Container Anomaly Detection

Tübix 2017

Stefan Jakoby - 24. Juni 2017

Trusted partner for your Digital Journey

Atos

Vorstellung

Stefan Jakoby
Computer Networking

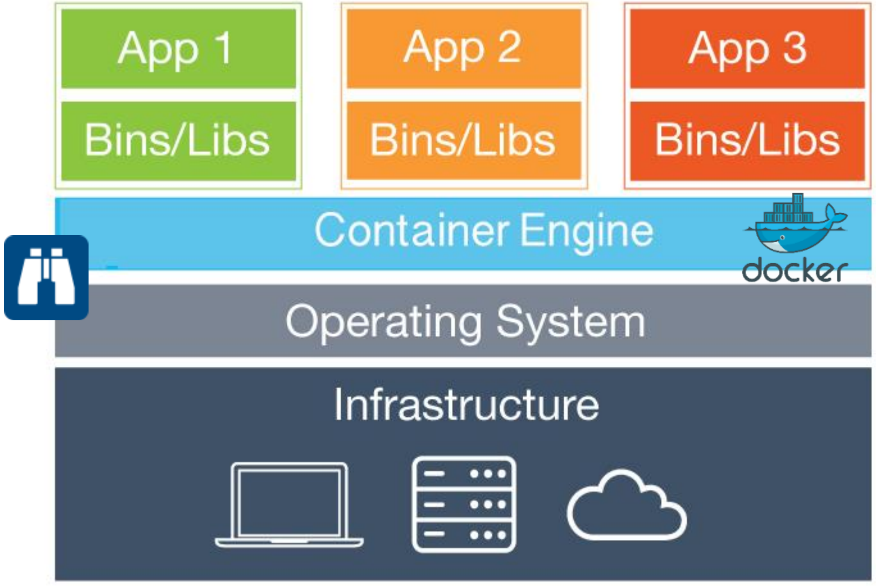
Prof. Dr. Reich
Hochschule Furtwangen

- High Performance Computing
- Systemmanagement
- IT-Sicherheit

Holger Gantikow
science & computing ag
Tübingen

1 Überblick

Container Anomaly Detection
The Big Picture



Container virtualization

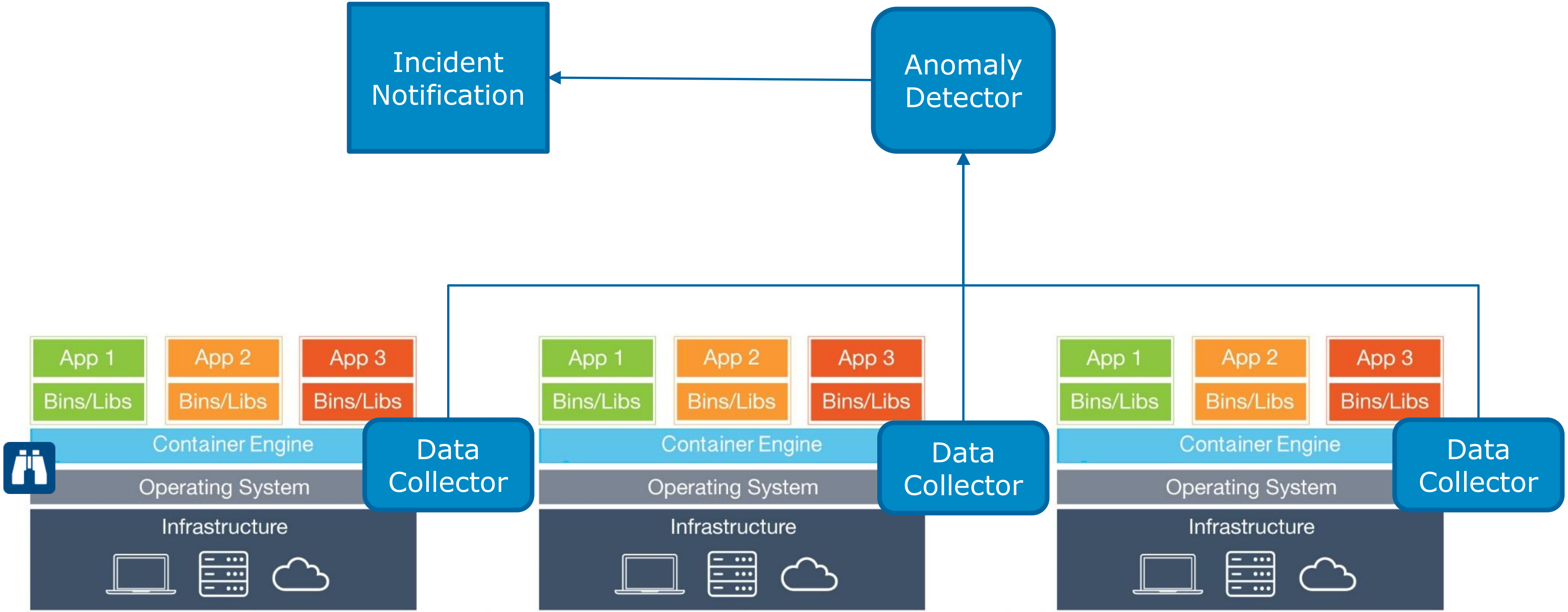
- *“Host-based IDS with Container Support”*
- *Agentless-approach*

- Keine Image-Modifikation erforderlich
- Stärkere Isolierung

- Anwender muss mit “Überwachung” einverstanden sein

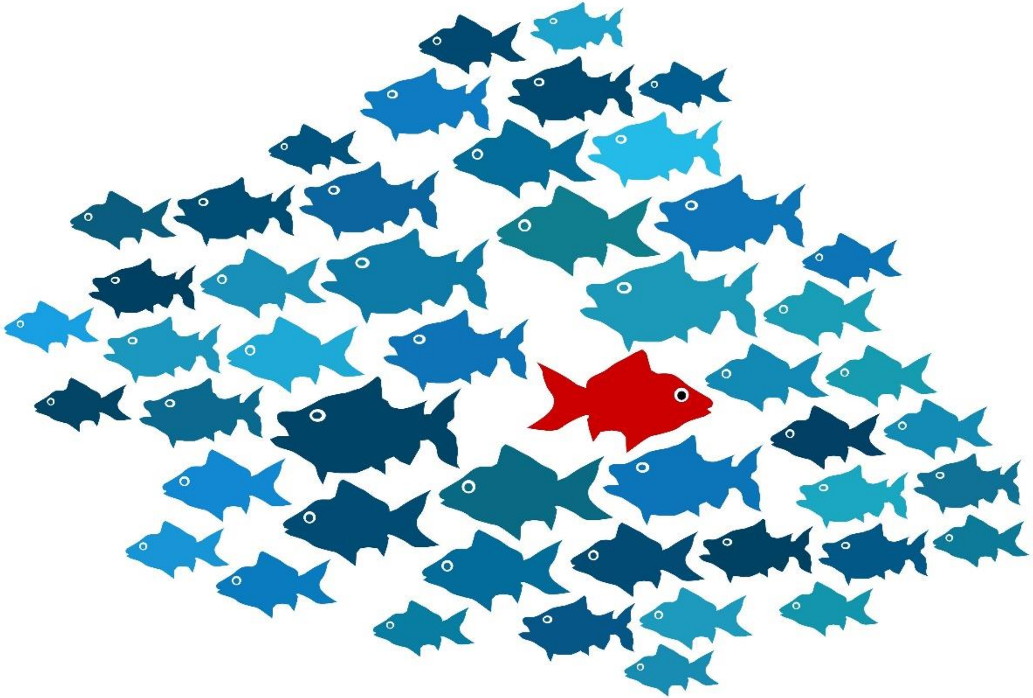
Container Anomaly Detection

The Big Picture²



Container Anomaly Detection

The Big Picture - Anomalien



- Erhöhte CPU-Last
- Prozesse
- Dateizugriffe
- Netzwerkverbindungen /-Ports
- Speicherallokation
- ...

2 Durchführung

Anomaly Detection
Werkzeug

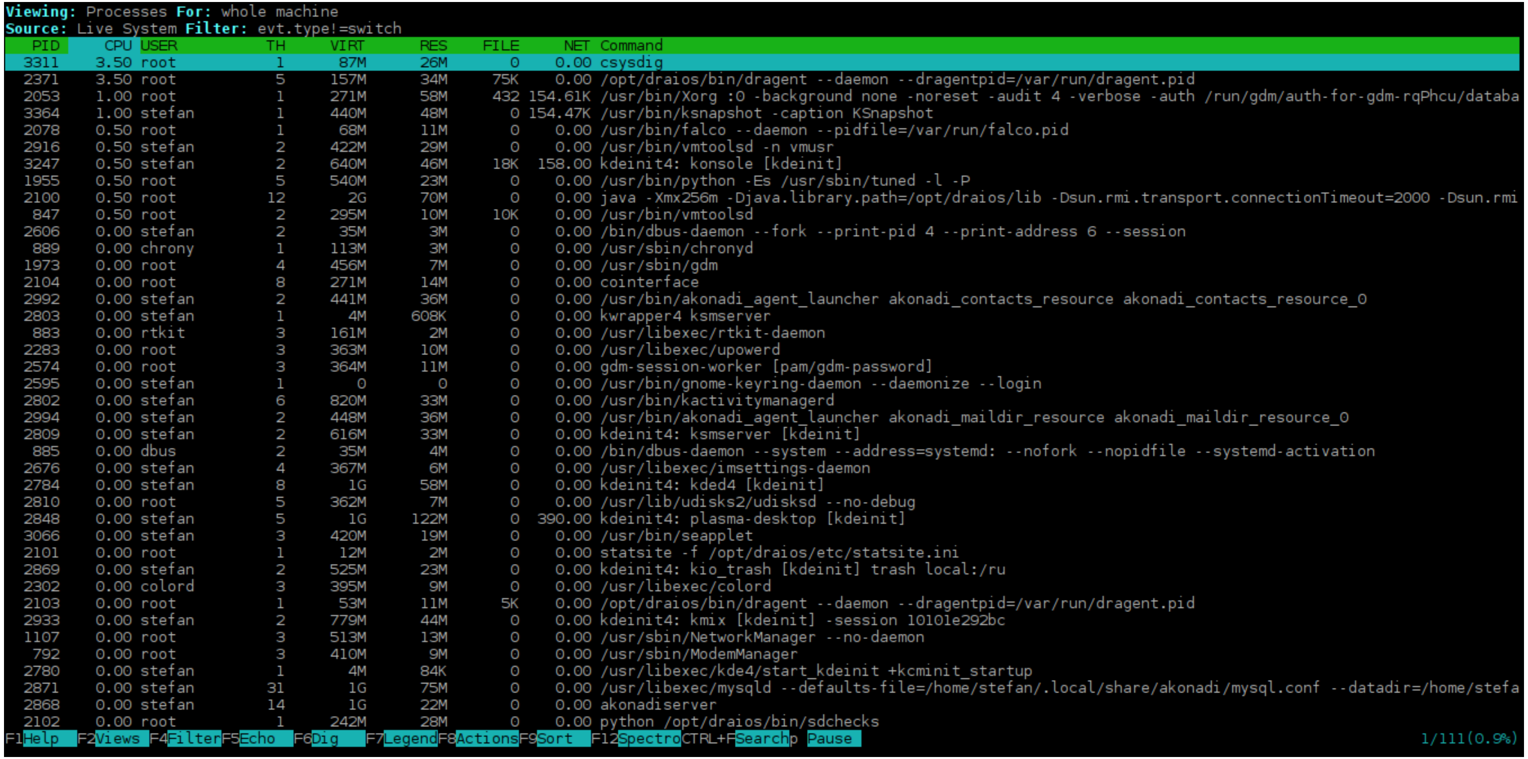
sysdig

- Werkzeug zur universellen Überwachung der Systemaktivitäten eines Linux-Systems
- Kernel-Modul
- System-Calls
- Native Container-Unterstützung
- *"strace + tcpdump + htop + iftop + lsof + transaction tracing + awesome sauce"*

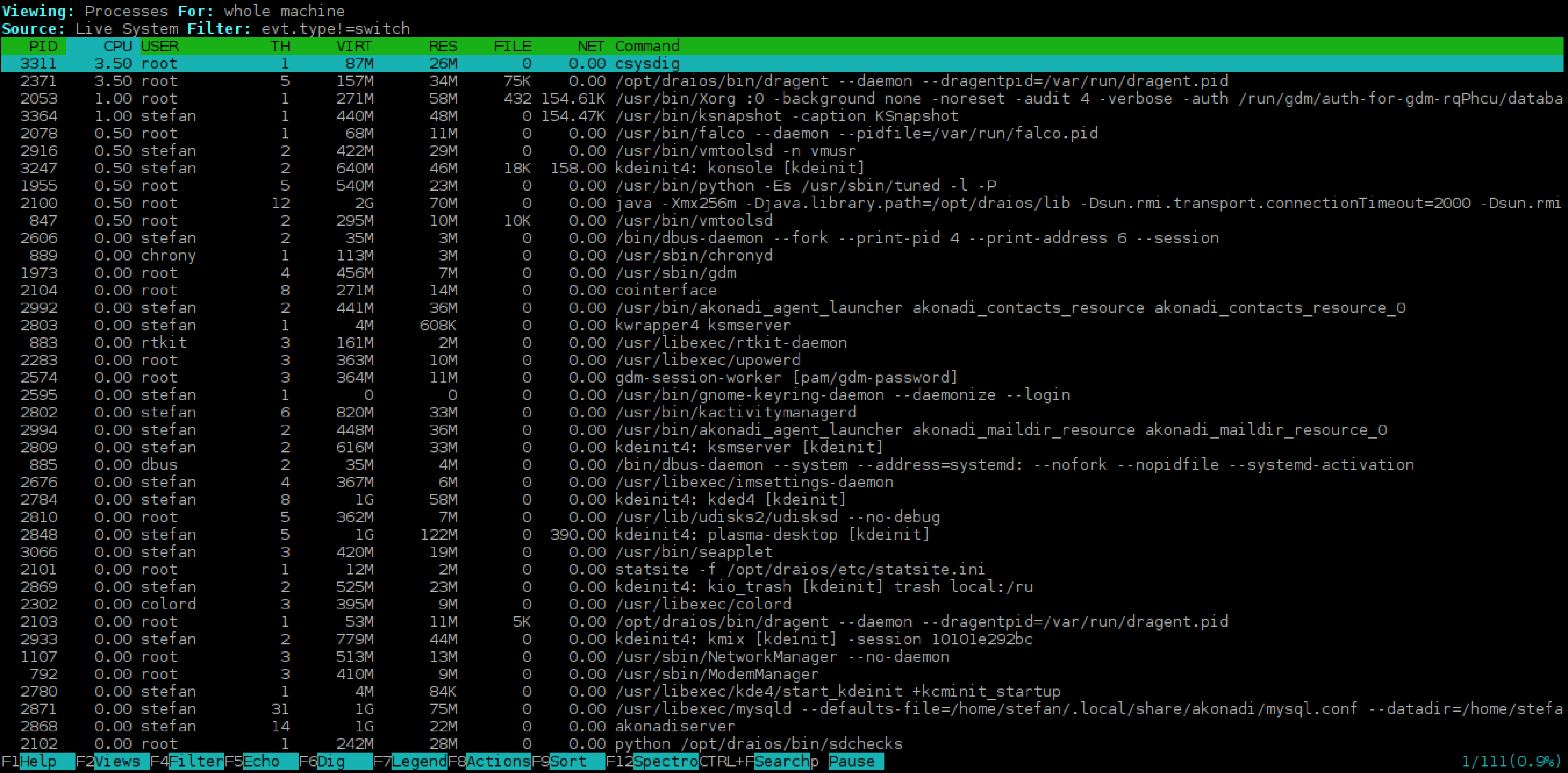
sysdig falco

- Regelbasierte Erkennung von Ereignissen

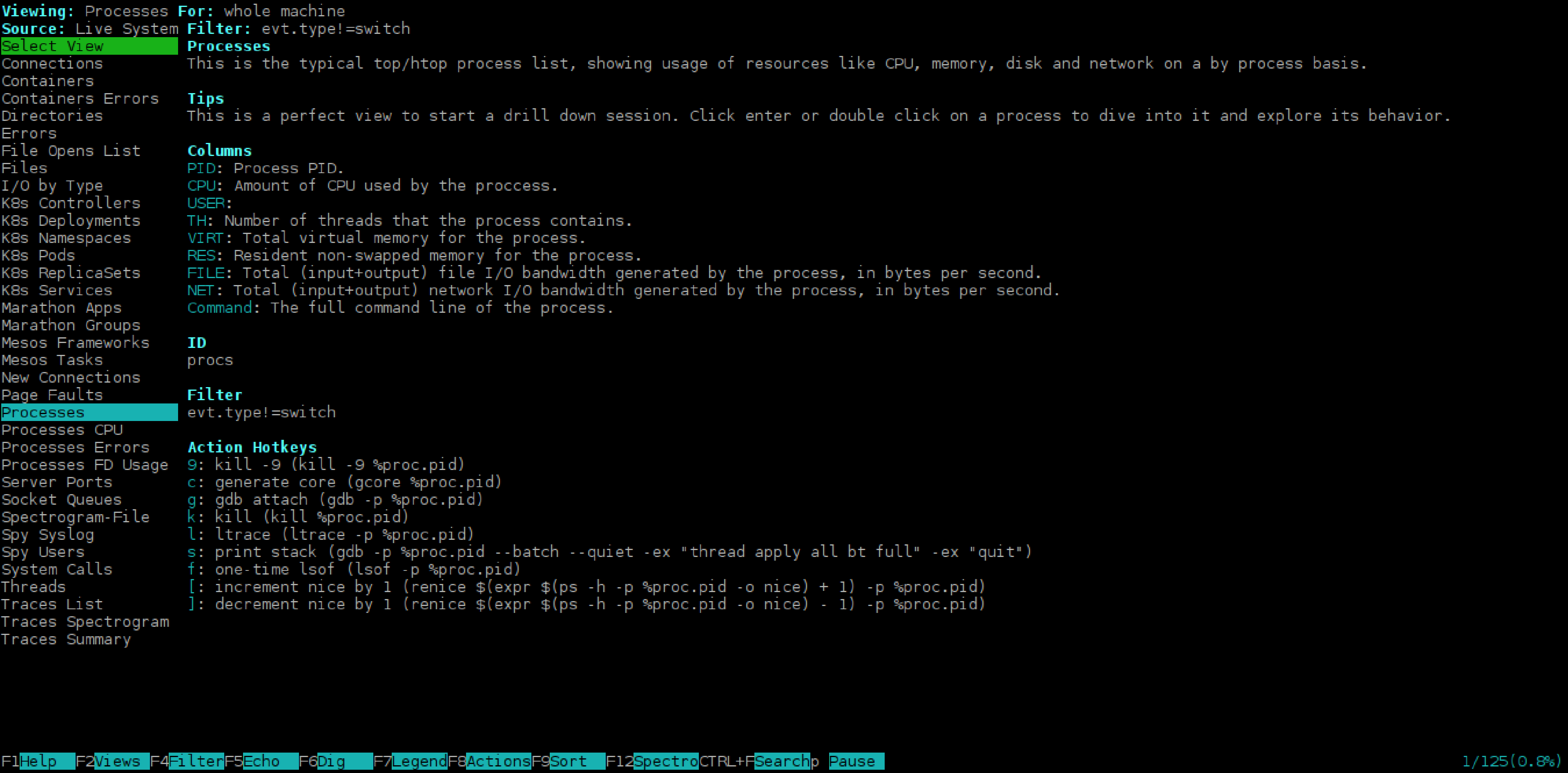
Anomaly Detection
Sysdig



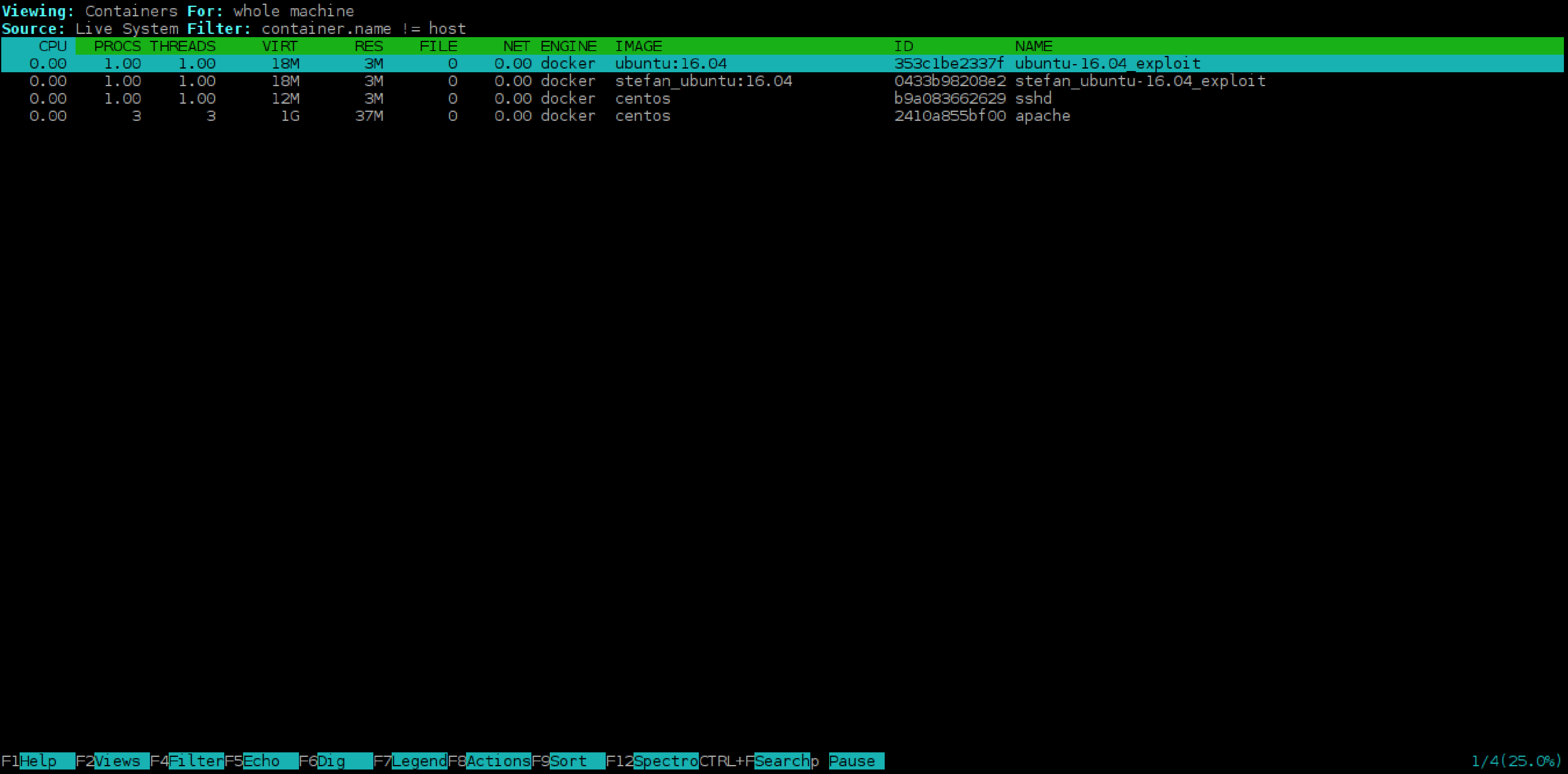
```
Viewing: Processes For: whole machine
Source: Live System Filter: evt.type!=switch
  PID    CPU USER         TH     VIRT      RES     FILE      NET Command
 3311   3.50 root          1      87M      26M        0     0.00 csysdig
 2371   3.50 root          5     157M      34M      75K     0.00 /opt/draios/bin/dragent --daemon --dragentpid=/var/run/dragent.pid
 2053   1.00 root          1     271M      58M      432  154.61K /usr/bin/Xorg :0 -background none -noreset -audit 4 -verbose -auth /run/gdm/auth-for-gdm-rqPhcu/databa
 3364   1.00 stefan        1     440M      48M        0  154.47K /usr/bin/ksnapshot -caption KSnapshot
 2078   0.50 root          1      68M      11M        0     0.00 /usr/bin/falco --daemon --pidfile=/var/run/falco.pid
 2916   0.50 stefan        2     422M      29M        0     0.00 /usr/bin/vmtoolsd -n vmusr
 3247   0.50 stefan        2     640M      46M      18K   158.00 kdeinit4: konsole [kdeinit]
 1955   0.50 root          5     540M      23M        0     0.00 /usr/bin/python -Es /usr/sbin/tuned -l -P
 2100   0.50 root         12       2G      70M        0     0.00 java -Xmx256m -Djava.library.path=/opt/draios/lib -Dsun.rmi.transport.connectionTimeout=2000 -Dsun.rmi
  847   0.50 root          2     295M      10M      10K     0.00 /usr/bin/vmtoolsd
 2606   0.00 stefan        2      35M       3M        0     0.00 /bin/dbus-daemon --fork --print-pid 4 --print-address 6 --session
  889   0.00 chrony        1     113M       3M        0     0.00 /usr/sbin/chronyd
 1973   0.00 root          4     456M       7M        0     0.00 /usr/sbin/gdm
 2104   0.00 root          8     271M      14M        0     0.00 cointerface
 2992   0.00 stefan        2     441M      36M        0     0.00 /usr/bin/akonadi_agent_launcher akonadi_contacts_resource akonadi_contacts_resource_0
 2803   0.00 stefan        1       4M     608K        0     0.00 kwrapper4 ksmserver
  883   0.00 rtkit         3     161M       2M        0     0.00 /usr/libexec/rtkit-daemon
 2283   0.00 root          3     363M      10M        0     0.00 /usr/libexec/upowerd
 2574   0.00 root          3     364M      11M        0     0.00 gdm-session-worker [pam/gdm-password]
 2595   0.00 stefan        1        0        0        0     0.00 /usr/bin/gnome-keyring-daemon --daemonize --login
 2802   0.00 stefan        6     820M      33M        0     0.00 /usr/bin/kactivitymanagerd
 2994   0.00 stefan        2     448M      36M        0     0.00 /usr/bin/akonadi_agent_launcher akonadi_maildir_resource akonadi_maildir_resource_0
 2809   0.00 stefan        2     616M      33M        0     0.00 kdeinit4: ksmserver [kdeinit]
  885   0.00 dbus          2      35M       4M        0     0.00 /bin/dbus-daemon --system --address=systemd: --nofork --nopidfile --systemd-activation
 2676   0.00 stefan        4     367M       6M        0     0.00 /usr/libexec/imsettings-daemon
 2784   0.00 stefan        8       1G      58M        0     0.00 kdeinit4: kded4 [kdeinit]
 2810   0.00 root          5     362M       7M        0     0.00 /usr/lib/udisks2/udisksd --no-debug
 2848   0.00 stefan        5       1G     122M        0   390.00 kdeinit4: plasma-desktop [kdeinit]
 3066   0.00 stefan        3     420M      19M        0     0.00 /usr/bin/seapplet
 2101   0.00 root          1      12M       2M        0     0.00 statsite -f /opt/draios/etc/statsite.ini
 2869   0.00 stefan        2     525M      23M        0     0.00 kdeinit4: kio_trash [kdeinit] trash local:/ru
 2302   0.00 colord        3     395M       9M        0     0.00 /usr/libexec/colord
 2103   0.00 root          1      53M      11M       5K     0.00 /opt/draios/bin/dragent --daemon --dragentpid=/var/run/dragent.pid
 2933   0.00 stefan        2     779M      44M        0     0.00 kdeinit4: kmix [kdeinit] -session 10101e292bc
 1107   0.00 root          3     513M      13M        0     0.00 /usr/sbin/NetworkManager --no-daemon
  792   0.00 root          3     410M       9M        0     0.00 /usr/sbin/ModemManager
 2780   0.00 stefan        1       4M      84K        0     0.00 /usr/libexec/kde4/start_kdeinit +kcminit_startup
 2871   0.00 stefan       31       1G      75M        0     0.00 /usr/libexec/mysqld --defaults-file=/home/stefan/.local/share/akonadi/mysql.conf --datadir=/home/stefa
 2868   0.00 stefan       14       1G      22M        0     0.00 akonadiserver
 2102   0.00 root          1     242M      28M        0     0.00 python /opt/draios/bin/sdchecks
F1Help  F2Views  F4FilterF5Echo  F6Dig    F7LegendF8ActionsF9Sort   F12SpectroCTRL+FSearchp Pause                                                       1/111(0.9%)
```



```
Viewing: Processes For: whole machine
Source: Live System Filter: evt.type!=switch
   PID     CPU USER           TH     VIRT      RES    FILE     NET Command
  3311    3.50 root           1      87M      26M       0    0.00 csysdig
  2371    3.50 root           5     157M      34M     75K    0.00 /opt/draios/bin/dragent --daemon --dragentpid=/var/run/dragent.pid
  2053    1.00 root           1     271M      58M     432 154.61K /usr/bin/Xorg :0 -background none -noreset -audit 4 -verbose -auth /run/gdm/auth-for-gdm-rqPhcu/databa
  3364    1.00 stefan         1     440M      48M       0 154.47K /usr/bin/ksnapshot -caption KSnapshot
  2078    0.50 root           1      68M      11M       0    0.00 /usr/bin/falco --daemon --pidfile=/var/run/falco.pid
  2916    0.50 stefan         2     422M      29M       0    0.00 /usr/bin/vmtoolsd -n vmusr
  3247    0.50 stefan         2     640M      46M     18K  158.00 kdeinit4: konsole [kdeinit]
  1955    0.50 root           5     540M      23M       0    0.00 /usr/bin/python -Es /usr/sbin/tuned -l -P
  2100    0.50 root          12       2G      70M       0    0.00 java -Xmx256m -Djava.library.path=/opt/draios/lib -Dsun.rmi.transport.connectionTimeout=2000 -Dsun.rmi
   847    0.50 root           2     295M      10M     10K    0.00 /usr/bin/vmtoolsd
  2606    0.00 stefan         2      35M       3M       0    0.00 /bin/dbus-daemon --fork --print-pid 4 --print-address 6 --session
   889    0.00 chrony         1     113M       3M       0    0.00 /usr/sbin/chronyd
  1973    0.00 root           4     456M       7M       0    0.00 /usr/sbin/gdm
  2104    0.00 root           8     271M      14M       0    0.00 cointerface
  2992    0.00 stefan         2     441M      36M       0    0.00 /usr/bin/akonadi_agent_launcher akonadi_contacts_resource akonadi_contacts_resource_0
  2803    0.00 stefan         1       4M     608K       0    0.00 kwrapper4 ksmserver
   883    0.00 rtkit          3     161M       2M       0    0.00 /usr/libexec/rtkit-daemon
  2283    0.00 root           3     363M      10M       0    0.00 /usr/libexec/upowerd
  2574    0.00 root           3     364M      11M       0    0.00 gdm-session-worker [pam/gdm-password]
  2595    0.00 stefan         1        0        0       0    0.00 /usr/bin/gnome-keyring-daemon --daemonize --login
  2802    0.00 stefan         6     820M      33M       0    0.00 /usr/bin/kactivitymanagerd
  2994    0.00 stefan         2     448M      36M       0    0.00 /usr/bin/akonadi_agent_launcher akonadi_maildir_resource akonadi_maildir_resource_0
  2809    0.00 stefan         2     616M      33M       0    0.00 kdeinit4: ksmserver [kdeinit]
   885    0.00 dbus           2      35M       4M       0    0.00 /bin/dbus-daemon --system --address=systemd: --nofork --nopidfile --systemd-activation
  2676    0.00 stefan         4     367M       6M       0    0.00 /usr/libexec/imsettings-daemon
  2784    0.00 stefan         8       1G      58M       0    0.00 kdeinit4: kded4 [kdeinit]
  2810    0.00 root           5     362M       7M       0    0.00 /usr/lib/udisks2/udisksd --no-debug
  2848    0.00 stefan         5       1G     122M       0  390.00 kdeinit4: plasma-desktop [kdeinit]
  3066    0.00 stefan         3     420M      19M       0    0.00 /usr/bin/seapplet
  2101    0.00 root           1      12M       2M       0    0.00 statsite -f /opt/draios/etc/statsite.ini
  2869    0.00 stefan         2     525M      23M       0    0.00 kdeinit4: kio_trash [kdeinit] trash local:/ru
  2302    0.00 colord         3     395M       9M       0    0.00 /usr/libexec/colord
  2103    0.00 root           1      53M      11M      5K    0.00 /opt/draios/bin/dragent --daemon --dragentpid=/var/run/dragent.pid
  2933    0.00 stefan         2     779M      44M       0    0.00 kdeinit4: kmix [kdeinit] -session 10101e292bc
  1107    0.00 root           3     513M      13M       0    0.00 /usr/sbin/NetworkManager --no-daemon
   792    0.00 root           3     410M       9M       0    0.00 /usr/sbin/ModemManager
  2780    0.00 stefan         1       4M      84K       0    0.00 /usr/libexec/kde4/start_kdeinit +kcminit_startup
  2871    0.00 stefan        31       1G      75M       0    0.00 /usr/libexec/mysqld --defaults-file=/home/stefan/.local/share/akonadi/mysql.conf --datadir=/home/stefa
  2868    0.00 stefan        14       1G      22M       0    0.00 akonadiserver
  2102    0.00 root           1     242M      28M       0    0.00 python /opt/draios/bin/sdchecks
F1Help  F2Views F4FilterF5Echo  F6Dig   F7LegendF8ActionsF9Sort  F12SpectroCTRL+FSearchp Pause                                                               1/111(0.9%)
```

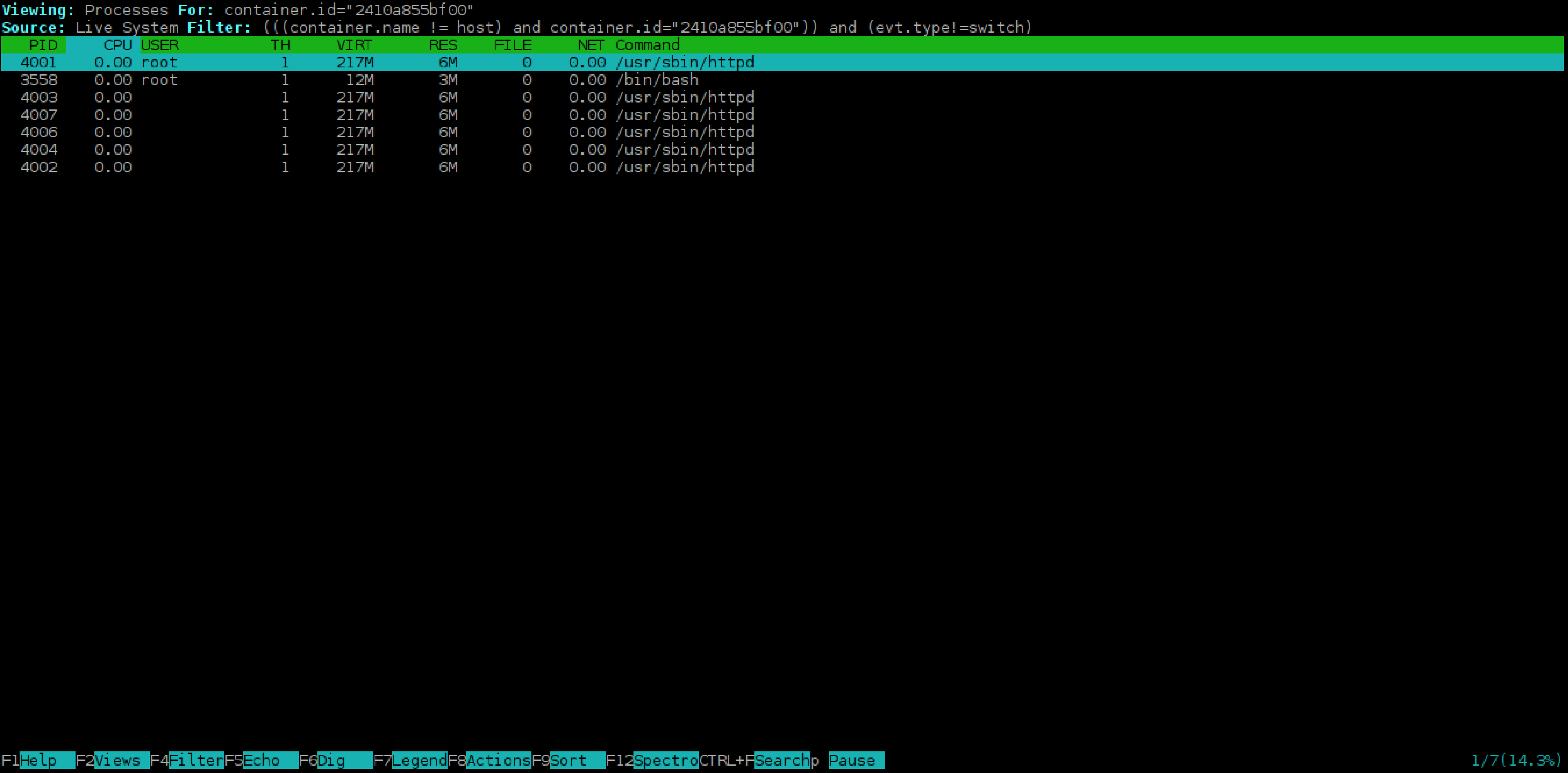


```
Viewing: Processes For: whole machine
Source: Live System Filter: evt.type!=switch
Select View         Processes
Connections         This is the typical top/htop process list, showing usage of resources like CPU, memory, disk and network on a by process basis.
Containers
Containers Errors   Tips
Directories         This is a perfect view to start a drill down session. Click enter or double click on a process to dive into it and explore its behavior.
Errors
File Opens List     Columns
Files               PID: Process PID.
I/O by Type         CPU: Amount of CPU used by the proccess.
K8s Controllers     USER:
K8s Deployments     TH: Number of threads that the process contains.
K8s Namespaces      VIRT: Total virtual memory for the process.
K8s Pods            RES: Resident non-swapped memory for the process.
K8s ReplicaSets     FILE: Total (input+output) file I/O bandwidth generated by the process, in bytes per second.
K8s Services        NET: Total (input+output) network I/O bandwidth generated by the process, in bytes per second.
Marathon Apps       Command: The full command line of the process.
Marathon Groups
Mesos Frameworks    ID
Mesos Tasks         procs
New Connections
Page Faults         Filter
Processes           evt.type!=switch
Processes CPU
Processes Errors    Action Hotkeys
Processes FD Usage  9: kill -9 (kill -9 %proc.pid)
Server Ports        c: generate core (gcore %proc.pid)
Socket Queues       g: gdb attach (gdb -p %proc.pid)
Spectrogram-File    k: kill (kill %proc.pid)
Spy Syslog          l: ltrace (ltrace -p %proc.pid)
Spy Users           s: print stack (gdb -p %proc.pid --batch --quiet -ex "thread apply all bt full" -ex "quit")
System Calls        f: one-time lsof (lsof -p %proc.pid)
Threads             [: increment nice by 1 (renice $(expr $(ps -h -p %proc.pid -o nice) + 1) -p %proc.pid)
Traces List         ]: decrement nice by 1 (renice $(expr $(ps -h -p %proc.pid -o nice) - 1) -p %proc.pid)
Traces Spectrogram
Traces Summary



F1Help  F2Views  F4FilterF5Echo  F6Dig    F7LegendF8ActionsF9Sort   F12SpectroCTRL+FSearchp Pause                                                         1/125(0.8%)
```

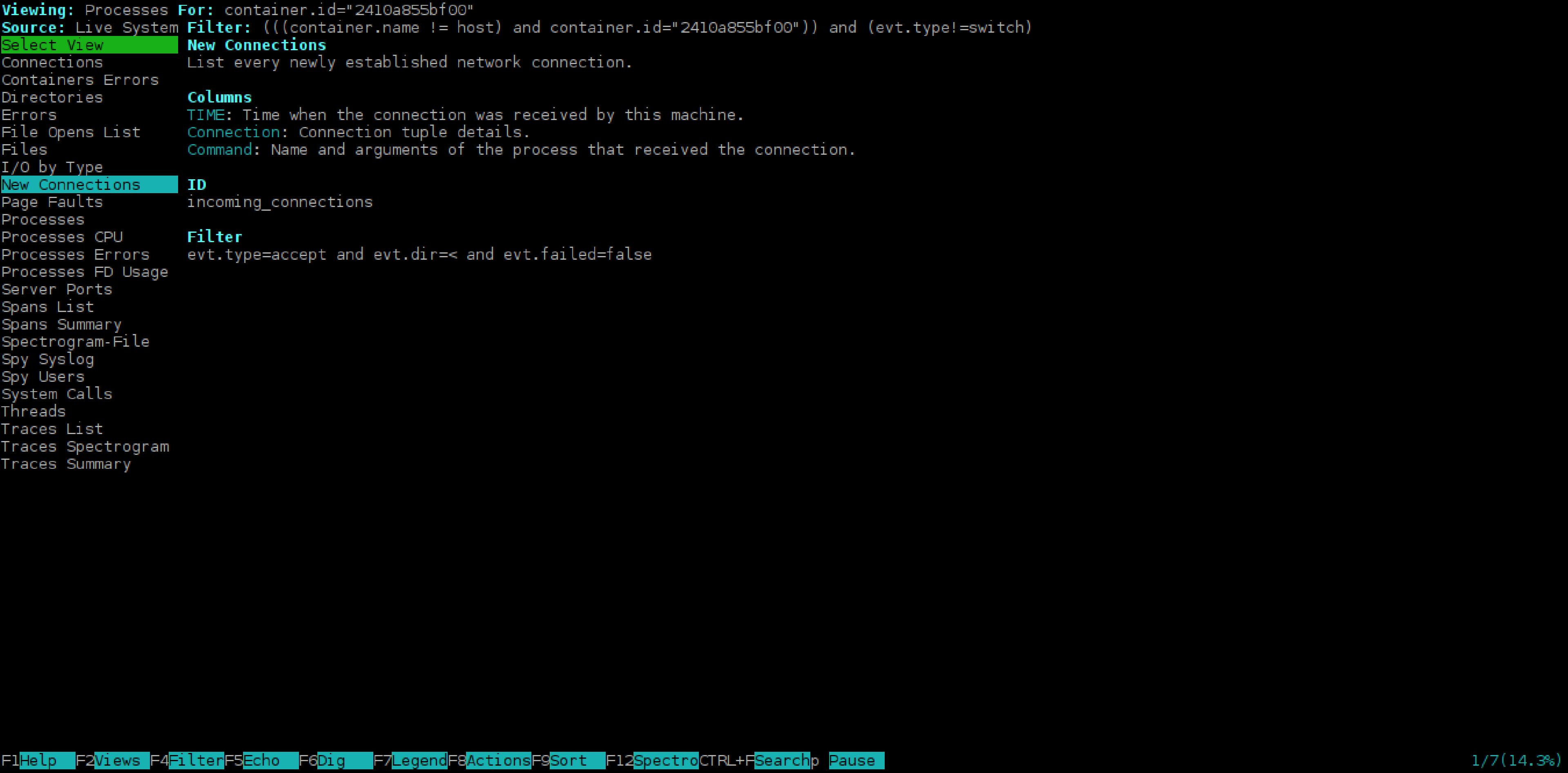


```
Viewing: Containers For: whole machine
Source: Live System Filter: container.name != host
    CPU   PROCS THREADS     VIRT      RES    FILE     NET ENGINE  IMAGE                         ID           NAME
   0.00    1.00    1.00      18M       3M       0    0.00 docker  ubuntu:16.04                  353c1be2337f ubuntu-16.04_exploit
   0.00    1.00    1.00      18M       3M       0    0.00 docker  stefan_ubuntu:16.04           0433b98208e2 stefan_ubuntu-16.04_exploit
   0.00    1.00    1.00      12M       3M       0    0.00 docker  centos                        b9a083662629 sshd
   0.00       3       3       1G      37M       0    0.00 docker  centos                        2410a855bf00 apache
```

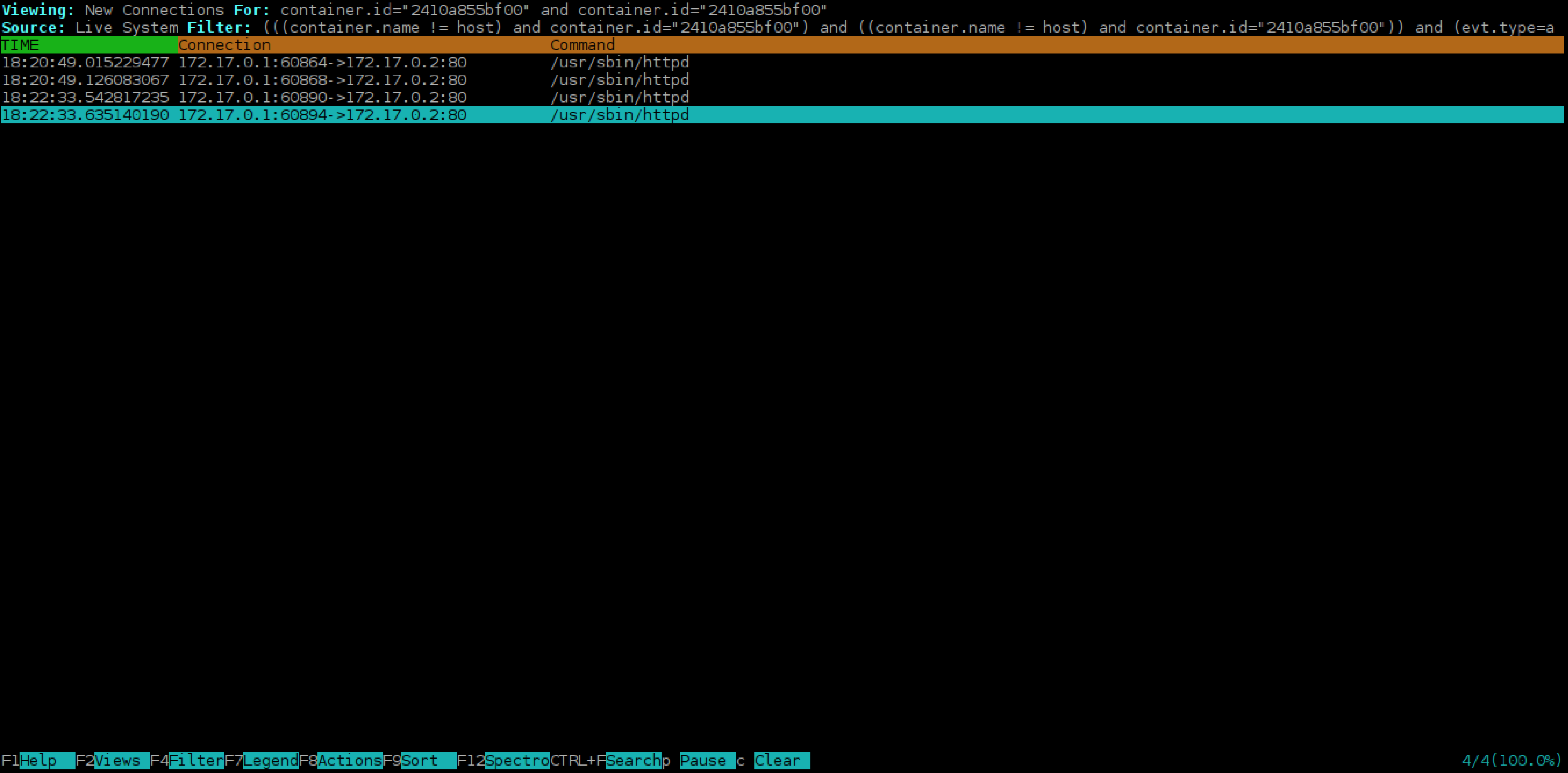
```
F1Help  F2Views  F4FilterF5Echo  F6Dig   F7LegendF8ActionsF9Sort  F12SpectroCTRL+FSearchp Pause                  1/4(25.0%)
```



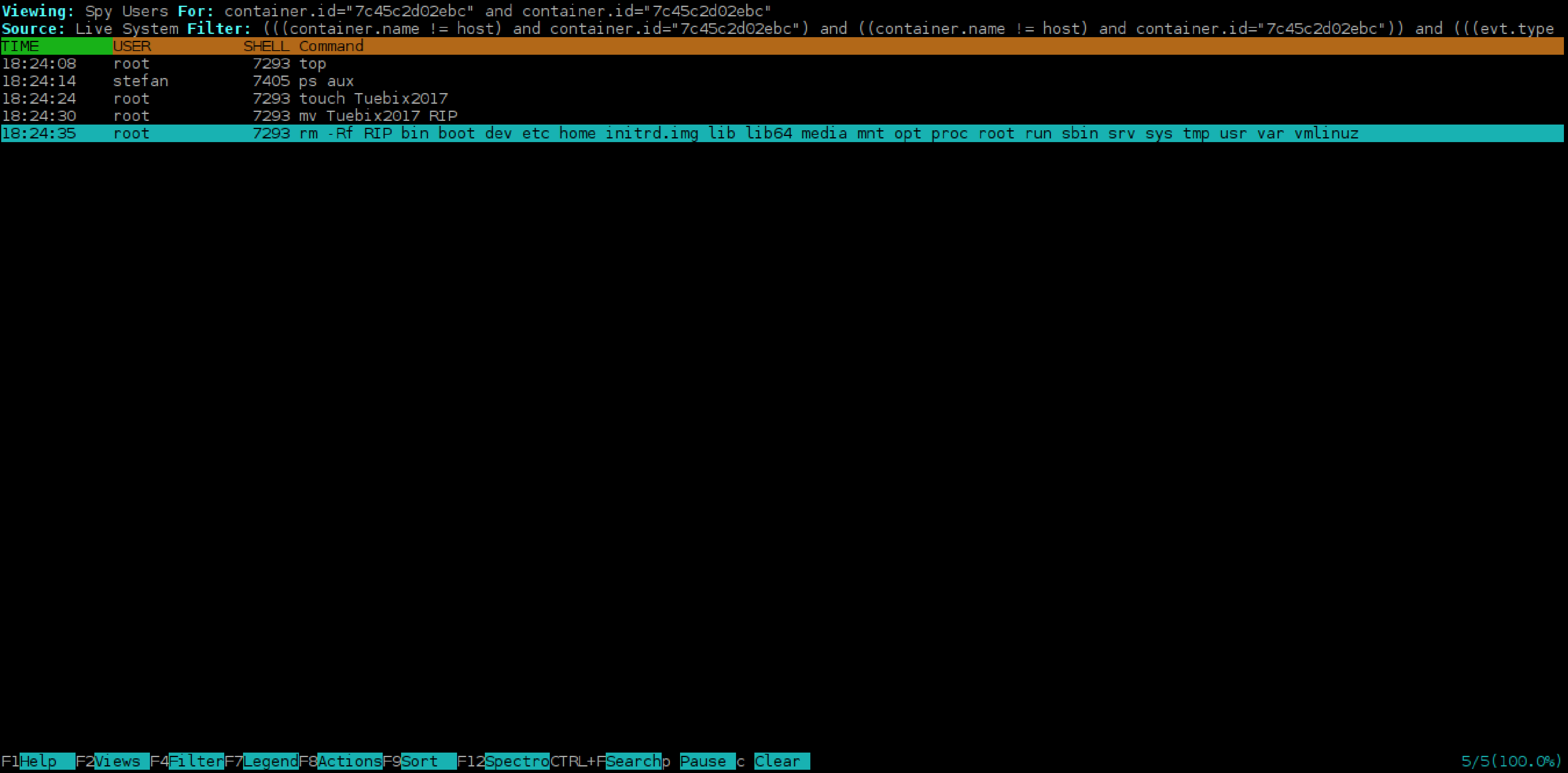
```
Viewing: Processes For: container.id="2410a855bf00"
Source: Live System Filter: (((container.name != host) and container.id="2410a855bf00")) and (evt.type!=switch)
  PID      CPU USER                TH     VIRT       RES      FILE       NET Command
 4001     0.00 root                 1     217M        6M         0      0.00 /usr/sbin/httpd
 3558     0.00 root                 1      12M        3M         0      0.00 /bin/bash
 4003     0.00                      1     217M        6M         0      0.00 /usr/sbin/httpd
 4007     0.00                      1     217M        6M         0      0.00 /usr/sbin/httpd
 4006     0.00                      1     217M        6M         0      0.00 /usr/sbin/httpd
 4004     0.00                      1     217M        6M         0      0.00 /usr/sbin/httpd
 4002     0.00                      1     217M        6M         0      0.00 /usr/sbin/httpd
```



```
Viewing: Processes For: container.id="2410a855bf00"
Source: Live System Filter: (((container.name != host) and container.id="2410a855bf00")) and (evt.type!=switch)
Select View         New Connections
Connections         List every newly established network connection.
Containers Errors
Directories         Columns
Errors              TIME: Time when the connection was received by this machine.
File Opens List     Connection: Connection tuple details.
Files               Command: Name and arguments of the process that received the connection.
I/O by Type
New Connections     ID
Page Faults         incoming_connections
Processes
Processes CPU       Filter
Processes Errors    evt.type=accept and evt.dir=< and evt.failed=false
Processes FD Usage
Server Ports
Spans List
Spans Summary
Spectrogram-File
Spy Syslog
Spy Users
System Calls
Threads
Traces List
Traces Spectrogram
Traces Summary









F1Help  F2Views  F4FilterF5Echo  F6Dig    F7LegendF8ActionsF9Sort   F12SpectroCTRL+FSearchp Pause                                                            1/7(14.3%)
```



```
Viewing: New Connections For: container.id="2410a855bf00" and container.id="2410a855bf00"
Source: Live System Filter: (((container.name != host) and container.id="2410a855bf00") and ((container.name != host) and container.id="2410a855bf00")) and (evt.type=a
TIME              Connection                              Command
18:20:49.015229477 172.17.0.1:60864->172.17.0.2:80         /usr/sbin/httpd
18:20:49.126083067 172.17.0.1:60868->172.17.0.2:80         /usr/sbin/httpd
18:22:33.542817235 172.17.0.1:60890->172.17.0.2:80         /usr/sbin/httpd
18:22:33.635140190 172.17.0.1:60894->172.17.0.2:80         /usr/sbin/httpd















F1Help  F2Views  F4FilterF7LegendF8ActionsF9Sort   F12SpectroCTRL+FSearchp Pause  c Clear                                                         4/4(100.0%)
```



```
Viewing: Spy Users For: container.id="7c45c2d02ebc" and container.id="7c45c2d02ebc"
Source: Live System Filter: (((container.name != host) and container.id="7c45c2d02ebc") and ((container.name != host) and container.id="7c45c2d02ebc")) and (((evt.type
TIME            USER              SHELL Command
18:24:08        root               7293 top
18:24:14        stefan             7405 ps aux
18:24:24        root               7293 touch Tuebix2017
18:24:30        root               7293 mv Tuebix2017 RIP
18:24:35        root               7293 rm -Rf RIP bin boot dev etc home initrd.img lib lib64 media mnt opt proc root run sbin srv sys tmp usr var vmlinuz
```

```
F1Help  F2Views  F4FilterF7LegendF8ActionsF9Sort   F12SpectroCTRL+FSearchp Pause c Clear                                                          5/5(100.0%)
```

Vielen Dank =)

Ansprechpartner für weitere Informationen:
stefan.jakoby@atos.net