

BLOCKBIT UTM CLI

(COMMAND LINE INTERFACE)



UTM

BLOCKBIT

Gerenciamento Unificado de Ameaças



Sumário

1	INTERFACE BLOCKBIT CLI - LINHA DE COMANDOS	16
1.1	[arp]	17
1.2	[arping]	19
1.3	[configure-bgp]	19
1.4	[configure-ospf]	20
1.5	[configure-ospf6]	22
2.1	[configure-pim]	22
2.2	[configure-rip]]	24
2.3	[configure-rip6]	25
2.4	[conntack]	26
2.5	[date]	27
2.6	[debug-auth]	28
3.1	[debug-dhcp]	29
4.1	[debug-events]	29
4.2	[debug-firewall]	30
4.3	[debug-ha]	30
4.4	[debug-threats]	31
5.1	[debug-vpn]	31

5.2	[debug-web]	32
5.3	[dig]	32
5.4	[disable-bgp]	34
5.5	[disable-ospf]	35
5.6	[disable-pim]	35
5.7	[disable-rip]	35
5.8	[disable-snmp]	36
5.9	[enable-bgp]	36
5.10	[enable-ospf]	36
5.11	[enable-pim]	37
5.12	[enable-rip]	37
5.13	[enable-root]	37
5.14	[enable-snmp]	37
5.15	[ethtool]	39
5.16	[exit]	40
5.17	[fdisk]	41
5.18	[free]	42
5.19	[fsck]	42
5.20	[fwrecovery]	43
5.21	[fwreload]	43

5.22	[grep]	44
5.23	[help]	44
5.24	[history]	45
5.25	[host]	45
5.26	[Hostname]	46
5.27	[ifconfig]	47
5.28	[ifstat]	49
5.29	[iostat]	50
5.30	[iotest]	51
5.31	[ip]	52
5.32	[ipcalc]	52
5.33	[iplist]	53
5.34	[iptraf]	53
5.35	[ldapsearch]	54
5.36	[less]	56
5.37	[lscpu]	57
5.38	[lsusb]	58
5.39	[mkfs]	59
5.40	[more]	59
5.41	[mtr]	60

5.42	[netads]	61
5.43	[netstat]	62
5.44	[nslookup]	62
5.45	[ntpdate]	63
5.46	[ping]	63
5.47	[passwd]	64
5.48	[reset]	64
5.49	[reboot]	65
5.50	[reset-admin-blocks]	65
5.51	[reset-admin-password]	66
5.52	[reset-admin-sessions]	66
5.53	[reset-logs]	66
5.54	[reset-stats]	67
5.55	[rewizard]	67
5.56	[route]	67
5.57	[sar]	69
5.58	[service-disable]	70
5.59	[service-enable]	70
5.60	[service-start]	71
5.61	[service-status]	72

5.62	[service-stop].....	73
5.63	[set-irqbalance-dynamic].....	73
5.64	[set-irqbalance-static].....	74
5.65	[show-sessions].....	74
5.66	[show-uuid]	74
5.67	[show-vpn-conn]	75
5.68	[show-vpn-info].....	75
5.69	[shutdown].....	75
5.70	[speedtest]	76
5.71	[system-status].....	76
5.72	[sync-users]	77
5.73	[sysctl].....	77
5.74	[tcpdump].....	78
5.75	[tcptop].....	79
5.76	[telnet].....	80
5.77	[tracepath].....	81
5.78	[traceroute]	81
5.79	[update-system]	84
5.80	[update-license]	84
5.81	[uptime].....	84

5.82	[vmstat]	85
5.83	[watch-cpu]	86
5.84	[watch-io]	86
5.85	[watch-mem]	87
5.86	[watch-srv]	87
5.87	[wc]	88
5.88	[whois]	88
	[vmstat]	90

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;

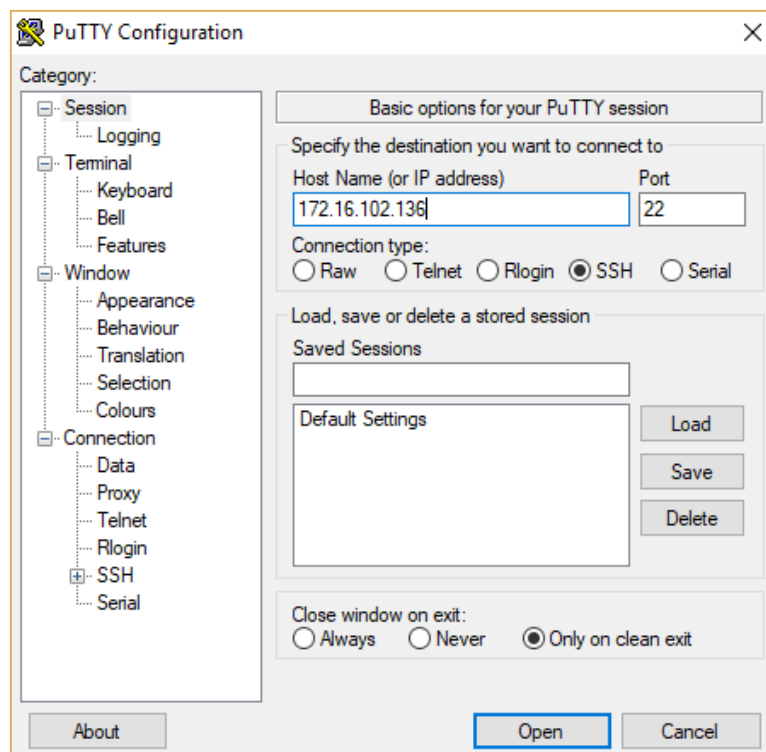


Figura 1 – PuTTY Configuration.

- 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        iptlist        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"

```
admin >configure-rip
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
BLOCKBIT Dynamic Router Config
+
+
User Access Verification
Password:
localhost> █
```

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 address from reply direction
-q, --reply-dst ip        Destination address from reply direction
-p, --protocol 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:

```

admin >conntrack -L
udp 17 29 src=172.16.13.214 dst=172.16.13.245 sport=34372 dport=53 packets=1 bytes=66 src=172.16.13.245 dst=172.16.13.214 sport=53 dport=34372 packets=1 bytes=155 mark=10015 use=1
tcp 6 28 TIME_WAIT src=127.0.0.1 dst=127.0.0.1 sport=25388 dport=5432 packets=10 bytes=761 src=127.0.0.1 dst=127.0.0.1 sport=5432 dport=25388 packets=7 bytes=819 [ASSURED] mark=0 use=1
tcp 6 28 TIME_WAIT src=127.0.0.1 dst=127.0.0.1 sport=31344 dport=9832 packets=10 bytes=719 src=127.0.0.1 dst=127.0.0.1 sport=9832 dport=31344 packets=7 bytes=1176 [ASSURED] mark=0 use=1
tcp 6 28 TIME_WAIT src=127.0.0.1 dst=127.0.0.1 sport=25372 dport=5432 packets=8 bytes=563 src=127.0.0.1 dst=127.0.0.1 sport=5432 dport=25372 packets=6 bytes=683 [ASSURED] mark=0 use=1
udp 17 28 src=172.16.13.214 dst=172.16.13.245 sport=43011 dport=53 packets=1 bytes=66 src=172.16.13.245 dst=172.16.13.214 sport=53 dport=43011 packets=1 bytes=155 mark=10015 use=1
udp 17 178 src=127.0.0.1 dst=127.0.0.1 sport=46502 dport=46502 packets=1 bytes=1004 src=127.0.0.1 dst=127.0.0.1 sport=46502 dport=46502 packets=53 bytes=38236 [ASSURED] mark=0 use=1
udp 17 29 src=172.16.12.52 dst=255.255.255.255 sport=68 dport=67 packets=1 bytes=328 [UNREPLIED] src=255.255.255.255 dst=172.16.12.52 sport=67 dport=68 packets=0 bytes=0 mark=10015 use=1
tcp 6 179998 ESTABLISHED src=172.16.13.82 dst=172.16.13.214 sport=63782 dport=98 packets=2 bytes=749 src=172.16.13.214 dst=172.16.13.82 sport=98 dport=63782 packets=2 bytes=514 [ASSURED] mark=10015 use=1
tcp 6 299 ESTABLISHED src=172.16.13.214 dst=172.16.13.82 sport=22 dport=52081 packets=22 bytes=6496 src=172.16.13.82 dst=172.16.13.214 sport=52081 dport=22 packets=21 bytes=1176 [ASSURED] mark=0 use=1
tcp 6 28 TIME_WAIT src=127.0.0.1 dst=127.0.0.1 sport=25376 dport=5432 packets=10 bytes=719 src=127.0.0.1 dst=127.0.0.1 sport=5432 dport=25376 packets=7 bytes=1176 [ASSURED] mark=0 use=1
tcp 6 28 TIME_WAIT src=127.0.0.1 dst=127.0.0.1 sport=25380 dport=5432 packets=10 bytes=719 src=127.0.0.1 dst=127.0.0.1 sport=5432 dport=25380 packets=7 bytes=1176 [ASSURED] mark=0 use=1
tcp 6 28 TIME_WAIT src=127.0.0.1 dst=127.0.0.1 sport=25384 dport=5432 packets=8 bytes=568 src=127.0.0.1 dst=127.0.0.1 sport=5432 dport=25384 packets=5 bytes=631 [ASSURED] mark=0 use=1
tcp 6 28 TIME_WAIT src=127.0.0.1 dst=127.0.0.1 sport=31356 dport=9832 packets=10 bytes=761 src=127.0.0.1 dst=127.0.0.1 sport=9832 dport=31356 packets=7 bytes=819 [ASSURED] mark=0 use=1
udp 17 29 src=172.16.13.214 dst=172.16.13.245 sport=64027 dport=53 packets=1 bytes=66 src=172.16.13.245 dst=172.16.13.214 sport=53 dport=64027 packets=1 bytes=155 mark=10015 use=1
tcp 6 28 TIME_WAIT src=127.0.0.1 dst=127.0.0.1 sport=31360 dport=9832 packets=13 bytes=1358 src=127.0.0.1 dst=127.0.0.1 sport=9832 dport=31360 packets=10 bytes=1214 [ASSURED] mark=0 use=1
tcp 6 179998 ESTABLISHED src=127.0.0.1 dst=127.0.0.1 sport=32658 dport=22 packets=53 bytes=4736 src=127.0.0.1 dst=127.0.0.1 sport=22 dport=32658 packets=48 bytes=4336 [ASSURED] mark=0 use=1
tcp 6 28 TIME_WAIT src=127.0.0.1 dst=127.0.0.1 sport=31348 dport=9832 packets=10 bytes=719 src=127.0.0.1 dst=127.0.0.1 sport=9832 dport=31348 packets=7 bytes=1176 [ASSURED] mark=0 use=1
tcp 6 28 TIME_WAIT src=127.0.0.1 dst=127.0.0.1 sport=31352 dport=9832 packets=8 bytes=568 src=127.0.0.1 dst=127.0.0.1 sport=9832 dport=31352 packets=5 bytes=631 [ASSURED] mark=0 use=1
tcp 6 28 TIME_WAIT src=127.0.0.1 dst=127.0.0.1 sport=31340 dport=9832 packets=9 bytes=615 src=127.0.0.1 dst=127.0.0.1 sport=9832 dport=31340 packets=5 bytes=631 [ASSURED] mark=0 use=1
tcp 6 28 TIME_WAIT src=127.0.0.1 dst=127.0.0.1 sport=25392 dport=5432 packets=13 bytes=1358 src=127.0.0.1 dst=127.0.0.1 sport=5432 dport=25392 packets=10 bytes=1214 [ASSURED] mark=0 use=1
tcp 6 28 TIME_WAIT src=127.0.0.1 dst=127.0.0.1 sport=31336 dport=9832 packets=10 bytes=894 src=127.0.0.1 dst=127.0.0.1 sport=9832 dport=31336 packets=7 bytes=901 [ASSURED] mark=0 use=1
tcp 6 28 TIME_WAIT src=127.0.0.1 dst=127.0.0.1 sport=25368 dport=5432 packets=10 bytes=894 src=127.0.0.1 dst=127.0.0.1 sport=5432 dport=25368 packets=8 bytes=953 [ASSURED] mark=0 use=1
conntrack v1.4.2 (conntrack-tools): 22 flow entries have been shown.

```

Figura 18 – Command Line Interface – conntrack - Exemplo.

2.5 [date]

Lista e permite alterar a data e hora atual.

Modo de uso:

```

admin >date --help
Usage: date [OPTION]... [+FORMAT]
       or: date [-u|--utc|--universal] [MMDDhhmm[[CC]YY][.ss]]
Display the current time in the given FORMAT, or set the system date.
...
Mandatory arguments to long options are mandatory for short options too.
-d, --date=STRING      display time described by STRING, not 'now'
-f, --file=DATEFILE    like --date once for each line of DATEFILE
-I[TIMESPEC], --iso-8601=[TIMESPEC] output date/time in ISO 8601 format.
                        TIMESPEC='date' for date only (the default),
                        'hours', 'minutes', 'seconds', or 'ns' for date
                        and time to the indicated precision.
-r, --reference=FILE    display the last modification time of FILE
-R, --rfc-2822          output date and time in RFC 2822 format.
                        Example: Mon, 07 Aug 2006 12:34:56 -0600

```

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:

```

admin >debug-auth
type=auth date=2018-03-13 14:07:29 AddrConn:172.16.13.82 AddrMac:84:7b:eb:e6:36:f1 Login:bb Action:AUTH_LOGIN Reply:110 AUTH_LOGIN_OK ticket:96bc40ba7bae6fd647f
6f91f38c28896 timeout:30
type=auth date=2018-03-13 14:07:31 AddrConn:172.16.13.82 AddrMac:84:7b:eb:e6:36:f1 Login:bb Action:AUTH_LOGIN Reply:110 AUTH_LOGIN_OK ticket:96bc40ba7bae6fd647f
6f91f38c28896 timeout:30
type=auth date=2018-03-13 14:07:53 AddrConn:172.16.102.162 AddrMac:- Login:suporte Action:AUTH_LOGIN Reply:110 AUTH_LOGIN_OK ticket:b6d138f097c6ff472623b92b1b73
7808 timeout:30
type=auth date=2018-03-13 14:08:03 AddrConn:172.16.102.162 AddrMac:- Login:suporte Action:AUTH_LOGOUT Reply:210 AUTH_LOGOUT_OK
type=auth date=2018-03-13 14:08:10 AddrConn:172.16.102.162 AddrMac:- Login:suporte Action:AUTH_LOGIN Reply:102 AUTH_LOGIN_ERR_PAM msg:'Wrong password'

```

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:

```

admin >debug-dhcp

```

Figura 25 – Command Line Interface – debug-dhcp.

4

Exemplo:

```

admin >debug-dhcp
type=dhcp date=2018-03-13 14:25:04 DHCPDISCOVER from d0:67:e5:f7:74:d5 via eth1
type=dhcp date=2018-03-13 14:25:05 DHCPPOFFER on 192.168.250.10 to d0:67:e5:f7:74:d5 (BLOCKBIT-PC) via eth1
type=dhcp date=2018-03-13 14:25:08 DHCPDISCOVER from d0:67:e5:f7:74:d5 (BLOCKBIT-PC) via eth1
type=dhcp date=2018-03-13 14:25:08 DHCPPOFFER on 192.168.250.10 to d0:67:e5:f7:74:d5 (BLOCKBIT-PC) via eth1
type=dhcp date=2018-03-13 14:25:08 DHCPREQUEST for 192.168.250.10 (192.168.250.1) from d0:67:e5:f7:74:d5 (BLOCKBIT-PC) via eth1
type=dhcp date=2018-03-13 14:25:08 DHCPACK on 192.168.250.10 to d0:67:e5:f7:74:d5 (BLOCKBIT-PC) via eth1
type=dhcp date=2018-03-13 14:25:11 DHCPINFORM from 192.168.250.10 via eth1: not authoritative for subnet 192.168.250.0
type=dhcp date=2018-03-13 14:25:11 If this DHCP server is authoritative for that subnet,
type=dhcp date=2018-03-13 14:25:11 please write an 'authoritative:' directive either in the
type=dhcp date=2018-03-13 14:25:11 subnet declaration or in some scope that encloses the
type=dhcp date=2018-03-13 14:25:11 subnet declaration - for example, write it at the top
type=dhcp date=2018-03-13 14:25:11 of the dhcpd.conf file.
type=dhcp date=2018-03-13 14:25:14 DHCPINFORM from 192.168.250.10 via eth1: not authoritative for subnet 192.168.250.0

```

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:

```
admin >debug-events
```

Figura 27 – Command Line Interface – debug-events.

Exemplo:

```
admin >debug-events
Mar 13 14:31:58 bb5sp INFO: Atualização realizada com sucesso, O servidor encontrou 1 atualizações e foi atualizado com sucesso
```

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

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

```
admin >debug-events
log not found
admin >
```

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:

```
admin >debug-firewall
```

Figura 30 – Command Line Interface – debug-firewall.

Exemplo:

```
admin >debug-firewall
type=firewall date=2018-03-13 15:25:04 in=eth0 out=eth0 mac=ce:7b:ea:d6:7e:66 src=172.16.102.162:55868 dst=172.16.13.214:80 proto=TCP user=- rule="ENCAMINHAMENTO ENT
RE AS REDES"
type=firewall date=2018-03-13 15:26:01 in=eth0 out=eth0 mac=ce:7b:ea:d6:7e:66 src=172.16.102.162:55874 dst=54.233.126.4:80 proto=TCP user=- rule="NAT: SERVIDOR DOMAI
N CONTROL"
type=firewall date=2018-03-13 15:26:01 in=eth0 out=eth0 mac=ce:7b:ea:d6:7e:66 src=172.16.102.162:55878 dst=172.217.1.98:80 proto=TCP user=- rule="NAT: SERVIDOR DOMAI
N CONTROL"
type=firewall date=2018-03-13 15:26:01 in=eth0 out=eth0 mac=ce:7b:ea:d6:7e:66 src=172.16.102.162:55880 dst=52.84.174.222:80 proto=TCP user=- rule="NAT: SERVIDOR DOMA
IN CONTROL"
type=firewall date=2018-03-13 15:26:01 in=eth0 out=eth0 mac=ce:7b:ea:d6:7e:66 src=172.16.102.162:55886 dst=172.217.2.202:443 proto=TCP user=- rule="NAT: SERVIDOR DOM
AIN CONTROL"
```

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:

```
admin >debug-ha
type=ha date=2018-03-17 11:54:49 Mar 1 11:54:49 master.blockbit.com blockbit-apply-cluster-master-notifyVI_2: conntrack primary
type=ha date=2018-03-17 11:54:50 Mar 1 11:54:50 master.blockbit.com blockbit-apply-cluster-master-notifyVI_1: reconfigure macaddr: eth7 (00:90:28:01:2f:48)
type=ha date=2018-03-17 11:54:50 Mar 1 11:54:50 master.blockbit.com blockbit-apply-cluster-master-notifyVI_1: conntrack primary
```

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:

```
admin >debug-threats
Feb 19 19:40:03 master log="-" box_id="73989d2f8ab2435ff3853b84872e23ac" logtype="atp" date="2018-02-19 19:30:00" src="172.16.12.37" dst="2.37" rule_action="allow" app_category="general" app_name="Wordpress"
Feb 19 19:40:03 master log="-" box_id="73989d2f8ab2435ff3853b84872e23ac" logtype="atp" date="2018-02-19 19:30:00" src="192.0.78.23" dst="192.0.78.23" rule_action="allow" app_category="general" app_name="Wordpress"
Feb 19 19:40:03 master log="-" box_id="73989d2f8ab2435ff3853b84872e23ac" logtype="atp" date="2018-02-19 19:30:00" src="172.16.12.37" dst="2.37" rule_action="allow" app_category="general" app_name="Wordpress"
Feb 19 19:40:03 master log="-" box_id="73989d2f8ab2435ff3853b84872e23ac" logtype="atp" date="2018-02-19 19:30:00" src="192.0.78.23" dst="192.0.78.23" rule_action="allow" app_category="general" app_name="Wordpress"
Feb 19 19:40:03 master log="-" box_id="73989d2f8ab2435ff3853b84872e23ac" logtype="atp" date="2018-02-19 19:30:00" src="172.16.12.37" dst="2.37" rule_action="allow" app_category="general" app_name="Wordpress"
Feb 19 19:40:03 master log="-" box_id="73989d2f8ab2435ff3853b84872e23ac" logtype="atp" date="2018-02-19 19:30:00" src="162.125.5.3" dst="192.0.78.23" rule_action="deny" app_category="storage" app_name="Dropbox"
```

Figura 33 – Command Line Interface – debug-threats.

5

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

```
admin >debug-threats
log not found
admin >
```

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:

```
admin >debug-vpn
10[NET] received packet: from 201.6.228.163[25049] to 187.8.187.66[4500] (92 bytes)
10[ENC] parsed INFORMATIONAL_V1 request 2727211931 [ HASH N(DPD) ]
10[ENC] generating INFORMATIONAL_V1 request 1228398341 [ HASH N(DPD_ACK) ]
10[NET] sending packet: from 187.8.187.66[4500] to 201.6.228.163[25049] (92 bytes)
13[IKE] sending keep alive to 186.231.58.210[4500]
03[NET] received packet: from 201.6.228.163[25049] to 187.8.187.66[4500] (92 bytes)
03[ENC] parsed INFORMATIONAL_V1 request 1222971852 [ HASH N(DPD) ]
03[ENC] generating INFORMATIONAL_V1 request 3566639645 [ HASH N(DPD_ACK) ]
03[NET] sending packet: from 187.8.187.66[4500] to 201.6.228.163[25049] (92 bytes)
```

Figura 35 – Command Line Interface – debug-vpn.

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

```
admin >debug-vpn
log not found
admin >
```

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:

```
admin >debug-web
```

Figura 37 – Command Line Interface – debug-web.

Exemplo:

```
admin >debug-web
type=web date=2018-03-13 15:46:06 bytes=61 mac=ce:7b:ea:d6:7e:66 src=172.16.102.162:56526 dst=172.217.8.78:443 code=TAG_NONE/- method=CONNECT rule=WEB: SITES BLOQUEA
DOS user=- site=www.youtube.com url=www.youtube.com agent=[-]
type=web date=2018-03-13 15:46:06 bytes=61949 mac=ce:7b:ea:d6:7e:66 src=172.16.102.162:56526 dst=-:- code=TCP_DENIED/- method=GET rule=WEB: SITES BLOQUEADOS user=- s
ite=- url=https://www.youtube.com/ agent=[Mozilla/5.0(WindowsNT10.0;Win64;x64;rv:58.0)Gecko/20100101Firefox/58.0]
type=web date=2018-03-13 15:46:06 bytes=61 mac=ce:7b:ea:d6:7e:66 src=172.16.102.162:56530 dst=172.217.8.78:443 code=TAG_NONE/- method=CONNECT rule=WEB: SITES BLOQUEA
DOS user=- site=www.youtube.com url=www.youtube.com agent=[-]
type=web date=2018-03-13 15:46:06 bytes=61 mac=ce:7b:ea:d6:7e:66 src=172.16.102.162:56528 dst=34.211.99.53:443 code=TAG_NONE/- method=CONNECT rule=WEB: Navegação Per
mitida user=- site=tiles.services.mozilla.com url=tiles.services.mozilla.com agent=[-]
type=web date=2018-03-13 15:46:06 bytes=61 mac=ce:7b:ea:d6:7e:66 src=172.16.102.162:56529 dst=34.211.99.53:443 code=TAG_NONE/- method=CONNECT rule=WEB: Navegação Per
mitida user=- site=tiles.services.mozilla.com url=tiles.services.mozilla.com agent=[-]
type=web date=2018-03-13 15:46:06 bytes=1392 mac=ce:7b:ea:d6:7e:66 src=172.16.102.162:56529 dst=34.211.99.53:443 code=TCP_MISS/200 method=POST rule=WEB: Navegação Pe
rmitida user=- site=- url=https://tiles.services.mozilla.com/v4/links/activity-stream agent=[Mozilla/5.0(WindowsNT10.0;Win64;x64;rv:58.0)Gecko/20100101Firefox/58.0]
type=web date=2018-03-13 15:46:06 bytes=1034 mac=ce:7b:ea:d6:7e:66 src=172.16.102.162:56528 dst=34.211.99.53:443 code=TCP_MISS/200 method=POST rule=WEB: Navegação Pe
rmitida user=- site=- url=https://tiles.services.mozilla.com/v4/links/activity-stream agent=[Mozilla/5.0(WindowsNT10.0;Win64;x64;rv:58.0)Gecko/20100101Firefox/58.0]
type=web date=2018-03-13 15:46:15 bytes=728 mac=ce:7b:ea:d6:7e:66 src=172.16.102.162:56537 dst=64.13.232.159:80 code=TCP_MISS/403 method=GET rule=WEB: Navegação Perm
itida user=- site=- url=http://wpad.supportlab.com/wpad.dat agent=[WinHttp-Autoproxy-Service/5.1]
type=web date=2018-03-13 15:46:29 bytes=65 mac=ce:7b:ea:d6:7e:66 src=172.16.102.162:56542 dst=216.58.202.196:443 code=TAG_NONE/- method=CONNECT rule=WEB: Navegação P
ermitida user=- site=www.google.com url=www.google.com agent=[-]
type=web date=2018-03-13 15:46:29 bytes=1146 mac=ce:7b:ea:d6:7e:66 src=172.16.102.162:56542 dst=216.58.202.196:443 code=TCP_MISS/200 method=GET rule=WEB: Navegação P
ermitida user=- site=- url=https://www.google.com/complete/search?client=firefox&q=ip agent=[Mozilla/5.0(WindowsNT10.0;Win64;x64;rv:58.0)Gecko/20100101Firefox/58.0]
type=web date=2018-03-13 15:46:29 bytes=65 mac=ce:7b:ea:d6:7e:66 src=172.16.102.162:56543 dst=216.58.202.196:443 code=TAG_NONE/- method=CONNECT rule=WEB: Navegação P
ermitida user=- site=www.google.com url=www.google.com agent=[-]
type=web date=2018-03-13 15:46:30 bytes=1154 mac=ce:7b:ea:d6:7e:66 src=172.16.102.162:56543 dst=216.58.202.196:443 code=TCP_MISS/200 method=GET rule=WEB: Navegação P
ermitida user=- site=- url=https://www.google.com/complete/search?client=firefox&q=ipo agent=[Mozilla/5.0(WindowsNT10.0;Win64;x64;rv:58.0)Gecko/20100101Firefox/58.0]
type=web date=2018-03-13 15:46:30 bytes=65 mac=ce:7b:ea:d6:7e:66 src=172.16.102.162:56544 dst=216.58.202.196:443 code=TAG_NONE/- method=CONNECT rule=WEB: Navegação P
ermitida user=- site=- url=https://www.google.com/complete/search?client=firefox&q=ipok agent=[Mozilla/5.0(WindowsNT10.0;Win64;x64;rv:58.0)Gecko/20100101Firefox/58.0]
type=web date=2018-03-13 15:46:33 bytes=57 mac=ce:7b:ea:d6:7e:66 src=172.16.102.162:56556 dst=31.13.85.4:443 code=TAG_NONE/- method=CONNECT rule=WEB: SITES BLOQUEADO
S user=- site=connect.facebook.net url=connect.facebook.net agent=[-]
type=web date=2018-03-13 15:46:34 bytes=61989 mac=ce:7b:ea:d6:7e:66 src=172.16.102.162:56556 dst=-:- code=TCP_DENIED/- method=GET rule=WEB: SITES BLOQUEADOS user=- s
ite=http://ipok.com.br/ url=https://connect.facebook.net/pt_BR/sdk.js agent=[Mozilla/5.0(WindowsNT10.0;Win64;x64;rv:58.0)Gecko/20100101Firefox/58.0]
type=web date=2018-03-13 15:46:34 bytes=63 mac=ce:7b:ea:d6:7e:66 src=172.16.102.162:56554 dst=172.217.30.99:443 code=TAG_NONE/- method=CONNECT rule=WEB: Navegação Pe
rmitida user=- site=fonts.gstatic.com url=fonts.gstatic.com agent=[-]
```

Figura 38 – Command Line Interface – debug-web.

5.3 [dig]

Exibe informações sobre domínios.

Modo de uso:


```

admin >dig -h
Usage: dig [@global-server] [domain] [q-type] [q-class] [q-opt]
       {global-d-opt} host [@local-server] {local-d-opt}
       [ host [@local-server] {local-d-opt} [...]]
Where: domain is in the Domain Name System
q-class is one of (in,hs,ch,...) [default: in]
q-type is one of (a,any,mx,ns,soa,hinfo,axfr,txt,...) [default:a]
       (Use ixfr=version for type ixfr)
q-opt is one of:
  -x dot-notation (shortcut for reverse lookups)
  -i (use IP6.INT for IPv6 reverse lookups)
  -f filename (batch mode)
  -b address[#port] (bind to source address/port)
  -p port (specify port number)
  -q name (specify query name)
  -t type (specify query type)
  -c class (specify query class)
  -u (display times in usec instead of msec)
  -k keyfile (specify tsig key file)
  -y [hmac:]name:key (specify named base64 tsig key)
  -4 (use IPv4 query transport only)
  -6 (use IPv6 query transport only)
  -m (enable memory usage debugging)
d-opt is of the form +keyword[=value], where keyword is:
  +[no]vc (TCP mode)
  +[no]tcp (TCP mode, alternate syntax)
  +time=### (Set query timeout) [5]
  +tries=### (Set number of UDP attempts) [3]
  +retry=### (Set number of UDP retries) [2]
  +domain=### (Set default domainname)
  +bufsize=### (Set EDNS0 Max UDP packet size)
  +ndots=### (Set NDOTS value)
  +subnet=addr (Set edns-client-subnet option)
  +[no]edns[=###] (Set EDNS version) [0]
  +[no]search (Set whether to use searchlist)
  +[no]showsearch (Search with intermediate results)
  +[no]defname (Ditto)
  +[no]recurse (Recursive mode)
  +[no]ignore (Don't revert to TCP for TC responses.)
  +[no]fail (Don't try next server on SERVFAIL)
  +[no]besteffort (Try to parse even illegal messages)

```

Figura 39 – Command Line Interface – dig.

```

  +[no]besteffort (Try to parse even illegal messages)
  +[no]aaonly (Set AA flag in query (+[no]aaflag))
  +[no]adflag (Set AD flag in query)
  +[no]cdflag (Set CD flag in query)
  +[no]cl (Control display of class in records)
  +[no]cmd (Control display of command line)
  +[no]comments (Control display of comment lines)
  +[no]rrcomments (Control display of per-record comments)
  +[no]crypto (Control display of cryptographic fields in records)
  +[no]question (Control display of question)
  +[no]answer (Control display of answer)
  +[no]authority (Control display of authority)
  +[no]additional (Control display of additional)
  +[no]stats (Control display of statistics)
  +[no]short (Disable everything except short form of answer)
  +[no]ttlid (Control display of ttls in records)
  +[no]all (Set or clear all display flags)
  +[no]qr (Print question before sending)
  +[no]nssearch (Search all authoritative nameservers)
  +[no]identify (ID responders in short answers)
  +[no]trace (Trace delegation down from root [+dnssec])
  +[no]dnssec (Request DNSSEC records)
  +[no]expire (Request time to expire)
  +[no]nsid (Request Name Server ID)
  +[no]split=## (Split hex/base64 fields into chunks)
  +[no]multiline (Print records in an expanded format)
  +[no]onesoa (AXFR prints only one soa record)
  +[no]keepopen (Keep the TCP socket open between queries)
global d-opts and servers (before host name) affect all queries.
local d-opts and servers (after host name) affect only that lookup.
-h (print help and exit)
-v (print version and exit)
admin >

```

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:

```
admin >enable-pim
Service is enable
admin >
```

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:

```
admin >enable-rip
Service is enable
admin >
```

Figura 51 – Command Line Interface – enable-rip.

5.13 [enable-root]

Eleva o privilégio de acesso ao sistema ao modo desenvolvedor.

Modo de uso:

```
admin >enable-root
Challenge: 1aeac24f42659c87ca3b27432e0b822a
Type the password: 
```

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
Community 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
Community: 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|mil|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|--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|--UI|--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.

```

[ spi %d [m %x] ]
[ vlan-etype %x [m %x] ]
[ vlan %x [m %x] ]
[ user-def %x [m %x] ]
[ dst-mac %x:%x:%x:%x:%x:%x [m %x:%x:%x:%x:%x:%x] ]
[ action %d ]
[ loc %d]] ]
delete %d
ethtool -T|--show-time-stamping DEVNAME Show time stamping capabilities
ethtool -X|--show-rxfh-indir|--show-rxfh DEVNAME Show Rx flow hash indirection and/or hash key
ethtool -X|--set-rxfh-indir|--rxfh DEVNAME Set Rx flow hash indirection and/or hash key
[ equal N | weight W0 W1 ... ]
[ hkey %x:%x:%x:%x:%x:%x:.... ]
ethtool -f|--flash DEVNAME Flash firmware image from the specified file to a region on the device
FILENAME [ REGION-NUMBER-TO-FLASH ]
ethtool -P|--show-permaddr DEVNAME Show permanent hardware address
ethtool -w|--get-dump DEVNAME Get dump flag, data
[ data FILENAME ]
ethtool -W|--set-dump DEVNAME Set dump flag of the device
N
ethtool -L|--show-channels DEVNAME Query Channels
ethtool -L|--set-channels DEVNAME Set Channels
[ rx N ]
[ tx N ]
[ other N ]
[ combined N ]
ethtool --show-priv-flags DEVNAME Query private flags
ethtool --set-priv-flags DEVNAME Set private flags
FLAG on|off ...
ethtool -m|--dump-module-eprom|--module-info DEVNAME Query/Decode Module EEPROM information and optical diagnostics if available
[ raw on|off ]
[ hex on|off ]
[ offset N ]
[ length N ]
ethtool --show-eee DEVNAME Show EEE settings
ethtool --set-eee DEVNAME Set EEE settings
[ eee on|off ]
[ advertise %x ]
[ tx-lpi on|off ]
[ tx-timer %d ]
ethtool -h|--help Show this help
ethtool --version Show version number

```

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:

```

admin >ethtool eth0
Settings for eth0:
    Supported ports: [ TP ]
    Supported link modes:   1000baseT/Full
                           10000baseT/Full
    Supported pause frame use: No
    Supports auto-negotiation: No
    Advertised link modes:  Not reported
    Advertised pause frame use: No
    Advertised auto-negotiation: No
    Speed: 10000Mb/s
    Duplex: Full
    Port: Twisted Pair
    PHYAD: 0
    Transceiver: internal
    Auto-negotiation: off
    MDI-X: Unknown
    Supports Wake-on: uag
    Wake-on: d
    Link detected: yes

```

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    27262976    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=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=172.16.13.82:16958 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]
```

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:

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

Figura 70 – Command Line Interface – help.

5.24 [history]

Exibe o histórico de comandos executados na CLI.

Modo de uso:

```
admin >history
```

Figura 71 – Command Line Interface – history.

5.25 [host]

Utilitário para consulta DNS.

Modo de uso:

```
admin >host
Usage: host [-aCdLriTwv] [-c class] [-N ndots] [-t type] [-W time]
        [-R number] [-m flag] hostname [server]
-a is equivalent to -v -t ANY
-c specifies query class for non-IN data
-C compares SOA records on authoritative nameservers
-d is equivalent to -v
-l lists all hosts in a domain, using AXFR
-i IP6.INT reverse lookups
-N changes the number of dots allowed before root lookup is done
-r disables recursive processing
-R specifies number of retries for UDP packets
-s a SERVFAIL response should stop query
-t specifies the query type
-T enables TCP/IP mode
-v enables verbose output
-w specifies to wait forever for a reply
-W specifies how long to wait for a reply
-4 use IPv4 query transport only
-6 use IPv6 query transport only
-m set memory debugging flag (trace|record|usage)
-V print version number and exit
```

Figura 72 – Command Line Interface – host.

Exemplo: consultar o IP de um determinado endereço:

```
admin >host www.blockbit.com
www.blockbit.com is an alias for blockbit.wpengine.com.
blockbit.wpengine.com has address 104.198.103.7
admin >
```

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:

```

blockbit >hostname --help
Usage: hostname [-b] {hostname|-F file}      set host name (from file)
        hostname [-a|-A|-d|-f|-i|-I|-s|-y]    display formatted name
        hostname                               display host name

        {yp,nis,}domainname {nisdomain|-F file} set NIS domain name (from file)
        {yp,nis,}domainname                  display NIS domain name

        dnsdomainname                        display dns domain name

        hostname -V|--version|-h|--help      print info and exit

Program name:
        {yp,nis,}domainname=hostname -y
        dnsdomainname=hostname -d

Program options:
        -a, --alias                alias names
        -A, --all-fqdns            all long host names (FQDNs)
        -b, --boot                 set default hostname if none available
        -d, --domain              DNS domain name
        -f, --fqdn, --long        long host name (FQDN)
        -F, --file                read host name or NIS domain name from given file
        -i, --ip-address          addresses for the host name
        -I, --all-ip-addresses    all addresses for the host
        -s, --short               short host name
        -y, --yp, --nis          NIS/YP domain name

Description:
        This command can get or set the host name or the NIS domain name. You can
        also get the DNS domain or the FQDN (fully qualified domain name).
        Unless you are using bind or NIS for host lookups you can change the
        FQDN (Fully Qualified Domain Name) and the DNS domain name (which is
        part of the FQDN) in the /etc/hosts file.
blockbit >

```

Figura 74 – Command Line Interface – hostname.

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

```

blockbit >hostname -f
vcm.blockbit.com
blockbit >

```

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] [[-]larp] [[-]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:

```

blockbit >iostat --help
Usage: iostat [ options ] [ <interval> [ <count> ] ]
Options are:
[ -c ] [ -d ] [ -h ] [ -k | -m ] [ -N ] [ -t ] [ -V ] [ -x ] [ -y ] [ -z ]
[ -j { ID | LABEL | PATH | UUID | ... } ]
[ [ -T ] -g <group_name> ] [ -p [ <device> [,...] | ALL ] ]
[ <device> [...] | ALL ]
blockbit >
blockbit >

```

Figura 80 – Command Line Interface – iostat.

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

```

blockbit >iostat -x -d 1 10
Linux 3.10.0-229.20.1.el7.x86_64 (vcm) 09/12/17      _x86_64_      (4 CPU)
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                0.03      0.02    0.06    1.53    1.36     8.48    12.33     0.00     0.25    0.53     0.24    0.07    0.01
dm-0                0.00      0.00    0.07    0.04    0.78     0.74    28.78     0.00     5.67    0.61    14.30    0.14    0.00
dm-1                0.00      0.00    0.02    1.51    0.55     7.72    10.81     0.00     0.25    0.70     0.24    0.07    0.01
dm-2                0.00      0.00    0.00    0.00    0.01     0.01     8.22     0.00     0.42    0.54     0.26    0.08    0.00
dm-3                0.00      0.00    0.00    0.00    0.00     0.00     8.00     0.00     0.55    0.55     0.00    0.07    0.00

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      0.00    0.00    0.00    0.00     0.00     0.00     0.00     0.00    0.00     0.00    0.00    0.00
dm-0                0.00      0.00    0.00    0.00    0.00     0.00     0.00     0.00     0.00    0.00     0.00    0.00    0.00
dm-1                0.00      0.00    0.00    0.00    0.00     0.00     0.00     0.00     0.00    0.00     0.00    0.00    0.00
dm-2                0.00      0.00    0.00    0.00    0.00     0.00     0.00     0.00     0.00    0.00     0.00    0.00    0.00
dm-3                0.00      0.00    0.00    0.00    0.00     0.00     0.00     0.00     0.00    0.00     0.00    0.00    0.00
blockbit >

```

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:

```

blockbit >iotest
Testing root filesystem
1000000+0 records in
1000000+0 records out
2048000000 bytes (2.0 GB) copied, 4.85572 s, 422 MB/s
Cleaning
blockbit >

```

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:

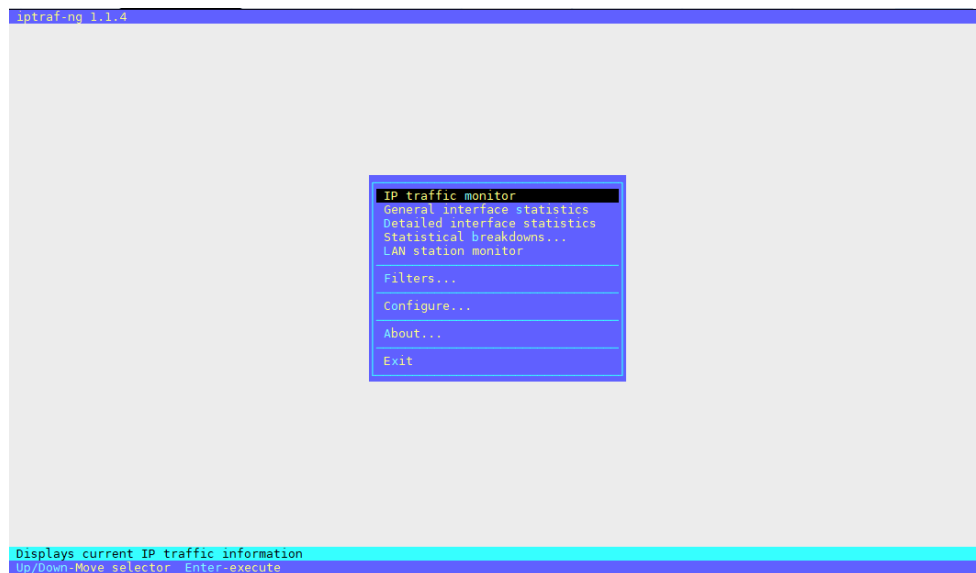


Figura 90 – Command Line Interface – iptraf - exemplo.

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

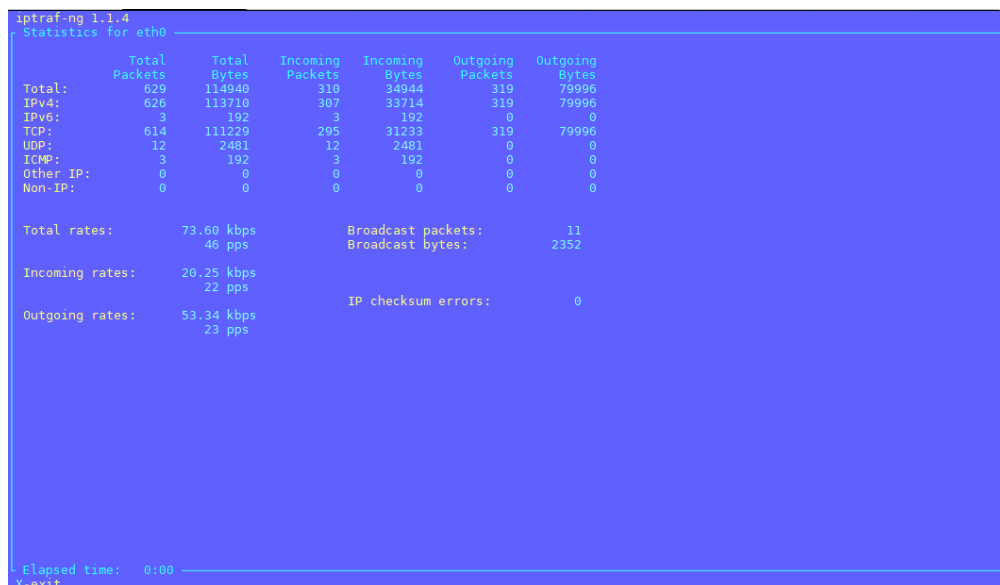


Figura 91 – Command Line Interface – iptraf – exemplo 2.

5.35 [ldapsearch]

Ferramenta para consultas em base LDAP.

Modo de uso:

```

admin >ldapsearch --help
ldapsearch: invalid option -- '-'
ldapsearch: unrecognized option --
usage: ldapsearch [options] [filter [attributes...]]
where:
  filter          RFC 4515 compliant LDAP search filter
  attributes      whitespace-separated list of attribute descriptions
                  which may include:
                    1.1 no attributes
                    *   all user attributes
                    +   all operational attributes
Search options:
-a deref         one of never (default), always, search, or find
-A             retrieve attribute names only (no values)
-b basedn       base dn for search
-c             continuous operation mode (do not stop on errors)
-E [!]<ext>[=<extparam>] search extensions (! indicates criticality)
                [!]domainScope (domain scope)
                [!]dontUseCopy (Don't Use Copy)
                [!]mv=<filter> (RFC 3876 matched values filter)
                [!]pr=<size>[/prompt|noprompt] (RFC 2696 paged results/prompt)
                [!]sss=[-]<attr[:OID]>[/[-]<attr[:OID]>...]]
                [!]subentries[=true|false] (RFC 3672 subentries)
                [!]sync=ro[/<cookie>] (RFC 4533 LDAP Sync refreshOnly)
                rp[/<cookie>][/<slimit>] (refreshAndPersist)
                [!]vlv=<before>/<after>[/<offset>/<count>[:<value>]]
                (ldapv3-vlv-09 virtual list views)
                [!]deref=derefAttr:attr[,...][;derefAttr:attr[,...][;...]]
                [!]<oid>[=:<b64value>] (generic control; no response handling)
-f file         read operations from 'file'
-F prefix       URL prefix for files (default: file:///tmp/)
-l limit        time limit (in seconds, or "none" or "max") for search
-L             print responses in LDIFv1 format
-LL            print responses in LDIF format without comments
-LLL           print responses in LDIF format without comments
               and version
-M             enable Manage DSA IT control (-MM to make critical)
-P version      protocol version (default: 3)
-s scope        one of base, one, sub or children (search scope)
-S attr        sort the results by attribute 'attr'
-t             write binary values to files in temporary directory
-tt            write all values to files in temporary directory
-T path        write files to directory specified by path (default: /tmp)
-u             include User Friendly entry names in the output
-z limit        size limit (in entries, or "none" or "max") for search

```

Figura 92 – Command Line Interface – ldapsearch.

```

Common options:
-d level       set LDAP debugging level to 'level'
-D binddn      bind DN
-e [!]<ext>[=<extparam>] general extensions (! indicates criticality)
                [!]assert=<filter> (RFC 4528; a RFC 4515 Filter string)
                [!]authzid=<authzid> (RFC 4370; "dn:<dn>" or "u:<user>")
                [!]chaining[=<resolveBehavior>[/<continuationBehavior>]]
                one of "chainingPreferred", "chainingRequired",
                "referralsPreferred", "referralsRequired"
                [!]manageDSAIT (RFC 3296)
                [!]noop
                ppolicy
                [!]postread[=<attrs>] (RFC 4527; comma-separated attr list)
                [!]preread[=<attrs>] (RFC 4527; comma-separated attr list)
                [!]relax
                [!]sessiontracking
                abandon, cancel, ignore (SIGINT sends abandon/cancel,
                or ignores response; if critical, doesn't wait for SIGINT.
                not really controls)
-h host        LDAP server
-H URI         LDAP Uniform Resource Identifier(s)
-I            use SASL Interactive mode
-n            show what would be done but don't actually do it
-N            do not use reverse DNS to canonicalize SASL host name
-O props       SASL security properties
-o <opt>[=<optparam>] general options
                nettimeout=<timeout> (in seconds, or "none" or "max")
                ldif-wrap=<width> (in columns, or "no" for no wrapping)
-p port        port on LDAP server
-Q            use SASL Quiet mode
-R realm       SASL realm
-U authcid     SASL authentication identity
-v            run in verbose mode (diagnostics to standard output)
-V            print version info (-VV only)
-w passwd      bind password (for simple authentication)
-W            prompt for bind password
-x            Simple authentication
-X authzid     SASL authorization identity ("dn:<dn>" or "u:<user>")
-y file        Read password from file
-Y mech        SASL mechanism
-Z            Start TLS request (-ZZ to require successful response)

```

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:: EaEgpi7FMUqK005rSS0ktg==
objectCategory: CN=Organizational-Unit,CN=Schema,CN=Configuration,DC=labsuporte,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=br
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.


```

dummy0: flags=130<BROADCAST,NOARP> mtu 1500
ether 8e:e0:1f:2a:14:d4 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

dummy1: flags=195<UP,BROADCAST,RUNNING,NOARP> mtu 2000
inet 192.168.222.1 netmask 255.255.255.0 broadcast 192.168.222.255
ether c6:7c:e0:39:30:b1 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

eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 172.16.102.78 netmask 255.255.255.0 broadcast 172.16.102.255
ether 00:0c:29:53:3d:16 txqueuelen 10000 (Ethernet)
RX packets 1671256 bytes 474969714 (452.9 MiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 1122153 bytes 417409238 (398.0 MiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

eth1: flags=4098<BROADCAST,MULTICAST> mtu 1500
ether 00:0c:29:53:3d:20 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:29:53:3d:2a 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:29:53:3d:34 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

gre0: flags=128<NOARP> mtu 1475
unspec 00-00-00-00-00-00-60-D0-00-00-00-00-00-00-00 txqueuelen 1 (UNSPEC)
RX packets 0 bytes 0 (0.0 B)

```

Figura 96 – Command Line Interface – less - exemplo.

```

gretap0: flags=4098<BROADCAST,MULTICAST> mtu 1462
ether 00:00:00:00:00:00 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 1 (Local Loopback)
RX packets 18263387 bytes 3479403782 (3.2 GiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 18263387 bytes 3479403782 (3.2 GiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

tun0: flags=4305<UP,POINTOPOINT,RUNNING,NOARP,MULTICAST> mtu 1500
inet 10.20.30.1 netmask 255.255.255.0 destination 10.20.30.1
unspec AC-10-66-4E-00-00-60-D0-00-00-00-00-00-00-00 txqueuelen 10000 (UNSPEC)
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
(END)

```

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] [-jnvDFKSV] 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.

```

dummy0: flags=130<BROADCAST,NOARP> mtu 1500
ether 8e:e0:1f:2a:14:d4 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

dummy1: flags=195<UP,BROADCAST,RUNNING,NOARP> mtu 2000
inet 192.168.222.1 netmask 255.255.255.0 broadcast 192.168.222.255
ether c6:7c:e0:39:30:b1 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

eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 172.16.102.78 netmask 255.255.255.0 broadcast 172.16.102.255
ether 00:0c:29:53:3d:16 txqueuelen 10000 (Ethernet)
RX packets 1734180 bytes 501763169 (478.5 MiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 1165992 bytes 448261438 (427.4 MiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

eth1: flags=4098<BROADCAST,MULTICAST> mtu 1500
ether 00:0c:29:53:3d:20 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:29:53:3d:2a 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:29:53:3d:34 txqueuelen 1000 (Ethernet)
RX packets 0 bytes 0 (0.0 B)
--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:

```

admin >mtr --help
usage: /usr/sbin/mtr [-BfhvrtglxspQomniuT46] [--help] [--version] [--report]
      [--report-wide] [--report-cycles=COUNT] [--curses] [--gtk]
      [--csv|-C] [--raw] [--xml] [--split] [--mpls] [--no-dns] [--show-ips]
      [--address interface] [--filename=FILE|-F]
      [--ipinfo=item_no|-y item_no]
      [--aslookup|-z]
      [--psize=bytes|-s bytes] [--order fields]
      [--report-wide|-w] [--inet] [--inet6] [--max-ttl=NUM] [--first-ttl=NUM]
      [--bitpattern=NUM] [--tos=NUM] [--udp] [--tcp] [--port=PORT] [--timeout=SECONDS]
      [--interval=SECONDS] HOSTNAME

```

Figura 105 – Command Line Interface – mtr.

Exemplo:

```
admin >mtr uol.com.br
```

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

```

bbv10-14.labsuporte.com.br (0.0.0.0)
Keys: Help Display mode Restart statistics Order of fields quit
Host
1. 172.16.102.1
2. 172.16.10.1
3. 192.168.5.1
4. ???
5. 187-100-40-101.dsl.telesp.net.br
6. 187-100-196-134.dsl.telesp.net.br
7. 187-100-53-182.dsl.telesp.net.br
8. ???
9. 200.221.136.174
10. home.uol.com.br

Packets
Loss% Snt Last Avg Best Wrst StDev
0.0% 7 1.5 1.5 1.4 1.6 0.0
0.0% 7 1.6 1.7 1.2 3.0 0.4
0.0% 7 1.2 1.2 1.0 1.5 0.0

Pings
Last Avg Best Wrst StDev
6.2 4.6 1.9 6.2 1.3
4.0 4.2 2.5 5.6 1.0
48.7 17.4 3.3 48.7 17.2
6.1 4.2 2.6 6.3 1.3
4.2 4.3 2.8 6.1 1.3

```

Figura 107 – Command Line Interface – mtr exemplo.

5.42 [netads]

Exibe e gerencia informações do servidor LDAP.

Modo de uso:

```

admin >netads --help
Usage:
net ads info
    Display details on remote ADS server
net ads join
    Join the local machine to ADS realm
net ads testjoin
    Validate machine account
net ads leave
    Remove the local machine from ADS
net ads status
    Display machine account details
net ads user
    List/modify users
net ads group
    List/modify groups
net ads dns
    Issue dynamic DNS update
net ads password
    Change user passwords
net ads changetrustpw
    Change trust account password
net ads printer
    List/modify printer entries
net ads search
    Issue LDAP search using filter
net ads dn
    Issue LDAP search by DN
net ads sid
    Issue LDAP search by SID
net ads workgroup
    Display the workgroup name
net ads lookup
    Find the ADS DC using CLDAP lookups
net ads keytab
    Manage local keytab file
net ads gpo
    Manage group policy objects
net ads kerberos
    Manage kerberos keytab
net ads encyptes
    List/modify encyptes

```

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:*               LISTEN
udp        0      0 0.0.0.0:67              0.0.0.0:*               LISTEN
udp        0      0 0.0.0.0:68              0.0.0.0:*               LISTEN
udp        0      0 0.0.0.0:123             0.0.0.0:*               LISTEN
udp        0      0 0.0.0.0:161             0.0.0.0:*               LISTEN
udp        0      0 0.0.0.0:4500            0.0.0.0:*               LISTEN
udp        0      0 0.0.0.0:500             0.0.0.0:*               LISTEN
udp        0      0 0.0.0.0:23375           0.0.0.0:*               LISTEN
udp        0      0 0.0.0.0:5353            0.0.0.0:*               LISTEN
udp        0      0 0.0.0.0:46602           0.0.0.0:*               LISTEN
udp        0      0 0.0.0.0:34387           0.0.0.0:*               LISTEN
udp        0      0 0.0.0.0:59050           0.0.0.0:*               LISTEN
udp6       0      0 :::123                  :::*                    LISTEN
udp6       0      0 :::4500                 :::*                    LISTEN
udp6       0      0 :::500                  :::*                    LISTEN
udp6       0      0 :::33636                :::*                    LISTEN
udp6       0      0 :::43923                :::*                    LISTEN
udp6       0      0 :::35941                :::*                    LISTEN
udp6       0      0 :::46196                :::*                    LISTEN
```

Figura 111 – Command Line Interface – netstat - exemplo.

5.44 [nslookup]

Envia pesquisas DNS para um servidor DNS remoto.

Modo de uso:

```
blockbit >nslookup exemplo.org 208.67.222.222
Server:      208.67.222.222
Address:     208.67.222.222#53

Non-authoritative answer:
Name:   exemplo.org
Address: 195.22.8.70

blockbit >█
```

Figura 113 – Command Line Interface – nslookup.

5.45 [ntptime]

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

Modo de uso:

```
blockbit >ntptime a.ntp.br
12 Sep 11:56:51 ntpdate[6923]: adjust time server 200.160.0.8 offset -0.000186 sec
blockbit >█
```

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:

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

5.60 [service-start]

Inicializa um determinado serviço.

Modo de uso:

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

Figura 128 – Command Line Interface – service-start.

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

5.61 [service-status]

Exibe o status de todos os serviços monitorados.

Modo de uso:

```

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

```

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
Irqlbalance 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
admin >
```

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:

```
admin >show-vpn-conn
tun1: #1, ESTABLISHED, IKEv1, 46b72d9f1eb1bde4:c90e3afe280a6bcf
local '200.200.100.101' @ 200.200.100.101[500]
remote '200.200.100.102' @ 200.200.100.102[500]
3DES_CBC/HMAC_SHA1_96/PRF_HMAC_SHA1/MODP_1024
established 14s ago, rekeying in 10308s
tun1: #1, reqid 1, INSTALLED, TUNNEL, ESP:3DES_CBC/HMAC_SHA1_96
installed 14s ago, rekeying in 3003s, expires in 3586s
in ce95e16d, 0 bytes, 0 packets
out c60db9a6, 0 bytes, 0 packets
local 192.168.200.0/24
remote 192.168.210.0/24
```

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:

```
admin >show-vpn-info
uptime: 16 seconds, since Mar 15 09:31:28 2018
malloc: sbrk 2703360, mmap 0, used 576032, free 2127328
worker threads: 11 of 16 idle, 5/0/0/0 working, job queue: 0/0/0/0, scheduled: 2
Listening IP addresses:
172.16.102.78
200.200.100.101
192.168.222.1
Connections:
tun1: 200.200.100.101...200.200.100.102,0.0.0.0/0,::/0 IKEv1
tun1: local: [200.200.100.101] uses pre-shared key authentication
tun1: remote: [200.200.100.102] uses pre-shared key authentication
tun1: child: 192.168.200.0/24 ==> 192.168.210.0/24 TUNNEL
Security Associations (1 up, 0 connecting):
tun1[1]: ESTABLISHED 16 seconds ago, 200.200.100.101[200.200.100.101]...200.200.100.102[200.200.100.102]
tun1[1]: IKEv1 SPIs: 46b72d9f1eb1bde4 i* c90e3afe280a6bcf r, rekeying in 2 hours
tun1[1]: IKE proposal: 3DES_CBC/HMAC_SHA1_96/PRF_HMAC_SHA1/MODP_1024
tun1[1]: INSTALLED, TUNNEL, reqid 1, ESP SPIs: ce95e16d i c60db9a6 o
tun1[1]: 3DES_CBC/HMAC_SHA1_96, 0 bytes_i, 0 bytes_o, rekeying in 50 minutes
tun1[1]: 192.168.200.0/24 ==> 192.168.210.0/24
```

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:

```
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 143 – Command Line Interface – speedtest - exemplo.

5.72 [sync-users]

Executa o sincronismo de usuários.

Modo de uso:

```
admin >sync-users
```

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 [-aAbdDefhHIJKLlNOpqRStuUvxx] [-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:

```

blockbit >tcpdump -i eth0 -nn
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 65535 bytes
13:55:48.261189 IP 172.16.102.136.22 > 172.16.100.15.59005: Flags [P.], seq 655814578:655814738, ack 1349706053, win 203, length 160
13:55:48.261316 IP 172.16.102.136.22 > 172.16.100.15.59005: Flags [P.], seq 160:240, ack 1, win 203, length 80
13:55:48.261359 IP 172.16.102.136.22 > 172.16.100.15.59005: Flags [P.], seq 240:288, ack 1, win 203, length 48
13:55:48.261404 IP 172.16.102.136.22 > 172.16.100.15.59005: Flags [P.], seq 288:336, ack 1, win 203, length 48
13:55:48.261445 IP 172.16.102.136.22 > 172.16.100.15.59005: Flags [P.], seq 336:384, ack 1, win 203, length 48
13:55:48.261477 IP 172.16.102.136.22 > 172.16.100.15.59005: Flags [P.], seq 384:432, ack 1, win 203, length 48
13:55:48.261491 IP 172.16.100.15.59005 > 172.16.102.136.22: Flags [I], ack 160, win 2048, length 0
13:55:48.261531 IP 172.16.102.136.22 > 172.16.100.15.59005: Flags [P.], seq 432:496, ack 1, win 203, length 64
13:55:48.261560 IP 172.16.102.136.22 > 172.16.100.15.59005: Flags [P.], seq 496:544, ack 1, win 203, length 48
13:55:48.261585 IP 172.16.102.136.22 > 172.16.100.15.59005: Flags [P.], seq 544:592, ack 1, win 203, length 48
13:55:48.261610 IP 172.16.102.136.22 > 172.16.100.15.59005: Flags [P.], seq 592:640, ack 1, win 203, length 48
13:55:48.261637 IP 172.16.102.136.22 > 172.16.100.15.59005: Flags [P.], seq 640:688, ack 1, win 203, length 48
13:55:48.261663 IP 172.16.102.136.22 > 172.16.100.15.59005: Flags [P.], seq 688:736, ack 1, win 203, length 48
13:55:48.261694 IP 172.16.102.136.22 > 172.16.100.15.59005: Flags [P.], seq 736:784, ack 1, win 203, length 48
13:55:48.261972 IP 172.16.100.15.59005 > 172.16.102.136.22: Flags [I], ack 640, win 2053, length 0
13:55:48.261978 IP 172.16.102.136.22 > 172.16.100.15.59005: Flags [P.], seq 784:832, ack 1, win 203, length 48

```

Figura 153 – Command Line Interface – tcpdump – Exemplo.

5.75 [tcptop]

Extraí 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:

```

Modo de uso
admin >tcptop
you must specify the interface: [eth0,eth1 ...]
admin >

```

Figura 154 – Command Line Interface – tcptop.

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

```

admin >tcptop eth1
Wait capturing frames ...
tcpdump: WARNING: eth1: no IPv4 address assigned
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth1, link-type EN10MB (Ethernet), capture size 65535 bytes
10000 packets captured
10070 packets received by filter
21 packets dropped by kernel
 3268 IP 177.185.5.137
 3090 IP 192.168.0.2
 1626 IP 192.168.3.2
  481 IP 201.86.139.109
  290 IP 8.8.8.8 > 192
  288 IP 192.168.3.2 > 8
  246 IP 201.31.172.3
admin >

```

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 [tracpath]

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 >tracpath -h
Usage: tracpath [-n] [-b] [-l <len>] [-p port] <destination>
blockbit >tracpath -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 – tracpath.

5.78 [traceroute]

Traça um caminho para um endereço de rede designado. O comando “traceroute” suporta alguns parâmetros avançados, o que o diferencia do “tracpath”, 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.

```

-t tos --tos=tos          Set the TOS (IPv4 type of service) or TC (IPv6
                           traffic class) value for outgoing packets
-l flow_label --flowlabel=flow_label
                           Use specified flow_label for IPv6 packets
-w waittime --wait=waittime
                           Set the number of seconds to wait for response
                           to a probe (default is 5.0). Non-integer (float
                           point) values allowed too
-q nqueries --queries=nqueries
                           Set the number of probes per each hop. Default is 3
-r                          Bypass the normal routing and send directly to a
                           host on an attached network
-s src_addr --source=src_addr
                           Use source src_addr for outgoing packets
-z sendwait --sendwait=sendwait
                           Minimal time interval between probes (default 0).
                           If the value is more than 10, then it specifies a
                           number in milliseconds, else it is a number of
                           seconds (float point values allowed too)
-e --extensions            how ICMP extensions (if present), including MPLS
-A --as-path-lookups       Perform AS path lookups in routing registries and
                           print results directly after the corresponding
                           addresses
-M name --module=name      Use specified module (either builtin or external)
                           for traceroute operations. Most methods have
                           their shortcuts ('-I' means '-M icmp' etc.)

-O OPTS,... --options=OPTS,...
                           Use module-specific option OPTS for the

```

Figura 161 – Command Line Interface – traceroute_2.

```

                           traceroute module. Several OPTS allowed,
                           separated by comma. If OPTS is "help", print
                           info about available options
--sport=num                Use source port num for outgoing packets.
                           Implies '-N 1'
--fwmark=num               Set firewall mark for outgoing packets
-U --udp                   Use UDP to particular port for tracerouting
                           (instead of increasing the port per each probe),
                           default port is 53
-UL                         Use UDPLITE for tracerouting (default dest port
                           is 53)
-D --dccp                  Use DCCP Request for tracerouting (default port
                           is 33434)
-P prot --protocol=prot    Use raw packet of protocol prot for tracerouting
--mtu                      Discover MTU along the path being traced. Implies
                           '-F -N 1'
--back                     Guess the number of hops in the backward path and
                           print if it differs
-V --version               Print version info and exit
--help                     Read this help and exit

Arguments:
+   host                   The host to traceroute to
    packetlen              The full packet length (default is the length of an IP
                           header plus 40). Can be ignored or increased to a minimal
                           allowed value
admin >

```

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 >tracert -n -p 53 -t 17 8.8.8.8
tracert 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:

```

admin >update-system
Loaded plugins: fastestmirror
bases-local                                | 2.9 kB  00:00:00
centos-local                               | 2.9 kB  00:00:00
elastic-local                              | 2.9 kB  00:00:00
epel-local                                 | 2.9 kB  00:00:00
lux-local                                  | 2.9 kB  00:00:00
utm-local                                  | 2.9 kB  00:00:00
Loading mirror speeds from cached hostfile
Metadata Cache Created
apply-update-s: running
apply-update-s: test connection on: updates.blockbit.com
apply-update-s: test connection on: license.blockbit.com
apply-update-s: update packages
Loaded plugins: fastestmirror
bases-local                                | 2.9 kB  00:00:00
centos-local                               | 2.9 kB  00:00:00
elastic-local                              | 2.9 kB  00:00:00
epel-local                                 | 2.9 kB  00:00:00
lux-local                                  | 2.9 kB  00:00:00
utm-local                                  | 2.9 kB  00:00:00
Loading mirror speeds from cached hostfile
No packages marked for update
apply-update-s: not found malwares in cache
apply-update-s: not found url's in cache
apply-update-s: finish

```

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    kB/s   avgrq-sz  avgqu-sz   await  r_await  w_await  svctm   %util
sda               0.00     0.15    0.51    0.91    9.60    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    0.66    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:

```
admin >watch-mem
```

Figura 151 – Command Line Interface – watch-mem.

Exemplo:

```
watch-mem: 07:31:04 up 1 day, 16:19, 2 users, load average: 0.04, 0.06, 0.05
              total      used      free      shared buff/cache   available
Mem:          4046896    1219144    2082484        317348        745268        2204372
Swap:         1751036     110496    1640540
```

press [CTRL+C] to stop

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:

```
admin >watch-srv
```

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: G00GLE.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.G00GLE.COM
Name Server: NS2.G00GLE.COM
Name Server: NS3.G00GLE.COM
Name Server: NS4.G00GLE.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]