



ASTERCONF  
- 2020

# Дебаг ASTERISK like a PRO.



IT-АУТСОРСИНГ

ИТ ПРОФИТ

ASTERCONF  
ТЕРРИТОРИЯ ОБМЕНА О



ОСТЬ НАД КЦИОНАЛЬНО

ОСТЬ



# 01

## Психология Дебага

---

# В мозге тоже есть баги

---

## Баги мешающие в дебаге:

- Семь бед один Reset
- Не знаю, что это за ошибка, но проблема точно не в ней
- Ну раньше же работало
- Наверно юзеру показалось
- Знаю как решить вопрос иначе

# Ненависть !!!!!11

---

## Один из злейших врагов дебагера

Злиться на себя/провайдера/пользователя/Марка Спенсера вредно и со стороны выглядит не странно.

Попей чайку, погляди пару мемов и продолжай!



# 02

## Тактика дебага

---

# Как надо

---

## Алгоритм быстрого решения проблемы:

- понять как воспроизвести проблему, без участия пользователя
- сравнить с рабочим вариантом
- придумать ряд проверяемых гипотез почему не работает
- проверять гипотезы начиная с наиболее вероятных
- писать баг репорт

# Генерация вызова из консоли

---

```
cli> channel originate pjsip/1001 extension 111@ivr1
```

# 03

## **Дебаг SIP Возможности консоли (CLI)**

---



# Можно видеть заголовки Либо SIP-пакеты целиком

---

## CHAN\_SIP

- sip set debug on
- sip set debug ip 1.1.1.1

## CHAN\_PJSIP

- pjsip set logger on
- pjsip set logger host 1.1.1.1

# CHAN\_PJSIP

- pjsip show history
- pjsip show history where sip.msg.request.method = OPTIONS

```
ITProfitPBX14*CLI>
-- Remote UNIX connection
-- Remote UNIX connection disconnected
ITProfitPBX14*CLI> pjsip show history where sip.msg.request.method = OPTIONS
No.      Timestamp  (Dir) Address                SIP Message
=====
00000 1600969618 * ==> 185.22.233.49:5060      OPTIONS sip:185.22.233.49:5060 SIP/2.0
00008 1600969620 * ==> 188.234.136.49:5060    OPTIONS sip:188.234.136.49:5060 SIP/2.0
00010 1600969625 * ==> 10.32.1.11:5060       OPTIONS sip:1030@10.32.1.11:5060 SIP/2.0
00012 1600969630 * ==> 10.32.0.117:5060      OPTIONS sip:1011@10.32.0.117:5060 SIP/2.0
00014 1600969632 * ==> 172.16.0.135:5060     OPTIONS sip:1007@172.16.0.135:5060 SIP/2.0
00016 1600969633 * ==> 10.32.0.70:32670      OPTIONS sip:1020@10.32.0.70:32670 SIP/2.0
00020 1600969640 * ==> 10.32.2.10:5060       OPTIONS sip:1021@10.32.2.10:5060 SIP/2.0
00022 1600969640 * ==> 79.137.209.155:5060   OPTIONS sip:          :5060 SIP/2.0
00024 1600969642 * ==> 10.32.2.11:5060       OPTIONS sip:1031@10.32.2.11:5060 SIP/2.0
00026 1600969646 * ==> 79.137.209.155:5060   OPTIONS sip:792@31.132.134.159:5060 SIP/2.0
```

# 04

## Применение ТСРDUMP

---

# TCPDUMP, SIP, RTP

**-s0** больше не нужно писать , это умолчательное поведение

---

Пишем в файл SIP+RTP

```
tcpdump -w /tmp/call.pcap port 5060 or portrange 10000-20000
```

---

Видим в консоли только sip-заголовки

```
tcpdump port 5060
```

---

Видим в консоли sip-пакеты целиком

```
tcpdump -A port 5060
```

# Возможные проблемы с TSPDUMP

1. Слишком мало пакетов
2. Слишком много пакетов

```
AS
1370 packets captured
1399 packets received by filter
29 packets dropped by kernel ←
```

# СОВЕТ

---

Будьте осторожны в общении с англоговорящими про дампы

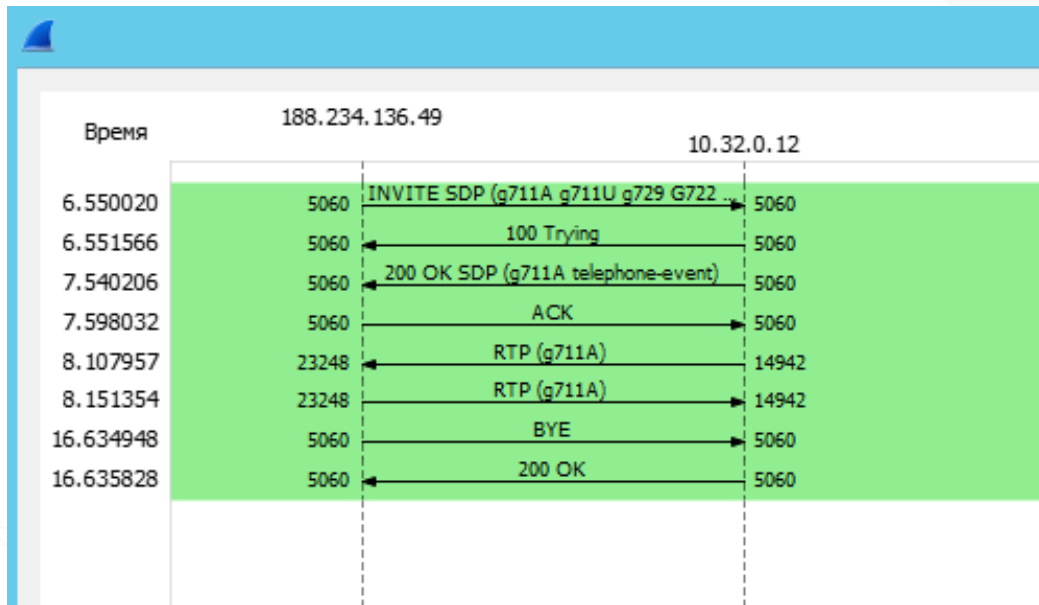
Please don't TAKE A DUMP here!

# 05

## Дебаг SIP/RTP-дампа Wireshark

---

# Wireshark



- Это знают все



# Wireshark

The screenshot shows the Wireshark interface with a SIP packet selected. The 'Details' pane is expanded to show the 'User-Agent' field, which is highlighted in blue. An orange arrow points from the 'User-Agent' field in the details pane to the corresponding hex and ASCII data in the 'Bytes' pane. The hex data shows the sequence of bytes for the 'User-Agent' header, and the ASCII data shows the text 'User-Agent: SkyNET'. The status bar at the bottom indicates 'RFC 3261: User-Agent Header (sip.User-Agent), 20 байты'.

```
<
  ▸ CSeq: 15636 INVITE
    Allow: OPTIONS, SUBSCRIBE, NOTIFY, PUBLISH, INVITE, ACK, BYE, CANCEL, UPD
    Supported: 100rel, timer, replaces, norefersub
    Session-Expires: 1800
    Min-SE: 90
  ▸ P-Asserted-Identity: "AsterTel_79206020084" <sip:79206020084@10.32.0.12>
    Max-Forwards: 70
    User-Agent: SkyNET
    Content-Type: application/sdp
    Content-Length: 223
  ▸ Message Body
02b0  72 64 73 3a 20 37 30 0d 0a 55 73 65 72 2d 41 67  rds: 70 · ·User-Ag
02c0  65 6e 74 3a 20 53 6b 79 4e 45 54 0d 0a 43 6f 6e  ent: Sky NET · ·Con
02d0  74 65 6e 74 2d 54 79 70 65 3a 20 61 70 70 6c 69  tent-Type e: appli
02e0  63 61 74 69 6f 6e 2f 73 64 70 0d 0a 43 6f 6e 74  cation/s dp · ·Cont
02f0  65 6e 74 2d 4c 65 6e 67 74 68 3a 20 20 20 32 32  ent-Leng th: 22
RFC 3261: User-Agent Header (sip.User-Agent), 20 байты
```

- При выборе любого поля пакета в нижней строке появляется имя параметра для фильтра

# Wireshark

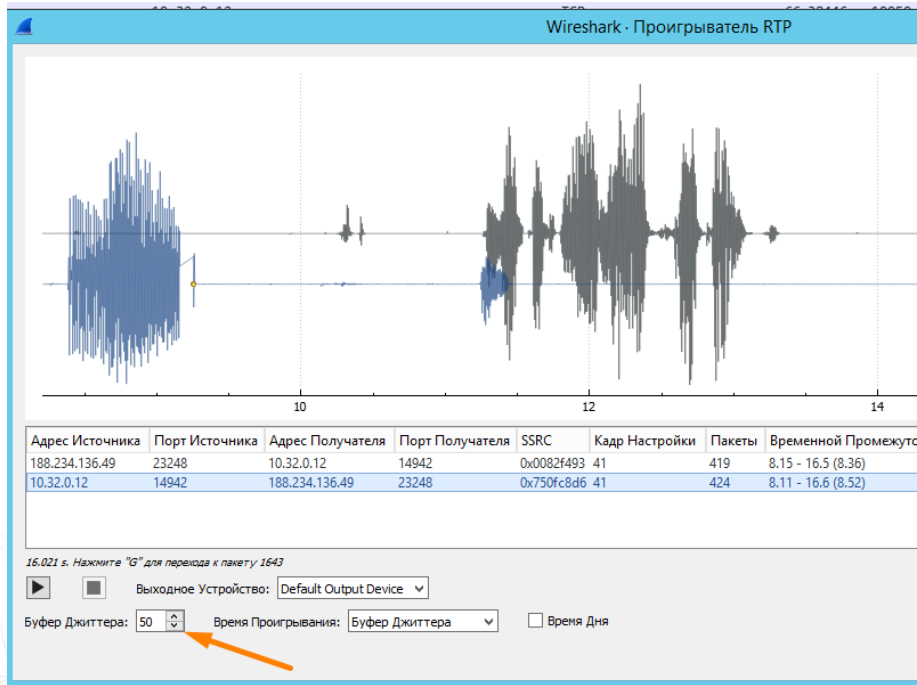
The screenshot shows the Wireshark interface with a packet list on the left and a packet details pane on the right. The packet list shows a packet with No. 21 and Time 2.067001. The packet details pane shows the following fields:

- Frame 82: 996 bytes captured on interface 0
- Ethernet II, Src: 36:01:00:00:00:00, Dst: 08:00:27:00:00:00
- Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.10
- User Datagram Protocol, Src Port: 5060, Dst Port: 5060
- Session Initiation Protocol
- Request-Line: INVITE
- Message Header
  - Via: SIP/2.0/UDP
  - From: "AsterTel" <sip:1005@192.168.1.1>
  - To: <sip:1005@192.168.1.10>
  - Contact: <sip:1005@192.168.1.1>
  - Call-ID: 5f58e512-1005@192.168.1.1
  - [Generated Call]
  - CSeq: 15636 INVITE
  - Allow: OPTIONS, INVITE, ACK, CANCEL, UPDATE, PRACK, REGISTER, MESSAGE, REFER
  - Supported: 100rel, progress, replaces
  - Session-Expires: 3600
  - Min-SE: 90
  - P-Asserted-Identity: "AsterTel" <tel:1005>
  - Max-Forwards: 70
  - User-Agent: SkyNET
  - Content-Type: application/sdp
  - Content-Length: 223
- Message Body

The 'User-Agent: SkyNET' field is selected. A context menu is open over this field, and the 'Prepare as Filter' option is highlighted. A secondary menu is also open, showing the filter expression: 'Prepare as Filter: sip.User-Agent == "SkyNET"'. The filter is then applied to the packet list, which is highlighted in green.

- Из любого поля SIP-пакета можно в два клика создать фильтр

# Wireshark



- Можно выставлять размер джиттер-буфера при воспроизведении захваченного RTP-трафика

# 06

## Дебаг SIP-дампа SNGREP

---

# Ivan Alonso (aka Kaian)

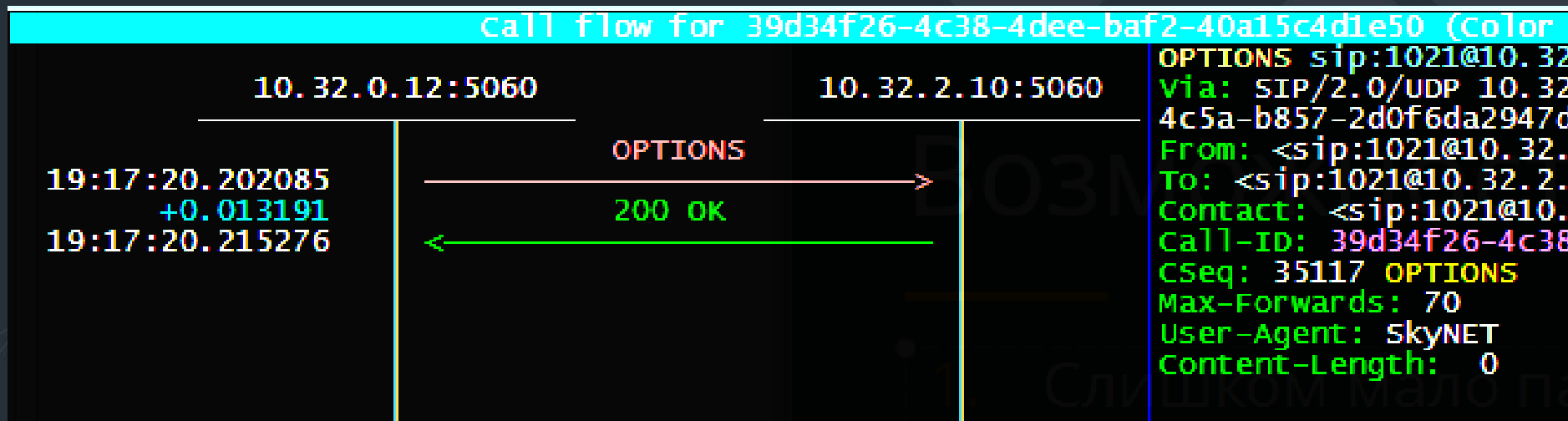
---



- Автор SNGREP-a

# Возможности SNGREP

Просмотр в реальном времени текущих SIP-диалогов



# Возможности SNGREP

Сохранение выбранных SIP-диалогов + RTP в \*.pcap

Save capture

Path: /root

Filename: \_\_\_\_\_ .pcap

**dialogs**

- all dialogs
- selected dialogs [0]
- filtered dialogs [1]

**Format**

- .pcap (SIP)
- .pcap (SIP + RTP)
- .txt

[ Save ] [ cancel ]

# Возможности SNGREP

Возможность построчно сравнить два любых пакета

```
sngrep - SIP messages flow viewer
2020/09/25 19:20:29.076628 10.32.0.12:5060 -> 10.32.0.201:5060 2020/09/25 19:21:13.361346 10.32.0.12:5060 -> 10.32.0.70:32670
OPTIONS sip:1001@10.32.0.201:5060 SIP/2.0 OPTIONS sip:1020@10.32.0.70:32670 SIP/2.0
Via: SIP/2.0/UDP 10.32.0.12:5060;rport;branch=z9hG4bKPjc5280c200b58-40e8-9d21-17c9fbca271f Via: SIP/2.0/UDP 10.32.0.12:5060;rport;branch=z9hG4bKPjf1b826e20478-4a8d-af7c-656c072de500
From: <sip:1001@10.32.0.12>;tag=71b44f60-ef1a-40fa-9cf5-02da7399ed4 From: <sip:1020@10.32.0.12>;tag=f6ddd584-3972-4e8f-b52a-6ddb12cdc63
To: <sip:1001@10.32.0.201> To: <sip:1020@10.32.0.70>
Contact: <sip:1001@10.32.0.12:5060> Contact: <sip:1020@10.32.0.12:5060>
Call-ID: 620ef552-e728-44c0-93b4-cb2f53e8867e Call-ID: 9b42e931-4279-4f9b-8958-e867fd0d5132
CSeq: 34208 OPTIONS CSeq: 42185 OPTIONS
Max-Forwards: 70 Max-Forwards: 70
User-Agent: SkyNET User-Agent: SkyNET
Content-Length: 0 Content-Length: 0
```



# Возможности SNGREP

---

- Полнотекстовый поиск
- Ставить дампы на паузу
- Фильтрации при запуске как в TCPDUMP
- Открывать сохраненный дампы
- Фильтровать трафик регулярками

# 07

## Дебаг диалплана

---

# Если в логах есть ошибки Не стоит их игнорировать

## Подход к дебагу диалплана:

- Не начинай тест не устранив ошибки при применении диалплана
- Если при выполнении диалплана есть WARNING-и, но при этом все работает – это проблема



Говорю что warning при  
релоаде диалплна это  
плохо



разработчики FreePBX

# Приложения для отладки

## Приложения диалплана:

- Milliwatt()
- Echo()
- DumpChan()
- Noop()

```
PJSIP/1001-00000368 15 Pinging
> 0x7f8b143e8d20 -- Strict RTP learning after remote address set to: 10.32.
-- PJSIP/1001-00000368 answered
> Launching DumpChan() on PJSIP/1001-00000368

Dumping Info For Channel: PJSIP/1001-00000368:
=====
Info:
Name=                PJSIP/1001-00000368
Type=                PJSIP
UniqueID=            1600977050.2001
LinkedID=            1600977050.2001
CallerIDNum=         1001
CallerIDName=        Nikolay shakin
ConnectedLineIDNum= (N/A)
ConnectedLineIDName=(N/A)
DNIDDigits=          (N/A)
RDNIS=               (N/A)
ParkingLot=          (N/A)
Language=            ru
State=               Up (6)
Rings=               0
NativeFormat=        (g722)
WriteFormat=          g722
ReadFormat=           g722
RawWriteFormat=       g722
RawReadFormat=        g722
WriteTranscode=       No
ReadTranscode=        No
1stFileDescriptor=   -1
Framesin=             8
Framesout=            0
TimeToHangup=         0
ElapsedTime=          0h0m2s
BridgeID=             (not bridged)
Context=              from-internal
Extension=            s
Priority=              1
CallGroup=            (N/A)
PickupGroup=          (N/A)
Application=          DumpChan
Data=                 (None)
Blocking_in=          (Not Blocking)

Variables:
=====
ITProfitPBX14*CLI>
```

# 08

## Подсистема Логирования Asterisk

---

# CLI управление логированием

---

- core set debug 10
- core set verbose 10
- logger add channel debug \*
- logger mute

# 10

## tmux+watch

---



# tmux+watch

- Создай свой дашборд для мониторинга чего угодно в реальном времени

```
Every 0.3s: asterisk -x 'core show calls'
Thu Sep 24 23:16:34 2020
0 active calls
685 calls processed

win 3509, length 1616
23:16:34.205737 IP 10.32.0.13.32861 > ITProfitPBX14.ssh: Flags [.], ack 235830912, win 392, length 0
23:16:34.205773 IP 10.32.0.13.32861 > ITProfitPBX14.ssh: Flags [.], ack 235832528, win 386, length 0
23:16:34.207132 IP ITProfitPBX14.ssh > 10.32.0.13.32861: Flags [P.], seq 235832528:235836688, ack 134609, win 3509, length 4160
23:16:34.207366 IP ITProfitPBX14.ssh > 10.32.0.13.32861: Flags [P.], seq 235836688:235838368, ack 134609, win 3509, length 1680
23:16:34.207654 IP 10.32.0.13.32861 > ITProfitPBX14.ssh: Flags [.], ack 235838368, win 363, length 0
23:16:34.208096 IP ITProfitPBX14.ssh > 10.32.0.13.32861: Flags [P.], seq 235838368:235841248, ack 134609, win 3509, length 2880
23:16:34.209485 IP ITProfitPBX14.ssh > 10.32.0.13.32861: Flags [P.], seq 235841248:235845408, ack 134609, win 3509, length 4160
23:16:34.209672 IP ITProfitPBX14.ssh > 10.32.0.13.32861: Flags [P.], seq 235845408:235846896, ack 134609, win 3509, length 1488
23:16:34.211064 IP ITProfitPBX14.ssh > 10.32.0.13.32861: Flags [P.], seq 235846896:235851056, ack 134609, win 3509, length 4160
23:16:34.211211 IP ITProfitPBX14.ssh > 10.32.0.13.32861: Flags [P.], seq 235851056:235852400, ack 134609, win 3509, length 1344
23:16:34.214852 IP 10.32.0.13.32861 > ITProfitPBX14.ssh: Flags [.], ack 235841248, win 352, length 0
23:16:34.214908 IP ITProfitPBX14.ssh > 10.32.0.13.32861: Flags [P.], seq 235852400:235857840, ack 134609, win 3509, length 5440
23:16:34.214943 IP 10.32.0.13.32861 > ITProfitPBX14.ssh: Flags [.], ack 235846896, win 330, length 0
23:16:34.215050 IP 10.32.0.13.32861 > ITProfitPBX14.ssh: Flags [.], ack 235852400, win 308, length 0
23:16:34.215246 IP 10.32.0.13.32861 > ITProfitPBX14.ssh: Flags [.], ack 235857840, win 287, length 0
23:16:34.217144 IP ITProfitPBX14.ssh > 10.32.0.13.32861: Flags [P.], seq 235857840:235862000, ack 134609, win 3509, length 4160
23:16:34.217360 IP ITProfitPBX14.ssh > 10.32.0.13.32861: Flags [P.], seq 235862000:235863408, ack 134609, win 3509, length 1408
23:16:34.217373 IP 10.32.0.13.32861 > ITProfitPBX14.ssh: Flags [.], ack 235862000, win 271, length 0
23:16:34.217512 IP 10.32.0.13.32861 > ITProfitPBX14.ssh: Flags [.], ack 235863408, win 265, length 0

sngrep - SIP messages flow viewer
Current Mode: online [any]      Dialogs: 6
Match Expression:             BPF Filter:
Display Filter:

#Msg Method      SIP From          SIP To           Msgrs Source
[ ] 7 OPTIONS      1004@10.32.0.12   1004@172.16.0.133 2 10.32.0.12:5060
[ ] 8 OPTIONS      1007@10.32.0.12   1007@172.16.0.135 1 10.32.0.12:5060
[ ] 9 REGISTER     74832320099@188.234.136.4 3006@172.16.0.109 2 10.32.0.12:5060
[ ] 10 OPTIONS    1005@10.32.0.12   1005@10.32.0.90 2 10.32.0.12:5060
[ ] 11 OPTIONS    9208380313@ru.nextell.r 93.92.91.90 2 10.32.0.12:5060

1 [ 16.9%] Tasks: 72, 162 thr; 2 running
2 [ 23.4%] Load average: 1.65 0.96 0.63
3 [ 22.3%] Uptime: 34 days, 11:40:32
4 [ 19.3%]

Mem [ 1.13G/3.70G]
Swap [ 123M/3.87G]

PID USER PRU NI VIRT RES SHR S CPU% MEM% TTY+ Command
13916 root 20 0 24808 4244 1232 R 39.7 0.1 0:49.33 tmux
5486 root 20 0 267M 102M 5212 S 31.0 2.7 38h25:18 sngrep
5487 root 20 0 267M 102M 5212 S 30.3 2.7 38h21:22 sngrep
1971 root 20 0 151M 4440 3884 S 18.8 0.1 2:59.52 sshd: root@pts/3
16861 root 20 0 201M 6328 5064 S 9.4 0.2 0:01.69 sngrep
16865 root 20 0 201M 6328 5064 S 9.4 0.2 0:01.35 sngrep
14624 tcpdump 20 0 59604 11680 9992 S 9.4 0.3 0:13.65 tcpdump
14656 root 20 0 153M 2272 1580 S 2.9 0.1 0:03.12 watch -n 0.3 asterisk -x 'core show calls'
8995 asterisk 20 0 3103M 175M 17528 S 2.2 4.6 11h29:25 /usr/sbin/asterisk -f -u asterisk -G asteri
15968 root 20 0 119M 2220 1452 R 2.2 0.1 0:01.00 htop
11971 root 20 0 43708 7152 2052 I 1.4 0.1 1h33:23 /usr/lib/systemd/systemd --switched-root --
1413 mongodb 20 0 4668M 6684 4836 S 0.7 0.2 4h12:34 /usr/bin/mongod --quiet -f /etc/mongod.conf
14928 asterisk 20 0 3103M 175M 17528 S 0.7 4.6 19:44.07 /usr/sbin/asterisk -f -u asterisk -G asteri
1375 zabbix 20 0 81104 1552 1412 S 0.7 0.0 22:10.31 /usr/sbin/zabbix_agentd: listener #3 [waiti
14948 asterisk 20 0 3103M 175M 17528 S 0.7 4.6 14:11.77 /usr/sbin/asterisk -f -u asterisk -G asteri
554 root 20 0 48424 13568 13412 S 0.7 0.3 33:58.18 /usr/lib/systemd/systemd-journald
14927 asterisk 20 0 3103M 175M 17528 S 0.0 4.6 20:47:33 /usr/sbin/asterisk -f -u asterisk -G asteri
750 dbus 20 0 58416 1972 1512 S 0.0 0.1 1h26:24 /usr/bin/dbus-daemon --system --address=sys
1349 mysql 20 0 1913M 217M 5800 S 0.0 5.8 2h26:16 /usr/libexec/mysqld --basedir=/usr --datadi
8890 root 20 0 1202M 10248 2432 S 0.0 0.3 1h42:35 /usr/bin/python /usr/bin/fail2ban-server -b

Esc Quit Enter Show space Select F1 Help F2 Save F3 Search F4 Extended F5 Clear F7 Filter
[0] 0:root@ITProfitPBX14:~
```



ASTERCONF  
- 2020

СПАСИБО  
ЗА ВНИМАНИЕ!



IT-АУТСОРСИНГ

ИТ ПРОФИТ

Николай Шакин

Telegram @ShakiNNN

ASTERCONF  
ТЕРРИТОРИЯ ОБМЕНА О

