:00 kingsley useradd[18634]: new user: name=poter, UID=1004, GID=1004, home=/home/poter, shell=/bin/bash, from=/dev/pts/1
2025-03-04T14:49:55+0800	2025-03-04T14:49:55.110834+08:00 kingsley groupadd[18627]: new group: name=poter, GID=1004
2025-03-04T14:49:55+0800	2025-03-04T14:49:55.109772+08:00 kingsley groupadd[18627]: group added to /etc/gshadow: name=poter
2025-03-04T14:49:55+0800	2025-03-04T14:49:55.106918+08:00 kingsley groupadd[18627]: group added to /etc/group: name=poter, GID=1004
2025-03-04T14:49:55+0800	2025-03-04T14:49:55.063132+08:00 kingsley sudo: pam_unix(sudo:session): session opened for user root(uid=0) by kingsley(uid=1000)
2025-03-04T14:49:55+0800	2025-03-04T14:49:55.062555+08:00 kingsley sudo: kingsley : TTY=pts/0 ; PWD=/opt/splunk/bin ; USER=root ; COMMAND=/usr/sbin/adduser poter
2025-03-04T14:49:47+0800	2025-03-04T14:49:47.887265+08:00 claire sudo: pam_unix(sudo:session): session closed for user root
2025-03-04T14:49:47+0800	2025-03-04T14:49:47.886763+08:00 claire passwd[22689]: pam_unix(passwd:chauthtok): password changed for karen
2025-03-04T14:49:41+0800	2025-03-04T14:49:41.379705+08:00 claire sudo: pam_unix(sudo:session): session opened for user root(uid=0) by claire(uid=1000)
2025-03-04T14:49:41+0800	2025-03-04T14:49:41.379446+08:00 claire sudo: claire : TTY=pts/0 ; PWD=/home/claire ; USER=root ; COMMAND=/usr/bin/passwd karen
2025-03-04T14:49:38+0800	2025-03-04T14:49:38.818720+08:00 server systemd-logind[874]: New session 34 of user byron.
2025-03-04T14:49:38+0800	2025-03-04T14:49:38.815384+08:00 server sshd[7589]: pam_unix(sshd:session): session opened for user byron(uid=1000) by byron(uid=0)
2025-03-04T14:49:38+0800	2025-03-04T14:49:38.813724+08:00 server sshd[7589]: Accepted password for byron from 10.167.214.35 port 3648 ssh2
2025-03-04T14:49:30+0800	2025-03-04T14:49:30.311808+08:00 server sshd[7587]: Server listening on :: port 22.
2025-03-04T14:49:07+0800	2025-03-04T14:49:07.873042+08:00 kingsley sudo: pam_unix(sudo:session): session closed for user root
2025-03-04T14:49:07+0800	2025-03-04T14:49:07.872394+08:00 kingsley passwd[18614]: pam_unix(passwd:chauthtok): password changed for ariana

Time	Event
2025-03-04T14:49:04+0800	2025-03-04T14:49:04.937208+08:00 claire sudo: pam_unix(sudo:session): session closed for user root
2025-03-04T14:49:04+0800	2025-03-04T14:49:04.935292+08:00 claire gpasswd[22649]: members of group users set by root to kcy,karen
2025-03-04T14:49:03+0800	2025-03-04T14:49:03.143608+08:00 claire chfn[22637]: changed user 'karen' information
2025-03-04T14:49:01+0800	2025-03-04T14:49:01.196561+08:00 kingsley sudo: pam_unix(sudo:session): session opened for user root(uid=0) by kingsley(uid=1000)
2025-03-04T14:49:01+0800	2025-03-04T14:49:01.196032+08:00 kingsley sudo: kingsley : TTY=pts/0 ; PWD=/opt/splunk/bin ; USER= root ; COMMAND=/usr/bin/passwd ariana
2025-03-04T14:49:01+0800	2025-03-04T14:49:01.174872+08:00 claire passwd[22628]: pam_unix(passwd:chauthtok): password changed for karen
2025-03-04T14:48:58+0800	2025-03-04T14:48:58.518010+08:00 judy-VirtualBox systemd-logind[1033]: New session 20 of user judy.
2025-03-04T14:48:58+0800	2025-03-04T14:48:58.515220+08:00 judy-VirtualBox sshd[15091]: pam_unix(sshd:session): session opened for user judy(uid=1000) by judy(uid=0)
2025-03-04T14:48:58+0800	2025-03-04T14:48:58.513972+08:00 judy-VirtualBox sshd[15091]: Accepted password for judy from 10.167.214.40 port 12888 ssh2
2025-03-04T14:48:56+0800	2025-03-04T14:48:56.880971+08:00 judy-VirtualBox sshd[15089]: Server listening on :: port 22.
2025-03-04T14:48:54+0800	2025-03-04T14:48:54.526241+08:00 claire useradd[22615]: new user: name=karen, UID=1003, GID=1003, home=/home/karen, shell=/bin/bash, from=/dev/pts/1
2025-03-04T14:48:54+0800	2025-03-04T14:48:54.445836+08:00 claire groupadd[22608]: new group: name=karen, GID=1003
2025-03-04T14:48:54+0800	2025-03-04T14:48:54.444903+08:00 claire groupadd[22608]: group added to /etc/gshadow: name=karen
2025-03-04T14:48:54+0800	2025-03-04T14:48:54.440878+08:00 claire groupadd[22608]: group added to /etc/group: name=karen, GID=1003
2025-03-04T14:48:54+0800	2025-03-04T14:48:54.043541+08:00 claire sudo: pam_unix(sudo:session): session opened for user root(uid=0) by claire(uid=1000)
2025-03-04T14:48:53+0800	2025-03-04T14:48:53.978544+08:00 claire sudo: claire : TTY=pts/0 ; PWD=/home/claire ; USER=root ; COMMAND=/usr/sbin/adduser karen
2025-03-04T14:48:44+0800	2025-03-04T14:48:44.283032+08:00 andrew mongod: looking for plugins in '/home/build/build-home/opt/mongo/ lib/sasl2', failed to open directory, error: No such file or directory
2025-03-04T14:48:43+0800	2025-03-04T14:48:43.756287+08:00 andrew mongod: looking for plugins in '/home/build/build-home/opt/mongo/ lib/sasl2', failed to open directory, error: No such file or directory
2025-03-04T14:48:41+0800	2025-03-04T14:48:41.744449+08:00 hostname su[17328]: FAILED SU (to root) sam on pts/0
2025-03-04T14:48:39+0800	2025-03-04T14:48:39.579102+08:00 hostname su: pam_unix(su-l:auth): authentication failure; logname=sam uid= 1000 euid=0 tty=/dev/pts/0 ruser=sam rhost= user=root
2025-03-04T14:48:29+0800	2025-03-04T14:48:29.910947+08:00 hostname su[17312]: FAILED SU (to root) sam on pts/0
2025-03-04T14:48:28+0800	2025-03-04T14:48:28.485620+08:00 server mongod: looking for plugins in '/home/build/build-home/opt/mongo/lib /sasl2', failed to open directory, error: No such file or directory
2025-03-04T14:48:28+0800	2025-03-04T14:48:28.485466+08:00 server mongod: looking for plugins in '/home/build/build-home/opt/mongo/lib /sasl2', failed to open directory, error: No such file or directory
2025-03-04T14:48:27+0800	2025-03-04T14:48:27.979749+08:00 hostname su: pam_unix(su-l:auth): authentication failure; logname=sam uid= 1000 euid=0 tty=/dev/pts/0 ruser=sam rhost= user=root
2025-03-04T14:47:59+0800	2025-03-04T14:47:59.848132+08:00 kingsley sudo: pam_unix(sudo:session): session closed for user root
2025-03-04T14:47:59+0800	2025-03-04T14:47:59.845770+08:00 kingsley gpasswd[18586]: members of group users set by root to kartrina,ariana
2025-03-04T14:47:59+0800	2025-03-04T14:47:59.325250+08:00 kingsley chfn[18578]: changed user 'ariana' information
2025-03-04T14:47:52+0800	2025-03-04T14:47:52.026484+08:00 kingsley passwd[18575]: pam_unix(passwd:chauthtok): password changed for ariana
2025-03-04T14:47:44+0800	2025-03-04T14:47:44.160802+08:00 kingsley useradd[18562]: new user: name=ariana, UID=1003, GID=1003, home=/home/ariana, shell=/bin/bash, from=/dev/pts/1
2025-03-04T14:47:44+0800	2025-03-04T14:47:44.094727+08:00 kingsley groupadd[18555]: new group: name=ariana, GID=1003
2025-03-04T14:47:44+0800	2025-03-04T14:47:44.093756+08:00 kingsley groupadd[18555]: group added to /etc/gshadow: name=ariana
2025-03-04T14:47:44+0800	2025-03-04T14:47:44.089309+08:00 kingsley groupadd[18555]: group added to /etc/group: name=ariana, GID=1003
2025-03-04T14:47:43+0800	2025-03-04T14:47:43.737797+08:00 kingsley sudo: pam_unix(sudo:session): session opened for user root(uid=0) by kingsley(uid=1000)
2025-03-04T14:47:43+0800	2025-03-04T14:47:43.724648+08:00 kingsley sudo: kingsley : TTY=pts/0 ; PWD=/opt/splunk/bin ; USER= root ; COMMAND=/usr/sbin/adduser ariana
2025-03-04T14:47:36+0800	2025-03-04T14:47:36.369882+08:00 claire mongod: looking for plugins in '/home/build/build-home/opt/mongo/lib/ sasl2', failed to open directory, error: No such file or directory
2025-03-04T14:47:36+0800	2025-03-04T14:47:36.365897+08:00 claire mongod: looking for plugins in '/home/build/build-home/opt/mongo/lib/ sasl2', failed to open directory, error: No such file or directory
2025-03-04T14:46:42+0800	2025-03-04T14:46:42.972431+08:00 kingsley mongod: looking for plugins in '/home/build/build-home/opt/mongo/ lib/sasl2', failed to open directory, error: No such file or directory
2025-03-04T14:46:42+0800	2025-03-04T14:46:42.972303+08:00 kingsley mongod: looking for plugins in '/home/build/build-home/opt/mongo/ lib/sasl2', failed to open directory, error: No such file or directory
2025-03-04T14:45:01+0800	2025-03-04T14:45:01.614330+08:00 andrew CRON[4571]: pam_unix(cron:session): session closed for user root
2025-03-04T14:45:01+0800	2025-03-04T14:45:01.526326+08:00 andrew CRON[4571]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
2025-03-04T14:45:01+0800	2025-03-04T14:45:01.389726+08:00 judy-VirtualBox CRON[14254]: pam_unix(cron:session): session closed for user root
2025-03-04T14:45:01+0800	2025-03-04T14:45:01.385325+08:00 judy-VirtualBox CRON[14254]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)

Time	Event
2025-03-04T14:45:01+0800	2025-03-04T14:45:01.269970+08:00 claire CRON[21705]: pam_unix(cron:session): session closed for user root
2025-03-04T14:45:01+0800	2025-03-04T14:45:01.268467+08:00 claire CRON[21705]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
2025-03-04T14:45:01+0800	2025-03-04T14:45:01.131878+08:00 hostname CRON[17203]: pam_unix(cron:session): session closed for user root
2025-03-04T14:45:01+0800	2025-03-04T14:45:01.130376+08:00 hostname CRON[17203]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
2025-03-04T14:44:30+0800	2025-03-04T14:44:30.904474+08:00 judy-VirtualBox mongod: looking for plugins in '/home/build/build-home/opt/mongo/lib/sasl2', failed to open directory, error: No such file or directory
2025-03-04T14:44:30+0800	2025-03-04T14:44:30.902624+08:00 judy-VirtualBox mongod: looking for plugins in '/home/build/build-home/opt/mongo/lib/sasl2', failed to open directory, error: No such file or directory
2025-03-04T14:44:27+0800	2025-03-04T14:44:27.844266+08:00 judy-VirtualBox gdm-password]: gkr-pam: unlocked login keyring
2025-03-04T14:42:37+0800	2025-03-04T14:42:37.378137+08:00 judy-VirtualBox CRON[13082]: pam_unix(cron:session): session closed for user root
2025-03-04T14:42:37+0800	2025-03-04T14:42:37.376920+08:00 judy-VirtualBox CRON[13082]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
2025-03-04T14:39:01+0800	2025-03-04T14:39:01.517610+08:00 andrew CRON[4432]: pam_unix(cron:session): session closed for user root
2025-03-04T14:39:01+0800	2025-03-04T14:39:01.491182+08:00 andrew CRON[4432]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
2025-03-04T14:35:01+0800	2025-03-04T14:35:01.475529+08:00 andrew CRON[4391]: pam_unix(cron:session): session closed for user root
2025-03-04T14:35:01+0800	2025-03-04T14:35:01.473942+08:00 andrew CRON[4391]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
2025-03-04T14:35:01+0800	2025-03-04T14:35:01.198429+08:00 claire CRON[21516]: pam_unix(cron:session): session closed for user root
2025-03-04T14:35:01+0800	2025-03-04T14:35:01.196162+08:00 claire CRON[21516]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
2025-03-04T14:35:01+0800	2025-03-04T14:35:01.119713+08:00 hostname CRON[17089]: pam_unix(cron:session): session closed for user root
2025-03-04T14:35:01+0800	2025-03-04T14:35:01.118267+08:00 hostname CRON[17089]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
2025-03-04T14:25:01+0800	2025-03-04T14:25:01.416563+08:00 andrew CRON[4279]: pam_unix(cron:session): session closed for user root
2025-03-04T14:25:01+0800	2025-03-04T14:25:01.414582+08:00 andrew CRON[4279]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
2025-03-04T14:25:01+0800	2025-03-04T14:25:01.109204+08:00 hostname CRON[16900]: pam_unix(cron:session): session closed for user root
2025-03-04T14:25:01+0800	2025-03-04T14:25:01.107763+08:00 hostname CRON[16900]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
2025-03-04T14:25:01+0800	2025-03-04T14:25:01.100308+08:00 claire CRON[21409]: pam_unix(cron:session): session closed for user root
2025-03-04T14:25:01+0800	2025-03-04T14:25:01.097298+08:00 claire CRON[21409]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
2025-03-04T14:17:01+0800	2025-03-04T14:17:01.377903+08:00 andrew CRON[4189]: pam_unix(cron:session): session closed for user root
2025-03-04T14:17:01+0800	2025-03-04T14:17:01.353100+08:00 andrew CRON[4189]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
2025-03-04T14:17:01+0800	2025-03-04T14:17:01.097658+08:00 hostname CRON[16805]: pam_unix(cron:session): session closed for user root
2025-03-04T14:17:01+0800	2025-03-04T14:17:01.093373+08:00 hostname CRON[16805]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
2025-03-04T14:17:01+0800	2025-03-04T14:17:01.043889+08:00 claire CRON[21271]: pam_unix(cron:session): session closed for user root
2025-03-04T14:17:01+0800	2025-03-04T14:17:01.021653+08:00 claire CRON[21271]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
2025-03-04T14:15:02+0800	2025-03-04T14:15:02.008168+08:00 claire CRON[21226]: pam_unix(cron:session): session closed for user root
2025-03-04T14:15:02+0800	2025-03-04T14:15:02.006644+08:00 claire CRON[21226]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
2025-03-04T14:15:01+0800	2025-03-04T14:15:01.381052+08:00 andrew CRON[4010]: pam_unix(cron:session): session closed for user root
2025-03-04T14:15:01+0800	2025-03-04T14:15:01.336440+08:00 andrew CRON[4010]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
2025-03-04T14:15:01+0800	2025-03-04T14:15:01.086392+08:00 hostname CRON[16712]: pam_unix(cron:session): session closed for user root
2025-03-04T14:15:01+0800	2025-03-04T14:15:01.083266+08:00 hostname CRON[16712]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
2025-03-04T14:09:01+0800	2025-03-04T14:09:01.299268+08:00 andrew CRON[3852]: pam_unix(cron:session): session closed for user root
2025-03-04T14:09:01+0800	2025-03-04T14:09:01.280035+08:00 andrew CRON[3852]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
2025-03-04T14:05:01+0800	2025-03-04T14:05:01.941641+08:00 claire CRON[21040]: pam_unix(cron:session): session closed for user root
2025-03-04T14:05:01+0800	2025-03-04T14:05:01.940266+08:00 claire CRON[21040]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
2025-03-04T14:05:01+0800	2025-03-04T14:05:01.243475+08:00 andrew CRON[3808]: pam_unix(cron:session): session closed for user root
2025-03-04T14:05:01+0800	2025-03-04T14:05:01.241714+08:00 andrew CRON[3808]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
2025-03-04T14:05:01+0800	2025-03-04T14:05:01.070385+08:00 hostname CRON[16607]: pam_unix(cron:session): session closed for user root
2025-03-04T14:05:01+0800	2025-03-04T14:05:01.068913+08:00 hostname CRON[16607]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
2025-03-04T13:55:15+0800	2025-03-04T13:55:15.856613+08:00 claire CRON[20934]: pam_unix(cron:session): session closed for user root
2025-03-04T13:55:15+0800	2025-03-04T13:55:15.851535+08:00 claire CRON[20934]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
2025-03-04T13:55:01+0800	2025-03-04T13:55:01.209164+08:00 andrew CRON[3691]: pam_unix(cron:session): session closed for user root
2025-03-04T13:55:01+0800	2025-03-04T13:55:01.205794+08:00 andrew CRON[3691]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
2025-03-04T13:55:01+0800	2025-03-04T13:55:01.054531+08:00 hostname CRON[16422]: pam_unix(cron:session): session closed for user root
2025-03-04T13:55:01+0800	2025-03-04T13:55:01.053007+08:00 hostname CRON[16422]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
2025-03-04T13:45:01+0800	2025-03-04T13:45:01.108462+08:00 claire CRON[20792]: pam_unix(cron:session): session closed for user root

Time	Event
2025-03-04T13:45:01+0800	2025-03-04T13:45:01.102716+08:00 claire CRON[20792]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
2025-03-04T13:45:01+0800	2025-03-04T13:45:01.037308+08:00 hostname CRON[16317]: pam_unix(cron:session): session closed for user root
2025-03-04T13:45:01+0800	2025-03-04T13:45:01.034348+08:00 hostname CRON[16317]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
2025-03-04T13:35:01+0800	2025-03-04T13:35:01.383338+08:00 judy-VirtualBox CRON[12913]: pam_unix(cron:session): session closed for user root
2025-03-04T13:35:01+0800	2025-03-04T13:35:01.348178+08:00 judy-VirtualBox CRON[12913]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
2025-03-04T13:35:01+0800	2025-03-04T13:35:01.022717+08:00 claire CRON[20606]: pam_unix(cron:session): session closed for user root
2025-03-04T13:35:01+0800	2025-03-04T13:35:01.021220+08:00 claire CRON[20606]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
2025-03-04T13:35:01+0800	2025-03-04T13:35:01.019641+08:00 hostname CRON[16211]: pam_unix(cron:session): session closed for user root
2025-03-04T13:35:01+0800	2025-03-04T13:35:01.016303+08:00 hostname CRON[16211]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
2025-03-04T13:30:01+0800	2025-03-04T13:30:01.341558+08:00 judy-VirtualBox CRON[12275]: pam_unix(cron:session): session closed for user root
2025-03-04T13:30:01+0800	2025-03-04T13:30:01.312974+08:00 judy-VirtualBox CRON[12275]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
2025-03-04T13:25:02+0800	2025-03-04T13:25:02.008938+08:00 hostname CRON[16027]: pam_unix(cron:session): session closed for user root
2025-03-04T13:25:02+0800	2025-03-04T13:25:02.004898+08:00 hostname CRON[16027]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
2025-03-04T13:25:01+0800	2025-03-04T13:25:01.921140+08:00 claire CRON[20498]: pam_unix(cron:session): session closed for user root
2025-03-04T13:25:01+0800	2025-03-04T13:25:01.917793+08:00 claire CRON[20498]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
2025-03-04T13:25:01+0800	2025-03-04T13:25:01.277855+08:00 judy-VirtualBox CRON[11948]: pam_unix(cron:session): session closed for user root
2025-03-04T13:25:01+0800	2025-03-04T13:25:01.276322+08:00 judy-VirtualBox CRON[11948]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
2025-03-04T13:17:02+0800	2025-03-04T13:17:02.019466+08:00 hostname CRON[15941]: pam_unix(cron:session): session closed for user root
2025-03-04T13:17:01+0800	2025-03-04T13:17:01.988861+08:00 hostname CRON[15941]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
2025-03-04T13:17:01+0800	2025-03-04T13:17:01.840427+08:00 claire CRON[20399]: pam_unix(cron:session): session closed for user root
2025-03-04T13:17:01+0800	2025-03-04T13:17:01.832706+08:00 claire CRON[20399]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
2025-03-04T13:17:01+0800	2025-03-04T13:17:01.267801+08:00 judy-VirtualBox CRON[11347]: pam_unix(cron:session): session closed for user root
2025-03-04T13:17:01+0800	2025-03-04T13:17:01.263488+08:00 judy-VirtualBox CRON[11347]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
2025-03-04T13:15:01+0800	2025-03-04T13:15:01.980374+08:00 hostname CRON[15849]: pam_unix(cron:session): session closed for user root
2025-03-04T13:15:01+0800	2025-03-04T13:15:01.977384+08:00 hostname CRON[15849]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
2025-03-04T13:15:01+0800	2025-03-04T13:15:01.810131+08:00 claire CRON[20287]: pam_unix(cron:session): session closed for user root
2025-03-04T13:15:01+0800	2025-03-04T13:15:01.808739+08:00 claire CRON[20287]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
2025-03-04T13:15:01+0800	2025-03-04T13:15:01.256576+08:00 judy-VirtualBox CRON[11172]: pam_unix(cron:session): session closed for user root
2025-03-04T13:15:01+0800	2025-03-04T13:15:01.250280+08:00 judy-VirtualBox CRON[11172]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
2025-03-04T13:08:20+0800	2025-03-04T13:08:20.488802+08:00 claire mongod: looking for plugins in '/home/build/build-home/opt/mongo/lib/sasl2', failed to open directory, error: No such file or directory
2025-03-04T13:08:20+0800	2025-03-04T13:08:20.488684+08:00 claire mongod: looking for plugins in '/home/build/build-home/opt/mongo/lib/sasl2', failed to open directory, error: No such file or directory
2025-03-04T13:05:01+0800	2025-03-04T13:05:01.962910+08:00 hostname CRON[15741]: pam_unix(cron:session): session closed for user root
2025-03-04T13:05:01+0800	2025-03-04T13:05:01.955808+08:00 hostname CRON[15741]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
2025-03-04T13:05:01+0800	2025-03-04T13:05:01.211306+08:00 judy-VirtualBox CRON[10490]: pam_unix(cron:session): session closed for user root
2025-03-04T13:05:01+0800	2025-03-04T13:05:01.182596+08:00 judy-VirtualBox CRON[10490]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
2025-03-04T12:57:39+0800	2025-03-04T12:57:39.833133+08:00 judy-VirtualBox dbus-daemon[1002]: [system] Failed to activate service 'org.bluez': timed out (service_start_timeout=25000ms)
2025-03-04T12:55:01+0800	2025-03-04T12:55:01.937782+08:00 hostname CRON[15544]: pam_unix(cron:session): session closed for user root
2025-03-04T12:55:01+0800	2025-03-04T12:55:01.936373+08:00 hostname CRON[15544]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
2025-03-04T12:55:01+0800	2025-03-04T12:55:01.155928+08:00 judy-VirtualBox CRON[9694]: pam_unix(cron:session): session closed for user root
2025-03-04T12:55:01+0800	2025-03-04T12:55:01.154098+08:00 judy-VirtualBox CRON[9694]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
2025-03-04T12:45:01+0800	2025-03-04T12:45:01.921325+08:00 hostname CRON[15439]: pam_unix(cron:session): session closed for user root
2025-03-04T12:45:01+0800	2025-03-04T12:45:01.919811+08:00 hostname CRON[15439]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
2025-03-04T12:45:01+0800	2025-03-04T12:45:01.064511+08:00 judy-VirtualBox CRON[8785]: pam_unix(cron:session): session closed for user root
2025-03-04T12:45:01+0800	2025-03-04T12:45:01.059433+08:00 judy-VirtualBox CRON[8785]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
2025-03-04T12:35:01+0800	2025-03-04T12:35:01.903444+08:00 hostname CRON[15334]: pam_unix(cron:session): session closed for user root

Time	Event
2025-03-04T12:35:01+0800	2025-03-04T12:35:01.896893+08:00 hostname CRON[15334]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
2025-03-04T12:35:01+0800	2025-03-04T12:35:01.029682+08:00 judy-VirtualBox CRON[8170]: pam_unix(cron:session): session closed for user root
2025-03-04T12:35:01+0800	2025-03-04T12:35:01.027757+08:00 judy-VirtualBox CRON[8170]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
2025-03-04T12:30:02+0800	2025-03-04T12:30:02.191117+08:00 judy-VirtualBox CRON[7798]: pam_unix(cron:session): session closed for user root
2025-03-04T12:30:02+0800	2025-03-04T12:30:02.008342+08:00 judy-VirtualBox CRON[7798]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
2025-03-04T12:25:01+0800	2025-03-04T12:25:01.986880+08:00 judy-VirtualBox CRON[7515]: pam_unix(cron:session): session closed for user root
2025-03-04T12:25:01+0800	2025-03-04T12:25:01.967077+08:00 judy-VirtualBox CRON[7515]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
2025-03-04T12:25:01+0800	2025-03-04T12:25:01.936472+08:00 hostname CRON[15157]: pam_unix(cron:session): session closed for user root
2025-03-04T12:25:01+0800	2025-03-04T12:25:01.880258+08:00 hostname CRON[15157]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
2025-03-04T12:17:01+0800	2025-03-04T12:17:01.919116+08:00 judy-VirtualBox CRON[7040]: pam_unix(cron:session): session closed for user root
2025-03-04T12:17:01+0800	2025-03-04T12:17:01.870228+08:00 hostname CRON[15068]: pam_unix(cron:session): session closed for user root
2025-03-04T12:17:01+0800	2025-03-04T12:17:01.866492+08:00 hostname CRON[15068]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
2025-03-04T12:17:01+0800	2025-03-04T12:17:01.803927+08:00 judy-VirtualBox CRON[7040]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
2025-03-04T12:15:01+0800	2025-03-04T12:15:01.856871+08:00 hostname CRON[14958]: pam_unix(cron:session): session closed for user root
2025-03-04T12:15:01+0800	2025-03-04T12:15:01.854024+08:00 hostname CRON[14958]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
2025-03-04T12:15:01+0800	2025-03-04T12:15:01.796529+08:00 judy-VirtualBox CRON[6823]: pam_unix(cron:session): session closed for user root
2025-03-04T12:15:01+0800	2025-03-04T12:15:01.794329+08:00 judy-VirtualBox CRON[6823]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
2025-03-04T12:05:01+0800	2025-03-04T12:05:01.841044+08:00 hostname CRON[14842]: pam_unix(cron:session): session closed for user root
2025-03-04T12:05:01+0800	2025-03-04T12:05:01.837966+08:00 hostname CRON[14842]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
2025-03-04T12:05:01+0800	2025-03-04T12:05:01.736224+08:00 judy-VirtualBox CRON[6070]: pam_unix(cron:session): session closed for user root
2025-03-04T12:05:01+0800	2025-03-04T12:05:01.648913+08:00 judy-VirtualBox CRON[6070]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
2025-03-04T12:04:52+0800	2025-03-04T12:04:52.162630+08:00 judy-VirtualBox mongod: looking for plugins in '/home/build/build-home/opt/mongo/lib/sasl2', failed to open directory, error: No such file or directory
2025-03-04T12:04:52+0800	2025-03-04T12:04:52.162527+08:00 judy-VirtualBox mongod: looking for plugins in '/home/build/build-home/opt/mongo/lib/sasl2', failed to open directory, error: No such file or directory
2025-03-04T12:03:01+0800	2025-03-04T12:03:01.248302+08:00 judy-VirtualBox dbus-daemon[1002]: [system] Failed to activate service 'org.bluez': timed out (service_start_timeout=25000ms)
2025-03-04T12:02:40+0800	2025-03-04T12:02:40.497404+08:00 judy-VirtualBox gnome-keyring-daemon[2486]: asked to register item /org/freedesktop/secrets/collection/login/1, but it's already registered
2025-03-04T12:02:15+0800	2025-03-04T12:02:15.920523+08:00 judy-VirtualBox pkexec[4678]: judy: Executing command [USER=root] [TTY=unknown] [CWD=/home/judy] [COMMAND=/usr/lib/update-notifier/package-system-locked]
2025-03-04T12:02:15+0800	2025-03-04T12:02:15.919663+08:00 judy-VirtualBox pkexec: pam_unix(polkit-1:session): session opened for user root(uid=0) by judy(uid=1000)
2025-03-04T12:02:13+0800	2025-03-04T12:02:13.072196+08:00 judy-VirtualBox sudo: pam_unix(sudo:session): session closed for user root
2025-03-04T12:02:01+0800	2025-03-04T12:02:01.547995+08:00 judy-VirtualBox mongod: looking for plugins in '/home/build/build-home/opt/mongo/lib/sasl2', failed to open directory, error: No such file or directory
2025-03-04T12:02:01+0800	2025-03-04T12:02:01.547719+08:00 judy-VirtualBox mongod: looking for plugins in '/home/build/build-home/opt/mongo/lib/sasl2', failed to open directory, error: No such file or directory
2025-03-04T12:01:40+0800	2025-03-04T12:01:40.980059+08:00 hostname mongod: looking for plugins in '/home/build/build-home/opt/mongo/lib/sasl2', failed to open directory, error: No such file or directory
2025-03-04T12:01:40+0800	2025-03-04T12:01:40.979412+08:00 hostname mongod: looking for plugins in '/home/build/build-home/opt/mongo/lib/sasl2', failed to open directory, error: No such file or directory
2025-03-04T12:01:30+0800	2025-03-04T12:01:30.584144+08:00 judy-VirtualBox sudo: pam_unix(sudo:session): session opened for user root(uid=0) by judy(uid=1000)
2025-03-04T12:01:30+0800	2025-03-04T12:01:30.583892+08:00 judy-VirtualBox sudo: judy : TTY=pts/0 ; PWD=/home/judy ; USER=root ; COMMAND=/opt/splunk/bin/./splunk start
2025-03-04T12:01:15+0800	2025-03-04T12:01:15.352764+08:00 judy-VirtualBox (sd-pam): pam_unix(systemd-user:session): session closed for user gdm
2025-03-04T12:01:05+0800	2025-03-04T12:01:05.183418+08:00 judy-VirtualBox systemd-logind[1033]: Removed session c1.
2025-03-04T12:01:02+0800	2025-03-04T12:01:02.681941+08:00 judy-VirtualBox polkitd[1021]: Unregistered Authentication Agent for unix-session:c1 (system bus name :1.39, object path /org/freedesktop/PolicyKit1/AuthenticationAgent, locale zh_TW.UTF-8) (disconnected from bus)
2025-03-04T12:01:02+0800	2025-03-04T12:01:02.666987+08:00 judy-VirtualBox systemd-logind[1033]: Session c1 logged out. Waiting for processes to exit.
2025-03-04T12:01:02+0800	2025-03-04T12:01:02.659866+08:00 judy-VirtualBox gdm-launch-environment]: pam_unix(gdm-launch-environment:session): session closed for user gdm

Time	Event
2025-03-04T12:00:57+0800	2025-03-04T12:00:57.229981+08:00 judy-VirtualBox polkitd[1021]: Registered Authentication Agent for unix-session: 2 (system bus name :1.76 [/usr/bin/gnome-shell], object path /org/freedesktop/PolicyKit1/AuthenticationAgent, locale zh_TW.UTF-8)
2025-03-04T12:00:54+0800	2025-03-04T12:00:54.300243+08:00 judy-VirtualBox gnome-keyring-daemon[2730]: discover_other_daemon: 1
2025-03-04T12:00:54+0800	2025-03-04T12:00:54.297858+08:00 judy-VirtualBox gnome-keyring-daemon[2729]: discover_other_daemon: 1
2025-03-04T12:00:54+0800	2025-03-04T12:00:54.297844+08:00 judy-VirtualBox gnome-keyring-daemon[2486]: The PKCS#11 component was already initialized
2025-03-04T12:00:54+0800	2025-03-04T12:00:54.296994+08:00 judy-VirtualBox gnome-keyring-daemon[2726]: discover_other_daemon: 1
2025-03-04T12:00:54+0800	2025-03-04T12:00:54.296838+08:00 judy-VirtualBox gnome-keyring-daemon[2486]: The Secret Service was already initialized
2025-03-04T12:00:51+0800	2025-03-04T12:00:51.723422+08:00 judy-VirtualBox gdm-password]: gkr-pam: unlocked login keyring
2025-03-04T12:00:50+0800	2025-03-04T12:00:50.791899+08:00 judy-VirtualBox (systemd): pam_unix(systemd-user:session): session opened for user judy(uid=1000) by judy(uid=0)
2025-03-04T12:00:50+0800	2025-03-04T12:00:50.776148+08:00 judy-VirtualBox systemd-logind[1033]: New session 2 of user judy.
2025-03-04T12:00:50+0800	2025-03-04T12:00:50.686627+08:00 judy-VirtualBox gdm-password]: pam_unix(gdm-password:session): session opened for user judy(uid=1000) by judy(uid=0)
2025-03-04T12:00:50+0800	2025-03-04T12:00:50.589757+08:00 judy-VirtualBox gdm-password]: gkr-pam: stashed password to try later in open session
2025-03-04T12:00:50+0800	2025-03-04T12:00:50.589618+08:00 judy-VirtualBox gdm-password]: gkr-pam: unable to locate daemon control file
2025-03-04T11:59:40+0800	2025-03-04T11:59:40.029038+08:00 judy-VirtualBox polkitd[1021]: Registered Authentication Agent for unix-session: c1 (system bus name :1.39 [/usr/bin/gnome-shell], object path /org/freedesktop/PolicyKit1/AuthenticationAgent, locale zh_TW.UTF-8)
2025-03-04T11:59:09+0800	2025-03-04T11:59:09.897529+08:00 judy-VirtualBox (systemd): pam_unix(systemd-user:session): session opened for user gdm(uid=120) by gdm(uid=0)
2025-03-04T11:59:09+0800	2025-03-04T11:59:09.680146+08:00 judy-VirtualBox systemd-logind[1033]: New session c1 of user gdm.
2025-03-04T11:59:09+0800	2025-03-04T11:59:09.446040+08:00 judy-VirtualBox gdm-launch-environment]: pam_unix(gdm-launch-environment: session): session opened for user gdm(uid=120) by (uid=0)
2025-03-04T11:58:55+0800	2025-03-04T11:58:55.957714+08:00 judy-VirtualBox polkitd[1021]: Acquired the name org.freedesktop.PolicyKit1 on the system bus
2025-03-04T11:58:55+0800	2025-03-04T11:58:55.956858+08:00 judy-VirtualBox polkitd[1021]: Finished loading, compiling and executing 16 rules
2025-03-04T11:58:55+0800	2025-03-04T11:58:55.601102+08:00 judy-VirtualBox polkitd[1021]: Loading rules from directory /usr/share/polkit-1/rules.d
2025-03-04T11:58:55+0800	2025-03-04T11:58:55.585730+08:00 judy-VirtualBox polkitd[1021]: Loading rules from directory /etc/polkit-1/rules.d
2025-03-04T11:58:54+0800	2025-03-04T11:58:54.647192+08:00 judy-VirtualBox systemd-logind[1033]: Watching system buttons on /dev/input/event2 (AT Translated Set 2 keyboard)
2025-03-04T11:58:54+0800	2025-03-04T11:58:54.647190+08:00 judy-VirtualBox systemd-logind[1033]: Watching system buttons on /dev/input/event1 (Sleep Button)
2025-03-04T11:58:54+0800	2025-03-04T11:58:54.647188+08:00 judy-VirtualBox systemd-logind[1033]: Watching system buttons on /dev/input/event0 (Power Button)
2025-03-04T11:58:54+0800	2025-03-04T11:58:54.647183+08:00 judy-VirtualBox systemd-logind[1033]: New seat seat0.
2025-03-04T11:46:38+0800	2025-03-04T11:46:38.343952+08:00 judy-VirtualBox gdm-password]: pam_unix(gdm-password:session): session closed for user judy
2025-03-04T11:46:38+0800	2025-03-04T11:46:38.335157+08:00 judy-VirtualBox systemd-logind[1035]: System is powering down.
2025-03-04T11:46:37+0800	2025-03-04T11:46:37.856262+08:00 judy-VirtualBox systemd-logind[1035]: The system will power off now!
2025-03-04T11:46:37+0800	2025-03-04T11:46:37.847840+08:00 judy-VirtualBox systemd-logind[1035]: Power key pressed short.
2025-03-04T11:45:13+0800	2025-03-04T11:45:13.391190+08:00 judy-VirtualBox CRON[3655]: pam_unix(cron:session): session closed for user root
2025-03-04T11:45:12+0800	2025-03-04T11:45:12.848149+08:00 judy-VirtualBox CRON[3655]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
2025-03-04T11:35:01+0800	2025-03-04T11:35:01.161661+08:00 judy-VirtualBox CRON[3635]: pam_unix(cron:session): session closed for user root
2025-03-04T11:35:01+0800	2025-03-04T11:35:01.147554+08:00 judy-VirtualBox CRON[3635]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
2025-03-04T11:30:01+0800	2025-03-04T11:30:01.143654+08:00 judy-VirtualBox CRON[3617]: pam_unix(cron:session): session closed for user root
2025-03-04T11:30:01+0800	2025-03-04T11:30:01.120628+08:00 judy-VirtualBox CRON[3617]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
2025-03-04T11:25:01+0800	2025-03-04T11:25:01.202371+08:00 judy-VirtualBox CRON[3605]: pam_unix(cron:session): session closed for user root
2025-03-04T11:25:01+0800	2025-03-04T11:25:01.095160+08:00 judy-VirtualBox CRON[3605]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
2025-03-04T11:17:01+0800	2025-03-04T11:17:01.051711+08:00 judy-VirtualBox CRON[3546]: pam_unix(cron:session): session closed for user root
2025-03-04T11:17:01+0800	2025-03-04T11:17:01.026694+08:00 judy-VirtualBox CRON[3546]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
2025-03-04T11:15:45+0800	2025-03-04T11:15:45.363034+08:00 judy-VirtualBox pkexec[3518]: judy: Executing command [USER=root] [TTY=unknown] [CWD=/home/judy] [COMMAND=/usr/lib/update-notifier/package-system-locked]
2025-03-04T11:15:45+0800	2025-03-04T11:15:45.361783+08:00 judy-VirtualBox pkexec: pam_unix(polkit-1:session): session opened for user root(uid=0) by judy(uid=1000)
2025-03-04T11:15:03+0800	2025-03-04T11:15:03.012845+08:00 judy-VirtualBox CRON[3444]: pam_unix(cron:session): session closed for user root

Time	Event
2025-03-04T11:15:02+0800	2025-03-04T11:15:02.967840+08:00 judy-VirtualBox CRON[3444]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
2025-03-04T11:14:56+0800	2025-03-04T11:14:56.066921+08:00 judy-VirtualBox (sd-pam): pam_unix(systemd-user:session): session closed for user gdm
2025-03-04T11:14:45+0800	2025-03-04T11:14:45.823933+08:00 judy-VirtualBox systemd-logind[1035]: Removed session c1.
2025-03-04T11:14:45+0800	2025-03-04T11:14:45.416936+08:00 judy-VirtualBox polkitd[1026]: Unregistered Authentication Agent for unix-session :c1 (system bus name :1.39, object path /org/freedesktop/PolicyKit1/AuthenticationAgent, locale zh_TW.UTF-8) (disconnected from bus)
2025-03-04T11:14:45+0800	2025-03-04T11:14:45.407887+08:00 judy-VirtualBox systemd-logind[1035]: Session c1 logged out. Waiting for processes to exit.
2025-03-04T11:14:45+0800	2025-03-04T11:14:45.401771+08:00 judy-VirtualBox gdm-launch-environment]: pam_unix(gdm-launch-environment: session): session closed for user gdm
2025-03-04T11:14:43+0800	2025-03-04T11:14:43.468421+08:00 judy-VirtualBox polkitd[1026]: Registered Authentication Agent for unix-session: 2 (system bus name :1.77 [/usr/bin/gnome-shell], object path /org/freedesktop/PolicyKit1/AuthenticationAgent, locale zh_TW.UTF-8)
2025-03-04T11:14:40+0800	2025-03-04T11:14:40.586900+08:00 judy-VirtualBox gnome-keyring-daemon[2547]: discover_other_daemon: 1
2025-03-04T11:14:40+0800	2025-03-04T11:14:40.584247+08:00 judy-VirtualBox gnome-keyring-daemon[2546]: discover_other_daemon: 1
2025-03-04T11:14:40+0800	2025-03-04T11:14:40.584070+08:00 judy-VirtualBox gnome-keyring-daemon[2311]: The PKCS#11 component was already initialized
2025-03-04T11:14:40+0800	2025-03-04T11:14:40.583069+08:00 judy-VirtualBox gnome-keyring-daemon[2541]: discover_other_daemon: 1
2025-03-04T11:14:40+0800	2025-03-04T11:14:40.582800+08:00 judy-VirtualBox gnome-keyring-daemon[2311]: The Secret Service was already initialized
2025-03-04T11:14:38+0800	2025-03-04T11:14:38.486040+08:00 judy-VirtualBox gdm-password]: gkr-pam: unlocked login keyring
2025-03-04T11:14:37+0800	2025-03-04T11:14:37.813099+08:00 judy-VirtualBox (systemd): pam_unix(systemd-user:session): session opened for user judy(uid=1000) by judy(uid=0)
2025-03-04T11:14:37+0800	2025-03-04T11:14:37.781347+08:00 judy-VirtualBox systemd-logind[1035]: New session 2 of user judy.
2025-03-04T11:14:37+0800	2025-03-04T11:14:37.762752+08:00 judy-VirtualBox gdm-password]: pam_unix(gdm-password:session): session opened for user judy(uid=1000) by judy(uid=0)
2025-03-04T11:14:37+0800	2025-03-04T11:14:37.674686+08:00 judy-VirtualBox gdm-password]: gkr-pam: stashed password to try later in open session
2025-03-04T11:14:37+0800	2025-03-04T11:14:37.674558+08:00 judy-VirtualBox gdm-password]: gkr-pam: unable to locate daemon control file
2025-03-04T11:14:27+0800	2025-03-04T11:14:27.558594+08:00 judy-VirtualBox polkitd[1026]: Registered Authentication Agent for unix-session: c1 (system bus name :1.39 [/usr/bin/gnome-shell], object path /org/freedesktop/PolicyKit1/AuthenticationAgent, locale zh_TW.UTF-8)
2025-03-04T11:14:03+0800	2025-03-04T11:14:03.666365+08:00 judy-VirtualBox (systemd): pam_unix(systemd-user:session): session opened for user gdm(uid=120) by gdm(uid=0)
2025-03-04T11:14:03+0800	2025-03-04T11:14:03.301618+08:00 judy-VirtualBox systemd-logind[1035]: New session c1 of user gdm.
2025-03-04T11:14:03+0800	2025-03-04T11:14:03.076079+08:00 judy-VirtualBox gdm-launch-environment]: pam_unix(gdm-launch-environment: session): session opened for user gdm(uid=120) by (uid=0)
2025-03-04T11:13:53+0800	2025-03-04T11:13:53.007676+08:00 judy-VirtualBox polkitd[1026]: Acquired the name org.freedesktop.PolicyKit1 on the system bus
2025-03-04T11:13:53+0800	2025-03-04T11:13:53.005066+08:00 judy-VirtualBox polkitd[1026]: Finished loading, compiling and executing 16 rules
2025-03-04T11:13:52+0800	2025-03-04T11:13:52.593010+08:00 judy-VirtualBox polkitd[1026]: Loading rules from directory /usr/share/polkit-1/rules.d
2025-03-04T11:13:52+0800	2025-03-04T11:13:52.553244+08:00 judy-VirtualBox polkitd[1026]: Loading rules from directory /etc/polkit-1/rules.d
2025-03-04T11:13:51+0800	2025-03-04T11:13:51.634988+08:00 judy-VirtualBox systemd-logind[1035]: Watching system buttons on /dev/input/ event2 (AT Translated Set 2 keyboard)
2025-03-04T11:13:51+0800	2025-03-04T11:13:51.634986+08:00 judy-VirtualBox systemd-logind[1035]: Watching system buttons on /dev/input/event1 (Sleep Button)
2025-03-04T11:13:51+0800	2025-03-04T11:13:51.634984+08:00 judy-VirtualBox systemd-logind[1035]: Watching system buttons on /dev/input/event0 (Power Button)
2025-03-04T11:13:51+0800	2025-03-04T11:13:51.634983+08:00 judy-VirtualBox systemd-logind[1035]: New seat seat0.
2025-03-04T11:06:42+0800	2025-03-04T11:06:42.941602+08:00 judy-VirtualBox gdm-password]: pam_unix(gdm-password:session): session closed for user judy
2025-03-04T11:06:42+0800	2025-03-04T11:06:42.931892+08:00 judy-VirtualBox systemd-logind[1034]: System is powering down.
2025-03-04T11:06:42+0800	2025-03-04T11:06:42.921040+08:00 judy-VirtualBox sudo: pam_unix(sudo:session): session closed for user root
2025-03-04T11:06:42+0800	2025-03-04T11:06:42.890129+08:00 judy-VirtualBox systemd-logind[1034]: The system will power off now!
2025-03-04T11:06:42+0800	2025-03-04T11:06:42.882284+08:00 judy-VirtualBox sudo: pam_unix(sudo:session): session opened for user root(uid=0) by judy(uid=1000)
2025-03-04T11:06:42+0800	2025-03-04T11:06:42.881656+08:00 judy-VirtualBox sudo: judy : TTY=pts/0 ; PWD=/home/judy ; USER=root ; COMMAND=/usr/sbin/shutdown now
2025-03-04T11:06:34+0800	2025-03-04T11:06:34.215824+08:00 judy-VirtualBox gdm-password]: gkr-pam: unlocked login keyring
2025-03-04T11:06:23+0800	2025-03-04T11:06:23.686295+08:00 judy-VirtualBox sshd[3568]: pam_unix(sshd:session): session closed for user judy
2025-03-04T11:06:23+0800	2025-03-04T11:06:23.677841+08:00 judy-VirtualBox systemd-logind[1034]: Session 4 logged out. Waiting for processes to exit.
2025-03-04T11:06:23+0800	2025-03-04T11:06:23.677663+08:00 judy-VirtualBox sshd[3636]: Disconnected from user judy 10.167.214.40 port 1347
2025-03-04T11:06:23+0800	2025-03-04T11:06:23.665370+08:00 judy-VirtualBox sshd[3636]: Received disconnect from 10.167.214.40 port 1347:11: disconnected by user
2025-03-04T11:05:01+0800	2025-03-04T11:05:01.897891+08:00 judy-VirtualBox CRON[15794]: pam_unix(cron:session): session closed for user root

Time	Event
2025-03-04T11:05:01+0800	2025-03-04T11:05:01.896396+08:00 judy-VirtualBox CRON[15794]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
2025-03-04T10:55:01+0800	2025-03-04T10:55:01.846832+08:00 judy-VirtualBox CRON[15115]: pam_unix(cron:session): session closed for user root
2025-03-04T10:55:01+0800	2025-03-04T10:55:01.845154+08:00 judy-VirtualBox CRON[15115]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
2025-03-04T10:45:01+0800	2025-03-04T10:45:01.787657+08:00 judy-VirtualBox CRON[14478]: pam_unix(cron:session): session closed for user root
2025-03-04T10:45:01+0800	2025-03-04T10:45:01.781573+08:00 judy-VirtualBox CRON[14478]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
2025-03-04T10:35:01+0800	2025-03-04T10:35:01.715156+08:00 judy-VirtualBox CRON[13857]: pam_unix(cron:session): session closed for user root
2025-03-04T10:35:01+0800	2025-03-04T10:35:01.701805+08:00 judy-VirtualBox CRON[13857]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
2025-03-04T10:30:01+0800	2025-03-04T10:30:01.692173+08:00 judy-VirtualBox CRON[13476]: pam_unix(cron:session): session closed for user root
2025-03-04T10:30:01+0800	2025-03-04T10:30:01.685377+08:00 judy-VirtualBox CRON[13476]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
2025-03-04T10:25:01+0800	2025-03-04T10:25:01.667674+08:00 judy-VirtualBox CRON[13192]: pam_unix(cron:session): session closed for user root
2025-03-04T10:25:01+0800	2025-03-04T10:25:01.664538+08:00 judy-VirtualBox CRON[13192]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
2025-03-04T10:17:01+0800	2025-03-04T10:17:01.601206+08:00 judy-VirtualBox CRON[12680]: pam_unix(cron:session): session closed for user root
2025-03-04T10:17:01+0800	2025-03-04T10:17:01.592881+08:00 judy-VirtualBox CRON[12680]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
2025-03-04T10:15:01+0800	2025-03-04T10:15:01.619382+08:00 judy-VirtualBox CRON[12490]: pam_unix(cron:session): session closed for user root
2025-03-04T10:15:01+0800	2025-03-04T10:15:01.562694+08:00 judy-VirtualBox CRON[12490]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
2025-03-04T10:05:01+0800	2025-03-04T10:05:01.497403+08:00 judy-VirtualBox CRON[11864]: pam_unix(cron:session): session closed for user root
2025-03-04T10:05:01+0800	2025-03-04T10:05:01.493532+08:00 judy-VirtualBox CRON[11864]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
2025-03-04T09:55:01+0800	2025-03-04T09:55:01.428917+08:00 judy-VirtualBox CRON[11143]: pam_unix(cron:session): session closed for user root
2025-03-04T09:55:01+0800	2025-03-04T09:55:01.426091+08:00 judy-VirtualBox CRON[11143]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
2025-03-04T09:51:06+0800	2025-03-04T09:51:06.492850+08:00 judy-VirtualBox pkexec[10897]: judy: Executing command [USER=root] [TTY=unknown] [CWD=/home/judy] [COMMAND=/usr/lib/update-notifier/package-system-locked]
2025-03-04T09:51:06+0800	2025-03-04T09:51:06.491753+08:00 judy-VirtualBox pkexec: pam_unix(polkit-1:session): session opened for user root(uid=0) by judy(uid=1000)
2025-03-04T09:48:06+0800	2025-03-04T09:48:06.606969+08:00 judy-VirtualBox pkexec[9647]: judy: Executing command [USER=root] [TTY=unknown] [CWD=/home/judy] [COMMAND=/usr/lib/update-notifier/package-system-locked]
2025-03-04T09:48:06+0800	2025-03-04T09:48:06.563761+08:00 judy-VirtualBox pkexec: pam_unix(polkit-1:session): session opened for user root(uid=0) by judy(uid=1000)
2025-03-04T09:45:01+0800	2025-03-04T09:45:01.351010+08:00 judy-VirtualBox CRON[8947]: pam_unix(cron:session): session closed for user root
2025-03-04T09:45:01+0800	2025-03-04T09:45:01.348865+08:00 judy-VirtualBox CRON[8947]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
2025-03-04T09:35:01+0800	2025-03-04T09:35:01.324589+08:00 judy-VirtualBox CRON[8315]: pam_unix(cron:session): session closed for user root
2025-03-04T09:35:01+0800	2025-03-04T09:35:01.304847+08:00 judy-VirtualBox CRON[8315]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
2025-03-04T09:30:01+0800	2025-03-04T09:30:01.241706+08:00 judy-VirtualBox CRON[7893]: pam_unix(cron:session): session closed for user root
2025-03-04T09:30:01+0800	2025-03-04T09:30:01.238085+08:00 judy-VirtualBox CRON[7893]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
2025-03-04T09:25:01+0800	2025-03-04T09:25:01.205601+08:00 judy-VirtualBox CRON[7544]: pam_unix(cron:session): session closed for user root
2025-03-04T09:25:01+0800	2025-03-04T09:25:01.202071+08:00 judy-VirtualBox CRON[7544]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
2025-03-04T09:24:59+0800	2025-03-04T09:24:59.913843+08:00 judy-VirtualBox sudo: pam_unix(sudo:session): session closed for user root
2025-03-04T09:24:59+0800	2025-03-04T09:24:59.820784+08:00 judy-VirtualBox sudo: pam_unix(sudo:session): session opened for user root(uid=0) by judy(uid=1000)
2025-03-04T09:24:59+0800	2025-03-04T09:24:59.820346+08:00 judy-VirtualBox sudo: judy : TTY=pts/0 ; PWD=/home/judy ; USER=root ; COMMAND=/usr/bin/fail2ban-client status sshd
2025-03-04T09:24:54+0800	2025-03-04T09:24:54.435591+08:00 judy-VirtualBox gdm-password]: gkr-pam: unlocked login keyring
2025-03-04T09:21:06+0800	2025-03-04T09:21:06.507088+08:00 judy-VirtualBox pkexec[7158]: judy: Executing command [USER=root] [TTY=unknown] [CWD=/home/judy] [COMMAND=/usr/lib/update-notifier/package-system-locked]
2025-03-04T09:21:06+0800	2025-03-04T09:21:06.451280+08:00 judy-VirtualBox pkexec: pam_unix(polkit-1:session): session opened for user root(uid=0) by judy(uid=1000)
2025-03-04T09:17:01+0800	2025-03-04T09:17:01.181044+08:00 judy-VirtualBox CRON[6217]: pam_unix(cron:session): session closed for user root

Time	Event
2025-03-04T09:17:01+0800	2025-03-04T09:17:01.153767+08:00 judy-VirtualBox CRON[6217]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
2025-03-04T09:15:01+0800	2025-03-04T09:15:01.133403+08:00 judy-VirtualBox CRON[5987]: pam_unix(cron:session): session closed for user root
2025-03-04T09:15:01+0800	2025-03-04T09:15:01.128016+08:00 judy-VirtualBox CRON[5987]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
2025-03-04T09:05:01+0800	2025-03-04T09:05:01.078060+08:00 judy-VirtualBox CRON[5276]: pam_unix(cron:session): session closed for user root
2025-03-04T09:05:01+0800	2025-03-04T09:05:01.069804+08:00 judy-VirtualBox CRON[5276]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
2025-03-04T09:00:50+0800	2025-03-04T09:00:50.964728+08:00 judy-VirtualBox sudo: pam_unix(sudo:session): session closed for user root
2025-03-04T09:00:44+0800	2025-03-04T09:00:44.231328+08:00 judy-VirtualBox mongod: looking for plugins in '/home/build/build-home/opt/mongo/lib/sasl2', failed to open directory, error: No such file or directory
2025-03-04T09:00:44+0800	2025-03-04T09:00:44.231068+08:00 judy-VirtualBox mongod: looking for plugins in '/home/build/build-home/opt/mongo/lib/sasl2', failed to open directory, error: No such file or directory
2025-03-04T09:00:18+0800	2025-03-04T09:00:18.401134+08:00 judy-VirtualBox sudo: pam_unix(sudo:session): session opened for user root(uid=0) by judy(uid=1000)
2025-03-04T09:00:18+0800	2025-03-04T09:00:18.400929+08:00 judy-VirtualBox sudo: judy : TTY=pts/1 ; PWD=/home/judy ; USER=root ; COMMAND=/opt/splunk/bin/./splunk start
2025-03-04T09:00:09+0800	2025-03-04T09:00:09.253336+08:00 judy-VirtualBox pkexec[3775]: judy: Executing command [USER=root] [TTY=unknown] [CWD=/home/judy] [COMMAND=/usr/lib/update-notifier/package-system-locked]
2025-03-04T09:00:09+0800	2025-03-04T09:00:09.252364+08:00 judy-VirtualBox pkexec: pam_unix(polkit-1:session): session opened for user root(uid=0) by judy(uid=1000)
2025-03-04T08:59:46+0800	2025-03-04T08:59:46.772334+08:00 judy-VirtualBox systemd-logind[1034]: New session 4 of user judy.
2025-03-04T08:59:46+0800	2025-03-04T08:59:46.769494+08:00 judy-VirtualBox sshd[3568]: pam_unix(sshd:session): session opened for user judy(uid=1000) by judy(uid=0)
2025-03-04T08:59:46+0800	2025-03-04T08:59:46.768051+08:00 judy-VirtualBox sshd[3568]: Accepted password for judy from 10.167.214.40 port 1347 ssh2
2025-03-04T08:59:43+0800	2025-03-04T08:59:43.828007+08:00 judy-VirtualBox sshd[3566]: Server listening on :: port 22.
2025-03-04T08:59:28+0800	2025-03-04T08:59:28.654937+08:00 judy-VirtualBox dbus-daemon[1002]: [system] Failed to activate service 'org.bluez': timed out (service_start_timeout=25000ms)
2025-03-04T08:59:20+0800	2025-03-04T08:59:20.506532+08:00 judy-VirtualBox (sd-pam): pam_unix(systemd-user:session): session closed for user gdm
2025-03-04T08:59:10+0800	2025-03-04T08:59:10.315927+08:00 judy-VirtualBox systemd-logind[1034]: Removed session c1.
2025-03-04T08:59:10+0800	2025-03-04T08:59:10.245468+08:00 judy-VirtualBox polkitd[1024]: Unregistered Authentication Agent for unix-session :c1 (system bus name :1.40, object path /org/freedesktop/PolicyKit1/AuthenticationAgent, locale zh_TW.UTF-8) (disconnected from bus)
2025-03-04T08:59:10+0800	2025-03-04T08:59:10.237210+08:00 judy-VirtualBox systemd-logind[1034]: Session c1 logged out. Waiting for processes to exit.
2025-03-04T08:59:10+0800	2025-03-04T08:59:10.232340+08:00 judy-VirtualBox gdm-launch-environment]: pam_unix(gdm-launch-environment:session): session closed for user gdm
2025-03-04T08:59:06+0800	2025-03-04T08:59:06.595638+08:00 judy-VirtualBox polkitd[1024]: Registered Authentication Agent for unix-session: 2 (system bus name :1.80 [/usr/bin/gnome-shell], object path /org/freedesktop/PolicyKit1/AuthenticationAgent, locale zh_TW.UTF-8)
2025-03-04T08:59:04+0800	2025-03-04T08:59:04.259705+08:00 judy-VirtualBox gnome-keyring-daemon[2644]: discover_other_daemon: 1
2025-03-04T08:59:04+0800	2025-03-04T08:59:04.235198+08:00 judy-VirtualBox gnome-keyring-daemon[2639]: discover_other_daemon: 1
2025-03-04T08:59:04+0800	2025-03-04T08:59:04.235051+08:00 judy-VirtualBox gnome-keyring-daemon[2641]: discover_other_daemon: 1
2025-03-04T08:59:04+0800	2025-03-04T08:59:04.234070+08:00 judy-VirtualBox gnome-keyring-daemon[2400]: The PKCS#11 component was already initialized
2025-03-04T08:59:04+0800	2025-03-04T08:59:04.233985+08:00 judy-VirtualBox gnome-keyring-daemon[2400]: The Secret Service was already initialized
2025-03-04T08:59:02+0800	2025-03-04T08:59:02.667523+08:00 judy-VirtualBox gdm-password]: gkr-pam: unlocked login keyring
2025-03-04T08:59:01+0800	2025-03-04T08:59:01.523615+08:00 judy-VirtualBox (systemd): pam_unix(systemd-user:session): session opened for user judy(uid=1000) by judy(uid=0)
2025-03-04T08:59:01+0800	2025-03-04T08:59:01.510513+08:00 judy-VirtualBox systemd-logind[1034]: New session 2 of user judy.
2025-03-04T08:59:01+0800	2025-03-04T08:59:01.495762+08:00 judy-VirtualBox gdm-password]: pam_unix(gdm-password:session): session opened for user judy(uid=1000) by judy(uid=0)
2025-03-04T08:59:01+0800	2025-03-04T08:59:01.435688+08:00 judy-VirtualBox gdm-password]: gkr-pam: stashed password to try later in open session
2025-03-04T08:59:01+0800	2025-03-04T08:59:01.435606+08:00 judy-VirtualBox gdm-password]: gkr-pam: unable to locate daemon control file
2025-03-04T08:58:57+0800	2025-03-04T08:58:57.368786+08:00 judy-VirtualBox gdm-password]: pam_unix(gdm-password:auth): authentication failure; logname= uid=0 euid=0 tty=/dev/tty1 ruser= rhost= user=judy
2025-03-04T08:58:48+0800	2025-03-04T08:58:48.232767+08:00 judy-VirtualBox polkitd[1024]: Registered Authentication Agent for unix-session: c1 (system bus name :1.40 [/usr/bin/gnome-shell], object path /org/freedesktop/PolicyKit1/AuthenticationAgent, locale zh_TW.UTF-8)
2025-03-04T08:58:28+0800	2025-03-04T08:58:28.490514+08:00 judy-VirtualBox (systemd): pam_unix(systemd-user:session): session opened for user gdm(uid=120) by gdm(uid=0)
2025-03-04T08:58:28+0800	2025-03-04T08:58:28.268224+08:00 judy-VirtualBox systemd-logind[1034]: New session c1 of user gdm.

Time	Event
2025-03-04T08:58:28+0800	2025-03-04T08:58:28.102287+08:00 judy-VirtualBox gdm-launch-environment]: pam_unix(gdm-launch-environment: session): session opened for user gdm(uid=120) by (uid=0)
2025-03-04T08:58:18+0800	2025-03-04T08:58:18.202107+08:00 judy-VirtualBox polkitd[1024]: Acquired the name org.freedesktop.PolicyKit1 on the system bus
2025-03-04T08:58:18+0800	2025-03-04T08:58:18.199509+08:00 judy-VirtualBox polkitd[1024]: Finished loading, compiling and executing 16 rules
2025-03-04T08:58:17+0800	2025-03-04T08:58:17.917746+08:00 judy-VirtualBox polkitd[1024]: Loading rules from directory /usr/share/polkit-1/rules.d
2025-03-04T08:58:17+0800	2025-03-04T08:58:17.907967+08:00 judy-VirtualBox polkitd[1024]: Loading rules from directory /etc/polkit-1/rules.d
2025-03-04T08:58:16+0800	2025-03-04T08:58:16.791633+08:00 judy-VirtualBox systemd-logind[1034]: Watching system buttons on /dev/input/ event2 (AT Translated Set 2 keyboard)
2025-03-04T08:58:16+0800	2025-03-04T08:58:16.791623+08:00 judy-VirtualBox systemd-logind[1034]: Watching system buttons on /dev/input/event1 (Sleep Button)
2025-03-04T08:58:16+0800	2025-03-04T08:58:16.791617+08:00 judy-VirtualBox systemd-logind[1034]: Watching system buttons on /dev/input/event0 (Power Button)
2025-03-04T08:58:16+0800	2025-03-04T08:58:16.791611+08:00 judy-VirtualBox systemd-logind[1034]: New seat seat0.
2025-03-03T16:42:59+0800	2025-03-03T16:42:59.865816+08:00 judy-VirtualBox gdm-password]: pam_unix(gdm-password:session): session closed for user judy
2025-03-03T16:42:59+0800	2025-03-03T16:42:59.851179+08:00 judy-VirtualBox systemd-logind[1046]: System is powering down.
2025-03-03T16:42:59+0800	2025-03-03T16:42:59.839771+08:00 judy-VirtualBox sudo: pam_unix(sudo:session): session closed for user root
2025-03-03T16:42:59+0800	2025-03-03T16:42:59.819144+08:00 judy-VirtualBox systemd-logind[1046]: The system will power off now!
2025-03-03T16:42:59+0800	2025-03-03T16:42:59.814091+08:00 judy-VirtualBox sudo: pam_unix(sudo:session): session opened for user root(uid=0) by judy(uid=1000)
2025-03-03T16:42:59+0800	2025-03-03T16:42:59.813683+08:00 judy-VirtualBox sudo: judy : TTY=pts/0 ; PWD=/home/judy ; USER=root ; COMMAND=/usr/sbin/shutdown now
2025-03-03T16:42:52+0800	2025-03-03T16:42:52.715827+08:00 judy-VirtualBox sudo: pam_unix(sudo:session): session closed for user root
2025-03-03T16:42:52+0800	2025-03-03T16:42:52.670020+08:00 judy-VirtualBox sudo: pam_unix(sudo:session): session opened for user root(uid=0) by judy(uid=1000)
2025-03-03T16:42:52+0800	2025-03-03T16:42:52.669478+08:00 judy-VirtualBox sudo: judy : TTY=pts/0 ; PWD=/home/judy ; USER=root ; COMMAND=/usr/bin/fail2ban-client status sshd
2025-03-03T16:42:51+0800	2025-03-03T16:42:51.465913+08:00 judy-VirtualBox sudo: pam_unix(sudo:session): session closed for user root
2025-03-03T16:42:51+0800	2025-03-03T16:42:51.402405+08:00 judy-VirtualBox sudo: pam_unix(sudo:session): session opened for user root(uid=0) by judy(uid=1000)
2025-03-03T16:42:51+0800	2025-03-03T16:42:51.401912+08:00 judy-VirtualBox sudo: judy : TTY=pts/0 ; PWD=/home/judy ; USER=root ; COMMAND=/usr/bin/fail2ban-client set sshd unbanip 10.167.214.35
2025-03-03T16:42:49+0800	2025-03-03T16:42:49.686319+08:00 judy-VirtualBox sudo: pam_unix(sudo:session): session closed for user root
2025-03-03T16:42:49+0800	2025-03-03T16:42:49.614806+08:00 judy-VirtualBox sudo: pam_unix(sudo:session): session opened for user root(uid=0) by judy(uid=1000)
2025-03-03T16:42:49+0800	2025-03-03T16:42:49.614155+08:00 judy-VirtualBox sudo: judy : TTY=pts/0 ; PWD=/home/judy ; USER=root ; COMMAND=/usr/bin/fail2ban-client set sshd unbanip 10.167.214.40
2025-03-03T16:42:45+0800	2025-03-03T16:42:45.893998+08:00 judy-VirtualBox sudo: pam_unix(sudo:session): session closed for user root
2025-03-03T16:42:45+0800	2025-03-03T16:42:45.847355+08:00 judy-VirtualBox sudo: pam_unix(sudo:session): session opened for user root(uid=0) by judy(uid=1000)
2025-03-03T16:42:45+0800	2025-03-03T16:42:45.846742+08:00 judy-VirtualBox sudo: judy : TTY=pts/0 ; PWD=/home/judy ; USER=root ; COMMAND=/usr/bin/fail2ban-client status sshd
2025-03-03T16:42:41+0800	2025-03-03T16:42:41.927554+08:00 judy-VirtualBox gdm-password]: gkr-pam: unlocked login keyring
2025-03-03T16:41:11+0800	2025-03-03T16:41:11.474709+08:00 judy-VirtualBox sshd[147679]: Connection reset by invalid user byron 10.167.214.35 port 9107 [preauth]
2025-03-03T16:41:11+0800	2025-03-03T16:41:11.464607+08:00 judy-VirtualBox sshd[147679]: Failed password for invalid user byron from 10.167.214.35 port 9107 ssh2
2025-03-03T16:41:11+0800	2025-03-03T16:41:11.305493+08:00 judy-VirtualBox sshd[147679]: Failed password for invalid user byron from 10.167.214.35 port 9107 ssh2
2025-03-03T16:41:11+0800	2025-03-03T16:41:11.160364+08:00 judy-VirtualBox sshd[147679]: Failed none for invalid user byron from 10.167.214.35 port 9107 ssh2
2025-03-03T16:41:11+0800	2025-03-03T16:41:11.068888+08:00 judy-VirtualBox sshd[147679]: Invalid user byron from 10.167.214.35 port 9107
2025-03-03T16:41:04+0800	2025-03-03T16:41:04.521834+08:00 judy-VirtualBox sshd[147670]: Connection reset by invalid user byron 10.167.214.35 port 9106 [preauth]
2025-03-03T16:41:04+0800	2025-03-03T16:41:04.512882+08:00 judy-VirtualBox sshd[147670]: Failed password for invalid user byron from 10.167.214.35 port 9106 ssh2
2025-03-03T16:41:04+0800	2025-03-03T16:41:04.297135+08:00 judy-VirtualBox sshd[147670]: Failed password for invalid user byron from 10.167.214.35 port 9106 ssh2
2025-03-03T16:41:04+0800	2025-03-03T16:41:04.105392+08:00 judy-VirtualBox sshd[147670]: Failed none for invalid user byron from 10.167.214.35 port 9106 ssh2
2025-03-03T16:41:03+0800	2025-03-03T16:41:03.176313+08:00 judy-VirtualBox sshd[147670]: Invalid user byron from 10.167.214.35 port 9106
2025-03-03T16:36:52+0800	2025-03-03T16:36:52.732339+08:00 judy-VirtualBox sshd[145589]: Connection reset by authenticating user judy 10. 167.214.40 port 4325 [preauth]
2025-03-03T16:36:52+0800	2025-03-03T16:36:52.720781+08:00 judy-VirtualBox sshd[145589]: Failed password for judy from 10.167.214.40 port 4325 ssh2
2025-03-03T16:36:52+0800	2025-03-03T16:36:52.529577+08:00 judy-VirtualBox sshd[145589]: Failed password for judy from 10.167.214.40 port 4325 ssh2
2025-03-03T16:36:51+0800	2025-03-03T16:36:51.173248+08:00 judy-VirtualBox sshd[145585]: Connection reset by authenticating user judy 10. 167.214.40 port 4324 [preauth]
2025-03-03T16:36:51+0800	2025-03-03T16:36:51.161153+08:00 judy-VirtualBox sshd[145585]: Failed password for judy from 10.167.214.40 port 4324 ssh2
2025-03-03T16:36:50+0800	2025-03-03T16:36:50.888642+08:00 judy-VirtualBox sshd[145585]: Failed password for judy from 10.167.214.40 port 4324 ssh2
2025-03-03T16:36:49+0800	2025-03-03T16:36:49.340505+08:00 judy-VirtualBox sshd[145581]: Connection reset by authenticating user judy 10. 167.214.40 port 4323 [preauth]
2025-03-03T16:36:49+0800	2025-03-03T16:36:49.328453+08:00 judy-VirtualBox sshd[145581]: Failed password for judy from 10.167.214.40 port 4323 ssh2

Time	Event
2025-03-03T16:36:49+0800	2025-03-03T16:36:49.064964+08:00 judy-VirtualBox sshd[145581]: Failed password for judy from 10.167.214.40 port 4323 ssh2
2025-03-03T16:36:42+0800	2025-03-03T16:36:42.328426+08:00 judy-VirtualBox systemd-logind[1046]: Removed session 62.
2025-03-03T16:36:42+0800	2025-03-03T16:36:42.327669+08:00 judy-VirtualBox systemd-logind[1046]: Session 62 logged out. Waiting for processes to exit.
2025-03-03T16:36:42+0800	2025-03-03T16:36:42.327539+08:00 judy-VirtualBox sshd[117803]: pam_unix(sshd:session): session closed for user judy
2025-03-03T16:36:42+0800	2025-03-03T16:36:42.327227+08:00 judy-VirtualBox sshd[117901]: Disconnected from user judy 10.167.214.40 port 3883
2025-03-03T16:36:42+0800	2025-03-03T16:36:42.322326+08:00 judy-VirtualBox sshd[117901]: Received disconnect from 10.167.214.40 port 3883:11: disconnected by user
2025-03-03T16:35:01+0800	2025-03-03T16:35:01.191989+08:00 judy-VirtualBox CRON[144980]: pam_unix(cron:session): session closed for user root
2025-03-03T16:35:01+0800	2025-03-03T16:35:01.189770+08:00 judy-VirtualBox CRON[144980]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
2025-03-03T16:30:01+0800	2025-03-03T16:30:01.175839+08:00 judy-VirtualBox CRON[142812]: pam_unix(cron:session): session closed for user root
2025-03-03T16:30:01+0800	2025-03-03T16:30:01.172645+08:00 judy-VirtualBox CRON[142812]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
2025-03-03T16:29:27+0800	2025-03-03T16:29:27.362780+08:00 judy-VirtualBox sudo: pam_unix(sudo:session): session closed for user root
2025-03-03T16:29:27+0800	2025-03-03T16:29:27.343049+08:00 judy-VirtualBox userdel[142695]: delete 'kevin' from shadow group 'users'
2025-03-03T16:29:27+0800	2025-03-03T16:29:27.343028+08:00 judy-VirtualBox userdel[142695]: removed shadow group 'kevin' owned by 'kevin'
2025-03-03T16:29:27+0800	2025-03-03T16:29:27.342991+08:00 judy-VirtualBox userdel[142695]: removed group 'kevin' owned by 'kevin'
2025-03-03T16:29:27+0800	2025-03-03T16:29:27.342577+08:00 judy-VirtualBox userdel[142695]: delete 'kevin' from group 'users'
2025-03-03T16:29:27+0800	2025-03-03T16:29:27.342492+08:00 judy-VirtualBox userdel[142695]: delete user 'kevin'
2025-03-03T16:29:27+0800	2025-03-03T16:29:27.214491+08:00 judy-VirtualBox sudo: pam_unix(sudo:session): session opened for user root(uid=0) by judy(uid=1000)
2025-03-03T16:29:27+0800	2025-03-03T16:29:27.213553+08:00 judy-VirtualBox sudo: judy : TTY=pts/1 ; PWD=/home/judy ; USER=root ; COMMAND=/usr/sbin/deluser kevin
2025-03-03T16:29:22+0800	2025-03-03T16:29:22.949840+08:00 judy-VirtualBox sudo: pam_unix(sudo:session): session closed for user root
2025-03-03T16:29:22+0800	2025-03-03T16:29:22.929167+08:00 judy-VirtualBox userdel[142677]: delete 'ziven' from shadow group 'users'
2025-03-03T16:29:22+0800	2025-03-03T16:29:22.929144+08:00 judy-VirtualBox userdel[142677]: removed shadow group 'ziven' owned by 'ziven'
2025-03-03T16:29:22+0800	2025-03-03T16:29:22.929087+08:00 judy-VirtualBox userdel[142677]: removed group 'ziven' owned by 'ziven'
2025-03-03T16:29:22+0800	2025-03-03T16:29:22.928697+08:00 judy-VirtualBox userdel[142677]: delete 'ziven' from group 'users'
2025-03-03T16:29:22+0800	2025-03-03T16:29:22.928627+08:00 judy-VirtualBox userdel[142677]: delete user 'ziven'
2025-03-03T16:29:22+0800	2025-03-03T16:29:22.871558+08:00 judy-VirtualBox sudo: pam_unix(sudo:session): session opened for user root(uid=0) by judy(uid=1000)
2025-03-03T16:29:22+0800	2025-03-03T16:29:22.871250+08:00 judy-VirtualBox sudo: judy : TTY=pts/1 ; PWD=/home/judy ; USER=root ; COMMAND=/usr/sbin/deluser ziven
2025-03-03T16:29:18+0800	2025-03-03T16:29:18.569207+08:00 judy-VirtualBox sudo: pam_unix(sudo:session): session closed for user root
2025-03-03T16:29:18+0800	2025-03-03T16:29:18.510553+08:00 judy-VirtualBox userdel[142657]: delete 'eunice' from shadow group 'users'
2025-03-03T16:29:18+0800	2025-03-03T16:29:18.510524+08:00 judy-VirtualBox userdel[142657]: removed shadow group 'eunice' owned by 'eunice'
2025-03-03T16:29:18+0800	2025-03-03T16:29:18.510493+08:00 judy-VirtualBox userdel[142657]: removed group 'eunice' owned by 'eunice'
2025-03-03T16:29:18+0800	2025-03-03T16:29:18.509957+08:00 judy-VirtualBox userdel[142657]: delete 'eunice' from group 'users'
2025-03-03T16:29:18+0800	2025-03-03T16:29:18.509888+08:00 judy-VirtualBox userdel[142657]: delete user 'eunice'
2025-03-03T16:29:18+0800	2025-03-03T16:29:18.350987+08:00 judy-VirtualBox sudo: pam_unix(sudo:session): session opened for user root(uid=0) by judy(uid=1000)
2025-03-03T16:29:18+0800	2025-03-03T16:29:18.350581+08:00 judy-VirtualBox sudo: judy : TTY=pts/1 ; PWD=/home/judy ; USER=root ; COMMAND=/usr/sbin/deluser eunice
2025-03-03T16:29:13+0800	2025-03-03T16:29:13.132208+08:00 judy-VirtualBox sudo: pam_unix(sudo:session): session closed for user root
2025-03-03T16:29:13+0800	2025-03-03T16:29:13.112940+08:00 judy-VirtualBox userdel[142642]: delete 'jordan' from shadow group 'users'
2025-03-03T16:29:13+0800	2025-03-03T16:29:13.112920+08:00 judy-VirtualBox userdel[142642]: removed shadow group 'jordan' owned by 'jordan'
2025-03-03T16:29:13+0800	2025-03-03T16:29:13.112884+08:00 judy-VirtualBox userdel[142642]: removed group 'jordan' owned by 'jordan'
2025-03-03T16:29:13+0800	2025-03-03T16:29:13.112353+08:00 judy-VirtualBox userdel[142642]: delete 'jordan' from group 'users'
2025-03-03T16:29:13+0800	2025-03-03T16:29:13.112284+08:00 judy-VirtualBox userdel[142642]: delete user 'jordan'
2025-03-03T16:29:13+0800	2025-03-03T16:29:13.007088+08:00 judy-VirtualBox sudo: pam_unix(sudo:session): session opened for user root(uid=0) by judy(uid=1000)
2025-03-03T16:29:13+0800	2025-03-03T16:29:13.006498+08:00 judy-VirtualBox sudo: judy : TTY=pts/1 ; PWD=/home/judy ; USER=root ; COMMAND=/usr/sbin/deluser jordan
2025-03-03T16:28:48+0800	2025-03-03T16:28:48.626385+08:00 judy-VirtualBox sudo: pam_unix(sudo:session): session closed for user root
2025-03-03T16:28:48+0800	2025-03-03T16:28:48.600369+08:00 judy-VirtualBox userdel[142590]: delete 'alex' from shadow group 'users'
2025-03-03T16:28:48+0800	2025-03-03T16:28:48.600353+08:00 judy-VirtualBox userdel[142590]: removed shadow group 'alex' owned by 'alex'
2025-03-03T16:28:48+0800	2025-03-03T16:28:48.600320+08:00 judy-VirtualBox userdel[142590]: removed group 'alex' owned by 'alex'
2025-03-03T16:28:48+0800	2025-03-03T16:28:48.599885+08:00 judy-VirtualBox userdel[142590]: delete 'alex' from group 'users'
2025-03-03T16:28:48+0800	2025-03-03T16:28:48.599826+08:00 judy-VirtualBox userdel[142590]: delete user 'alex'

Time	Event
2025-03-03T16:28:48+0800	2025-03-03T16:28:48.547430+08:00 judy-VirtualBox sudo: pam_unix(sudo:session): session opened for user root(uid=0) by judy(uid=1000)
2025-03-03T16:28:48+0800	2025-03-03T16:28:48.542514+08:00 judy-VirtualBox sudo: judy : TTY=pts/1 ; PWD=/home/judy ; USER=root ; COMMAND=/usr/sbin/deluser alex
2025-03-03T16:27:19+0800	2025-03-03T16:27:19.715174+08:00 judy-VirtualBox sudo: pam_unix(sudo:session): session closed for user root
2025-03-03T16:27:19+0800	2025-03-03T16:27:19.695701+08:00 judy-VirtualBox userdel[142252]: delete 'sharon' from shadow group 'users'
2025-03-03T16:27:19+0800	2025-03-03T16:27:19.695684+08:00 judy-VirtualBox userdel[142252]: removed shadow group 'sharon' owned by 'sharon'
2025-03-03T16:27:19+0800	2025-03-03T16:27:19.695655+08:00 judy-VirtualBox userdel[142252]: removed group 'sharon' owned by 'sharon'
2025-03-03T16:27:19+0800	2025-03-03T16:27:19.695272+08:00 judy-VirtualBox userdel[142252]: delete 'sharon' from group 'users'
2025-03-03T16:27:19+0800	2025-03-03T16:27:19.695211+08:00 judy-VirtualBox userdel[142252]: delete user 'sharon'
2025-03-03T16:27:19+0800	2025-03-03T16:27:19.391905+08:00 judy-VirtualBox sudo: pam_unix(sudo:session): session opened for user root(uid=0) by judy(uid=1000)
2025-03-03T16:27:19+0800	2025-03-03T16:27:19.391373+08:00 judy-VirtualBox sudo: judy : TTY=pts/1 ; PWD=/home/judy ; USER=root ; COMMAND=/usr/sbin/deluser sharon
2025-03-03T16:25:01+0800	2025-03-03T16:25:01.158101+08:00 judy-VirtualBox CRON[141815]: pam_unix(cron:session): session closed for user root
2025-03-03T16:25:01+0800	2025-03-03T16:25:01.154630+08:00 judy-VirtualBox CRON[141815]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
2025-03-03T16:24:04+0800	2025-03-03T16:24:04.233759+08:00 judy-VirtualBox sudo: pam_unix(sudo:session): session closed for user root
2025-03-03T16:24:04+0800	2025-03-03T16:24:04.231959+08:00 judy-VirtualBox gpasswd[141597]: members of group users set by root to judy ,ziven,jordan,kevin,eunice,alex,sharon
2025-03-03T16:24:03+0800	2025-03-03T16:24:03.282849+08:00 judy-VirtualBox chfn[141583]: changed user 'sharon' information
2025-03-03T16:24:01+0800	2025-03-03T16:24:01.716070+08:00 judy-VirtualBox passwd[141576]: gkr-pam: couldn't update the login keyring password: no old password was entered
2025-03-03T16:24:01+0800	2025-03-03T16:24:01.715138+08:00 judy-VirtualBox passwd[141576]: pam_unix(passwd:chauthtok): password changed for sharon
2025-03-03T16:23:57+0800	2025-03-03T16:23:57.292463+08:00 judy-VirtualBox useradd[141563]: new user: name=sharon, UID=1007, GID=1007, home=/home/sharon, shell=/bin/bash, from=/dev/pts/2
2025-03-03T16:23:57+0800	2025-03-03T16:23:57.279480+08:00 judy-VirtualBox groupadd[141556]: new group: name=sharon, GID=1007
2025-03-03T16:23:57+0800	2025-03-03T16:23:57.278507+08:00 judy-VirtualBox groupadd[141556]: group added to /etc/gshadow: name=sharon
2025-03-03T16:23:57+0800	2025-03-03T16:23:57.274283+08:00 judy-VirtualBox groupadd[141556]: group added to /etc/group: name=sharon, GID=1007
2025-03-03T16:23:57+0800	2025-03-03T16:23:57.200574+08:00 judy-VirtualBox sudo: pam_unix(sudo:session): session opened for user root(uid=0) by judy(uid=1000)
2025-03-03T16:23:57+0800	2025-03-03T16:23:57.200170+08:00 judy-VirtualBox sudo: judy : TTY=pts/1 ; PWD=/home/judy ; USER=root ; COMMAND=/usr/sbin/adduser sharon
2025-03-03T16:22:41+0800	2025-03-03T16:22:41.961466+08:00 judy-VirtualBox sudo: pam_unix(sudo:session): session closed for user root
2025-03-03T16:22:41+0800	2025-03-03T16:22:41.959621+08:00 judy-VirtualBox gpasswd[140878]: members of group users set by root to judy ,ziven,jordan,kevin,eunice,alex
2025-03-03T16:22:40+0800	2025-03-03T16:22:40.583625+08:00 judy-VirtualBox chfn[140861]: changed user 'alex' information
2025-03-03T16:22:38+0800	2025-03-03T16:22:38.485249+08:00 judy-VirtualBox passwd[140854]: gkr-pam: couldn't update the login keyring password: no old password was entered
2025-03-03T16:22:38+0800	2025-03-03T16:22:38.485062+08:00 judy-VirtualBox passwd[140854]: pam_unix(passwd:chauthtok): password changed for alex
2025-03-03T16:22:33+0800	2025-03-03T16:22:33.484414+08:00 judy-VirtualBox useradd[140845]: new user: name=alex, UID=1006, GID=1006, home=/home/alex, shell=/bin/bash, from=/dev/pts/2
2025-03-03T16:22:33+0800	2025-03-03T16:22:33.470190+08:00 judy-VirtualBox groupadd[140838]: new group: name=alex, GID=1006
2025-03-03T16:22:33+0800	2025-03-03T16:22:33.469270+08:00 judy-VirtualBox groupadd[140838]: group added to /etc/gshadow: name=alex
2025-03-03T16:22:33+0800	2025-03-03T16:22:33.466560+08:00 judy-VirtualBox groupadd[140838]: group added to /etc/group: name=alex, GID=1006
2025-03-03T16:22:33+0800	2025-03-03T16:22:33.430855+08:00 judy-VirtualBox sudo: pam_unix(sudo:session): session opened for user root(uid=0) by judy(uid=1000)
2025-03-03T16:22:33+0800	2025-03-03T16:22:33.423914+08:00 judy-VirtualBox sudo: judy : TTY=pts/1 ; PWD=/home/judy ; USER=root ; COMMAND=/usr/sbin/adduser alex
2025-03-03T16:17:01+0800	2025-03-03T16:17:01.174832+08:00 judy-VirtualBox CRON[139572]: pam_unix(cron:session): session closed for user root
2025-03-03T16:17:01+0800	2025-03-03T16:17:01.134925+08:00 judy-VirtualBox CRON[139572]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
2025-03-03T16:15:01+0800	2025-03-03T16:15:01.129163+08:00 judy-VirtualBox CRON[139010]: pam_unix(cron:session): session closed for user root
2025-03-03T16:15:01+0800	2025-03-03T16:15:01.125226+08:00 judy-VirtualBox CRON[139010]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
2025-03-03T16:05:01+0800	2025-03-03T16:05:01.066543+08:00 judy-VirtualBox CRON[133873]: pam_unix(cron:session): session closed for user root
2025-03-03T16:05:01+0800	2025-03-03T16:05:01.060356+08:00 judy-VirtualBox CRON[133873]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
2025-03-03T16:01:09+0800	2025-03-03T16:01:09.655108+08:00 judy-VirtualBox sudo: pam_unix(sudo:session): session closed for user root
2025-03-03T16:01:09+0800	2025-03-03T16:01:09.654995+08:00 judy-VirtualBox passwd[130586]: gkr-pam: couldn't update the login keyring password: no old password was entered

Time	Event
2025-03-03T16:01:09+0800	2025-03-03T16:01:09.654428+08:00 judy-VirtualBox passwd[130586]: pam_unix(passwd:chauthtok): password changed for eunice
2025-03-03T16:00:29+0800	2025-03-03T16:00:29.816667+08:00 judy-VirtualBox sudo: pam_unix(sudo:session): session opened for user root(uid=0) by judy(uid=1000)
2025-03-03T16:00:29+0800	2025-03-03T16:00:29.816437+08:00 judy-VirtualBox sudo: judy : TTY=pts/1 ; PWD=/home/judy ; USER=root ; COMMAND=/usr/bin/passwd eunice
2025-03-03T16:00:16+0800	2025-03-03T16:00:16.943074+08:00 judy-VirtualBox sudo: pam_unix(sudo:auth): auth could not identify password for [judy]
2025-03-03T16:00:16+0800	2025-03-03T16:00:16.938650+08:00 judy-VirtualBox sudo: pam_unix(sudo:auth): conversation failed
2025-03-03T15:55:01+0800	2025-03-03T15:55:01.028774+08:00 judy-VirtualBox CRON[130048]: pam_unix(cron:session): session closed for user root
2025-03-03T15:55:01+0800	2025-03-03T15:55:01.026843+08:00 judy-VirtualBox CRON[130048]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
2025-03-03T15:45:02+0800	2025-03-03T15:45:02.000462+08:00 judy-VirtualBox CRON[124679]: pam_unix(cron:session): session closed for user root
2025-03-03T15:45:01+0800	2025-03-03T15:45:01.998383+08:00 judy-VirtualBox CRON[124679]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
2025-03-03T15:35:01+0800	2025-03-03T15:35:01.927543+08:00 judy-VirtualBox CRON[120898]: pam_unix(cron:session): session closed for user root
2025-03-03T15:35:01+0800	2025-03-03T15:35:01.905796+08:00 judy-VirtualBox CRON[120898]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
2025-03-03T15:30:55+0800	2025-03-03T15:30:55.886789+08:00 judy-VirtualBox sudo: pam_unix(sudo:session): session closed for user root
2025-03-03T15:30:55+0800	2025-03-03T15:30:55.884739+08:00 judy-VirtualBox gpasswd[119304]: members of group users set by root to judy,ziven,jordan,kevin,eunice
2025-03-03T15:30:54+0800	2025-03-03T15:30:54.877055+08:00 judy-VirtualBox chfn[119291]: changed user 'eunice' information
2025-03-03T15:30:53+0800	2025-03-03T15:30:53.708184+08:00 judy-VirtualBox passwd[119283]: gkr-pam: couldn't update the login keyring password: no old password was entered
2025-03-03T15:30:53+0800	2025-03-03T15:30:53.708087+08:00 judy-VirtualBox passwd[119283]: pam_unix(passwd:chauthtok): password changed for eunice
2025-03-03T15:30:48+0800	2025-03-03T15:30:48.097220+08:00 judy-VirtualBox useradd[119270]: new user: name=eunice, UID=1005, GID=1005, home=/home/eunice, shell=/bin/bash, from=/dev/pts/2
2025-03-03T15:30:48+0800	2025-03-03T15:30:48.083448+08:00 judy-VirtualBox groupadd[119263]: new group: name=eunice, GID=1005
2025-03-03T15:30:48+0800	2025-03-03T15:30:48.082408+08:00 judy-VirtualBox groupadd[119263]: group added to /etc/gshadow: name=eunice
2025-03-03T15:30:48+0800	2025-03-03T15:30:48.080039+08:00 judy-VirtualBox groupadd[119263]: group added to /etc/group: name=eunice, GID=1005
2025-03-03T15:30:48+0800	2025-03-03T15:30:48.039054+08:00 judy-VirtualBox sudo: pam_unix(sudo:session): session opened for user root(uid=0) by judy(uid=1000)
2025-03-03T15:30:48+0800	2025-03-03T15:30:48.038607+08:00 judy-VirtualBox sudo: judy : TTY=pts/1 ; PWD=/home/judy ; USER=root ; COMMAND=/usr/sbin/adduser eunice
2025-03-03T15:30:44+0800	2025-03-03T15:30:44.512406+08:00 judy-VirtualBox sudo: pam_unix(sudo:session): session closed for user root
2025-03-03T15:30:44+0800	2025-03-03T15:30:44.510487+08:00 judy-VirtualBox gpasswd[119235]: members of group users set by root to judy,ziven,jordan,kevin
2025-03-03T15:30:43+0800	2025-03-03T15:30:43.064785+08:00 judy-VirtualBox chfn[119219]: changed user 'kevin' information
2025-03-03T15:30:41+0800	2025-03-03T15:30:41.297773+08:00 judy-VirtualBox passwd[119212]: gkr-pam: couldn't update the login keyring password: no old password was entered
2025-03-03T15:30:41+0800	2025-03-03T15:30:41.297663+08:00 judy-VirtualBox passwd[119212]: pam_unix(passwd:chauthtok): password changed for kevin
2025-03-03T15:30:35+0800	2025-03-03T15:30:35.637061+08:00 judy-VirtualBox useradd[119199]: new user: name=kevin, UID=1004, GID=1004, home=/home/kevin, shell=/bin/bash, from=/dev/pts/2
2025-03-03T15:30:35+0800	2025-03-03T15:30:35.619993+08:00 judy-VirtualBox groupadd[119192]: new group: name=kevin, GID=1004
2025-03-03T15:30:35+0800	2025-03-03T15:30:35.618995+08:00 judy-VirtualBox groupadd[119192]: group added to /etc/gshadow: name=kevin
2025-03-03T15:30:35+0800	2025-03-03T15:30:35.616507+08:00 judy-VirtualBox groupadd[119192]: group added to /etc/group: name=kevin, GID=1004
2025-03-03T15:30:35+0800	2025-03-03T15:30:35.574647+08:00 judy-VirtualBox sudo: pam_unix(sudo:session): session opened for user root(uid=0) by judy(uid=1000)
2025-03-03T15:30:35+0800	2025-03-03T15:30:35.574220+08:00 judy-VirtualBox sudo: judy : TTY=pts/1 ; PWD=/home/judy ; USER=root ; COMMAND=/usr/sbin/adduser kevin
2025-03-03T15:30:30+0800	2025-03-03T15:30:30.453473+08:00 judy-VirtualBox sudo: pam_unix(sudo:session): session closed for user root
2025-03-03T15:30:30+0800	2025-03-03T15:30:30.451522+08:00 judy-VirtualBox gpasswd[119139]: members of group users set by root to judy,ziven,jordan
2025-03-03T15:30:29+0800	2025-03-03T15:30:29.384163+08:00 judy-VirtualBox chfn[119099]: changed user 'jordan' information
2025-03-03T15:30:27+0800	2025-03-03T15:30:27.919589+08:00 judy-VirtualBox passwd[118972]: gkr-pam: couldn't update the login keyring password: no old password was entered
2025-03-03T15:30:27+0800	2025-03-03T15:30:27.919488+08:00 judy-VirtualBox passwd[118972]: pam_unix(passwd:chauthtok): password changed for jordan
2025-03-03T15:30:21+0800	2025-03-03T15:30:21.212208+08:00 judy-VirtualBox useradd[118959]: new user: name=jordan, UID=1002, GID=1002, home=/home/jordan, shell=/bin/bash, from=/dev/pts/2
2025-03-03T15:30:21+0800	2025-03-03T15:30:21.180185+08:00 judy-VirtualBox groupadd[118952]: new group: name=jordan, GID=1002
2025-03-03T15:30:21+0800	2025-03-03T15:30:21.179271+08:00 judy-VirtualBox groupadd[118952]: group added to /etc/gshadow: name=jordan
2025-03-03T15:30:21+0800	2025-03-03T15:30:21.173771+08:00 judy-VirtualBox groupadd[118952]: group added to /etc/group: name=jordan, GID=1002
2025-03-03T15:30:21+0800	2025-03-03T15:30:21.100876+08:00 judy-VirtualBox sudo: pam_unix(sudo:session): session opened for user root(uid=0) by judy(uid=1000)
2025-03-03T15:30:21+0800	2025-03-03T15:30:21.100528+08:00 judy-VirtualBox sudo: judy : TTY=pts/1 ; PWD=/home/judy ; USER=root ; COMMAND=/usr/sbin/adduser jordan

Time	Event
2025-03-03T15:30:13+0800	2025-03-03T15:30:13.658195+08:00 judy-VirtualBox sudo: pam_unix(sudo:session): session closed for user root
2025-03-03T15:30:13+0800	2025-03-03T15:30:13.656066+08:00 judy-VirtualBox gpasswd[118805]: members of group users set by root to judy,ziven
2025-03-03T15:30:12+0800	2025-03-03T15:30:12.242396+08:00 judy-VirtualBox chfn[118741]: changed user 'ziven' information
2025-03-03T15:30:10+0800	2025-03-03T15:30:10.195809+08:00 judy-VirtualBox passwd[118389]: gkr-pam: couldn't update the login keyring password: no old password was entered
2025-03-03T15:30:10+0800	2025-03-03T15:30:10.195134+08:00 judy-VirtualBox passwd[118389]: pam_unix(passwd:chauthtok): password changed for ziven
2025-03-03T15:30:01+0800	2025-03-03T15:30:01.886886+08:00 judy-VirtualBox CRON[118583]: pam_unix(cron:session): session closed for user root
2025-03-03T15:30:01+0800	2025-03-03T15:30:01.885788+08:00 judy-VirtualBox CRON[118583]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
2025-03-03T15:29:50+0800	2025-03-03T15:29:50.402302+08:00 judy-VirtualBox useradd[118376]: new user: name=ziven, UID=1001, GID= 1001, home=/home/ziven, shell=/bin/bash, from=/dev/pts/2
2025-03-03T15:29:50+0800	2025-03-03T15:29:50.388699+08:00 judy-VirtualBox groupadd[118369]: new group: name=ziven, GID=1001
2025-03-03T15:29:50+0800	2025-03-03T15:29:50.387801+08:00 judy-VirtualBox groupadd[118369]: group added to /etc/gshadow: name=ziven
2025-03-03T15:29:50+0800	2025-03-03T15:29:50.384267+08:00 judy-VirtualBox groupadd[118369]: group added to /etc/group: name=ziven, GID=1001
2025-03-03T15:29:50+0800	2025-03-03T15:29:50.318611+08:00 judy-VirtualBox sudo: pam_unix(sudo:session): session opened for user root(uid=0) by judy(uid=1000)
2025-03-03T15:29:50+0800	2025-03-03T15:29:50.318194+08:00 judy-VirtualBox sudo: judy : TTY=pts/1 ; PWD=/home/judy ; USER=root ; COMMAND=/usr/sbin/adduser ziven
2025-03-03T15:29:40+0800	2025-03-03T15:29:40.108341+08:00 judy-VirtualBox sudo: pam_unix(sudo:session): session closed for user root
2025-03-03T15:29:40+0800	2025-03-03T15:29:40.079699+08:00 judy-VirtualBox sudo: pam_unix(sudo:session): session opened for user root(uid=0) by judy(uid=1000)
2025-03-03T15:29:40+0800	2025-03-03T15:29:40.078649+08:00 judy-VirtualBox sudo: judy : TTY=pts/1 ; PWD=/home/judy ; USER=root ; COMMAND=/usr/sbin/adduser AAA
2025-03-03T15:29:24+0800	2025-03-03T15:29:24.853754+08:00 judy-VirtualBox systemd-logind[1046]: New session 62 of user judy.
2025-03-03T15:29:24+0800	2025-03-03T15:29:24.850671+08:00 judy-VirtualBox sshd[117803]: pam_unix(sshd:session): session opened for user judy(uid=1000) by judy(uid=0)
2025-03-03T15:29:24+0800	2025-03-03T15:29:24.848103+08:00 judy-VirtualBox sshd[117803]: Accepted password for judy from 10.167.214.40 port 3883 ssh2
2025-03-03T15:29:17+0800	2025-03-03T15:29:17.148870+08:00 judy-VirtualBox sudo: pam_unix(sudo:session): session closed for user root
2025-03-03T15:29:17+0800	2025-03-03T15:29:17.081044+08:00 judy-VirtualBox sudo: pam_unix(sudo:session): session opened for user root(uid=0) by judy(uid=1000)
2025-03-03T15:29:17+0800	2025-03-03T15:29:17.080747+08:00 judy-VirtualBox sudo: judy : TTY=pts/0 ; PWD=/home/judy ; USER=root ; COMMAND=/usr/bin/fail2ban-client set sshd unbanip 10.167.214.40
2025-03-03T15:29:15+0800	2025-03-03T15:29:15.809741+08:00 judy-VirtualBox sudo: pam_unix(sudo:session): session closed for user root
2025-03-03T15:29:15+0800	2025-03-03T15:29:15.761553+08:00 judy-VirtualBox sudo: pam_unix(sudo:session): session opened for user root(uid=0) by judy(uid=1000)
2025-03-03T15:29:15+0800	2025-03-03T15:29:15.761051+08:00 judy-VirtualBox sudo: judy : TTY=pts/0 ; PWD=/home/judy ; USER=root ; COMMAND=/usr/bin/fail2ban-client status sshd
2025-03-03T15:29:12+0800	2025-03-03T15:29:12.128002+08:00 judy-VirtualBox sudo: pam_unix(sudo:auth): authentication failure; logname= judy uid=1000 euid=0 tty=/dev/pts/0 ruser=judy rhost= user=judy
2025-03-03T15:29:02+0800	2025-03-03T15:29:02.658823+08:00 judy-VirtualBox gdm-password]: gkr-pam: unlocked login keyring
2025-03-03T15:25:01+0800	2025-03-03T15:25:01.869125+08:00 judy-VirtualBox CRON[114586]: pam_unix(cron:session): session closed for user root
2025-03-03T15:25:01+0800	2025-03-03T15:25:01.865141+08:00 judy-VirtualBox CRON[114586]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
2025-03-03T15:21:07+0800	2025-03-03T15:21:07.469918+08:00 judy-VirtualBox sshd[112476]: Connection reset by authenticating user judy 10. 167.214.40 port 3851 [preauth]
2025-03-03T15:21:07+0800	2025-03-03T15:21:07.439335+08:00 judy-VirtualBox sshd[112476]: Failed password for judy from 10.167.214.40 port 3851 ssh2
2025-03-03T15:21:07+0800	2025-03-03T15:21:07.263533+08:00 judy-VirtualBox sshd[112476]: Failed password for judy from 10.167.214.40 port 3851 ssh2
2025-03-03T15:21:05+0800	2025-03-03T15:21:05.318327+08:00 judy-VirtualBox sshd[112441]: Connection reset by authenticating user judy 10. 167.214.40 port 3850 [preauth]
2025-03-03T15:21:05+0800	2025-03-03T15:21:05.295021+08:00 judy-VirtualBox sshd[112441]: Failed password for judy from 10.167.214.40 port 3850 ssh2
2025-03-03T15:21:05+0800	2025-03-03T15:21:05.127773+08:00 judy-VirtualBox sshd[112441]: Failed password for judy from 10.167.214.40 port 3850 ssh2
2025-03-03T15:21:03+0800	2025-03-03T15:21:03.670416+08:00 judy-VirtualBox sshd[112398]: Connection reset by authenticating user judy 10. 167.214.40 port 3849 [preauth]
2025-03-03T15:21:03+0800	2025-03-03T15:21:03.655104+08:00 judy-VirtualBox sshd[112398]: Failed password for judy from 10.167.214.40 port 3849 ssh2
2025-03-03T15:21:03+0800	2025-03-03T15:21:03.495996+08:00 judy-VirtualBox sshd[112398]: Failed password for judy from 10.167.214.40 port 3849 ssh2
2025-03-03T15:21:00+0800	2025-03-03T15:21:00.842557+08:00 judy-VirtualBox systemd-logind[1046]: Removed session 58.
2025-03-03T15:21:00+0800	2025-03-03T15:21:00.841877+08:00 judy-VirtualBox systemd-logind[1046]: Session 58 logged out. Waiting for processes to exit.
2025-03-03T15:21:00+0800	2025-03-03T15:21:00.836888+08:00 judy-VirtualBox sshd[101218]: pam_unix(sshd:session): session closed for user judy
2025-03-03T15:21:00+0800	2025-03-03T15:21:00.835819+08:00 judy-VirtualBox sshd[101263]: Disconnected from user judy 10.167.214.40 port 3643
2025-03-03T15:21:00+0800	2025-03-03T15:21:00.835689+08:00 judy-VirtualBox sshd[101263]: Received disconnect from 10.167.214.40 port 3643:11: disconnected by user

Time	Event
2025-03-03T15:20:43+0800	2025-03-03T15:20:43.471888+08:00 judy-VirtualBox sudo: pam_unix(sudo:session): session closed for user root
2025-03-03T15:20:43+0800	2025-03-03T15:20:43.451382+08:00 judy-VirtualBox userdel[112184]: delete 'bob' from shadow group 'users'
2025-03-03T15:20:43+0800	2025-03-03T15:20:43.451365+08:00 judy-VirtualBox userdel[112184]: removed shadow group 'bob' owned by 'bob'
2025-03-03T15:20:43+0800	2025-03-03T15:20:43.451338+08:00 judy-VirtualBox userdel[112184]: removed group 'bob' owned by 'bob'
2025-03-03T15:20:43+0800	2025-03-03T15:20:43.450815+08:00 judy-VirtualBox userdel[112184]: delete 'bob' from group 'users'
2025-03-03T15:20:43+0800	2025-03-03T15:20:43.450754+08:00 judy-VirtualBox userdel[112184]: delete user 'bob'
2025-03-03T15:20:43+0800	2025-03-03T15:20:43.380171+08:00 judy-VirtualBox sudo: pam_unix(sudo:session): session opened for user root(uid=0) by judy(uid=1000)
2025-03-03T15:20:43+0800	2025-03-03T15:20:43.379609+08:00 judy-VirtualBox sudo: judy : TTY=pts/1 ; PWD=/home/judy ; USER=root ; COMMAND=/usr/sbin/deluser bob
2025-03-03T15:20:40+0800	2025-03-03T15:20:40.274208+08:00 judy-VirtualBox sudo: pam_unix(sudo:session): session closed for user root
2025-03-03T15:20:40+0800	2025-03-03T15:20:40.252264+08:00 judy-VirtualBox userdel[112161]: delete 'alex' from shadow group 'users'
2025-03-03T15:20:40+0800	2025-03-03T15:20:40.252205+08:00 judy-VirtualBox userdel[112161]: removed shadow group 'alex' owned by 'alex'
2025-03-03T15:20:40+0800	2025-03-03T15:20:40.252124+08:00 judy-VirtualBox userdel[112161]: removed group 'alex' owned by 'alex'
2025-03-03T15:20:40+0800	2025-03-03T15:20:40.251902+08:00 judy-VirtualBox userdel[112161]: delete 'alex' from group 'users'
2025-03-03T15:20:40+0800	2025-03-03T15:20:40.251364+08:00 judy-VirtualBox userdel[112161]: delete user 'alex'
2025-03-03T15:20:40+0800	2025-03-03T15:20:40.179778+08:00 judy-VirtualBox sudo: pam_unix(sudo:session): session opened for user root(uid=0) by judy(uid=1000)
2025-03-03T15:20:40+0800	2025-03-03T15:20:40.179505+08:00 judy-VirtualBox sudo: judy : TTY=pts/1 ; PWD=/home/judy ; USER=root ; COMMAND=/usr/sbin/deluser alex
2025-03-03T15:19:56+0800	2025-03-03T15:19:56.684477+08:00 judy-VirtualBox sudo: pam_unix(sudo:session): session closed for user root
2025-03-03T15:19:56+0800	2025-03-03T15:19:56.684329+08:00 judy-VirtualBox sudo: pam_unix(sudo:session): session opened for user root(uid=0) by judy(uid=1000)
2025-03-03T15:19:56+0800	2025-03-03T15:19:56.628778+08:00 judy-VirtualBox sudo: judy : TTY=pts/1 ; PWD=/home/judy ; USER=root ; COMMAND=/usr/sbin/adduser alicecat /etc/passwd
2025-03-03T15:17:01+0800	2025-03-03T15:17:01.829432+08:00 judy-VirtualBox CRON[110720]: pam_unix(cron:session): session closed for user root
2025-03-03T15:17:01+0800	2025-03-03T15:17:01.825348+08:00 judy-VirtualBox CRON[110720]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
2025-03-03T15:15:01+0800	2025-03-03T15:15:01.820155+08:00 judy-VirtualBox CRON[109236]: pam_unix(cron:session): session closed for user root
2025-03-03T15:15:01+0800	2025-03-03T15:15:01.817411+08:00 judy-VirtualBox CRON[109236]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
2025-03-03T15:10:03+0800	2025-03-03T15:10:03.822620+08:00 judy-VirtualBox sudo: pam_unix(sudo:session): session closed for user root
2025-03-03T15:10:03+0800	2025-03-03T15:10:03.793015+08:00 judy-VirtualBox userdel[105166]: delete 'alice' from shadow group 'users'
2025-03-03T15:10:03+0800	2025-03-03T15:10:03.792994+08:00 judy-VirtualBox userdel[105166]: removed shadow group 'alice' owned by 'alice'
2025-03-03T15:10:03+0800	2025-03-03T15:10:03.792960+08:00 judy-VirtualBox userdel[105166]: removed group 'alice' owned by 'alice'
2025-03-03T15:10:03+0800	2025-03-03T15:10:03.792195+08:00 judy-VirtualBox userdel[105166]: delete 'alice' from group 'users'
2025-03-03T15:10:03+0800	2025-03-03T15:10:03.792108+08:00 judy-VirtualBox userdel[105166]: delete user 'alice'
2025-03-03T15:10:03+0800	2025-03-03T15:10:03.600343+08:00 judy-VirtualBox sudo: pam_unix(sudo:session): session opened for user root(uid=0) by judy(uid=1000)
2025-03-03T15:10:03+0800	2025-03-03T15:10:03.600046+08:00 judy-VirtualBox sudo: judy : TTY=pts/1 ; PWD=/home/judy ; USER=root ; COMMAND=/usr/sbin/deluser alice
2025-03-03T15:06:03+0800	2025-03-03T15:06:03.879902+08:00 judy-VirtualBox sudo: pam_unix(sudo:session): session closed for user root
2025-03-03T15:06:03+0800	2025-03-03T15:06:03.877787+08:00 judy-VirtualBox gpasswd[101360]: members of group users set by root to judy,alex,bob,alice
2025-03-03T15:06:01+0800	2025-03-03T15:06:01.857057+08:00 judy-VirtualBox chfn[101336]: changed user 'alice' information
2025-03-03T15:05:53+0800	2025-03-03T15:05:53.752018+08:00 judy-VirtualBox passwd[101317]: gkr-pam: couldn't update the login keyring password: no old password was entered
2025-03-03T15:05:53+0800	2025-03-03T15:05:53.751895+08:00 judy-VirtualBox passwd[101317]: pam_unix(passwd:chauthtok): password changed for alice
2025-03-03T15:05:37+0800	2025-03-03T15:05:37.847511+08:00 judy-VirtualBox useradd[101303]: new user: name=alice, UID=1004, GID=1004, home=/home/alice, shell=/bin/bash, from=/dev/pts/2
2025-03-03T15:05:37+0800	2025-03-03T15:05:37.770923+08:00 judy-VirtualBox groupadd[101296]: new group: name=alice, GID=1004
2025-03-03T15:05:37+0800	2025-03-03T15:05:37.769969+08:00 judy-VirtualBox groupadd[101296]: group added to /etc/gshadow: name=alice
2025-03-03T15:05:37+0800	2025-03-03T15:05:37.767069+08:00 judy-VirtualBox groupadd[101296]: group added to /etc/group: name=alice, GID=1004
2025-03-03T15:05:37+0800	2025-03-03T15:05:37.478811+08:00 judy-VirtualBox sudo: pam_unix(sudo:session): session opened for user root(uid=0) by judy(uid=1000)
2025-03-03T15:05:37+0800	2025-03-03T15:05:37.478453+08:00 judy-VirtualBox sudo: judy : TTY=pts/1 ; PWD=/home/judy ; USER=root ; COMMAND=/usr/sbin/adduser alice
2025-03-03T15:05:26+0800	2025-03-03T15:05:26.408846+08:00 judy-VirtualBox systemd-logind[1046]: New session 58 of user judy.
2025-03-03T15:05:26+0800	2025-03-03T15:05:26.407965+08:00 judy-VirtualBox sshd[101218]: pam_unix(sshd:session): session opened for user judy(uid=1000) by judy(uid=0)
2025-03-03T15:05:26+0800	2025-03-03T15:05:26.279209+08:00 judy-VirtualBox sshd[101218]: Accepted password for judy from 10.167.214.40 port 3643 ssh2
2025-03-03T15:05:22+0800	2025-03-03T15:05:22.026193+08:00 judy-VirtualBox sudo: pam_unix(sudo:session): session closed for user root

Time	Event
2025-03-03T15:05:21+0800	2025-03-03T15:05:21.974050+08:00 judy-VirtualBox sudo: pam_unix(sudo:session): session opened for user root(uid=0) by judy(uid=1000)
2025-03-03T15:05:21+0800	2025-03-03T15:05:21.961130+08:00 judy-VirtualBox sudo:　　judy : TTY=pts/0 ; PWD=/home/judy ; USER=root ; COMMAND=/usr/bin/fail2ban-client set sshd unbanip 10.167.214.40
2025-03-03T15:05:01+0800	2025-03-03T15:05:01.757162+08:00 judy-VirtualBox CRON[101182]: pam_unix(cron:session): session closed for user root
2025-03-03T15:05:01+0800	2025-03-03T15:05:01.754227+08:00 judy-VirtualBox CRON[101182]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
2025-03-03T15:04:24+0800	2025-03-03T15:04:24.979666+08:00 judy-VirtualBox sshd[100717]: Connection reset by invalid user byron 10.167.214.35 port 8509 [preauth]
2025-03-03T15:04:24+0800	2025-03-03T15:04:24.971027+08:00 judy-VirtualBox sshd[100717]: message repeated 2 times: [Failed password for invalid user byron from 10.167.214.35 port 8509 ssh2]
2025-03-03T15:04:15+0800	2025-03-03T15:04:15.311186+08:00 judy-VirtualBox sshd[100717]: Failed password for invalid user byron from 10.167.214.35 port 8509 ssh2
2025-03-03T15:04:13+0800	2025-03-03T15:04:13.118821+08:00 judy-VirtualBox sshd[100717]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=10.167.214.35
2025-03-03T15:04:13+0800	2025-03-03T15:04:13.118563+08:00 judy-VirtualBox sshd[100717]: pam_unix(sshd:auth): check pass; user unknown
2025-03-03T15:04:10+0800	2025-03-03T15:04:10.821628+08:00 judy-VirtualBox sshd[100717]: Invalid user byron from 10.167.214.35 port 8509
2025-03-03T15:03:32+0800	2025-03-03T15:03:32.440861+08:00 judy-VirtualBox sudo: pam_unix(sudo:session): session closed for user root
2025-03-03T15:03:32+0800	2025-03-03T15:03:32.392737+08:00 judy-VirtualBox sudo: pam_unix(sudo:session): session opened for user root(uid=0) by judy(uid=1000)
2025-03-03T15:03:32+0800	2025-03-03T15:03:32.392103+08:00 judy-VirtualBox sudo:　　judy : TTY=pts/0 ; PWD=/home/judy ; USER=root ; COMMAND=/usr/bin/fail2ban-client status sshd
2025-03-03T15:03:27+0800	2025-03-03T15:03:27.045576+08:00 judy-VirtualBox sshd[100505]: Connection reset by authenticating user judy 10. 167.214.40 port 3632 [preauth]
2025-03-03T15:03:27+0800	2025-03-03T15:03:27.033583+08:00 judy-VirtualBox sshd[100505]: Failed password for judy from 10.167.214.40 port 3632 ssh2
2025-03-03T15:03:26+0800	2025-03-03T15:03:26.817503+08:00 judy-VirtualBox sshd[100505]: Failed password for judy from 10.167.214.40 port 3632 ssh2
2025-03-03T15:03:24+0800	2025-03-03T15:03:24.729469+08:00 judy-VirtualBox sshd[100468]: Connection reset by authenticating user judy 10. 167.214.40 port 3631 [preauth]
2025-03-03T15:03:24+0800	2025-03-03T15:03:24.713310+08:00 judy-VirtualBox sshd[100468]: Failed password for judy from 10.167.214.40 port 3631 ssh2
2025-03-03T15:03:24+0800	2025-03-03T15:03:24.505993+08:00 judy-VirtualBox sshd[100468]: Failed password for judy from 10.167.214.40 port 3631 ssh2
2025-03-03T15:03:23+0800	2025-03-03T15:03:23.254710+08:00 judy-VirtualBox sshd[100417]: Connection reset by authenticating user judy 10. 167.214.40 port 3630 [preauth]
2025-03-03T15:03:23+0800	2025-03-03T15:03:23.241864+08:00 judy-VirtualBox sshd[100417]: Failed password for judy from 10.167.214.40 port 3630 ssh2
2025-03-03T15:03:23+0800	2025-03-03T15:03:23.073364+08:00 judy-VirtualBox sshd[100417]: Failed password for judy from 10.167.214.40 port 3630 ssh2

authlog-time

PDF export is not available for visualizations using trellis layout.

difhost-changepw

splunk>