BLOCKBIT

BLOCKBIT UTM CLI

(COMMAND LINE INTERFACE)

UTM | BLOCKBIT
Gerenciamento Unificado de Ameaças

www.blockbit.com

Sumário

1 INTERFACE BLOCKBIT CLI - LINHA DE COMANDOS

O BLOCKBIT UTM disponibiliza um recurso de console Command Line Interface - CLI, que possibilita ao administrador executar comandos de administração e troubleshooting dos principais serviços do sistema. Para executar a configuração é necessário um cliente SSH e Console. As aplicações mínimas recomendadas são:

- PUTTY;
- CygWin;
- Mobaxterm.

A seguir apresentaremos passo a passo como acessar o console CLI do BLOCKBIT UTM:

1. Verifique se o dispositivo de acesso possui um cliente SSH recomendado já instalado. Vamos exemplificar o processo utilizando o aplicativo “PUTTY”;
2. Acesse a console SSH. Preencha os campos:
   - **Host Name (or IP Address):** inserir o endereço IP do BLOCKBIT UTM. Ex.: 172.16.102.136;

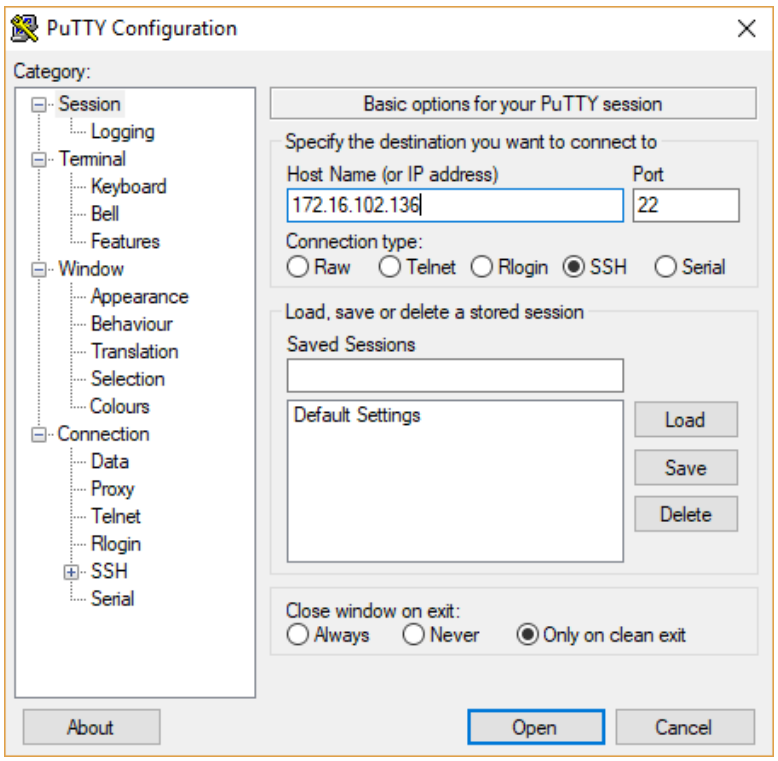

Figura 1 – PuTTY Configuration.

   - Clique no botão “Open”.

3. A console será exibida, solicitando usuário e senha:

Em “login as:” digite o usuário admin e pressione “Enter”

Após “password:” entre com a senha admin e pressione “Enter”

A imagem abaixo apresenta os comandos dos principais serviços do sistema.

```
admin  >help
arp               enable-pim    lscpu               set-irqbalance-dynamic
arping            enable-rip    lsusb               set-irqbalance-static
configure-bgp     enable-root   mkfs                show-sessions
configure-ospf    enable-snmp   more                show-uuid
configure-ospf6   ethtool       mtr                 show-vpn-conn
configure-pim     exit          netads              show-vpn-info
configure-rip     fdisk         netstat             shutdown
configure-rip6    free          nslookup            speedtest
conntrack         fsck          ntpdate             sync-users
date              fwrecovery    passwd              sysctl
debug-auth        fwreload      ping                tcpdump
debug-dhcp        grep          reboot              tcptop
debug-events      help          reset               tcptrack
debug-firewall    history       reset-admin-blocks  telnet
debug-ha          host          reset-admin-password tracepath
debug-threats     hostname      reset-admin-sessions traceroute
debug-vpn         ifconfig      reset-logs          update-license
debug-web         ifstat        reset-stats         update-system
dig               iostat        rewizard            uptime
disable-bgp       iotest        route               vmstat
disable-ospf      ip            sar                 watch-cpu
disable-pim       ipcalc        service-disable     watch-io
disable-rip       iplist        service-enable      watch-mem
disable-snmp      iptraf        service-start       watch-srv
enable-bgp        ldapsearch    service-status      wc
enable-ospf       less          service-stop        whois
```

Figura 2 – BLOCKBIT UTM – Command Line Interface.

A seguir, apresentaremos cada comando.

1.1 [arp]

Utilizado para mapear o endereço de rede (por exemplo, um endereço IPv4) para um endereço físico, como um endereço Ethernet (também chamado endereço MAC). Exibe e modifica esta tabela de relação de endereços da Internet para endereços Ethernet. O ARP foi implementado com muitas combinações de tecnologias de rede e camada de enlace de dados. O IPv4 é o caso mais comum.

Utilize este comando para identificar um problema de comunicação de rede ou identificar eventos e

status de IP conectados.

Modo de uso:

```
Modo de uso
admin  >arp -h
Usage:
  arp [-vn]  [<HW>] [-i <if>] [-a] [<hostname>] <-Display ARP cache
  arp [-v]          [-i <if>] -d  <host> [pub]  <-Delete ARP entry
  arp [-vnD] [<HW>] [-i <if>] -f  [<filename>]  <-Add entry from file
  arp [-v]   [<HW>] [-i <if>] -s  <host> <hwaddr> [temp] <-Add entry
  arp [-v]   [<HW>] [-i <if>] -Ds <host> <if> [netmask <nm>] pub <-''-

        -a  display (all) hosts in alternative (BSD) style
        -e  display (all) hosts in default (Linux) style
        -s, --set               set a new ARP entry
        -d, --delete            delete a specified entry
        -v, --verbose           be verbose
        -n, --numeric           don't resolve names
        -i, --device            specify network interface (e.g. eth0)
        -D, --use-device        read <hwaddr> from given device
        -A, -p, --protocol      specify protocol family
        -f, --file              read new entries from file or from /etc/ethers

  <HW>=Use '-H <hw>' to specify hardware address type. Default: ether
  List of possible hardware types (which support ARP):
    ash (Ash) ether (Ethernet) ax25 (AMPR AX.25)
    netrom (AMPR NET/ROM) rose (AMPR ROSE) arcnet (ARCnet)
    dlci (Frame Relay DLCI) fddi (Fiber Distributed Data Interface) hippi (HIPPI)
    irda (IrLAP) x25 (generic X.25) infiniband (InfiniBand)
    eui64 (Generic EUI-64)
admin  >
```

Figura 3 – Command Line Interface – arp.

Exemplo: Apresentar a tabela de endereços IP e endereços de hosts físicos (dispositivos) na rede:

```
admin  >arp -a
? (172.16.12.85) at 00:26:8b:04:eb:bd [ether] on eth0
? (192.168.254.15) at 00:30:48:c2:02:a4 [ether] on eth2.254
? (172.16.13.248) at 0c:c4:7a:11:0f:96 [ether] on eth0
? (172.16.12.81) at 00:30:48:de:78:ae [ether] on eth0
? (192.168.254.4) at e6:9c:1f:89:11:32 [ether] on eth2.254
? (192.168.253.34) at 7e:49:6f:55:42:00 [ether] on eth2.253
? (172.16.12.92) at <incomplete> on eth0
? (172.16.12.90) at 10:98:36:fb:c9:1b [ether] on eth0
? (172.16.20.22) at 00:0b:ab:f1:9b:bc [ether] on eth3
? (172.16.12.71) at <incomplete> on eth0
? (172.16.20.20) at 00:0c:29:b7:34:cf [ether] on eth3
? (172.16.20.19) at 04:7d:7b:fd:53:d7 [ether] on eth3
? (172.16.12.65) at 78:2b:cb:c4:e7:12 [ether] on eth0
? (172.16.12.64) at <incomplete> on eth0
? (172.16.12.77) at 90:b1:1c:f6:2f:e2 [ether] on eth0
? (192.168.254.22) at 00:e0:4c:68:19:bf [ether] on eth2.254
admin  >
```

Figura 4 – Command Line Interface – arp – Exemplo.

1.2 [arping]

Descobre e identifica os hosts conectados utilizando a associação da tabela ARP com a resposta análoga ao ping que adota o protocolo ICMP.

Modo de uso:

```
admin  >arping -h
Usage: arping [-fqbDUAV] [-c count] [-w timeout] [-I device] [-s source] destination
  -f : quit on first reply
  -q : be quiet
  -b : keep broadcasting, don't go unicast
  -D : duplicate address detection mode
  -U : Unsolicited ARP mode, update your neighbours
  -A : ARP answer mode, update your neighbours
  -V : print version and exit
  -c count : how many packets to send
  -w timeout : how long to wait for a reply
  -I device : which ethernet device to use
  -s source : source ip address
  destination : ask for what ip address
admin  >
```

Figura 5 – Command Line Interface – arping.

Exemplo: Descobrir o endereço MAC de um determinado IP:

```
admin  >arping -c 5 -I eth0 172.16.12.85
ARPING 172.16.12.85 from 172.16.12.1 eth0
Unicast reply from 172.16.12.85 [00:26:8B:04:EB:BD]  6.465ms
Unicast reply from 172.16.12.85 [00:26:8B:04:EB:BD]  2.099ms
Unicast reply from 172.16.12.85 [00:26:8B:04:EB:BD]  0.773ms
Unicast reply from 172.16.12.85 [00:26:8B:04:EB:BD]  0.761ms
^CSent 4 probes (1 broadcast(s))
Received 4 response(s)
admin  >
```

Figura 6 – Command Line Interface – arping - Exemplo.

1.3 [configure-bgp]

Command Line Interface de configuração do roteamento dinâmico BGP.

Modo de uso:

Por padrão a senha de usuário e do modo privilegiado é admin.

Após "password:" entre com a senha admin e pressione "Enter"

```
admin  >configure-bgp
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
BLOCKBIT Dynamic Router Config
+
+

User Access Verification

Password:
localhost>
```

Figura 7 – Command Line Interface – configure-bgp.

Na interface web, em **[System] >> [Network] >> [Dynamic Routing]**, ao clicar no ícone [ ], é possível visualizar o exemplo de configuração:

```
Exemplo de configuração: BGP

configure-bgp

BLOCKBIT Dynamic Router Config
+
+
User Access Verification
Password:
localhost> enable
Password:
localhost# configure terminal
localhost(config)# hostname utm-bb
utm-bb(config)# bgp multiple-instance
utm-bb(config)# router bgp 180
utm-bb(config)# bgp router-id 0.0.0.180
utm-bb(config-router)# network 172.16.0.0/24
utm-bb(config-router)# timers bgp 1 5
utm-bb(config-router)# neighbor 192.168.20.2 remote-as 181
utm-bb(config-router)# neighbor 172.15.0.1 remote-as 181
utm-bb(config-router)# do wr
utm-bb(config)# exit
Connection closed by foreign host
```

Figura 8 – Command Line Interface – Exemplo de configuração BGP.

1.4 [configure-ospf]

Command Line Interface de configuração do roteamento dinâmico OSPF.

Modo de uso:

Por padrão a senha de usuário e do modo privilegiado é admin.

Após "password:" entre com a senha admin e pressione "Enter"

```
admin  >configure-ospf
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
BLOCKBIT Dynamic Router Config
+
+

User Access Verification

Password:
localhost>
```

Figura 9 – Command Line Interface – configure-ospf.

Na interface web, em **[System] >> [Network] >> [Dynamic Routing]**, ao clicar no ícone [ ], é possível visualizar o exemplo de configuração:

```
Exemplo de configuração: OSPF

configure-ospf

BLOCKBIT Dynamic Router Config
+
+
User Access Verification
Password:
localhost> enable
Password:
localhost# configure terminal
localhost(config)# hostname utm-bb
utm-bb(config)# router ospf
utm-bb(config-router)# network 192.168.10.0/24 area 0
utm-bb(config-router)# network 172.16.0.0/24 area 0
utm-bb(config-router)# network 192.168.20.0/24 area 0
utm-bb(config-router)# exit
utm-bb(config)# do wr
utm-bb# exit
Connection closed by foreign host
```

Figura 10 – Command Line Interface – Exemplo de configuração OSPF.

1.5 [configure-ospf6]

Command Line Interface de configuração do roteamento dinâmico OSPF para IPV6.

Modo de uso:

Por padrão a senha de usuário e do modo privilegiado é admin.

Após "password:" entre com a senha admin e pressione "Enter"

```
admin  >configure-ospf6
Trying ::1...
Connected to ::1.
Escape character is '^]'.
BLOCKBIT Dynamic Router Config
+
+

User Access Verification

Password:
bb5sp.labsuporte.com.br>
```

Figura 11 – Command Line Interface – configure-ospf6.

2.1 [configure-pim]

Command Line Interface de configuração do roteamento dinâmico PIM-SM.

Modo de uso:

Por padrão a senha de usuário e do modo privilegiado é admin.

Após "password:" entre com a senha admin e pressione "Enter"

```
admin  >configure-pim
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
BLOCKBIT Dynamic Router Config
+
+

User Access Verification

Password:
bb5sp.labsuporte.com.br>
```

Figura 12 – Command Line Interface – configure-pim.

Na interface web, em **[System] >> [Network] >> [Dynamic Routing]**, ao clicar no ícone [ ], é possível visualizar o exemplo de configuração:

```
Exemplo de configuração: PIM

configure-pim

BLOCKBIT Dynamic Router Config
+
+
User Access Verification
Password:
localhost> enable
Password:
localhost# configure terminal
localhost(config)# hostname utm-bb
utm-bb(config)# interface eth0
utm-bb(config-if)# ip pim ssm
utm-bb(config-if)# ip igmp
utm-bb(config-if)# interface eth1
utm-bb(config-if)# ip pim ssm
utm-bb(config-if)# ip igmp
utm-bb(config-if)# exit
utm-bb(config)# ip multicast-routing
utm-bb(config)# do wr
utm-bb# exit
Connection closed by foreign host
```

Figura 13 – Command Line Interface – Exemplo de configuração PIM.

2.2 [configure-rip]]

Command Line Interface de configuração do roteamento dinâmico RIP.

Modo de uso:

Por padrão a senha de usuário e do modo privilegiado é admin.

Após "password:" entre com a senha admin e pressione "Enter"

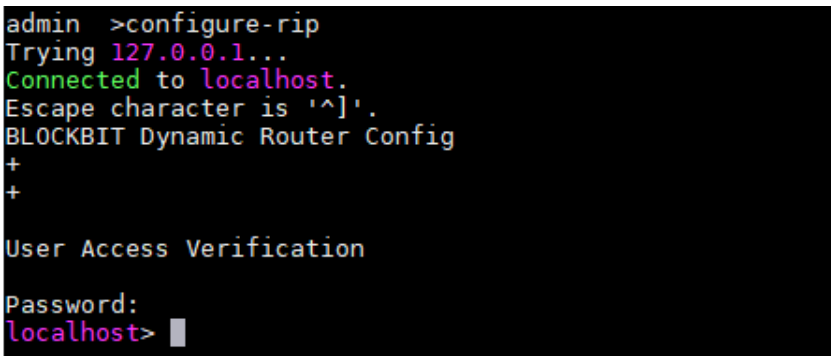

Figura 14 – Command Line Interface – configure-rip.

Na interface web, em **[System] >> [Network] >> [Dynamic Routing]**, ao clicar no ícone [ ], é possível visualizar o exemplo de configuração:

```
Exemplo de configuração: RIP

configure-rip

BLOCKBIT Dynamic Router Config
+
+
User Access Verification
Password:
localhost> enable
Password:
localhost# configure terminal
localhost(config)# hostname utm-bb
utm-bb(config)# router rip
utm-bb(config-router)# version 2
utm-bb(config-router)# network 10.0.0.0/8
utm-bb(config-router)# passive-interface eth0
utm-bb(config-router)# interface eth0
utm-bb(config-if)# no ip rip authentication mode text
utm-bb(config-if)# exit
utm-bb(config)# do wr
utm-bb# exit
Connection closed by foreign host
```

Figura 15 – Command Line Interface – Exemplo de configuração RIP.

2.3 [configure-rip6]

Command Line Interface de configuração do roteamento dinâmico RIP para IPV6.

Modo de uso:

Por padrão a senha de usuário e do modo privilegiado é admin.

Após "password:" entre com a senha admin e pressione "Enter"

```
admin  >configure-rip6
Trying ::1...
Connected to ::1.
Escape character is '^]'.
BLOCKBIT Dynamic Router Config
+
+

User Access Verification

Password:
bb5sp.labsuporte.com.br>
```

Figura 16 – Command Line Interface – configure-rip6.

2.4 [conntrack]

Visualizar e gerenciar a tabela de conexões do servidor.

Modo de uso:

```
admin  >conntrack --help
Command line interface for the connection tracking system. Version 1.4.2
Usage: /usr/sbin/conntrack [commands] [options]

Commands:
  -L [table] [options]          List conntrack or expectation table
  -G [table] parameters         Get conntrack or expectation
  -D [table] parameters         Delete conntrack or expectation
  -I [table] parameters         Create a conntrack or expectation
  -U [table] parameters         Update a conntrack
  -E [table] [options]          Show events
  -F [table]                    Flush table
  -C [table]                    Show counter
  -S                            Show statistics

Tables: conntrack, expect

Conntrack parameters and options:
  -n, --src-nat ip                      source NAT ip
  -g, --dst-nat ip                      destination NAT ip
  -j, --any-nat ip                      source or destination NAT ip
  -m, --mark mark                       Set mark
  -c, --secmark secmark                 Set selinux secmark
  -e, --event-mask eventmask            Event mask, eg. NEW,DESTROY
  -z, --zero                            Zero counters while listing
  -o, --output type[,...]               Output format, eg. xml
  -l, --label label[,...]               conntrack labels

Expectation parameters and options:
  --tuple-src ip        Source address in expect tuple
  --tuple-dst ip        Destination address in expect tuple
  --mask-src ip         Source mask address
  --mask-dst ip         Destination mask address

Common parameters and options:
  -s, --orig-src ip             Source address from original direction
  -d, --orig-dst ip             Destination address from original direction
  -r, --reply-src ip            Source addres from reply direction
  -q, --reply-dst ip            Destination address from reply direction
  -p, --protonum proto          Layer 4 Protocol, eg. 'tcp'
  -f, --family proto            Layer 3 Protocol, eg. 'ipv6'
  -t, --timeout timeout         Set timeout
  -u, --status status           Set status, eg. ASSURED
  -w, --zone value              Set conntrack zone
  -b, --buffer-size             Netlink socket buffer size
```

Figura 17 – Command Line Interface – conntrack.

Exemplo: Exibir todos os registros da tabela de conexões:

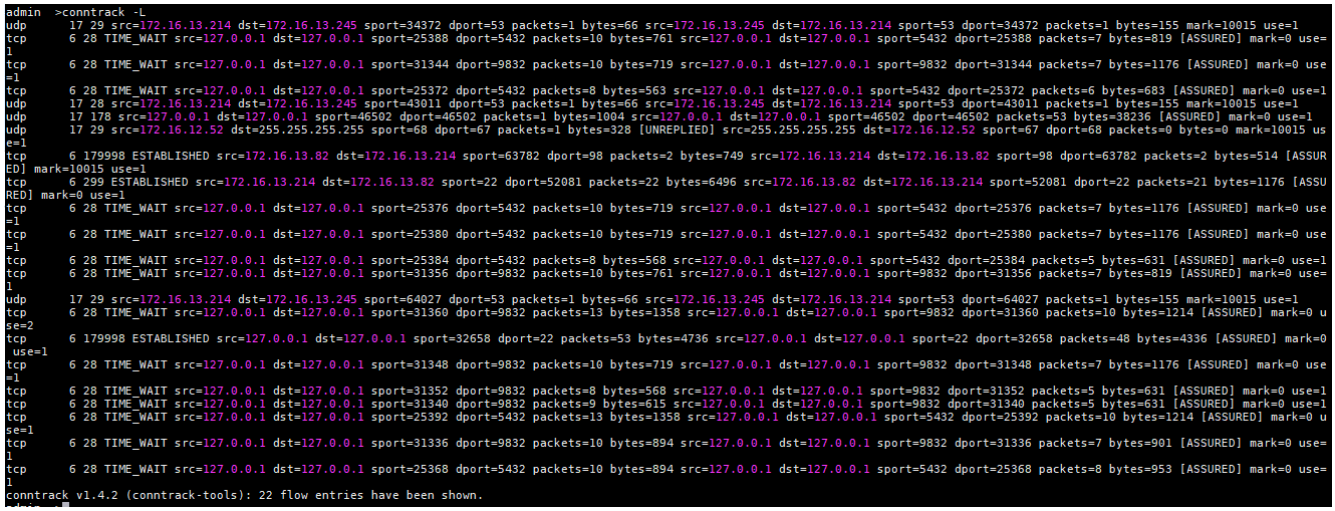

Figura 18 – Command Line Interface – conntrack - Exemplo.

2.5 [date]

Lista e permite alterar a data e hora atual.

Modo de uso:

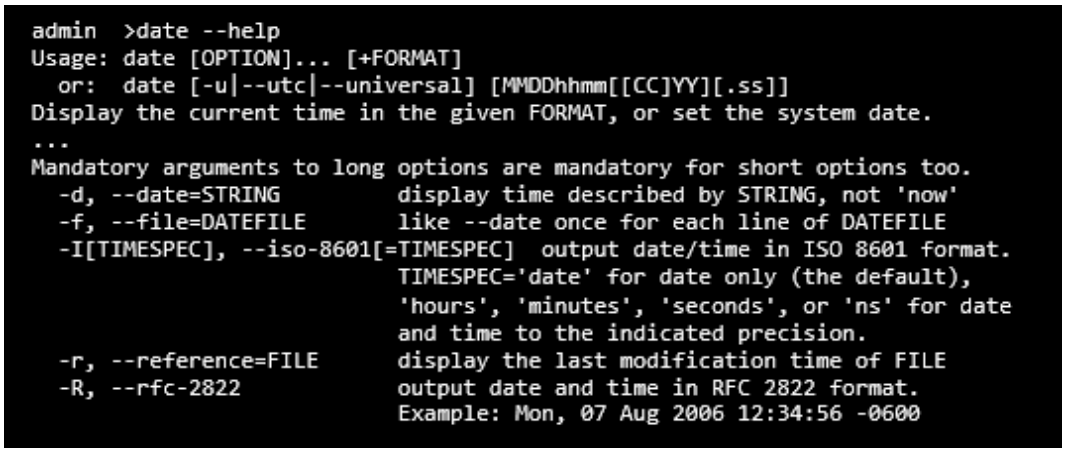

Figura 19 – Command Line Interface – date.

```
      --rfc-3339=TIMESPEC   output date and time in RFC 3339 format.
                            TIMESPEC='date', 'seconds', or 'ns' for
                            date and time to the indicated precision.
                            Date and time components are separated by
                            a single space: 2006-08-07 12:34:56-06:00
  -s, --set=STRING          set time described by STRING
  -u, --utc, --universal    print or set Coordinated Universal Time (UTC)
      --help     display this help and exit
      --version  output version information and exit

admin  >
```

Figura 20 – Command Line Interface – date 1.

Exemplo 1: Listar a data e hora atual:

```
admin  >date
Thu Sep  1 09:59:08 BRT 2016
admin  >
```

Figura 21 – Command Line Interface – date – Exemplo 1.

Exemplo 2: Atualizar data e hora baseados no fuso horário América/São Paulo:

```
admin  > date --date='TZ="America/Sao_Paulo" 11:00'
Thu Sep  1 11:00:00 BRT 2016
admin  >
_OK ticket:57ddcb336098c149eebca22604e3a01a
```

Figura 22 – Command Line Interface – date – Exemplo 2.

2.6 [debug-auth]

Exibe os logs de debug em tempo real das autenticações (login, logout, keepalive e erros).

Modo de uso:

```
admin  >debug-auth
```

Figura 23 – Command Line Interface – debug-auth.

3

Exemplo:

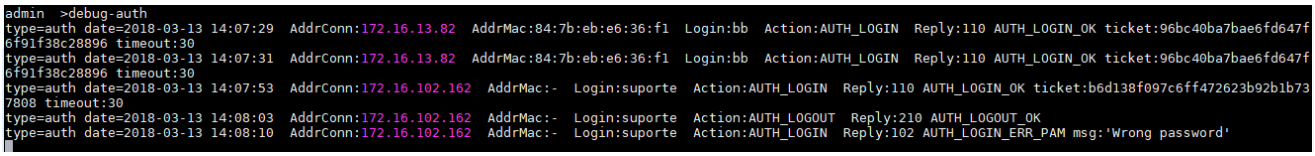

Figura 24 – Command Line Interface – debug-auth - exemplo.

3.1 [debug-dhcp]

Exibe os logs de debug em tempo real do serviço de DHCP.

Modo de uso:

Figura 25 – Command Line Interface – debug-dhcp.

4

Exemplo:

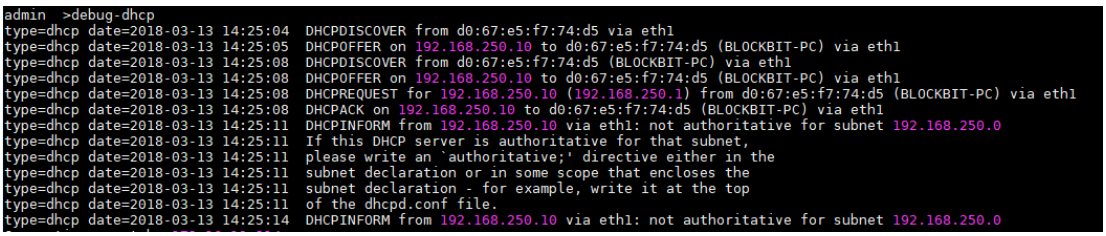

Figura 26 – Command Line Interface – debug-dhcp - exemplo.

4.1 [debug-events]

Exibe os logs em tempo real dos eventos do sistema.

Modo de uso:

Figura 27 – Command Line Interface – debug-events.

Exemplo:

Figura 28 – Command Line Interface – debug-events - exemplo.

Exemplo 2: Caso não haja qualquer registro de log, será apresentada a informação abaixo:

Figura 29 – Command Line Interface – debug-events – log not found.

4.2 [debug-firewall]

Exibe os logs de debug em tempo real do Firewall.

Modo de uso:

Figura 30 – Command Line Interface – debug-firewall.

Exemplo:

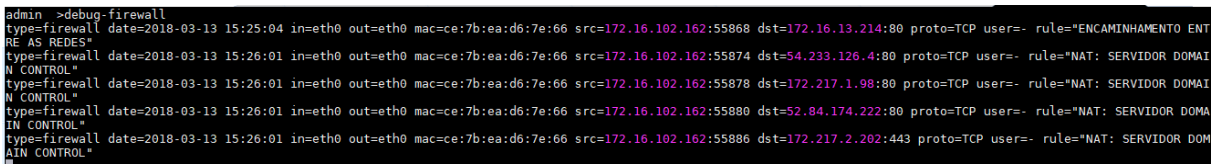

Figura 31 – Command Line Interface – debug-auth – exemplo.

4.3 [debug-ha]

Exibe os logs de debug do serviço de Alta Disponibilidade (H.A).

Modo de uso:

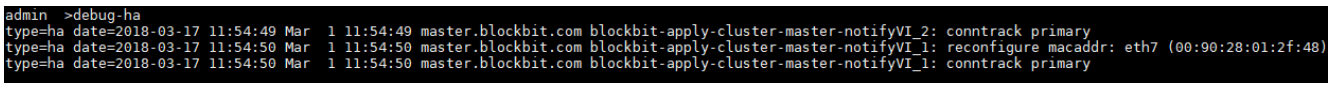

Figura 32 – Command Line Interface – debug-ha.

4.4 [debug-threats]

Exibe os logs de debug em tempo real dos tratamentos de ATP e IPS.

Modo de uso:

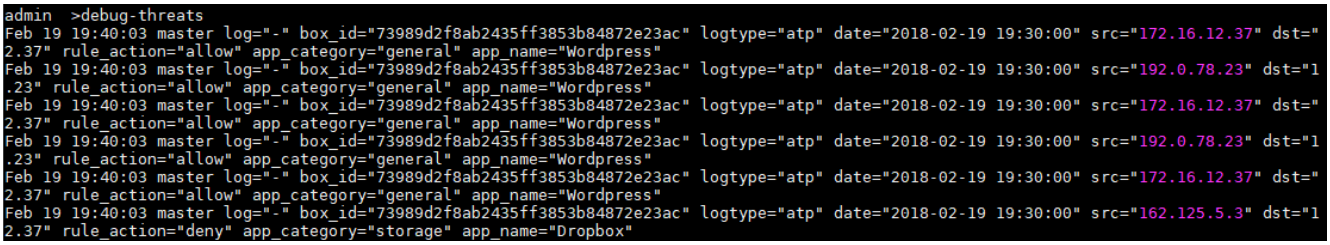

Figura 33 – Command Line Interface – debug-threats.

Exemplo: Caso não haja qualquer registro de log, será apresentada a informação abaixo:

Figura 34 – Command Line Interface – debug-threats – log not found.

5.1 [debug-vpn]

Exibe os logs de debug em tempo real do serviço de VPN IPSEC.

Modo de uso:

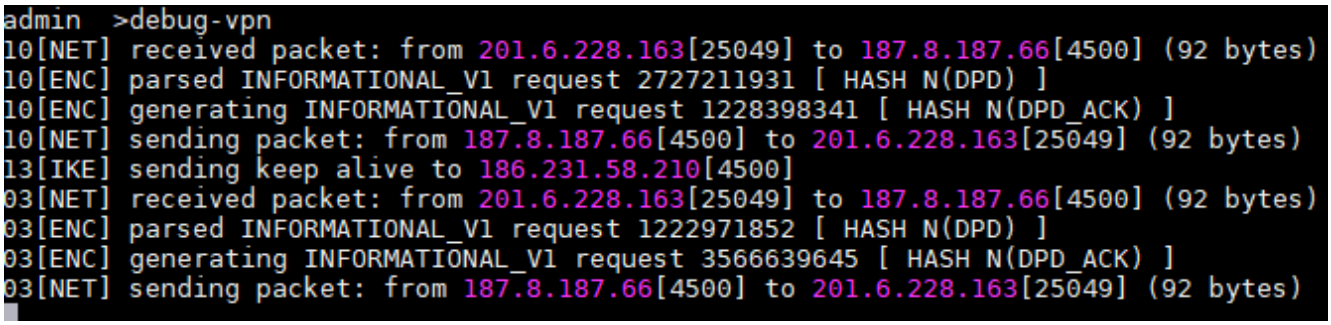

Figura 35 – Command Line Interface – debug-vpn.

Exemplo: Caso não haja qualquer registro de log, será apresentada a informação abaixo:

Figura 36 – Command Line Interface – debug-vpn – log not found.

5.2 [debug-web]

Exibe os logs de debug em tempo real dos acessos que passam pelo serviço do proxy web.

Modo de uso:

Figura 37 – Command Line Interface – debug-web.

Exemplo:

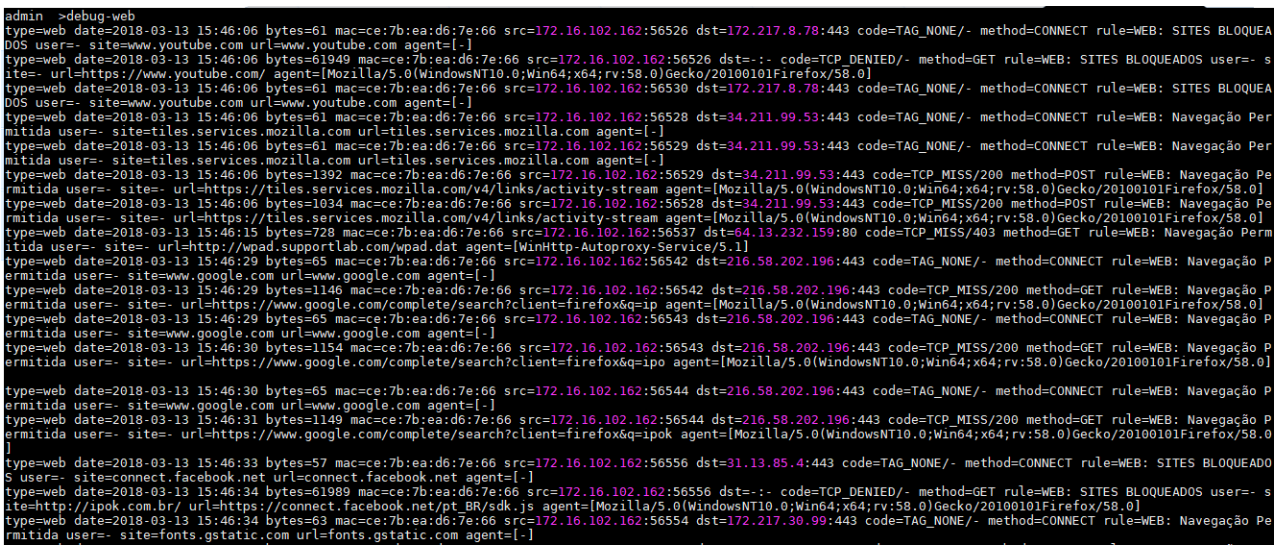

Figura 38 – Command Line Interface – debug-web.

5.3 [dig]

Exibe informações sobre domínios.

Modo de uso:

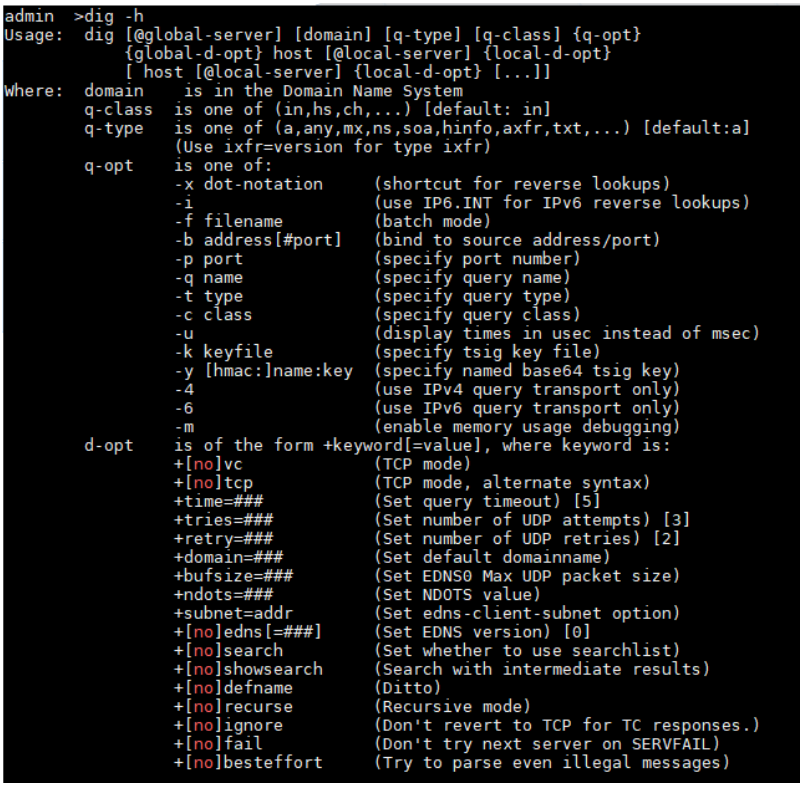

Figura 39 – Command Line Interface – dig.

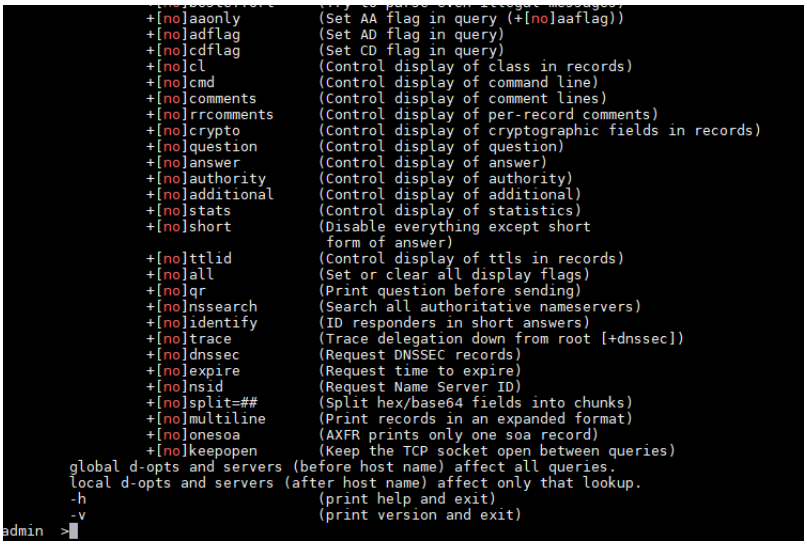

Figura 40 – Command Line Interface – dig 2.

Exemplo: Verifica o apontamento tipo A do site:

```
admin  >dig A www.uol.com.br

; <<>> DiG 9.10.2 <<>> A www.uol.com.br
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 6375
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;www.uol.com.br.                        IN      A

;; ANSWER SECTION:
www.uol.com.br.         9       IN      CNAME   homeuol-ib.uol.com.br.
homeuol-ib.uol.com.br.  9       IN      A       200.221.2.45

;; Query time: 130 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: Tue Mar 13 17:01:04 BRT 2018
;; MSG SIZE  rcvd: 84
```

Figura 41 – Command Line Interface – dig - exemplo.

Exemplo 2: Verificar apontamento MX (Mail Exchanger) do domínio:

```
admin  >dig MX uol.com.br

; <<>> DiG 9.10.2 <<>> MX uol.com.br
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 28055
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;uol.com.br.                    IN      MX

;; ANSWER SECTION:
uol.com.br.             11162   IN      MX      10 mx.uol.com.br.

;; Query time: 129 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: Tue Mar 13 17:01:32 BRT 2018
;; MSG SIZE  rcvd: 58
```

Figura 42 – Command Line Interface – dig – exemplo 2.

5.4 [disable-bgp]

Desabilita o serviço de roteamento dinâmico BGP.

Modo de uso:

```
admin  >disable-bgp
Service is disabled
admin  >
```

Figura 43 – Command Line Interface – disable-bgp.

Desabilita apenas o serviço, as configurações permanecerão.

5.5 [disable-ospf]

Desabilita o serviço de roteamento dinâmico OSPF tanto para IPv4 como também para IPv6.

Modo de uso:

```
admin  >disable-ospf
Service is disabled
admin  >
```

Figura 44 – Command Line Interface – disable-ospf.

Desabilita apenas o serviço, as configurações permanecerão.

5.6 [disable-pim]

Desabilita o serviço de roteamento dinâmico PIM-SM.

Modo de uso:

```
admin  >disable-pim
Service is disabled
admin  >
```

Figura 45 – Command Line Interface – disable-pim.

Desabilita apenas o serviço, as configurações permanecerão.

5.7 [disable-rip]

Desabilita o serviço de roteamento dinâmico RIP tanto para IPv4 como também para IPv6.

Modo de uso:

```
admin  >disable-rip
Service is disabled
admin  >
```

Figura 46 – Command Line Interface – disable-rip.

Desabilita apenas o serviço, as configurações permanecerão.

5.8 [disable-snmp]

Desabilita o serviço de SNMP.

Modo de uso:

```
admin  >disable-snmp
snmpd is disabled!
admin  >
```

Figura 47 – Command Line Interface – disable-snmp.

Desabilita apenas o serviço, as configurações permanecerão.

5.9 [enable-bgp]

Habilita o serviço de roteamento dinâmico BGP.

Modo de uso:

```
admin  >enable-bgp
Service is enable
admin  >
```

Figura 48 – Command Line Interface – enable-bgp.

5.10 [enable-ospf]

Habilita o serviço de roteamento dinâmico OSPF tanto para IPv4 como também IPv6.

Modo de uso:

```
admin  >enable-ospf
Service is enable
admin  >
```

Figura 49 – Command Line Interface – enable-ospf.

5.11 [enable-pim]

Habilita o serviço de roteamento dinâmico PIM-SM.

Modo de uso:

Figura 50 – Command Line Interface – enable-pim.

5.12 [enable-rip]

Habilita o serviço de roteamento dinâmico RIP tanto para IPv4 como também IPv6.

Modo de uso:

Figura 51 – Command Line Interface – enable-rip.

5.13 [enable-root]

Eleva o privilégio de acesso ao sistema ao modo desenvolvedor.

Modo de uso:

Figura 52 – Command Line Interface – enable-root.

5.14 [enable-snmp]

Habilita e configura o SNMP (SNMPv1, SNMPv2 ou SNMPv3).

Modo de uso:

```
admin  >enable-snmp
```

Figura 53 – Command Line Interface – enable-snmp.

Exemplo:

```
admin  >enable-snmp
Enable SNMPv1 (Y/N)? Y
Enable SNMPv2 (Y/N)? Y
Comunity name: BLOCKBIT
Network Access (Leave blank to default 0.0.0.0/0): 172.16.102.0/24
Enable SNMPv3 (Y/N)? Y
Auth Protocol (MD5 or SHA): MD5
Username: blockbit
User password (minimum of 8 characters): password
Encryption Protocol (3DES or DES): 3DES
Encryption Password: password
Enable SNMPv1
Enable SNMPv2
Comunity: BLOCKBIT
Network Access: 172.16.102.0/24
Enable SNMPv3
Auth Protocol: MD5
Username: blockbit
Encryption Protocol: 3DES

Confirm (Y/N)? Y
```

Figura 54 – Command Line Interface – enable-snmp - exemplo.

Após confirmar a configuração acima, são exibidas as seguintes informações:

```
snmp is enabled!

syslocation  "Sao Paulo"

syscontact "suporte@labsuporte.com.br"
syscontact  "LABSUPORTE"

extend ALERTS /usr/bin/perl /home/admin/bin/show-alerts
extend SERVICES /usr/bin/perl /home/admin/bin/service-status

com2sec local     localhost BLOCKBIT
com2sec mynetwork 172.16.102.0/24       BLOCKBIT

group MyRWGroup v1      local
group MyRWGroup v2c     local
group MyRWGroup usm     local

group MyROGroup v1      mynetwork
group MyROGroup v2c     mynetwork
group MyROGroup usm     mynetwork


view all    included  .1.3.6.1.2.1.1
view all    included  .1.3.6.1.2.1.2
view all    included  .1.3.6.1.4.1.2021
view all    included  .iso.org.dod.internet.mgmt.mib-2.system
view all    included  .iso.org.dod.internet.mgmt.mib-2.host.hrDevice
view all    included  .iso.org.dod.internet.mgmt.mib-2.host.hrSWRunPerf
view all    included  .iso.org.dod.internet.mgmt.mib-2.host.hrStorage
view all    included  .iso.org.dod.internet.private.enterprises.ucdavis.laTable.laEntry
view all    included .1.3.6.1.4.1.8072.1.3.2.4.1.2

access MyROGroup ""      any       noauth    exact  all    none   none
access MyRWGroup ""      any       noauth    exact  all    none    none
rouser blockbit
admin  >
```

Figura 55 – Command Line Interface – enable-snmp – exemplo de configuração.

5.15 [ethtool]

Exibe e modifica informações sobre as interfaces de rede do servidor.

Modo de uso:

```
admin  >ethtool -h
ethtool version 3.15
Usage:
        ethtool DEVNAME Display standard information about device
        ethtool -s|--change DEVNAME     Change generic options
                [ speed %d ]
                [ duplex half|full ]
                [ port tp|aui|bnc|mii|fibre ]
                [ mdix auto|on|off ]
                [ autoneg on|off ]
                [ advertise %x ]
                [ phyad %d ]
                [ xcvr internal|external ]
                [ wol p|u|m|b|a|g|s|d... ]
                [ sopass %x:%x:%x:%x:%x:%x ]
                [ msglvl %d | msglvl type on|off ... ]
        ethtool -a|--show-pause DEVNAME Show pause options
        ethtool -A|--pause DEVNAME      Set pause options
                [ autoneg on|off ]
                [ rx on|off ]
                [ tx on|off ]
        ethtool -c|--show-coalesce DEVNAME      Show coalesce options
        ethtool -C|--coalesce DEVNAME   Set coalesce options
                [adaptive-rx on|off]
                [adaptive-tx on|off]
                [rx-usecs N]
                [rx-frames N]
                [rx-usecs-irq N]
                [rx-frames-irq N]
                [tx-usecs N]
                [tx-frames N]
                [tx-usecs-irq N]
                [tx-frames-irq N]
                [stats-block-usecs N]
                [pkt-rate-low N]
                [rx-usecs-low N]
                [rx-frames-low N]
                [tx-usecs-low N]
                [tx-frames-low N]
                [pkt-rate-high N]
                [rx-usecs-high N]
                [rx-frames-high N]
                [tx-usecs-high N]
                [tx-frames-high N]
```

Figura 56 – Command Line Interface – ethtool.

```
                [sample-interval N]
        ethtool -g|--show-ring DEVNAME  Query RX/TX ring parameters
        ethtool -G|--set-ring DEVNAME   Set RX/TX ring parameters
                [ rx N ]
                [ rx-mini N ]
                [ rx-jumbo N ]
                [ tx N ]
        ethtool -k|--show-features|--show-offload DEVNAME       Get state of protocol offload and other features
        ethtool -K|--features|--offload DEVNAME Set protocol offload and other features
                FEATURE on|off ...
        ethtool -i|--driver DEVNAME     Show driver information
        ethtool -d|--register-dump DEVNAME      Do a register dump
                [ raw on|off ]
                [ file FILENAME ]
        ethtool -e|--eeprom-dump DEVNAME        Do a EEPROM dump
                [ raw on|off ]
                [ offset N ]
                [ length N ]
        ethtool -E|--change-eeprom DEVNAME      Change bytes in device EEPROM
                [ magic N ]
                [ offset N ]
                [ length N ]
                [ value N ]
        ethtool -r|--negotiate DEVNAME  Restart N-WAY negotiation
        ethtool -p|--identify DEVNAME   Show visible port identification (e.g. blinking)
               [ TIME-IN-SECONDS ]
        ethtool -t|--test DEVNAME       Execute adapter self test
               [ online | offline | external_lb ]
        ethtool -S|--statistics DEVNAME Show adapter statistics
        ethtool -n|-u|--show-nfc|--show-ntuple DEVNAME  Show Rx network flow classification options or rules
                [ rx-flow-hash tcp4|udp4|ah4|esp4|sctp4|tcp6|udp6|ah6|esp6|sctp6 |
                  rule %d ]
        ethtool -N|-U|--config-nfc|--config-ntuple DEVNAME      Configure Rx network flow classification options or rules
                rx-flow-hash tcp4|udp4|ah4|esp4|sctp4|tcp6|udp6|ah6|esp6|sctp6 m|v|t|s|d|f|n|r... |
                flow-type ether|ip4|tcp4|udp4|sctp4|ah4|esp4
                        [ src %x:%x:%x:%x:%x:%x [m %x:%x:%x:%x:%x:%x] ]
                        [ dst %x:%x:%x:%x:%x:%x [m %x:%x:%x:%x:%x:%x] ]
                        [ proto %d [m %x] ]
                        [ src-ip %d.%d.%d.%d [m %d.%d.%d.%d] ]
                        [ dst-ip %d.%d.%d.%d [m %d.%d.%d.%d] ]
                        [ tos %d [m %x] ]
                        [ l4proto %d [m %x] ]
                        [ src-port %d [m %x] ]
                        [ dst-port %d [m %x] ]
```

Figura 57 – Command Line Interface – ethtool 2.

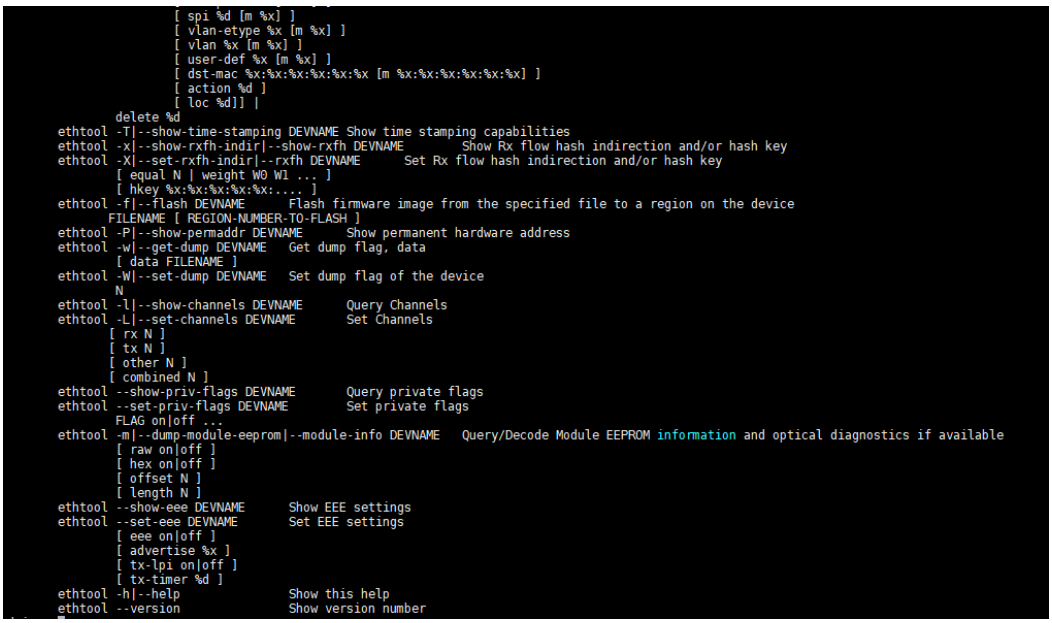

Figura 58 – Command Line Interface – ethtool 3.

Exemplo: Ver as informações sobre a interface eth0: modos suportados, velocidade negociada, modo de negociação e se há cabo conectado:

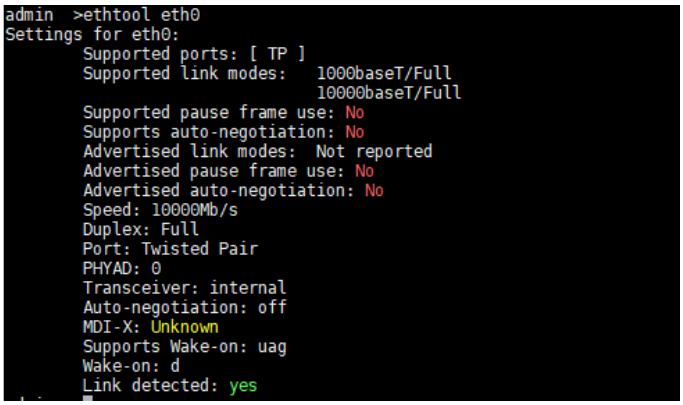

Figura 59 – Command Line Interface – ethtool - exemplo.

5.16 [exit]

Abandona a sessão.

Modo de uso:

```
Modo de uso
admin  >exit  |
```

Figura 60 – Command Line Interface – exit.

5.17 [fdisk]

Exibe e gerencia as partições do(s) disco(s).

Modo de uso:

```
admin  >fdisk -h
Usage:
 fdisk [options] <disk>    change partition table
 fdisk [options] -l <disk> list partition table(s)
 fdisk -s <partition>      give partition size(s) in blocks

Options:
 -b <size>             sector size (512, 1024, 2048 or 4096)
 -c[=<mode>]           compatible mode: 'dos' or 'nondos' (default)
 -h                    print this help text
 -u[=<unit>]           display units: 'cylinders' or 'sectors' (default)
 -v                    print program version
 -C <number>           specify the number of cylinders
 -H <number>           specify the number of heads
 -S <number>           specify the number of sectors per track
```

Figura 61 – Command Line Interface – fdisk.

Exemplo: Exibir todos os discos e partições:

```
admin  >fdisk -l
WARNING: fdisk GPT support is currently new, and therefore in an experimental phase. Use at your own discretion.

Disk /dev/sda: 34.4 GB, 34359738368 bytes, 67108864 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk label type: gpt


#         Start          End    Size  Type            Name
 1          2048        47103     22M  BIOS boot parti no-fs
 2         47104      2789375    1.3G  Microsoft basic primary
 3       2789376      6291455    1.7G  Microsoft basic primary
 4       6291456     10485759      2G  Microsoft basic primary
 5      10485760     27262975      8G  Microsoft basic primary
 6      27262976     67106815     19G  Microsoft basic primary

Disk /dev/mapper/luks-50f7104f-0886-4598-bfcb-c5644fc0cffa: 8587 MB, 8587837440 bytes, 16773120 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes


Disk /dev/mapper/luks-7ebec2b9-b7b3-4f54-9e45-06da007443a3: 2145 MB, 2145386496 bytes, 4190208 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes


Disk /dev/mapper/luks-454dcc5c-c107-4b6b-b6aa-0c0a5eba77bd: 20.4 GB, 20397948928 bytes, 39839744 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes


Disk /dev/mapper/cryptoswap: 1793 MB, 1793064960 bytes, 3502080 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
```

Figura 62 – Command Line Interface – fdisk - exemplo.

5.18 [free]

Exibe o status de uso de memória RAM do sistema.

Modo de uso:

```
admin  >free --h
free: option '--h' is ambiguous; possibilities: '--human' '--help'

Usage:
 free [options]

Options:
 -b, --bytes         show output in bytes
 -k, --kilo          show output in kilobytes
 -m, --mega          show output in megabytes
 -g, --giga          show output in gigabytes
     --tera          show output in terabytes
 -h, --human         show human-readable output
     --si            use powers of 1000 not 1024
 -l, --lohi          show detailed low and high memory statistics
 -t, --total         show total for RAM + swap
 -s N, --seconds N   repeat printing every N seconds
 -c N, --count N     repeat printing N times, then exit
 -w, --wide          wide output

     --help     display this help and exit
 -V, --version  output version information and exit

For more details see free(1).
admin  >
```

Figura 63 – Command Line Interface – free.

Exemplo: Verificar o consumo de memória:

```
admin  >free -m
               total        used        free      shared  buff/cache   available
Mem:            3952         172         186         216        3593        3324
Swap:           1995          80        1915
admin  >
```

Figura 64 – Command Line Interface – free – Exemplo.

5.19 [fsck]

Analisa e efetua tentativa de correção a problemas no disco ou partição.

Modo de uso:

```
admin  >fsck
Usage: /usr/sbin/fsck.ext4 [-panyrcdfvtDFV] [-b superblock] [-B blocksize]
                [-I inode_buffer_blocks] [-P process_inode_size]
                [-l|-L bad_blocks_file] [-C fd] [-j external_journal]
                [-E extended-options] device

Emergency help:
 -p                   Automatic repair (no questions)
 -n                   Make no changes to the filesystem
 -y                   Assume "yes" to all questions
 -c                   Check for bad blocks and add them to the badblock list
 -f                   Force checking even if filesystem is marked clean
 -v                   Be verbose
 -b superblock        Use alternative superblock
 -B blocksize         Force blocksize when looking for superblock
 -j external_journal  Set location of the external journal
 -l bad_blocks_file   Add to badblocks list
 -L bad_blocks_file   Set badblocks list
```

Figura 65 – Command Line Interface – fsck.

NUNCA executar a checagem em partições montadas, isso poderá corromper as informações no sistema de arquivo.

5.20 [fwrecovery]

Libera temporariamente toda a entrada e o encaminhamento no Firewall.

Modo de uso:

```
admin  >fwrecovery
Recovery firewall
Be brief, be sure to apply the settings in the admin interface.

Firewall is open !!!
```

Figura 66 – Command Line Interface – fwrecovery.

ASSIM QUE POSSÍVEL, acessar a interface WEB e clicar em aplicar (canto superior direito) para que as regras temporárias sejam removidas.

5.21 [fwreload]

Recarrega todas as regras.

Modo de uso:

```
admin  >fwreload
reloading firewall chains
reloading firewall zones
reloading firewall input
reloading firewall redirects
reloading firewall security rules
reloading firewall multilink rules
reloading firewall vpn rules
reloading firewall atp rules
```

Figura 67 – Command Line Interface – fwreload.

Ocorrerá uma breve interrupção nos acessos!

5.22 [grep]

Utilizado em conjunto com outros comandos para filtrar a saída.

Exemplo: Filtrar a saída do debug-web para visualizar apenas requisições com destino a uma URL específica:

```
admin  >debug-web|grep blockbit.com
type=web date=2018-03-14 10:51:43 bytes=745 mac=00:00:00:00:00:00 src=172.16.13.82:16959 dst=104.198.103.7:443 code=TCP_TUNNEL/- method=CONNECT rule=WEB: Navegação Permitida user=- site=ww
w.blockbit.com url=www.blockbit.com agent=[Mozilla/5.0(WindowsNT10.0;Win64;x64)AppleWebKit/537.36(KHTML,likeGecko)Chrome/64.0.3282.186Safari/537.36]
type=web date=2018-03-14 10:52:10 bytes=1011 mac=00:00:00:00:00:00 src=172.16.13.82:16962 dst=104.198.103.7:443 code=TCP_TUNNEL/- method=CONNECT rule=WEB: Navegação Permitida user=- site=w
ww.blockbit.com url=www.blockbit.com agent=[Mozilla/5.0(WindowsNT10.0;Win64;x64)AppleWebKit/537.36(KHTML,likeGecko)Chrome/64.0.3282.186Safari/537.36]
type=web date=2018-03-14 10:52:10 bytes=1011 mac=00:00:00:00:00:00 src=172.16.13.82:16958 dst=104.198.103.7:443 code=TCP_TUNNEL/- method=CONNECT rule=WEB: Navegação Permitida user=- site=w
ww.blockbit.com url=www.blockbit.com agent=[Mozilla/5.0(WindowsNT10.0;Win64;x64)AppleWebKit/537.36(KHTML,likeGecko)Chrome/64.0.3282.186Safari/537.36]
```

Figura 68 – Command Line Interface – grep - exemplo.

Exemplo 2: Filtrar a saída do comando ethtool utilizando regex:

```
admin  >ethtool eth0|grep -ie "speed\|detected"
        Speed: 10000Mb/s
        Link detected: yes
```

Figura 69 – Command Line Interface – grep – exemplo 2.

5.23 [help]

Lista todos os comandos disponíveis na interface CLI.

Modo de uso:

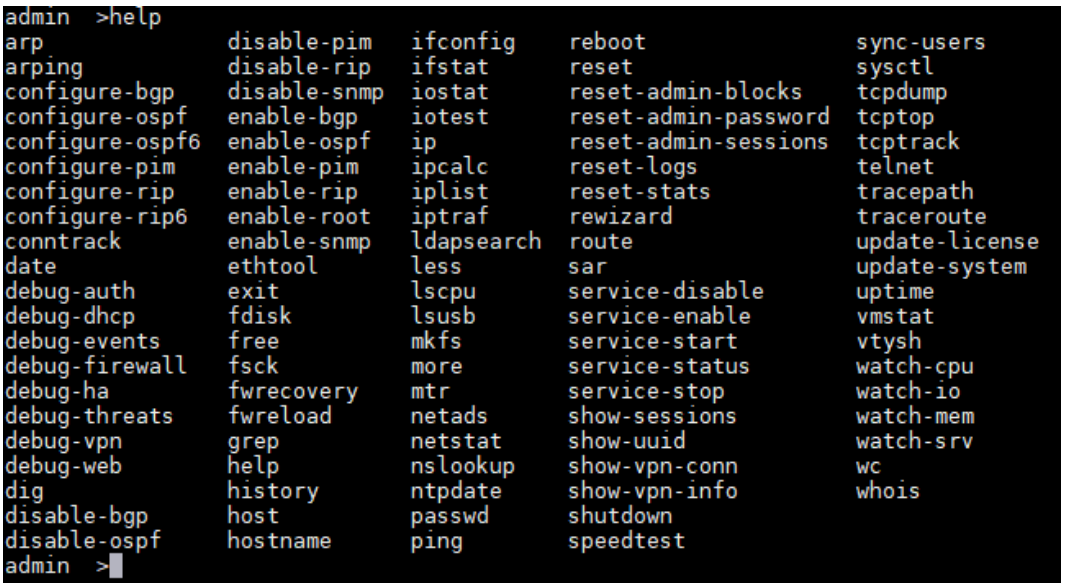

Figura 70 – Command Line Interface – help.

5.24 [history]

Exibe o histórico de comandos executados na CLI.

Modo de uso:

Figura 71 – Command Line Interface – history.

5.25 [host]

Utilitário para consulta DNS.

Modo de uso:

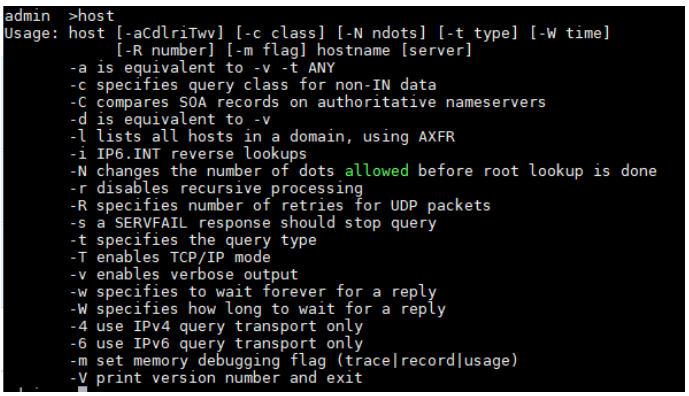

Figura 72 – Command Line Interface – host.

Exemplo: consultar o IP de um determinado endereço:

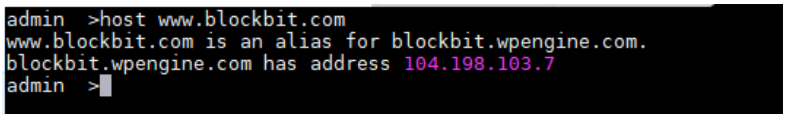

Figura 73 – Command Line Interface – host - exemplo.

5.26 [Hostname]

Exibe ou altera o nome de host do seu dispositivo BLOCKBIT UTM.

Modo de uso:

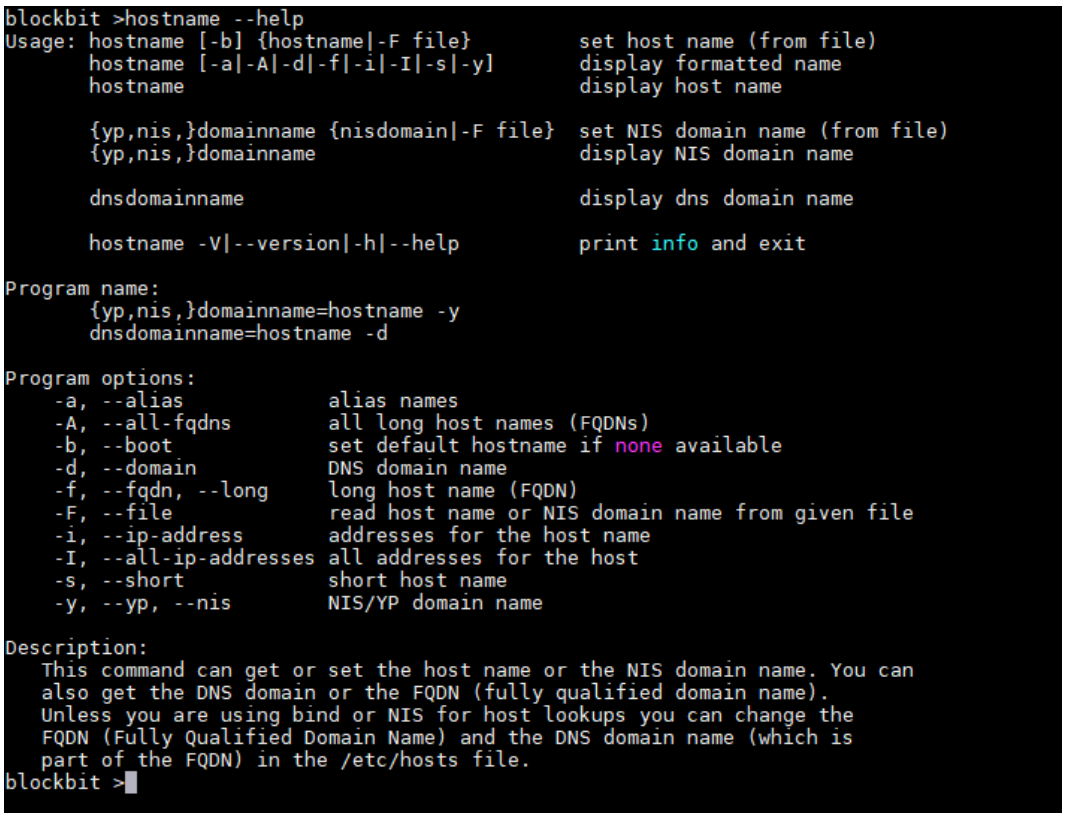

Figura 74 – Command Line Interface – hostname.

Exemplo: Utilizando o comando para exibir o nome atual do seu dispositivo BLOCKBIT UTM:

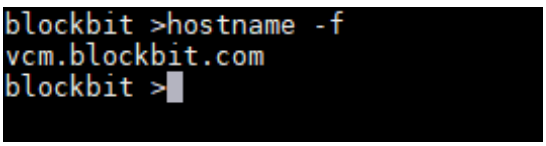

Figura 75 – Command Line Interface – hostname - Exemplo.

5.27 [ifconfig]

Configura e mantém as configurações da interface. Pode ativar, desativar e listar o status de cada uma das interfaces. Também pode ser utilizado para otimizar a configuração do sistema.

Modo de uso:

```
blockbit >ifconfig -h
Usage:
  ifconfig [-a] [-v] [-s] <interface> [[<AF>] <address>]
  [add <address>[/<prefixlen>]]
  [del <address>[/<prefixlen>]]
  [[-]broadcast [<address>]]  [[-]pointopoint [<address>]]
  [netmask <address>]  [dstaddr <address>]  [tunnel <address>]
  [outfill <NN>] [keepalive <NN>]
  [hw <HW> <address>]  [mtu <NN>]
  [[-]trailers]  [[-]arp]  [[-]allmulti]
  [multicast]  [[-]promisc]
  [mem_start <NN>]  [io_addr <NN>]  [irq <NN>]  [media <type>]
  [txqueuelen <NN>]
  [[-]dynamic]
  [up|down] ...

  <HW>=Hardware Type.
  List of possible hardware types:
    loop (Local Loopback) slip (Serial Line IP) cslip (VJ Serial Line IP)
    slip6 (6-bit Serial Line IP) cslip6 (VJ 6-bit Serial Line IP) adaptive (Adaptive Serial Line IP)
    ash (Ash) ether (Ethernet) ax25 (AMPR AX.25)
    netrom (AMPR NET/ROM) rose (AMPR ROSE) tunnel (IPIP Tunnel)
    ppp (Point-to-Point Protocol) hdlc ((Cisco)-HDLC) lapb (LAPB)
    arcnet (ARCnet) dlci (Frame Relay DLCI) frad (Frame Relay Access Device)
    sit (IPv6-in-IPv4) fddi (Fiber Distributed Data Interface) hippi (HIPPI)
    irda (IrLAP) ec (Econet) x25 (generic X.25)
    infiniband (InfiniBand) eui64 (Generic EUI-64)
  <AF>=Address family. Default: inet
  List of possible address families:
    unix (UNIX Domain) inet (DARPA Internet) inet6 (IPv6)
    ax25 (AMPR AX.25) netrom (AMPR NET/ROM) rose (AMPR ROSE)
    ipx (Novell IPX) ddp (Appletalk DDP) ec (Econet)
    ash (Ash) x25 (CCITT X.25)
blockbit >
```

Figura 76 – Command Line Interface – ifconfig.

Exemplo: Exibir as informações sobre todas as interfaces de rede, ativas ou desabilitadas:

```
blockbit >ifconfig -a
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.16.102.136  netmask 255.255.255.0  broadcast 172.16.102.255
        ether 00:0c:29:bf:b2:c7  txqueuelen 1000  (Ethernet)
        RX packets 1290671  bytes 251526124 (239.8 MiB)
        RX errors 0  dropped 321  overruns 0  frame 0
        TX packets 142921  bytes 68344332 (65.1 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

eth1: flags=4098<BROADCAST,MULTICAST>  mtu 1500
        ether 00:0c:29:bf:b2:d1  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

eth2: flags=4098<BROADCAST,MULTICAST>  mtu 1500
        ether 00:0c:29:bf:b2:db  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

eth3: flags=4098<BROADCAST,MULTICAST>  mtu 1500
        ether 00:0c:29:bf:b2:e5  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        loop  txqueuelen 0  (Local Loopback)
        RX packets 3123752  bytes 3502571850 (3.2 GiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 3123752  bytes 3502571850 (3.2 GiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

blockbit >
```

Figura 77 – Command Line Interface – ifconfig - Exemplo.

5.28 [ifstat]

Exibe estatísticas do tráfego de rede.

Modo de uso:

```
blockbit >ifstat -h
Usage: ifstat [OPTION] [ PATTERN [ PATTERN ] ]
   -h, --help           this message
   -a, --ignore ignore history
   -d, --scan=SECS      sample every statistics every SECS
   -e, --errors show errors
   -n, --nooutput       do history only
   -r, --reset          reset history
   -s, --noupdate       don;t update history
   -t, --interval=SECS  report average over the last SECS
   -V, --version        output version information
   -z, --zeros          show entries with zero activity
blockbit >
```

Figura 78 – Command Line Interface – ifstat.

Exemplo: Listar relatório estatístico geral do tráfego de todas as interfaces da rede:

```
blockbit >ifstat
#kernel
Interface        RX Pkts/Rate    TX Pkts/Rate    RX Data/Rate    TX Data/Rate
                 RX Errs/Drop    TX Errs/Drop    RX Over/Rate    TX Coll/Rate
lo                 34054 0         34054 0        84632K 0        84632K 0
                       0 0             0 0             0 0             0 0
eth0               18848 0          3665 0         1700K 0         1466K 0
                       0 10            0 0             0 0             0 0
blockbit >
```

Figura 79 – Command Line Interface – ifstat - Exemplo.

5.29 [iostat]

Monitora a escrita de entrada e saída (I/O) na estrutura de partições *"file system"* do disco do BLOCKBIT UTM.

Modo de uso:

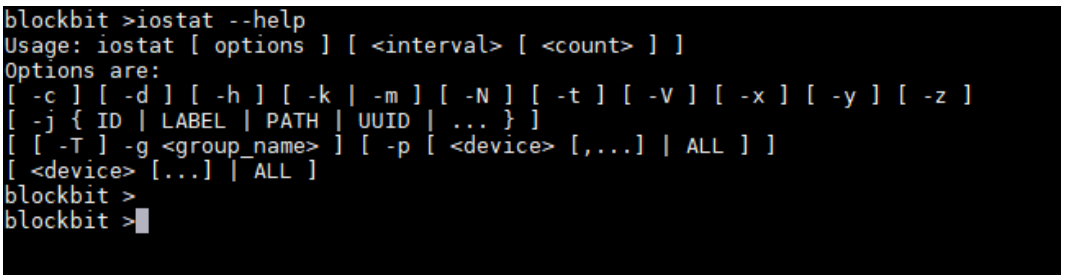

Figura 80 – Command Line Interface – iostat.

Exemplo: Listar o uso de (I/O) das partições do BLOCKBIT UTM.

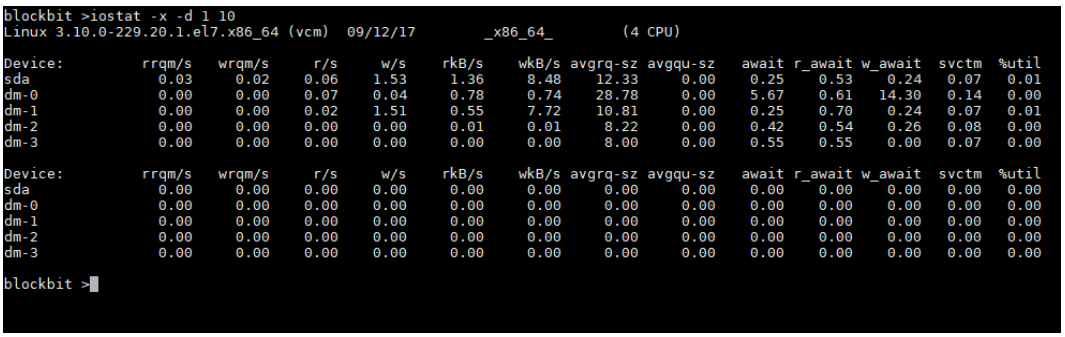

Figura 81 – Command Line Interface – iostat - Exemplo.

5.30 [iotest]

Executa um teste de escrita de entrada e saída (I/O) na estrutura de partições *"file system"* do disco do BLOCKBIT UTM.

Modo de uso:

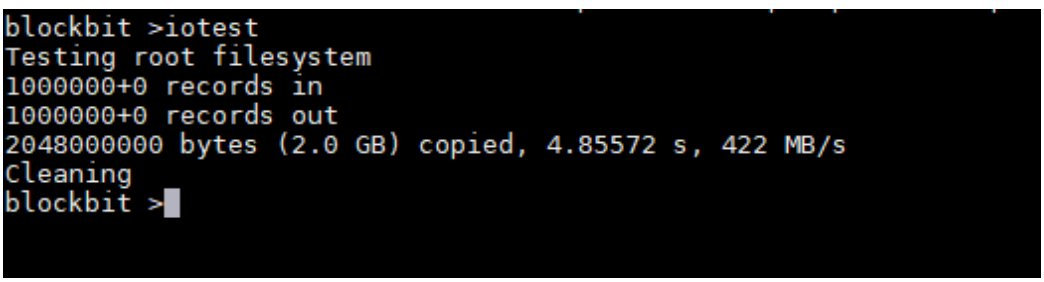

Figura 82 – Command Line Interface – iotest.

5.31 [ip]

Exibe e modifica roteamento, device e tunnels.

Modo de uso:

```
admin  >ip --help
Usage: ip [ OPTIONS ] OBJECT { COMMAND | help }
       ip [ -force ] -batch filename
where  OBJECT := { link | addr | addrlabel | route | rule | neigh | ntable |
                   tunnel | tuntap | maddr | mroute | mrule | monitor | xfrm |
                   netns | l2tp | tcp_metrics | token }
       OPTIONS := { -V[ersion] | -s[tatistics] | -d[etails] | -r[esolve] |
                    -f[amily] { inet | inet6 | ipx | dnet | bridge | link } |
                    -4 | -6 | -I | -D | -B | -0 |
                    -l[oops] { maximum-addr-flush-attempts } |
                    -o[neline] | -t[imestamp] | -b[atch] [filename] |
                    -rc[vbuf] [size]}
```

Figura 83 – Command Line Interface - ip.

Exemplo: Exibir tabela de rotamento:

```
admin  >ip route
default via 172.16.102.1 dev eth0
10.20.30.0/24 dev tun0  proto kernel  scope link  src 10.20.30.1
172.16.102.0/24 dev eth0  proto kernel  scope link  src 172.16.102.78
192.168.222.0/24 dev dummy1  proto kernel  scope link  src 192.168.222.1
```

Figura 84 – Command Line Interface – ip - exemplo.

Exemplo 2: Limpar tabela arp do device eth0:

```
admin  >ip neigh flush dev eth0
admin  >
```

Figura 85 – Command Line Interface – ip – exemplo 2.

5.32 [ipcalc]

Utilitário para cálculo de endereçamento IP.

Modo de uso:

```
admin  >ipcalc --help
Usage: ipcalc [OPTION...]
  -c, --check         Validate IP address for specified address family
  -4, --ipv4          IPv4 address family (default)
  -6, --ipv6          IPv6 address family
  -b, --broadcast     Display calculated broadcast address
  -h, --hostname      Show hostname determined via DNS
  -m, --netmask       Display default netmask for IP (class A, B, or C)
  -n, --network       Display network address
  -p, --prefix        Display network prefix
  -s, --silent        Don't ever display error messages

Help options:
  -?, --help          Show this help message
  --usage             Display brief usage message
```

Figura 86 – Command Line Interface – ipcalc.

Exemplo:

```
admin  >ipcalc 192.168.1.0/22 -mnpb
NETMASK=255.255.252.0
PREFIX=22
BROADCAST=192.168.3.255
NETWORK=192.168.0.0
```

Figura 87 – Command Line Interface – ipcalc - exemplo.

5.33 [iplist]

Lista uma ou todas as interfaces de rede, zona e status da conexão física.

Modo de uso:

```
admin  >iplist eth0
ZONE LAN (1) 2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP qlen 10000
    link/ether 00:0c:29:53:3d:16 brd ff:ff:ff:ff:ff:ff
    inet 172.16.102.78/24 brd 172.16.102.255 scope global eth0
       valid_lft forever preferred_lft forever
SIOCGMIIPHY on 'eth0' failed: Operation not supported
```

Figura 88 – Command Line Interface – iplist.

5.34 [iptraf]

Monitor de tráfego de rede com GUI (Graphical User Interface*)*.

Modo de uso:

```
admin  >iptraf --help
usage: iptraf-ng [options]
   or: iptraf-ng [options] -B [-i <iface> | -d <iface> | -s <iface> | -z <iface> | -l <iface> | -g]

    -h, --help            show this help message

    -i <iface>            start the IP traffic monitor (use '-i all' for all interfaces)
    -d <iface>            start the detailed statistics facility on an interface
    -s <iface>            start the TCP and UDP monitor on an interface
    -z <iface>            shows the packet size counts on an interface
    -l <iface>            start the LAN station monitor (use '-l all' for all LAN interfaces)
    -g                    start the general interface statistics

    -B                    run in background (use only with one of the above parameters
    -f                    clear all locks and counters
    -t <n>                run only for the specified <n> number of minutes
    -L <logfile>          specifies an alternate log file
```

Figura 89 – Command Line Interface – iptraf.

Exemplo: Ao executar o comando **iptraf**, é aberta a seguinte interface interativa:

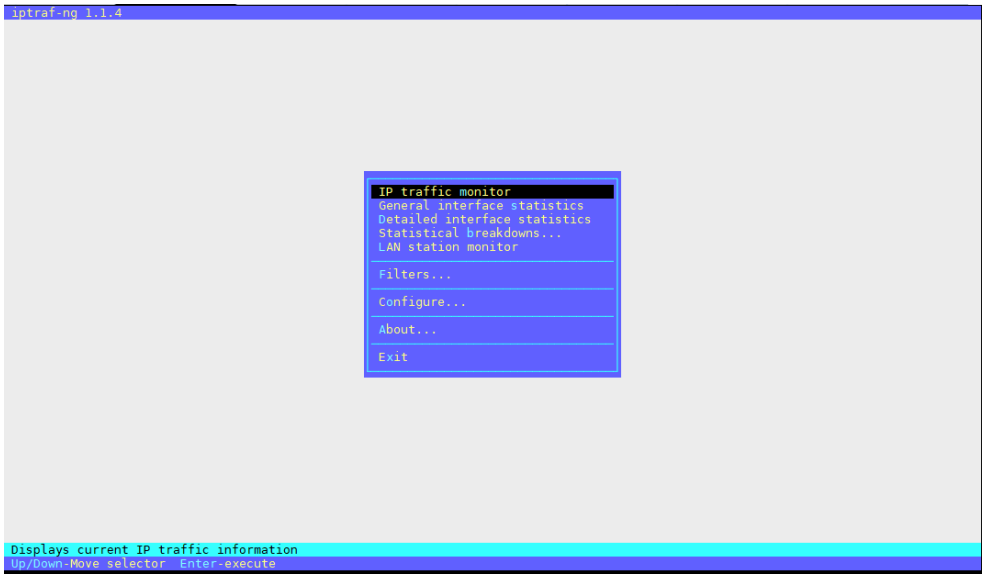

Figura 90 – Command Line Interface – iptraf - exemplo.

Exemplo 2: iptraf -d eth0 – Estatísticas detalhadas em tempo real da interface eth0:

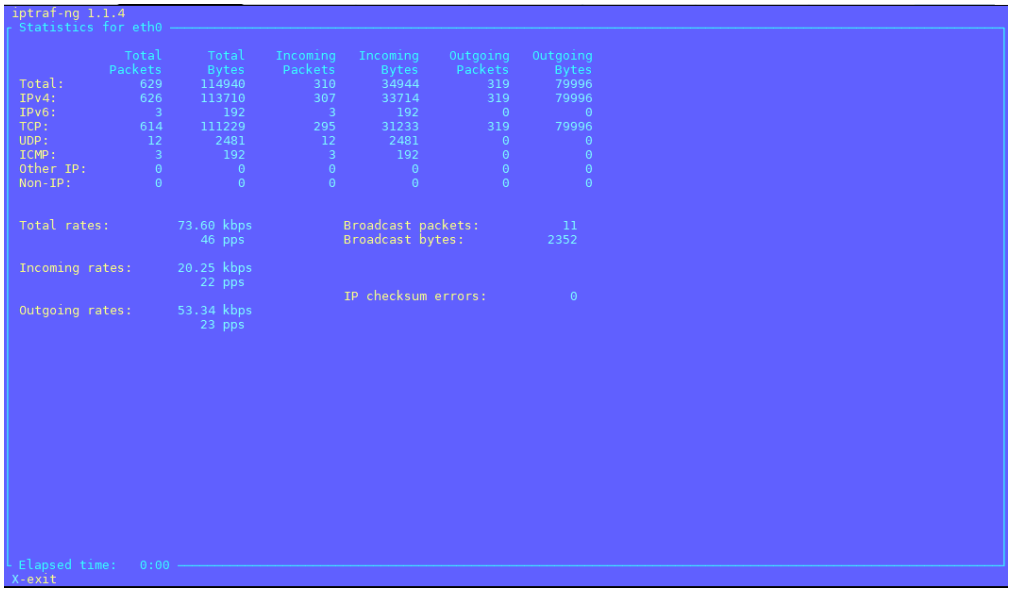

Figura 91 – Command Line Interface – iptraf – exemplo 2.

5.35 [ldapsearch]

Ferramenta para consultas em base LDAP.

Modo de uso:

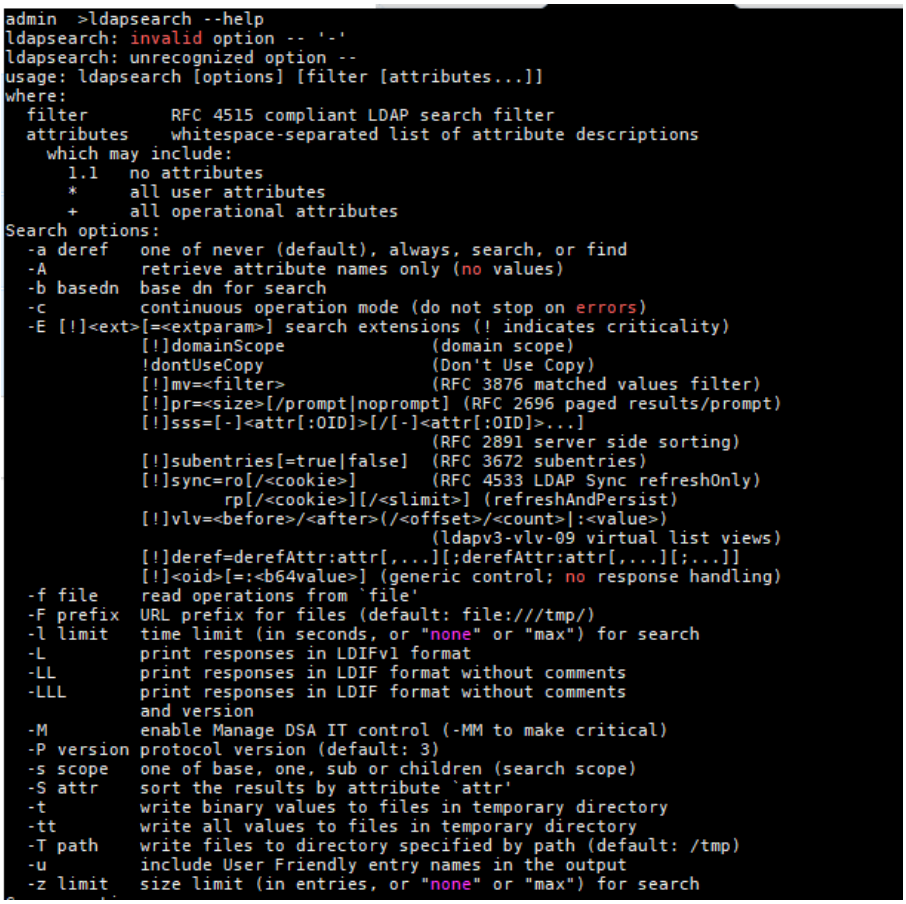

Figura 92 – Command Line Interface – ldapsearch.

Figura 93 – Command Line Interface – ldapsearch 2.

Exemplo: Listar os atributos da OU e de seus membros:

```
admin  >ldapsearch -z0 -x -b "OU=suporte,OU=BLOCKBIT,DC=labsuporte,DC=com,DC=br" -D "administrador@labsuporte.com.br" -h 172.16.102.161 -p 389 -W
Enter LDAP Password:
# extended LDIF
#
# LDAPv3
# base <OU=suporte,OU=BLOCKBIT,DC=labsuporte,DC=com,DC=br> with scope subtree
# filter: (objectclass=*)
# requesting: ALL
#

# SUPORTE, BLOCKBIT, labsuporte.com.br
dn: OU=SUPORTE,OU=BLOCKBIT,DC=labsuporte,DC=com,DC=br
objectClass: top
objectClass: organizationalUnit
ou: SUPORTE
distinguishedName: OU=SUPORTE,OU=BLOCKBIT,DC=labsuporte,DC=com,DC=br
instanceType: 4
whenCreated: 20180314161706.0Z
whenChanged: 20180314161707.0Z
uSNCreated: 2307979
uSNChanged: 2307980
name: SUPORTE
objectGUID:: EaEgpi7FMUqKQD5rSSOktg==
objectCategory: CN=Organizational-Unit,CN=Schema,CN=Configuration,DC=labsuport
 e,DC=com,DC=br
dSCorePropagationData: 20180314161707.0Z
dSCorePropagationData: 20180314161707.0Z
dSCorePropagationData: 16010101000000.0Z

# charlie, SUPORTE, BLOCKBIT, labsuporte.com.br
dn: CN=charlie,OU=SUPORTE,OU=BLOCKBIT,DC=labsuporte,DC=com,DC=br
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: user
cn: charlie
givenName: Charlie
distinguishedName: CN=charlie,OU=SUPORTE,OU=BLOCKBIT,DC=labsuporte,DC=com,DC=b
 r
instanceType: 4
whenCreated: 20171214114002.0Z
whenChanged: 20180314161856.0Z
displayName: Charlie
uSNCreated: 2265501
memberOf: CN=Marketing,OU=Usuarios,OU=Suporte,DC=labsuporte,DC=com,DC=br
uSNChanged: 2307983
wWWHomePage: www.blockbit.com
name: charlie
```

Figura 94 – Command Line Interface – ldapsearch - exemplo.

5.36 [less]

Paginação da saída de um determinado comando, com ele é possível navegar para cima ou para baixo nas informações:

Exemplo de uso:

```
admin  >ifconfig -a|less
```

Figura 95 – Command Line Interface - less.

Ao final, clique na letra [q] para sair.

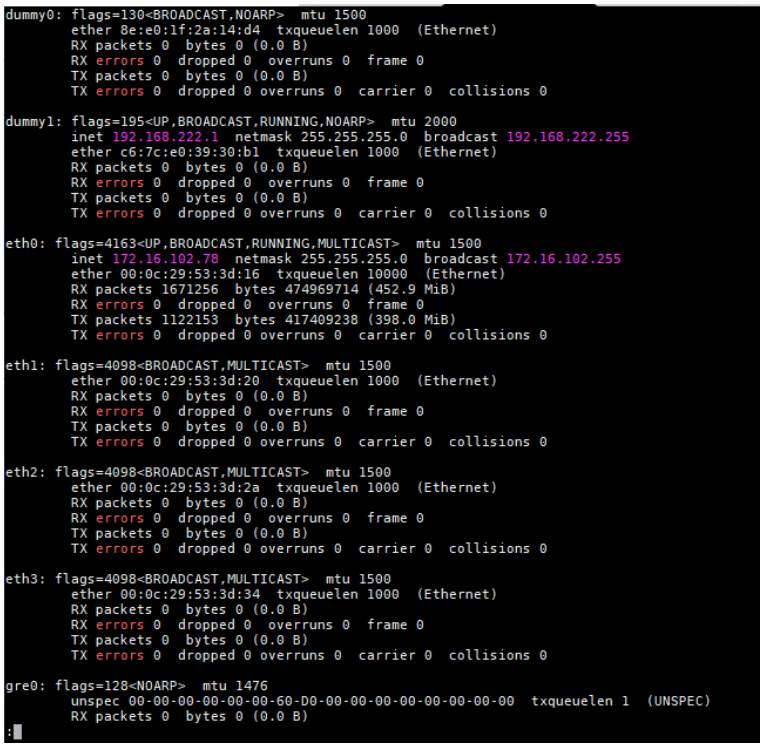

Figura 96 – Command Line Interface – less - exemplo.

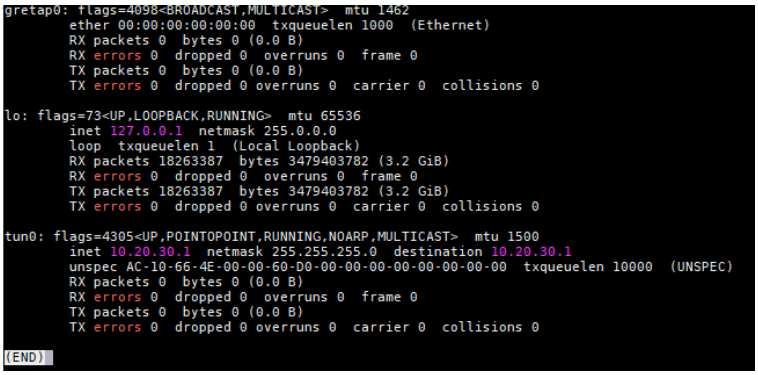

Figura 97 – Command Line Interface – less – exemplo 2.

5.37 [lscpu]

Exibe informações sobre a arquitetura da CPU.

Modo de uso:

```
blockbit >lscpu
Architecture:          x86_64
CPU op-mode(s):        32-bit, 64-bit
Byte Order:            Little Endian
CPU(s):                4
On-line CPU(s) list:   0-3
Thread(s) per core:    1
Core(s) per socket:    1
Socket(s):             4
NUMA node(s):          1
Vendor ID:             GenuineIntel
CPU family:            6
Model:                 60
Model name:            Intel(R) Xeon(R) CPU E3-1275 v3 @ 3.50GHz
Stepping:              3
CPU MHz:               3491.913
BogoMIPS:              6983.82
Hypervisor vendor:     VMware
Virtualization type:   full
L1d cache:             32K
L1i cache:             32K
L2 cache:              256K
L3 cache:              8192K
NUMA node0 CPU(s):     0-3
blockbit >
```

Figura 98 – Command Line Interface – lscpu.

5.38 [lsusb]

Exibe informações sobre as portas USB e os dispositivos conectados a eles.

Modo de uso:

```
admin  >lsusb --help
Usage: lsusb [options]...
List USB devices
  -v, --verbose
      Increase verbosity (show descriptors)
  -s [[bus]:][devnum]
      Show only devices with specified device and/or
      bus numbers (in decimal)
  -d vendor:[product]
      Show only devices with the specified vendor and
      product ID numbers (in hexadecimal)
  -D device
      Selects which device lsusb will examine
  -t, --tree
      Dump the physical USB device hierarchy as a tree
  -V, --version
      Show version of program
  -h, --help
      Show usage and help
```

Figura 99 – Command Line Interface – lsusb.

Exemplo:

```
admin  >lsusb
Bus 001 Device 002: ID 8087:07e6 Intel Corp.
Bus 001 Device 001: ID 1d6b:0002 Linux Foundation 2.0 root hub
Bus 001 Device 003: ID 058f:6387 Alcor Micro Corp. Flash Drive
```

Figura 100 – Command Line Interface – lsusb – exemplo.

5.39 [mkfs]

Cria sistema de arquivos Linux (formatar).

Modo de uso:

```
admin  >mkfs
Usage: mkfs.ext4 [-c|-l filename] [-b block-size] [-C cluster-size]
       [-i bytes-per-inode] [-I inode-size] [-J journal-options]
       [-G flex-group-size] [-N number-of-inodes]
       [-m reserved-blocks-percentage] [-o creator-os]
       [-g blocks-per-group] [-L volume-label] [-M last-mounted-directory]
       [-O feature[,...]] [-r fs-revision] [-E extended-option[,...]]
       [-t fs-type] [-T usage-type ] [-U UUID] [-jnqvDFKSV] device [blocks-count]
```

Figura 101 – Command Line Interface – mkfs.

Exemplo: Formatar o dispositivo USB para utilização em armazenamento:

```
admin  >mkfs -t ext4 /dev/sdb1
mke2fs 1.42.9 (28-Dec-2013)
Filesystem label=
OS type: Linux
Block size=4096 (log=2)
Fragment size=4096 (log=2)
Stride=0 blocks, Stripe width=0 blocks
477664 inodes, 1907968 blocks
95398 blocks (5.00%) reserved for the super user
First data block=0
Maximum filesystem blocks=1954545664
59 block groups
32768 blocks per group, 32768 fragments per group
8096 inodes per group
Superblock backups stored on blocks:
        32768, 98304, 163840, 229376, 294912, 819200, 884736, 1605632

Allocating group tables: done
Writing inode tables: done
Creating journal (32768 blocks): done
Writing superblocks and filesystem accounting information: done
```

Figura 102 – Command Line Interface – mkfs - exemplo.

5.40 [more]

Semelhante ao comando **less,** porém não sendo possível subir ou descer as informações de saída no comando executado. Ao terminar o resultado do comando, automaticamente é finaliza sua execução.

Modo de uso:

```
admin  >ifconfig -a|more
```

Figura 103 – Command Line Interface – more.

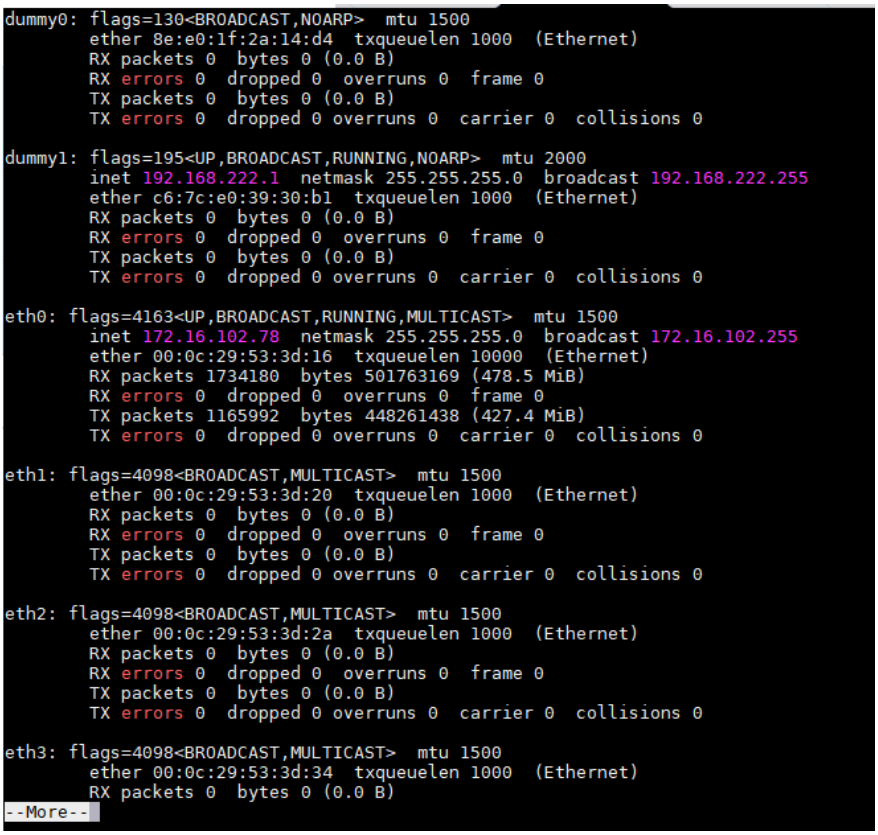

Figura 104 – Command Line Interface – more - exemplo.

5.41 [mtr]

Ferramenta de diagnóstico que combina testes de ping e traceroute para identificar perdas de pacotes e latência alta.

Modo de uso:

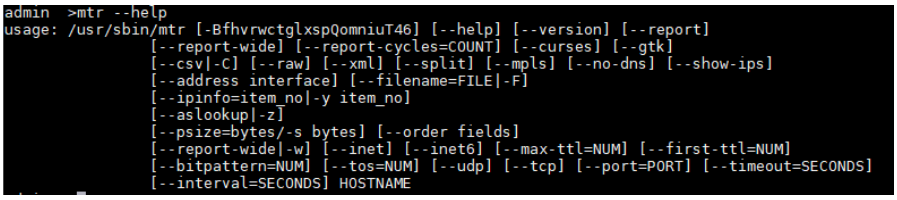

Figura 105 – Command Line Interface – mtr.

Exemplo:

Figura 106 – Command Line Interface – mtr uol.com.br.

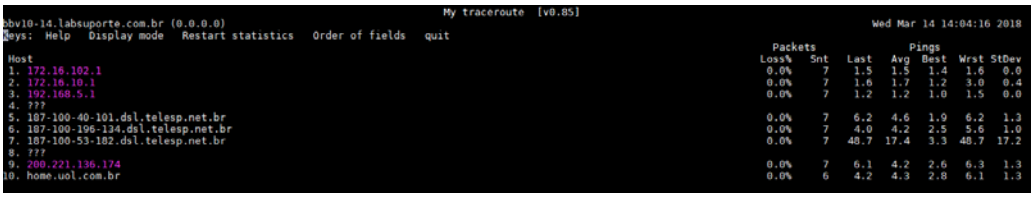

Figura 107 – Command Line Interface – mtr exemplo.

5.42 [netads]

Exibe e gerencia informações do servidor LDAP.

Modo de uso:

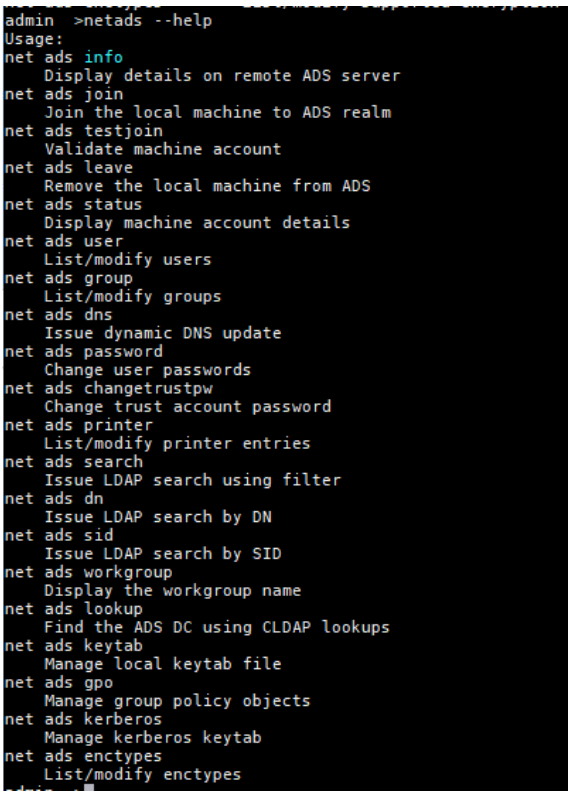

Figura 108 – Command Line Interface – netads.

Exemplo: Exibir informações do servidor LDAP:

```
admin  >netads info
LDAP server: 172.16.102.161
LDAP server name: WIN-KUJ3AT9LI1Q.labsuporte.com.br
Realm: LABSUPORTE.COM.BR
Bind Path: dc=LABSUPORTE,dc=COM,dc=BR
LDAP port: 389
Server time: Wed, 14 Mar 2018 14:12:13 BRT
KDC server: 172.16.102.161
Server time offset: 35
```

Figura 109 – Command Line Interface – netads - exemplo.

5.43 [netstat]

Exibe as portas TCP e UDP (IPv4 e IPv6) que estão em escuta (listen) no servidor.

Modo de uso:

```
admin  >netstat
```

Figura 110 – Command Line Interface – netstat.

Exemplo:

```
admin  >netstat
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 0.0.0.0:9803            0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:80              0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:5432            0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:443             0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:1344            0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:98              0.0.0.0:*               LISTEN
tcp6       0      0 :::9815                 :::*                    LISTEN
tcp6       0      0 :::5432                 :::*                    LISTEN
tcp6       0      0 :::126                  :::*                    LISTEN
tcp6       0      0 :::127                  :::*                    LISTEN
tcp6       0      0 :::128                  :::*                    LISTEN
udp        0      0 0.0.0.0:49118           0.0.0.0:*
udp        0      0 0.0.0.0:67              0.0.0.0:*
udp        0      0 0.0.0.0:68              0.0.0.0:*
udp        0      0 0.0.0.0:123             0.0.0.0:*
udp        0      0 0.0.0.0:161             0.0.0.0:*
udp        0      0 0.0.0.0:4500            0.0.0.0:*
udp        0      0 0.0.0.0:500             0.0.0.0:*
udp        0      0 0.0.0.0:23375           0.0.0.0:*
udp        0      0 0.0.0.0:5353            0.0.0.0:*
udp        0      0 0.0.0.0:46602           0.0.0.0:*
udp        0      0 0.0.0.0:34387           0.0.0.0:*
udp        0      0 0.0.0.0:59050           0.0.0.0:*
udp6       0      0 :::123                  :::*
udp6       0      0 :::4500                 :::*
udp6       0      0 :::500                  :::*
udp6       0      0 :::33636                :::*
udp6       0      0 :::43923                :::*
udp6       0      0 :::35941                :::*
udp6       0      0 :::46196                :::*
```

Figura 111 – Command Line Interface – netstat - exemplo.

5.44 [nslookup]

Envia pesquisas DNS para um servidor DNS remoto.

Modo de uso:

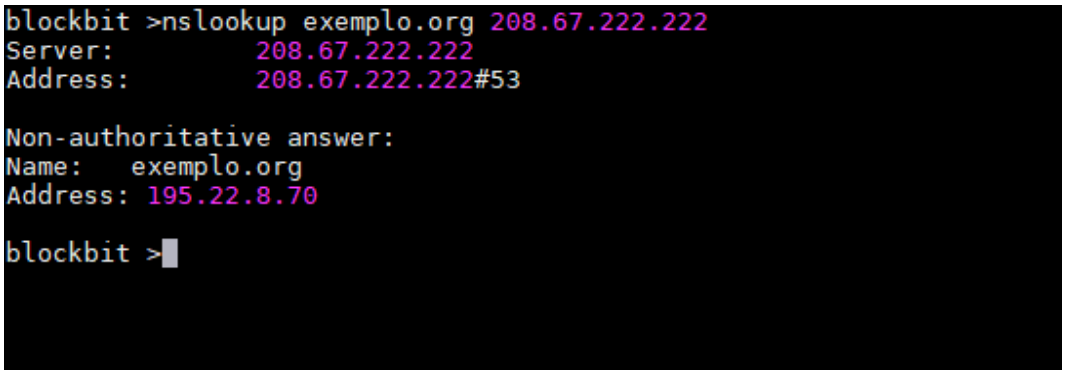

Figura 113 – Command Line Interface – nslookup.

5.45 [ntpdate]

Ajusta a data e hora local do seu dispositivo consultando servidores NTP (Network Time Protocol) disponíveis na rede.

Modo de uso:

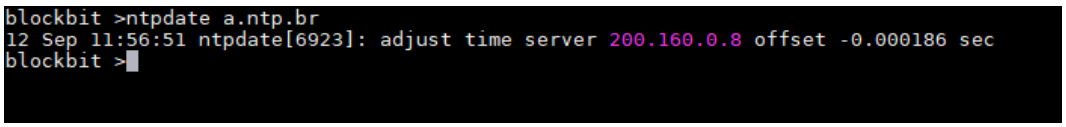

Figura 114 – Command Line Interface – ntpdate.

5.46 [ping]

Testa a conectividade entre dispositivos na rede. Utiliza o datagrama do protocolo ICMP.

Modo de uso:

```
blockbit >ping 172.16.102.1
PING 172.16.102.1 (172.16.102.1) 56(84) bytes of data.
64 bytes from 172.16.102.1: icmp_seq=1 ttl=64 time=1.60 ms
64 bytes from 172.16.102.1: icmp_seq=2 ttl=64 time=1.47 ms
64 bytes from 172.16.102.1: icmp_seq=3 ttl=64 time=1.70 ms
64 bytes from 172.16.102.1: icmp_seq=4 ttl=64 time=1.69 ms
64 bytes from 172.16.102.1: icmp_seq=5 ttl=64 time=1.79 ms

--- 172.16.102.1 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4006ms
rtt min/avg/max/mdev = 1.475/1.656/1.795/0.114 ms
blockbit >
```

Figura 115 – Command Line Interface – ping.

5.47 [passwd]

Altera a senha do usuário “admin” padrão do console.

Modo de uso:

```
admin >passwd
Mudando senha para o usuário admin.
Mudando senha para admin.
Senha UNIX (atual):
Nova senha:
Redigite a nova senha:
passwd: todos os tokens de autenticações foram atualizados com sucesso.
admin >
```

Figura 116 – Command Line Interface – passwd.

5.48 [reset]

Reinicializa as variáveis da sessão corrente no terminal.

Modo de uso:

```
admin  >reset --help
reset: invalid option -- '-'
Usage: tset [options] [terminal]

Options:
  -c          set control characters
  -e ch       erase character
  -I          no initialization strings
  -i ch       interrupt character
  -k ch       kill character
  -m mapping  map identifier to type
  -Q          do not output control key settings
  -r          display term on stderr
  -s          output TERM set command
  -V          print curses-version
  -w          set window-size
```

Figura 117 – Command Line Interface – reset.

5.49 [reboot]

Reinicializa o sistema.

Modo de uso:

```
blockbit >reboot
PolicyKit daemon disconnected from the bus.
We are no longer a registered authentication agent.
Connection to 172.16.102.137 closed by remote host.
Connection to 172.16.102.137 closed.

[2017-09-12 12:08.23]  ~
[maderno.SPLT7BMM2K2] ➤
```

Figura 118 – Command Line Interface – reboot.

5.50 [reset-admin-blocks]

Libera sessões bloqueadas do usuário *"admin"* da interface WEB.

Modo de uso:

```
Modo de uso [Saída padrão do comando]
admin >reset-admin-blocks
blocked sessions removed
admin >
```

Figura 119 – Command Line Interface – reset-admin-blocks – Exemplo.

5.51 [reset-admin-password]

Altera a senha do usuário *"admin"* da Interface WEB.

Modo de uso:

```
admin  >reset-admin-password
Type admin password:
Re-type admin password:
```

Figura 112 – Command Line Interface – reset-admin-password.

5.52 [reset-admin-sessions]

Libera todas as sessões da interface WEB.

Modo de uso:

```
admin  >reset-admin-sessions
admin sessions removed
admin  >
```

Figura 113 – Command Line Interface – reset-admin-sessions.

5.53 [reset-logs]

Remove os logs, sejam globais ou de serviços específicos.

Modo de uso:

```
admin  >reset-logs
usage: reset-stats <module>
modules: [all, web, atp, ips, firewall, antimalware]
```

Figura 114 – Command Line Interface – reset-logs.

Exemplo: Remover todos os logs de firewall e Web:

```
admin  >reset-logs firewall
Do you really want remove (Y/N)? Y
removed firewall log
admin  >reset-logs web
Do you really want remove (Y/N)? Y
removed web log
```

Figura 115 – Command Line Interface – reset-logs - exemplo.

5.54 [reset-stats]

Remove as sumarizações, sejam globais ou de serviços específicos.

Modo de uso:

```
admin  >reset-stats
usage: reset-stats <module>
modules: [all, web, network, atp, ips, firewall, antimalware]
admin  >
```

Figura 116 – Command Line Interface – reset-stats.

Exemplo: Remover todas as sumarizações (estatísticas):

```
admin  >reset-stats all
Do you really want remove (Y/N)? Y
removed web stats
removed network stats
removed atp stats
removed ips stats
removed firewall stats
removed antimalware stats
```

Figura 117 – Command Line Interface – reset-stats - exemplo.

5.55 [rewizard]

Apaga todas as configurações contidas no banco de dados, voltando assim o banco de dados ao padrão de fábrica.

Modo de uso:

```
admin  >rewizard
Do you want to reset this device (y/n)?y
admin  >
```

Figura 118 – Command Line Interface – rewizard.

Esta ação não poderá ser desfeita!

5.56 [route]

Exibe e manipula a tabela de roteamento de endereços IP.

Modo de uso:

```
blockbit >route -h
Usage: route [-nNvee] [-FC] [<AF>]          List kernel routing tables
       route [-v] [-FC] {add|del|flush} ...  Modify routing table for AF.

       route {-h|--help} [<AF>]              Detailed usage syntax for specified AF.
       route {-V|--version}                  Display version/author and exit.

        -v, --verbose            be verbose
        -n, --numeric            don't resolve names
        -e, --extend             display other/more information
        -F, --fib                display Forwarding Information Base (default)
        -C, --cache              display routing cache instead of FIB

  <AF>=Use -4, -6, '-A <af>' or '--<af>'; default: inet
  List of possible address families (which support routing):
    inet (DARPA Internet) inet6 (IPv6) ax25 (AMPR AX.25)
    netrom (AMPR NET/ROM) ipx (Novell IPX) ddp (Appletalk DDP)
    x25 (CCITT X.25)
blockbit >
```

Figura 119 – Command Line Interface – route.

Rotas estáticas adicionadas pela console CLI (linha de comando) não são salvas ou carregadas após o boot.

Exemplo 1:

```
blockbit >route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         172.16.102.1    0.0.0.0         UG    100    0        0 eth0
172.16.102.0    0.0.0.0         255.255.255.0   U     100    0        0 eth0
blockbit >
```

Figura 120 – Command Line Interface – route – Exemplo 1.

Exemplo 2: Configurando um roteamento estático para uma rede estendida:

```
blockbit >route add -net 192.168.254.0/24 gw 172.16.102.1 dev eth0
blockbit >route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         172.16.102.1    0.0.0.0         UG    100    0        0 eth0
172.16.102.0    0.0.0.0         255.255.255.0   U     100    0        0 eth0
192.168.254.0   172.16.102.1    255.255.255.0   UG    0      0        0 eth0
blockbit >
```

Figura 121 – Command Line Interface – route – Exemplo 2.

5.57 [sar]

Exibe a utilização dos recursos como memória, processamento e disco em tempo real ou do dia corrente (média gerada a cada 10 minutos).

Modo de uso:

```
admin  >sar --help
Usage: sar [ options ] [ <interval> [ <count> ] ]
Options are:
[ -A ] [ -B ] [ -b ] [ -C ] [ -d ] [ -H ] [ -h ] [ -p ] [ -q ] [ -R ]
[ -r ] [ -S ] [ -t ] [ -u [ ALL ] ] [ -V ] [ -v ] [ -W ] [ -w ] [ -y ]
[ -I { <int> [,...] | SUM | ALL | XALL } ] [ -P { <cpu> [,...] | ALL } ]
[ -m { <keyword> [,...] | ALL } ] [ -n { <keyword> [,...] | ALL } ]
[ -j { ID | LABEL | PATH | UUID | ... } ]
[ -f [ <filename> ] | -o [ <filename> ] | -[0-9]+ ]
[ -i <interval> ] [ -s [ <hh:mm:ss> ] ] [ -e [ <hh:mm:ss> ] ]
```

Figura 122 – Command Line Interface – sar.

Exemplo: Exibe o consumo de memória em tempo real (a cada segundo por 60 segundos):

```
admin  >sar -r 1 60
Linux 3.10.0-514.26.2.el7.x86_64 (bb5sp.labsuporte.com.br)      03/14/18        _x86_64_        (2 CPU)

15:44:45    kbmemfree kbmemused  %memused kbbuffers  kbcached  kbcommit   %commit  kbactive   kbinact   kbdirty
15:44:46      1189704   2747224     69.78    223640   1671080   1777908     31.26   1338448   1072436        72
15:44:47      1191832   2745096     69.73    223648   1671072   1771120     31.14   1336600   1072428        76
15:44:48      1191832   2745096     69.73    223648   1671112   1771120     31.14   1336608   1072460       108
15:44:49      1189800   2747128     69.78    223648   1671112   1780476     31.30   1338708   1072460       108
15:44:50      1191708   2745220     69.73    223648   1671080   1771120     31.14   1336604   1072432       108
15:44:51      1189776   2747152     69.78    223648   1671080   1780852     31.31   1338828   1072432       108
15:44:52      1191312   2745616     69.74    223648   1671112   1771120     31.14   1336612   1072456       108
15:44:53      1191312   2745616     69.74    223648   1671080   1771120     31.14   1336608   1072428       108
15:44:54      1189692   2747236     69.78    223648   1671084   1780476     31.30   1338812   1072428       112
15:44:55      1191312   2745616     69.74    223648   1671084   1771120     31.14   1336612   1072428       112
15:44:56      1191336   2745592     69.74    223648   1671084   1771120     31.14   1336612   1072428       112
15:44:57      1191156   2745772     69.74    223648   1671084   1771120     31.14   1336612   1072428       116
15:44:58      1191212   2745716     69.74    223648   1671084   1771120     31.14   1336612   1072428       116
15:44:59      1191212   2745716     69.74    223648   1671084   1771120     31.14   1336612   1072428       116
15:45:00      1191212   2745716     69.74    223648   1671084   1771120     31.14   1336612   1072428       116
15:45:01      1191212   2745716     69.74    223648   1671084   1771120     31.14   1336612   1072428        88
15:45:02      1182768   2754160     69.96    223648   1671232   1797708     31.61   1343128   1072424       124
15:45:03      1149040   2787888     70.81    223648   1671316   1827188     32.12   1375828   1072480       152
15:45:04      1113380   2823548     71.72    223648   1671468   1878276     33.02   1410576   1072600       300
15:45:05      1170824   2766104     70.26    223648   1671156   1794884     31.56   1356240   1072420       176
15:45:06      1191356   2745572     69.74    223648   1671156   1771148     31.14   1336976   1072368       256
15:45:07      1191452   2745476     69.74    223648   1671092   1771120     31.14   1336696   1072352       248
15:45:08      1191476   2745452     69.74    223648   1671092   1771120     31.14   1336696   1072352       248
15:45:09      1191476   2745452     69.74    223648   1671092   1771120     31.14   1336696   1072352       248
15:45:10      1191476   2745452     69.74    223648   1671092   1771120     31.14   1336696   1072352       248
15:45:11      1191352   2745576     69.74    223648   1671096   1771120     31.14   1336700   1072352       252
15:45:12      1191228   2745700     69.74    223648   1671096   1771120     31.14   1336700   1072352       252
15:45:13      1191328   2745600     69.74    223648   1671096   1771120     31.14   1336704   1072352       252
15:45:14      1191328   2745600     69.74    223648   1671096   1771120     31.14   1336684   1072352       256
15:45:15      1191352   2745576     69.74    223648   1671096   1771120     31.14   1336684   1072352       256
15:45:16      1191080   2745848     69.75    223648   1671128   1771120     31.14   1336688   1072380       108
15:45:17      1191228   2745700     69.74    223648   1671096   1771120     31.14   1336708   1072348       120
15:45:18      1191172   2745756     69.74    223648   1671096   1771120     31.14   1336708   1072348       120
15:45:19      1191172   2745756     69.74    223648   1671096   1771120     31.14   1336708   1072348       120
15:45:20      1191228   2745700     69.74    223648   1671096   1771120     31.14   1336708   1072348       120
15:45:21      1191304   2745624     69.74    223648   1671096   1771120     31.14   1336708   1072348       120
15:45:22      1191352   2745576     69.74    223648   1671096   1771120     31.14   1336708   1072348        88
15:45:23      1191352   2745576     69.74    223648   1671096   1771120     31.14   1336708   1072348        88
15:45:24      1191228   2745700     69.74    223648   1671096   1771120     31.14   1336708   1072348        88

15:45:24    kbmemfree kbmemused  %memused kbbuffers  kbcached  kbcommit   %commit  kbactive   kbinact   kbdirty
15:45:25      1191724   2745204     69.73    223648   1671096   1771120     31.14   1336708   1072348        88
15:45:26      1191848   2745080     69.73    223648   1671100   1771120     31.14   1336712   1072348        92
15:45:27      1191576   2745352     69.73    223648   1671100   1771120     31.14   1336720   1072340        92
```

Figura 123 – Command Line Interface – sar - exemplo.

5.58 [service-disable]

Desabilita um determinado serviço para não ser carregado automaticamente ao reiniciar o servidor.

Modo de uso:

```
admin  >service-disable
usage: service-disable <service-name>
admin  >
```

Figura 124 – Command Line Interface – service-disable.

Service names:

```
antimalware
atp
auth-ldap
auth-radius
auth-server
auth-windows
dhcp-relay
dhcp-server
dns
firewall
gsm-deployer
gsm-logger
ips
proxy-email
proxy-ftp
proxy-http
router-bgp
router-nat64
router-ospf
router-pim
router-rip
snmp
system-admin
system-db
system-ha
system-storage
system-syslog
system-terminal
vpn-ipsec
vpn-ssl
```

Figura 125 – Command Line Interface – service-disable - service-names.

5.59 [service-enable]

Habilita um determinado serviço para ser carregado automaticamente ao reiniciar o servidor.

Modo de uso:

```
admin  >service-enable
usage: service-enable <service-name>
admin  >
```

Figura 126 – Command Line Interface – service-enable.

Service names:

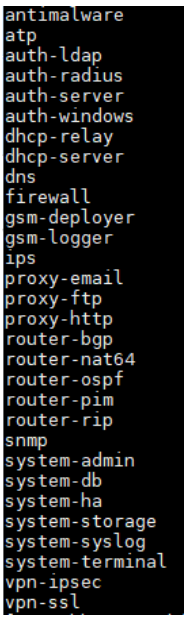

Figura 127 – Command Line Interface – service-enable - service-names.

5.60 [service-start]

Inicializa um determinado serviço.

Modo de uso:

Figura 128 – Command Line Interface – service-start.

Service names:

Figura 129 – Command Line Interface – service-start - service-names.

5.61 [service-status]

Exibe o status de todos os serviços monitorados.

Modo de uso:

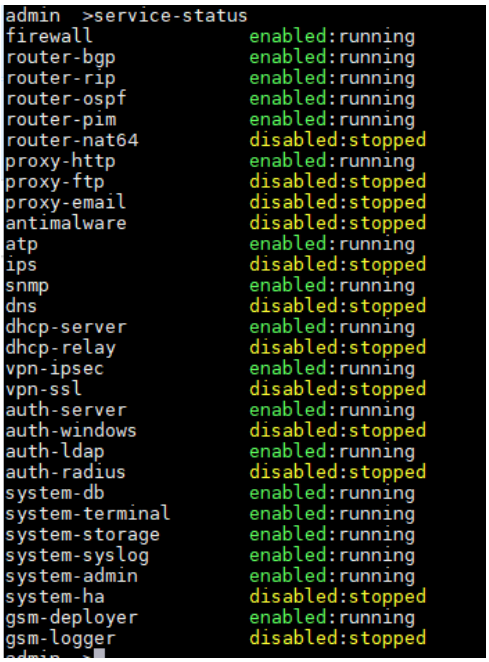

Figura 130 – Command Line Interface – service-status.

5.62 [service-stop]

Parar um determinado serviço.

Modo de uso:

```
admin  >service-stop
usage: service-stop <service-name>
admin  >
```

Figura 131 – Command Line Interface – service-stop.

Service names:

```
antimalware
atp
auth-ldap
auth-radius
auth-server
auth-windows
dhcp-relay
dhcp-server
dns
firewall
gsm-deployer
gsm-logger
ips
proxy-email
proxy-ftp
proxy-http
router-bgp
router-nat64
router-ospf
router-pim
router-rip
snmp
system-admin
system-db
system-ha
system-storage
system-syslog
system-terminal
vpn-ipsec
vpn-ssl
```

Figura 132 – Command Line Interface – service-stop - service-names.

5.63 [set-irqbalance-dynamic]

Habilita o IRQ Balance Dinâmico.

Modo de uso:

```
admin  >set-irqbalance-dynamic
Irqbalance dynamic active
admin  >
```

Figura 133 – Command Line Interface – set-irqbalance-dynamic.

5.64 [set-irqbalance-static]

Habilita o IRQ Balance Estático.

Modo de uso:

```
admin  >set-irqbalance-static
Irqbalance static active
admin  >
```

Figura 134 – Command Line Interface – set-irqbalance-static.

5.65 [show-sessions]

Exibe as sessões de autenticação.

Modo de uso:

```
admin  >show-sessions
c74df4dbbd29994fa68c9124d4433925|1521059793|1521059793|rodrigo@blockbit.com|172.16.13.82|172.16.13.82|-|BLOCKBIT Portal/1.0#Mozilla/5.0 (Windows NT 10.0; Win64; x64;
 rv:58.0) Gecko/20100101 Firefox/58.0|0|30
```

Figura 135 – Command Line Interface – show-sessions.

5.66 [show-uuid]

Exibe o número do device (UUID), ou seja o Identificador Universal Único do appliance.

Modo de uso:

```
BlockBit Network Appliance UUID
59B41AC0-0821-11E7-AE03-47560F1768CB
admin  >
```

Figura 136 – Command Line Interface – show-uuid.

A licença do servidor é vinculada a esse ID.

5.67 [show-vpn-conn]

Exibe os túneis VPN IPSEC no ar (site-to-site e acesso remoto), criptografia utilizada, tempo da conexão, rede de origem e destino e pacotes trafegados.

Modo de uso:

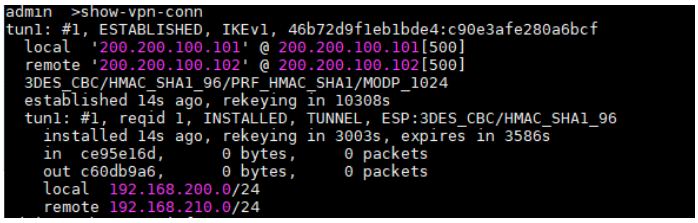

Figura 137 – Command Line Interface – show-vpn-conn.

5.68 [show-vpn-info]

Exibe os túneis VPN IPSEC no ar (site-to-site e acesso remoto), criptografia utilizada, tempo da conexão, rede de origem e destino e pacotes trafegados. Além disso, exibe também quanto tempo o serviço está no ar, quantidade de workers e o(s) IP(s) que o serviço está em escuta (listen).

Modo de uso:

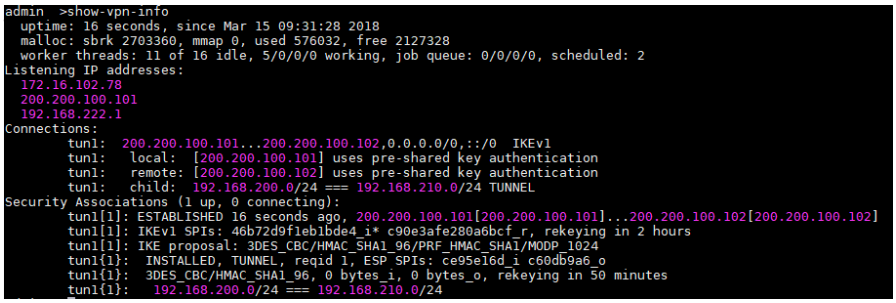

Figura 138 – Command Line Interface – show-vpn-info.

5.69 [shutdown]

Desliga o sistema.

Modo de uso:

```
admin  >shutdown
Connection to 172.16.13.214 closed by remote host.
Connection to 172.16.13.214 closed.
```

Figura 139 – Command Line Interface – shutdown.

5.70 [speedtest]

Teste de velocidade do link para download e upload.

Modo de uso:

```
admin  >speedtest -h
usage: speedtest [-h] [--bytes] [--share] [--simple] [--list] [--server SERVER] [--mini MINI] [--source SOURCE] [--version]

Command line interface for testing internet bandwidth using speedtest.net. ------------------------------------------------------------------------
https://github.com/sivel/speedtest-cli

optional arguments:
  -h, --help       show this help message and exit
  --bytes          Display values in bytes instead of bits. Does not affect the image generated by --share
  --share          Generate and provide a URL to the speedtest.net share results image
  --simple         Suppress verbose output, only show basic information
  --list           Display a list of speedtest.net servers sorted by distance
  --server SERVER  Specify a server ID to test against
  --mini MINI      URL of the Speedtest Mini server
  --source SOURCE  Source IP address to bind to
  --version        Show the version number and exit
```

Figura 140 – Command Line Interface – speedtest.

Exemplo:

```
admin  >speedtest
Retrieving speedtest.net configuration...
Retrieving speedtest.net server list...
Testing from Vivo (191.13.128.45)...
Selecting best server based on latency...
Hosted by CenturyLink (Sao Paulo) [14.70 km]: 69.484 ms
Testing download speed.....................................
Download: 59.95 Mbits/s
Testing upload speed.......................................................
Upload: 49.07 Mbits/s
```

Figura 141 – Command Line Interface – speedtest - exemplo.

5.71 [system-status]

Teste de velocidade do link para download e upload.

Modo de uso:

```
admin  >speedtest -h
usage: speedtest [-h] [--bytes] [--share] [--simple] [--list] [--server SERVER] [--mini MINI] [--source SOURCE] [--version]

Command line interface for testing internet bandwidth using speedtest.net. ------------------------------------------------------------------------
https://github.com/sivel/speedtest-cli

optional arguments:
  -h, --help       show this help message and exit
  --bytes          Display values in bytes instead of bits. Does not affect the image generated by --share
  --share          Generate and provide a URL to the speedtest.net share results image
  --simple         Suppress verbose output, only show basic information
  --list           Display a list of speedtest.net servers sorted by distance
  --server SERVER  Specify a server ID to test against
  --mini MINI      URL of the Speedtest Mini server
  --source SOURCE  Source IP address to bind to
  --version        Show the version number and exit
```

Figura 142 – Command Line Interface – speedtest.

Exemplo:

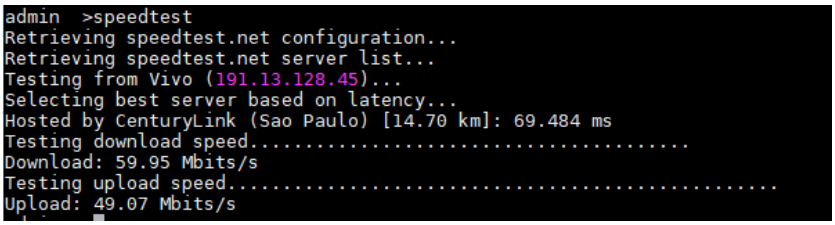

Figura 143 – Command Line Interface – speedtest - exemplo.

5.72 [sync-users]

Executa o sincronismo de usuários.

Modo de uso:

Figura 144 – Command Line Interface – sync-users.

5.73 [sysctl]

Modifica parâmetros do kernel em tempo de execução.

Modo de uso:

```
admin  >sysctl

Usage:
 sysctl [options] [variable[=value] ...]

Options:
  -a, --all            display all variables
  -A                   alias of -a
  -X                   alias of -a
      --deprecated     include deprecated parameters to listing
  -b, --binary         print value without new line
  -e, --ignore         ignore unknown variables errors
  -N, --names          print variable names without values
  -n, --values         print only values of a variables
  -p, --load[=<file>]  read values from file
  -f                   alias of -p
      --system         read values from all system directories
  -r, --pattern <expression>
                       select setting that match expression
  -q, --quiet          do not echo variable set
  -w, --write          enable writing a value to variable
  -o                   does nothing
  -x                   does nothing
  -d                   alias of -h

 -h, --help     display this help and exit
 -V, --version  output version information and exit

For more details see sysctl(8).
```

Figura 145 – Command Line Interface – sysctl.

Parâmetros alterados por esse comando não são mantidos após reiniciar o servidor.

5.74 [tcpdump]

Monitora, captura e analisa pacotes transmitidos pela rede. Assim, permite ao administrador analisar o comportamento da rede, auxiliando na identificação de problemas, estações infectadas, tráfego malicioso, gargalos etc.

Modo de uso:

```
blockbit >tcpdump -h
tcpdump version 4.5.1
libpcap version 1.5.3
Usage: tcpdump [-aAbdDefhHIJKlLnNOpqRStuUvxX] [ -B size ] [ -c count ]
                [ -C file_size ] [ -E algo:secret ] [ -F file ] [ -G seconds ]
                [ -i interface ] [ -j tstamptype ] [ -M secret ]
                [ -P in|out|inout ]
                [ -r file ] [ -s snaplen ] [ -T type ] [ -V file ] [ -w file ]
                [ -W filecount ] [ -y datalinktype ] [ -z command ]
                [ -Z user ] [ expression ]

blockbit >
```

Figura 152 – Command Line Interface – tcpdump.

Exemplo: Monitorando todo o tráfego da interface da rede local – interface Eth0:

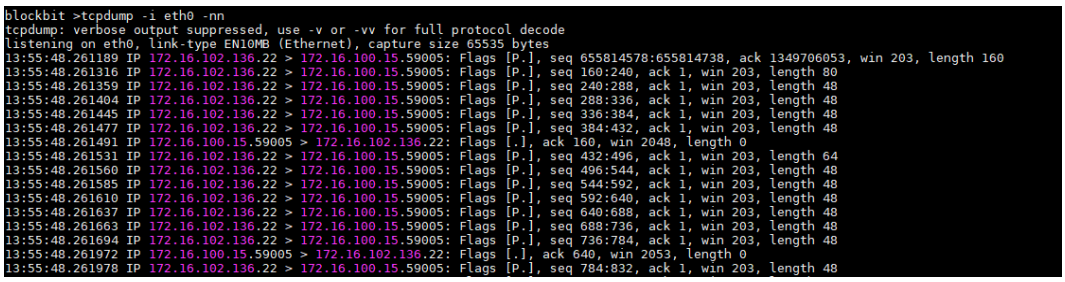

Figura 153 – Command Line Interface – tcpdump – Exemplo.

5.75 [tcptop]

Extrai e exibe informações de tráfego das interfaces de rede, tais como: total de pacotes capturados, total de pacotes recebidos, total de pacotes bloqueados pelo kernel e total de pacotes trafegados pelo TOP 10 endereços IP.

Modo de uso:

Figura 154 – Command Line Interface – tcptop.

Exemplo: Exibir informações de tráfego top 10 da interface eth0:

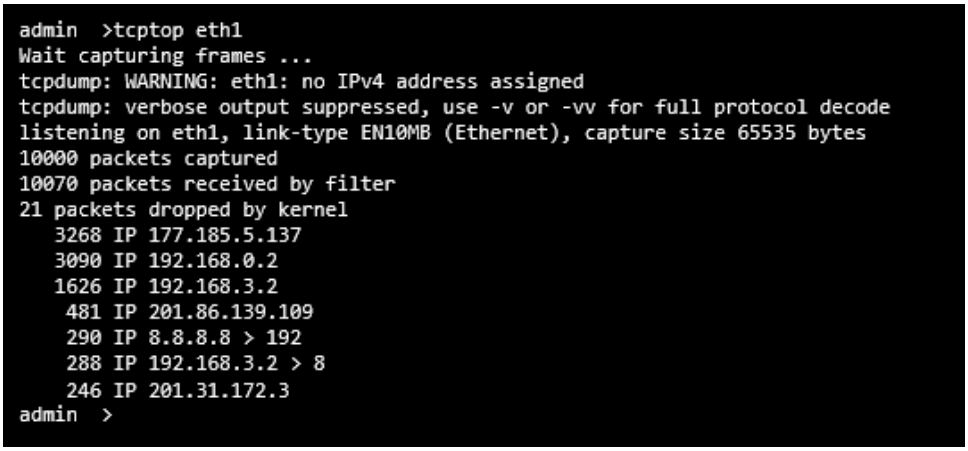

Figura 155 – Command Line Interface – tcptop – Exemplo.

5.76 [telnet]

Utilizado para: acesso remoto e testes de simulação de um terminal; resposta de conexão de um serviço; e envio de uma mensagem de e-mail.

Modo de uso:

```
blockbit >telnet -h
telnet: invalid option -- 'h'
Usage: telnet [-8] [-E] [-L] [-S tos] [-a] [-c] [-d] [-e char] [-l user]
        [-n tracefile] [-b hostalias ] [-r]
 [host-name [port]]
blockbit >
```

Figura 156 – Command Line Interface – telnet.

Exemplo 1:

```
blockbit >telnet
telnet> ?
Commands may be abbreviated.  Commands are:

close           close current connection
logout          forcibly logout remote user and close the connection
display         display operating parameters
mode            try to enter line or character mode ('mode ?' for more)
open            connect to a site
quit            exit telnet
send            transmit special characters ('send ?' for more)
set             set operating parameters ('set ?' for more)
unset           unset operating parameters ('unset ?' for more)
status          print status information
toggle          toggle operating parameters ('toggle ?' for more)
slc             change state of special charaters ('slc ?' for more)
z               suspend telnet
!               invoke a subshell
environ         change environment variables ('environ ?' for more)
?               print help information
telnet>
```

Figura 157 – Command Line Interface – telnet – Exemplo 1.

Exemplo 2: Testes de conexão com um serviço remoto (terminal Service) em uma porta específica:

```
blockbit >telnet 172.16.13.245 3389
Trying 172.16.13.245...
Connected to 172.16.13.245.
Escape character is '^]'.
^]

telnet>
```

Figura 158 – Command Line Interface – telnet – Exemplo 2.

5.77 [tracepath]

Traça um caminho para um endereço de rede designado, informando sobre o “tempo de vida” ou lag TTL e a unidade de transmissão máxima (MTU) ao longo do caminho.

Modo de uso:

```
blockbit >tracepath -h
Usage: tracepath [-n] [-b] [-l <len>] [-p port] <destination>
blockbit >tracepath -p 3389 172.16.13.245
 1?: [LOCALHOST]                                         pmtu 1500
 1:  gateway                                               1.684ms
 1:  gateway                                               3.150ms
 2:  no reply
 3:  no reply
 4:  no reply
 5:  no reply
 6:  no reply
 7:  no reply
 8:  no reply
 9:  no reply
10:  no reply
11:  no reply
12:  no reply
13:  no reply
14:  no reply
15:  no reply
16:  no reply
17:  no reply
18:  no reply
19:  no reply
20:  no reply
21:  no reply
22:  no reply
23:  no reply
24:  no reply
25:  no reply
26:  no reply
27:  no reply
28:  no reply
29:  no reply
30:  no reply
31:  no reply
     Too many hops: pmtu 1500
     Resume: pmtu 1500
blockbit >
```

Figura 159 – Command Line Interface – tracepath.

5.78 [traceroute]

Traça um caminho para um endereço de rede designado. O comando “traceroute” suporta alguns parâmetros avançados, o que o diferencia do “tracepath”, incluindo a seleção dos protocolos: TCP, UDP ou ICMP.

Modo de uso:

```
admin  >traceroute --help
Usage:
  traceroute [ -46dFITnreAUDV ] [ -f first_ttl ] [ -g gate,... ] [ -i device ] [ -m
max_ttl ] [ -N squeries ] [ -p port ] [ -t tos ] [ -l flow_label ] [ -w waittime ] [
-q nqueries ] [ -s src_addr ] [ -z sendwait ] [ --fwmark=num ] host [ packetlen ]


Options:
  -4                          Use IPv4
  -6                          Use IPv6
  -d  --debug                 Enable socket level debugging
  -F  --dont-fragment         Do not fragment packets
  -f first_ttl  --first=first_ttl
                             Start from the first_ttl hop (instead from 1)
  -g gate,...  --gateway=gate,...
                             Route packets through the specified gateway
                             (maximum 8 for IPv4 and 127 for IPv6)
  -I  --icmp                 Use ICMP ECHO for tracerouting
  -T  --tcp                  Use TCP SYN for tracerouting (default port is 80)
  -i device  --interface=device
                             Specify a network interface to operate with
  -m max_ttl  --max-hops=max_ttl
                             Set the max number of hops (max TTL to be
                             reached). Default is 30
  -N squeries  --sim-queries=squeries
                             Set the number of probes to be tried
                             simultaneously (default is 16)
  -n                         Do not resolve IP addresses to their domain names
  -p port  --port=port
                          Set the destination port to use. It is either
                             initial udp port value for "default" method
                             (incremented by each probe, default is
                             33434), or initial seq for "icmp" incremented
                             as well, default from 1), or some constant
                            destination port for other methods (with default of 80
for "tcp", 53 for "udp", etc.)
```

Figura 160 – Command Line Interface – traceroute_1.

Figura 161 – Command Line Interface – traceroute_2.

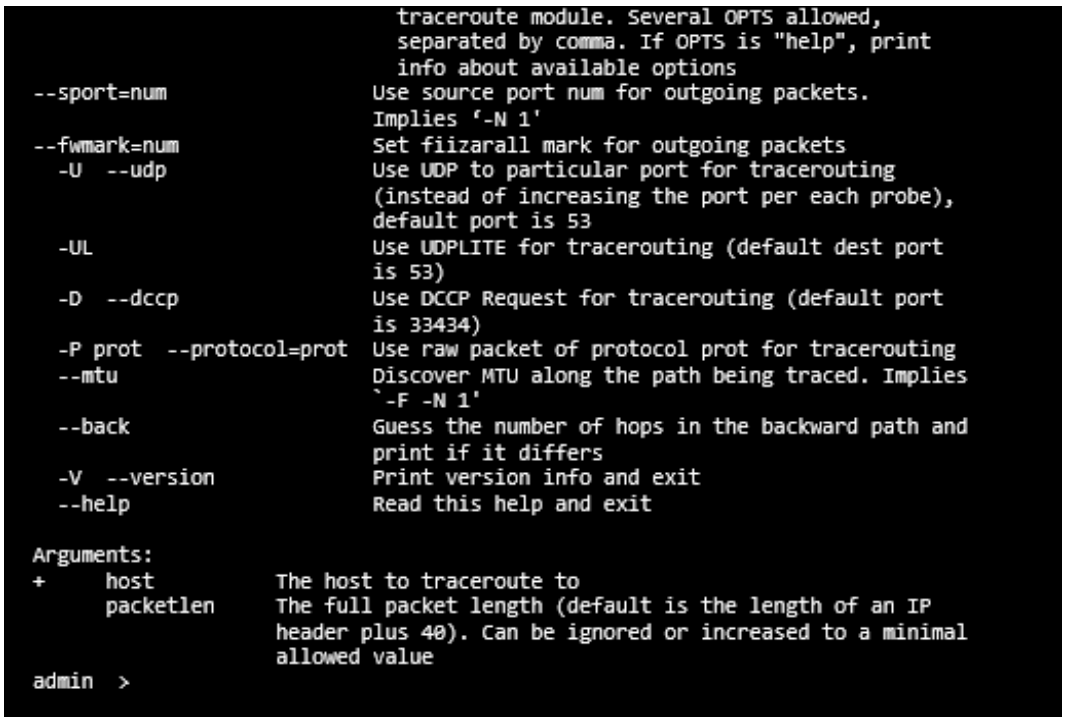

Figura 162 – Command Line Interface – traceroute_3.

Exemplo: Testes para traçar o roteamento ou caminho até o endereço IP de DNS do Google, IP 8.8.8.8 no protocolo UDP (17):

```
admin  >traceroute -n -p 53 -t 17 8.8.8.8
traceroute to 8.8.8.8 (8.8.8.8), 30 hops max, 60 byte packets
 1  10.70.64.1  15.412 ms  15.242 ms  15.152 ms
 2  201.6.37.65  15.607 ms  15.618 ms  15.566 ms
 3  201.6.40.37  15.511 ms  16.380 ms  21.774 ms
 4  201.6.42.93  22.970 ms  22.917 ms  22.697 ms
 5  * * *
 6  * * *
 7  * * *
 8  * * *
 9  * * *
...
27  * * *
28  * * *
29  * * *
30  * * *
admin  >
```

Figura 163 – Command Line Interface – traceroute – Exemplo 1.

5.79 [update-system]

Utilizado para verificação, download e instalação dos pacotes de atualização do BLOCKBIT UTM.

Modo de uso:

Figura 146 - Command Line Interface – update-UTM.

5.80 [update-license]

Utilizado para verificação do status da licença do BLOCKBIT UTM.

5.81 [uptime]

Exibe há quanto tempo o servidor está ligado.

Modo de uso:

```
blockbit >uptime
 16:19:24 up 4 days,  1:26,  2 users,  load average: 0.01, 0.12, 0.11
blockbit >
```

Figura 165 – Command Line Interface – uptime.

5.82 [vmstat]

Relata informações sobre processos, memória, paginação, I/O de blocos e atividades da CPU.

Modo de uso:

```
[root@vcm bin]# vmstat --help

Usage:
 vmstat [options] [delay [count]]

Options:
 -a, --active           active/inactive memory
 -f, --forks            number of forks since boot
 -m, --slabs            slabinfo
 -n, --one-header       do not redisplay header
 -s, --stats            event counter statistics
 -d, --disk             disk statistics
 -D, --disk-sum         summarize disk statistics
 -p, --partition <dev>  partition specific statistics
 -S, --unit <char>      define display unit
 -w, --wide             wide output
 -t, --timestamp        show timestamp

 -h, --help     display this help and exit
 -V, --version  output version information and exit

For more details see vmstat(8).
[root@vcm bin]#
```

Figura 166 – Command Line Interface – vmstat.

Exemplo:

```
[root@vcm bin]# vmstat
procs -----------memory---------- ---swap-- -----io---- -system-- ------cpu-----
 r  b   swpd   free   buff  cache   si   so    bi    bo   in   cs us sy id wa st
 1  0      0 1816712 182256 1040896    0    0     0     2   23    5  0  0 100  0  0
[root@vcm bin]#
```

Figura 167 – Command Line Interface – vmstat - Exemplo.

5.83 [watch-cpu]

Monitora em tempo real a utilização dos processadores do servidor.

Modo de uso:

```
admin  >watch-cpu
```

Figura 147 – Command Line Interface – watch-cpu.

Exemplo:

```
watch-cpu: 07:24:31 up 1 day, 16:13,  2 users,  load average: 0.00, 0.01, 0.05
Linux 3.10.0-514.26.2.el7.x86_64 (bbv10-14.labsuporte.com.br)   03/15/18        _x86_64_        (4 CPU)

07:24:31     CPU    %usr   %nice    %sys %iowait    %irq   %soft  %steal  %guest  %gnice   %idle
07:24:31     all    1.22    0.15    1.10    0.04    0.00    0.07    0.00    0.00    0.00   97.42
07:24:31       0    1.51    0.15    1.17    0.04    0.00    0.12    0.00    0.00    0.00   97.02
07:24:31       1    1.16    0.15    1.12    0.04    0.00    0.06    0.00    0.00    0.00   97.47
07:24:31       2    1.13    0.15    1.09    0.04    0.00    0.06    0.00    0.00    0.00   97.53
07:24:31       3    1.07    0.15    1.03    0.04    0.00    0.05    0.00    0.00    0.00   97.67

press [CTRL+C] to stop
```

Figura 148 – Command Line Interface – watch-cpu - exemplo.

5.84 [watch-io]

Monitora em tempo real a utilização do I/O do servidor (utilização de escrita e leitura em disco).

Modo de uso:

```
admin  >watch-io
```

Figura 149 – Command Line Interface – watch-io.

Exemplo:

```
watch-io: 07:26:59 up 1 day, 16:15,  2 users,  load average: 0.12, 0.09, 0.07
Linux 3.10.0-514.26.2.el7.x86_64 (bbv10-14.labsuporte.com.br)   03/15/18        _x86_64_        (4 CPU)

avg-cpu:  %user   %nice %system %iowait  %steal   %idle
           1.22    0.15    1.17    0.04    0.00   97.42

Device:         rrqm/s   wrqm/s     r/s     w/s    rkB/s    wkB/s avgrq-sz avgqu-sz   await r_await w_await  svctm  %util
sda               0.00     8.15    0.51    6.91     9.66    88.92    26.59     0.01    1.25    6.98    0.83   0.25   0.19
dm-0              0.00     0.00    0.27    0.46     5.87     3.52    25.92     0.00    2.79    5.68    1.08   0.47   0.03
dm-1              0.00     0.00    0.00    1.83     0.06     7.41     8.14     0.00    0.13    0.65    0.13   0.04   0.01
dm-2              0.00     0.00    0.23   12.58     3.69    77.22    12.64     0.02    1.32    9.47    1.17   0.16   0.21
dm-3              0.00     0.00    0.00    0.19     0.01     0.77     8.01     0.02   95.34    1.96   96.60   0.09   0.00


press [CTRL+C] to stop
```

Figura 150 – Command Line Interface – watch-io - exemplo.

5.85 [watch-mem]

Monitora em tempo real a utilização da memória do servidor.

Modo de uso:

Figura 151 – Command Line Interface – watch-mem.

Exemplo:

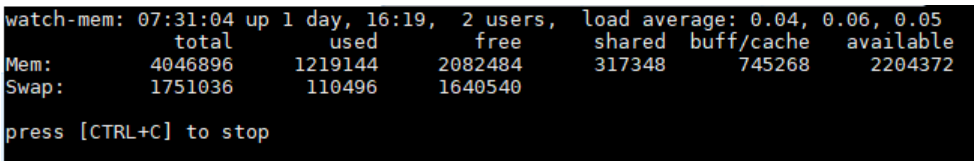

Figura 152 – Command Line Interface – watch-mem - exemplo.

5.86 [watch-srv]

Monitora em tempo real a utilização de processamento e memória de cada serviço.

Modo de uso:

Figura 153 – Command Line Interface – watch-srv.

Exemplo:

```
watch-srv: 07:33:35 up 1 day, 16:22,  2 users,  load average: 0.49, 0.16, 0.08
SERVICE                    %CPU      %MEM
firewall                    0.0       0.0
router-bgp                  0.0       0.0
router-rip                  0.0       0.0
router-ospf                 0.0       0.0
router-pim                  0.0       0.0
router-nat64                0.0       0.0
proxy-http                  0.4       1.5
proxy-ftp                   0.0       0.0
proxy-email                 0.0       0.0
antimalware                 0.0       0.0
atp                         0.0      11.2
ips                         0.0       0.0
snmp                        0.0       0.1
dns                         0.0       0.0
dhcp-server                 0.0       0.2
dhcp-relay                  0.0       0.0
vpn-ipsec                   0.0       0.0
vpn-ssl                     0.0       0.0
auth-server                 0.0       0.0
auth-windows                0.0       0.0
auth-ldap                   0.0       0.0
auth-radius                 0.0       0.0
system-db                   0.0       3.1
system-terminal             0.0       0.0
system-storage              0.0       0.0
system-syslog               0.0       0.1
system-admin                0.0       4.4
system-ha                   0.0       0.0
gsm-deployer                0.0       0.0
gsm-logger                  0.3       0.0

press [CTRL+C] to stop
```

Figura 154 – Command Line Interface – watch-srv - exemplo.

5.87 [wc]

Contador de quantidade de linhas da saída de um comando.

Exemplo: Verificar a quantidade de usuários autenticados no servidor:

```
admin  >show-sessions|wc -l
1
```

Figura 155 – Command Line Interface – wc.

5.88 [whois]

Busca de mais informações a respeito de um domínio.

Modo de uso:

```
admin  >whois
Usage: whois [OPTION]... OBJECT...

-h HOST, --host HOST   connect to server HOST
-p PORT, --port PORT   connect to PORT
-H                     hide legal disclaimers
      --verbose        explain what is being done
      --help           display this help and exit
      --version        output version information and exit

These flags are supported by whois.ripe.net and some RIPE-like servers:
-l                     find the one level less specific match
-L                     find all levels less specific matches
-m                     find all one level more specific matches
-M                     find all levels of more specific matches
-c                     find the smallest match containing a mnt-irt attribute
-x                     exact match
-b                     return brief IP address ranges with abuse contact
-B                     turn off object filtering (show email addresses)
-G                     turn off grouping of associated objects
-d                     return DNS reverse delegation objects too
-i ATTR[,ATTR]...      do an inverse look-up for specified ATTRibutes
-T TYPE[,TYPE]...      only look for objects of TYPE
-K                     only primary keys are returned
-r                     turn off recursive look-ups for contact information
-R                     force to show local copy of the domain object even
                       if it contains referral
-a                     also search all the mirrored databases
-s SOURCE[,SOURCE]...  search the database mirrored from SOURCE
-g SOURCE:FIRST-LAST   find updates from SOURCE from serial FIRST to LAST
-t TYPE                request template for object of TYPE
-v TYPE                request verbose template for object of TYPE
-q [version|sources|types]  query specified server info
```

Figura 156 – Command Line Interface – whois.

Exemplo:

```
admin  >whois google.com
   Domain Name: GOOGLE.COM
   Registry Domain ID: 2138514_DOMAIN_COM-VRSN
   Registrar WHOIS Server: whois.markmonitor.com
   Registrar URL: http://www.markmonitor.com
   Updated Date: 2018-02-21T18:36:40Z
   Creation Date: 1997-09-15T04:00:00Z
   Registry Expiry Date: 2020-09-14T04:00:00Z
   Registrar: MarkMonitor Inc.
   Registrar IANA ID: 292
   Registrar Abuse Contact Email: abusecomplaints@markmonitor.com
   Registrar Abuse Contact Phone: +1.2083895740
   Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
   Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
   Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
   Domain Status: serverDeleteProhibited https://icann.org/epp#serverDeleteProhibited
   Domain Status: serverTransferProhibited https://icann.org/epp#serverTransferProhibited
   Domain Status: serverUpdateProhibited https://icann.org/epp#serverUpdateProhibited
   Name Server: NS1.GOOGLE.COM
   Name Server: NS2.GOOGLE.COM
   Name Server: NS3.GOOGLE.COM
   Name Server: NS4.GOOGLE.COM
   DNSSEC: unsigned
   URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2018-03-15T10:45:11Z <<<

For more information on Whois status codes, please visit https://icann.org/epp

NOTICE: The expiration date displayed in this record is the date the
registrar's sponsorship of the domain name registration in the registry is
currently set to expire. This date does not necessarily reflect the expiration
date of the domain name registrant's agreement with the sponsoring
registrar.  Users may consult the sponsoring registrar's Whois database to
view the registrar's reported date of expiration for this registration.

TERMS OF USE: You are not authorized to access or query our Whois
database through the use of electronic processes that are high-volume and
automated except as reasonably necessary to register domain names or
modify existing registrations; the Data in VeriSign Global Registry
Services' ("VeriSign") Whois database is provided by VeriSign for
information purposes only, and to assist persons in obtaining information
```

Figura 157 – Command Line Interface – whois - exemplo.

[vmstat]