Umbrella Virtual Appliance Commands

Contents

Introduction

Overview

clear

config

date

df

execute

free

help

iostat

netstat

nslookup

passwd

ping

ping6

reboot

tcptraceroute

traceroute

traceroute6

uptime

version

Introduction

This document describes the commands for the Umbrella Virtual Appliacnes (VAs).

Overview

The Umbrella VAs run on the Ubuntu operating system, which is a Linux distribution based on Debian. Not all of the commands typically available in Linux are available to customers within the VA's "Configuration Mode" command line. Instead, the VAs utilize a restricted shell environment which provides a number of troubleshooting / diagnostic commands, as well as config commands to change relevant settings within the VAs.

For more information about configuring the VAs using the Configuration Mode, see https://docs.umbrella.com/deployment-umbrella/docs/5-configuring-the-vas

The commands in this article are all available as of VA software version 3.4.



Note: The command descriptions cover the supported syntax on the VAs. Links are provided for many of the commands to a third party resource for additional information about the commands themselves. Please note that not all Linux command options are supported on the VAs.

clear

The **clear** command clears the terminal screen. It is the equivalent of "cls" in the Windows command prompt.

Note: This is not the command used to clear AD mappings.

config

config is used to configure the virtual appliances. There are nine subcommands for config:

- tunnel
- snmp
- anycast
- va
- ntp
- admap
- logexport
- localdns
- loadbalancer

```
You have entered the Configuration Mode on this VA. Use the 'config' command for any configuration c
hanges.
Type 'help' to get a list of supported commands.
test-VA-1 ~ $ config help
 Usage : config <commands> help
        tunnel          for tunnel commands
        snmp            for snmp commands
        anycast         for anycast commands
        va              for Virtual Appliance Configuration.
        ntp             for ntp configuration command
        admap           for admap commands
        logexport       for logexport configuration commands.
        localdns        for localdns configuration commands.
        loadbalancer    for configuring LoadBalancer that injects ECS.
```

5720351776404

1) The **tunnel** subcommand is used for enabling and configuring the support tunnels, similar to doing so via **Ctrl+B** from the VA console.

```
Home-VA-01 ~ $ config tunnel ?
 Usage : config tunnel <options> <args>

        options has to be one of the following -

        enable <int>      Enable the config tunnel connection.
        reenable <int>    ReEnable the config tunnel, if it was disabled.
        disable           Disable the config tunnel connection.
        status            Show status.
        -h, --help        Display this usage information.
        <int> is tunnel duration in hours, default would be 72 hours.
```

360037483772

Example commands:

```
config tunnel enable <optional time open, default is 72hrs, range is 7 to 240 hours>
config tunnel reenable <optional time open, default is 72hrs>
config tunnel disable
config tunnel status
```

For more information about configuring support tunnels, please see https://docs.umbrella.com/deployment-umbrella/docs/appendix-d-troubleshooting-the-va-using-a-restricted-shell#tunnel

2) The **snmp** subcommand is used for enabling and configuring SNMP support.

```
Home-VA-01 ~ $ config snmp ?
 Usage : config snmp <options> <args>

        options has to be one of the following -

        configure      -v2 [ -c <community string> ]
                           Enables SNMP v2
                           * c - Community string; Default public
                       -v3 -u <username> -p <password> [-a [MD5|SHA] -x [AES|DES] -X [password]]
                           Enables SNMP v3 with username and password
                           * u - Username consist of alphanumeric characters up to 32 characters.
                           * p - Password consist of alphanumeric characters 8 to 12 characters.
                           * a - Optional password hash algorithm; Default SHA
                           * x - Optional encryption algorithm; Default AES
                           * X - Privacy password to be used along with AES algorithm.

        enable         Enable the SNMP.
        disable        Disable the SNMP.
        status         Show SNMP service status and Version information.
        -h, --help     Display this usage information.
```

360037482211

Example commands:

```
config snmp enable
config snmp configure -v2 -c <community string>
config snmp status
```

For more information about configuring SNMP, please see https://docs.umbrella.com/deployment-umbrella/docs/appendix-c-enable-snmp-monitoring

3) The **anycast** subcommand is used to configure AnyCast BGP.

```
Home-VA-01 ~ $ config anycast ?
 Usage : config anycast bgp <options> <args>

         'bgp' options has to be one of the following:

         enable <anycast_ip> <bgp_info> : Enable the anycast mode.
         disable                        : Disable anycast mode.
         status                         : Show status of anycast.
         summary                        : Show BGP Summary
         stats                          : Show BGP Neighbour statistics
         add    <bgp_info>              : Add additional peer routers
         delete <router-ip>             : Delete additional peer routers
         test                           : Test anycast connectivity
         help                           : Display this usage information.

         args :
         anycast_ip : Anycast IP address
         bgp_info   : ASN:ROUTER-IP:HOP-COUNT of the BGP router to publish
         router-ip  : IP Address of the BGP Router

         Range :
         HOP-Count  : 2 - 255 Default: 255
```

360055492572

Example commands:

```
config anycast enable <anycast ip> <ASN:ROUTER-IP:HOP-COUNT of BGP router>
config anycast status
config anycast disable
config anycast stats
config anycast add <ASN:ROUTER-IP:HOP-COUNT of BGP router>
config anycast delete <BGP router IP address>
```

For more information about configuring AnyCast, please see https://docs.umbrella.com/deployment-umbrella/docs/appendix-e-other-configurations#anycast

4) The **va** subcommand is used for all of the routine configurations on the VAs.

```
Home-VA-01 ~ $ config va ?

       Usage : config va <commands> <args>

        commands has to be one of the following -
```

360055639691

```
        interface <interface name> <ipaddress> <netmask> <gateway> : Configure the Interface.
        interface6 <interface name> <ipv6-address>/<prefix> <gw>   : Configure the IPv6 address to
Interface
        name <string>                                              : Name of this Virtual Appliance
        show                                                       : Show running configuration.
        status                                                     : Display the status of this VA.
        ssh [ enable | disable ]                                   : Enable or Disable ssh access t
o VA
        dmz [ enable | disable ]                                   : Enable or Disable DMZ mode to
VA
        ssl [ enable | disable | ( [ key | cert ] "hash" ) ]       : Enable or Disable or Add Key a
nd cert for HTTPS
        per-ip-rate-limit [ enable <pps> <burst> | disable ]       : Configure the Per-IP based Rat
e Limiting to VA
        resolvers [US | US-v6 | global | global-v6 | alternate]    : Configure the root resolvers
        dnssec [ enable | disable ]                                : Enable or Disable DNSSEC for i
nternal domains
        help                                                       : Display this usage information
.

        args -
        ipaddress      : Ip Address for the interface
        netmask        : Netmask for the interface
        gateway        : Interface gateway ip address
        ipv6-address   : IPv6 Address for the interface
        prefix         : Prefix Length for IPv6 address
        gw             : IPv6 Gateway
        hash           : ssl/tls hash
        interface name : Name of the interface should be given when dual nic is enabled  Ex: eth0,
ens32
        pps            : Number of packets to be accepted per second for per IP. Range [ 10 - 10000
 ]
        burst          : Packet Burst rate. Range [ 10 - 100 ]
```

4417123559060

Example commands:

```
config va status
config va name <New name for the VA>
config va interface <interface name> <ip address> <subnet mask> <gateway>
config va interface6 <interface name> <IPv6 address/prefix> <IPv6 gateway>
config va show
config va ssh enable
config va dmz enable
config va dnssec enable
config va per-ip-rate-limit enable <packets/sec> <burst rate>
```

For more information about configuring rate-limiting, see https://docs.umbrella.com/deployment-umbrella/docs/appendix-e-other-configurations#section-configure-rate-limiting

For more information about configuring DNSSEC support, see https://docs.umbrella.com/deployment-umbrella/docs/appendix-e-other-configurations#section-configure-dnssec-support

It is also possible to configure the VAs to use specific resolvers using the **resolvers** subcommand, with these options being available:

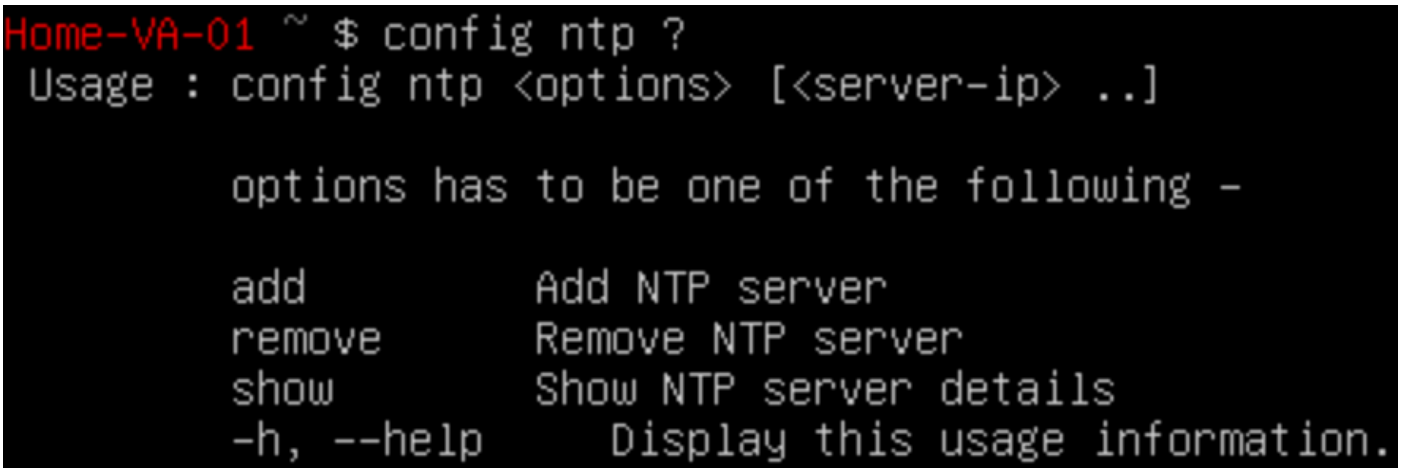
```
config va resolvers US (Uses 208.67.221.76 and 208.67.223.76)
```

```
config va resolvers US-v6 (Uses 2620:119:17::76 and 2620:119:76::76)

config va resolvers global (Uses 208.67.220.220 and 208.67.222.222)
config va resolvers global-v6 (Uses 2620:119:35::35 and 2620:119:53::53)
config va resolvers alternate (Uses 208.67.222.220 and 208.67.220.222)
```

For more information, see https://docs.umbrella.com/deployment-umbrella/docs/appendix-e-other-configurations#section-configure-umbrella-resolvers

5) The **ntp** subcommand can be used to define custom NTP servers on the VAs.



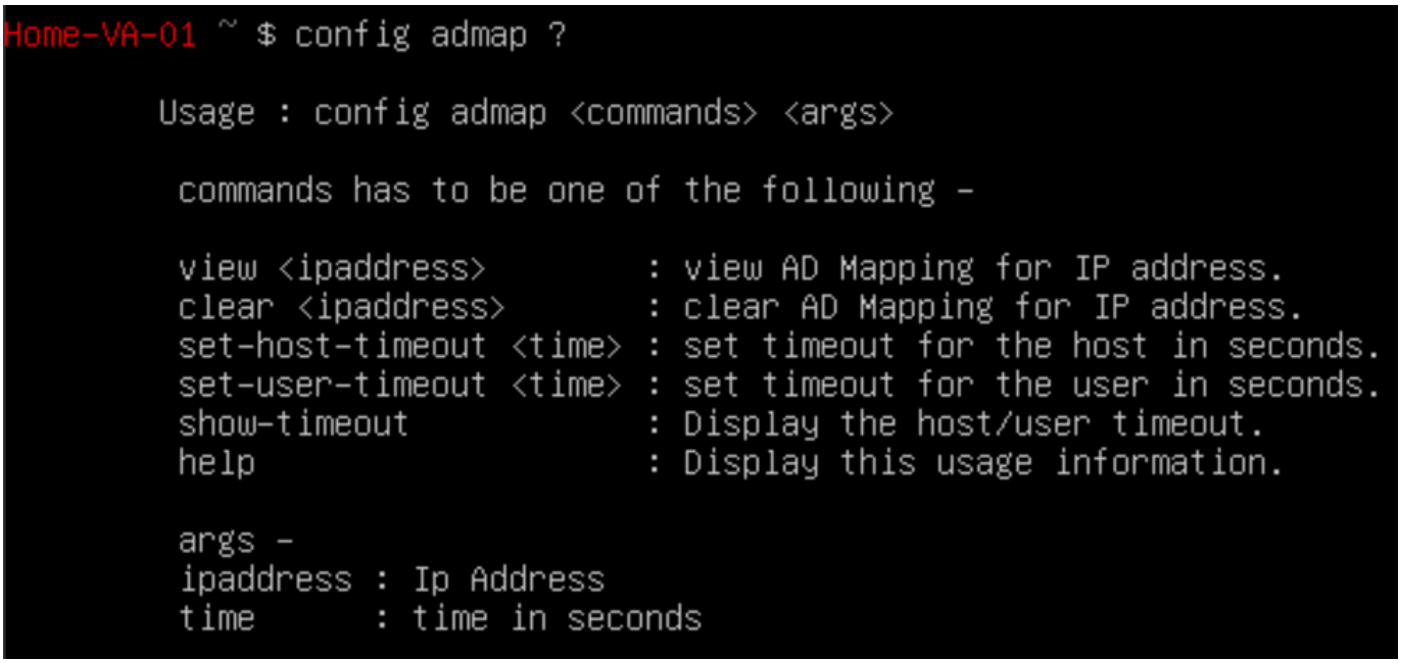
360055626811

Example commands:

```
config ntp add <New NTP server>
config ntp show
```

For more information, see https://docs.umbrella.com/deployment-umbrella/docs/appendix-e-other-configurations#section-configure-ntp-servers

6) The **admap** subcommand is the command used to configure identity association timeouts as well as viewing or clearing the AD Mapping. As this time, it is possible only to clear clear out the mappings of an individual IP address. There is not currently a way to clear all AD mappings from the restricted shell.



360037483672

Example commands:

```
config admap view <ip address>
config admap clear <ip address>
config admap set-user-timeout 28800 (This would set it for 8hrs)
config admap show-timeout
```

For more information, please see:

https://docs.umbrella.com/deployment-umbrella/docs/appendix-e-other-configurations#identity

Additional information can be found in these knowledge base articles:

Virtual Appliance: Manage/Delete Cached AD Users

Virtual Appliance: Tuning User Cache Settings

7) The **logexport** subcommand is used to export audit logs, health logs, and/or internal DNS request logs to a remote syslog server.

```
test-VA-1 ~ $ config logexport help
 Usage : config logexport <options> <args>

        options has to be one of the following -

        destination <rsyslog-ip:port> [tcp|udp|tls]    Add destination to send logs to remote serve
r.
        enable <service>                               Enable the service to send logs to destinati
on
        disable <service>                              Disable the service.
        [key|cert|ca] "hash"                           Add key, cert or CA hash for TLS
        status                                         Show logexport status.
        -h, --help                                     Display this usage information.

        args:
        service : internaldns | health | audit | all
```

4412434552084

For more information, please see:

https://docs.umbrella.com/deployment-umbrella/docs/appendix-e-other-configurations#syslog

The **localdns** subcommand is used to configure conditional forwarding of internal domains to specific internal DNS servers. It is new to version 3.2.

```
test-VA-1 ~ $ config localdns help
 Usage : config localdns <commands> <args>

        commands has to be one of the following -

        add <server-ip> <domains ... >  : Add new localdns server and map the domains
        remove <server-ip>              : Delete a localdns server
        show                            : Show current localdns server-domain mapping

        args -
        server-ip    : IPv4/IPv6 address for the localdns
        domains      : List of domains to be mapped to particular internal dns server.
                       Default value is all-internal-domains (domains configured in dashboard)
```

4417131713684

For more information, please run "config localdns help" or see:

https://docs.umbrella.com/deployment-umbrella/docs/6-local-dns-forwarding

9) The **loadbalancer** subcommand is used for configuring a LoadBalancer that injects ECS. It is new to version 3.3.

```
test-VA-1 ~ $ config loadbalancer help
 Usage : config loadbalancer <commands> <args>

        commands has to be one of the following -

        add <server-ip/prefix>          : Add new loadbalancer server
        remove <server-ip/prefix>       : Delete a loadbalancer server
        show                            : Show existing loadbalancers

        args -
        server-ip/prefix    : IPv4/IPv6 address for the loadbalancer (or) subnet/prefix_length
        Only loadbalancers that inject the source IP in the EDNS Client Subnet Field
        of the DNS query are supported.
        VA supports a maximum of 8 Load Balancer configurations.
```

5720280448276

For more information, please run "config loadbalancer help" or see:

https://docs.umbrella.com/deployment-umbrella/docs/appendix-e-other-configurations#section-configure-load-balancing

date

The **date** command can be used to print the current system time/date in the VA. The time is returned in Coordinated Universal Time (UTC). The date, time, and timezone cannot be reconfigured.

```
test-VA-1 ~ $ date
Wed Dec  8 23:03:01 UTC 2021
test-VA-1 ~ $
```

4412412915604

df

The **df** command can be used to display the current disk utilization of the VA.

For more information, see http://manpages.ubuntu.com/manpages/focal/en/man1/df.1.html

```
Home-VA-01 ~ $ df
Filesystem     1K-blocks    Used Available Use% Mounted on
udev              497232       4    497228   1% /dev
tmpfs             101564     876    100688   1% /run
/dev/sda1        2030736 1144928    764604  60% /
none                   4       0         4   0% /sys/fs/cgroup
none                5120       0      5120   0% /run/lock
none              507808       0    507808   0% /run/shm
none              102400       0    102400   0% /run/user
/dev/sda4        2030768  316300   1593260  17% /data
```

360037483652

execute

The **execute** command is available in newer build - version 3.4.6

Usage : execute <commands>
Commands have to be one of these:
force_upgrade : Perform "disk_cleanup" > re-download new VA image > force VA upgrade immediately.
disk_cleanup : Remove VA images, upgrade error files and Azure extension (no logs are removed).

free

The **free** command displays the amount of free and used memory in the system.

For more information, see http://manpages.ubuntu.com/manpages/focal/en/man1/free.1.html

```
Home-VA-01 ~ $ free
              total        used        free      shared  buff/cache   available
Mem:        1015616      518656      195716         172      301244      335340
Swap:        522108      131052      391056
```

360037482111

help

help can be used to display all of the commands available to the user within the restricted shell environment.

```
Home-VA-02 ~ $ help
Following is the list of commands available
clear  config  date  df  free  help  iostat  netstat  nslookup  passwd  ping ping6 tcptraceroute  tr
aceroute traceroute6 version
```

360055506372

Note: While help is supported, man is not, so you need to pull up any man pages you need elsewhere.

Links are included at the top of this article for each available command.

iostat

iostat displays CPU statistics and input/output statistics for devices and partitions.
For more information, see http://manpages.ubuntu.com/manpages/focal/en/man1/iostat.1.html

```
Home-VA-01 ~ $ iostat
Linux 4.8.0-53-generic (forwarder)      08/30/19        _x86_64_        (2 CPU)

avg-cpu:  %user   %nice %system %iowait  %steal   %idle
           0.47    0.00    0.47    0.01    0.00   99.04

Device:            tps    kB_read/s    kB_wrtn/s    kB_read    kB_wrtn
sda               0.79         1.07         5.84    3463273   18971540
sdb               0.00         0.00         0.00        406          0
```

360037482091

netstat

netstat prints network connections, routing tables, interface statistics, masquerade connections, and multicast memberships.

For more information, see http://manpages.ubuntu.com/manpages/focal/en/man8/netstat.8.html

```
Home-VA-01 ~ $ netstat
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 forwarder:42753         forwarder:domain        TIME_WAIT
tcp        0      0 192.168.1.223:19331     192.168.1.221:domain    TIME_WAIT
tcp        0      0 192.168.1.223:10221     resolver4.opendn:domain TIME_WAIT
tcp        0      0 forwarder:ssh           forwarder:54991         ESTABLISHED
tcp        0      0 192.168.1.223:36857     192.168.1.222:domain    TIME_WAIT
tcp        0      0 192.168.1.223:22499     resolver3.opendn:domain TIME_WAIT
tcp        0      0 192.168.1.223:18479     146.112.255.101:https   TIME_WAIT
tcp        0      0 192.168.1.223:33123     resolver1.opendn:domain TIME_WAIT
tcp        0      0 forwarder:54991         forwarder:ssh           ESTABLISHED
tcp        0      0 192.168.1.223:28423     resolver2.opendn:domain TIME_WAIT
Active UNIX domain sockets (w/o servers)
Proto RefCnt Flags       Type       State         I-Node   Path
unix  2      [ ]         DGRAM                    10612    /var/spool/postfix/dev/log
unix  7      [ ]         DGRAM                    10611    /dev/log
unix  3      [ ]         STREAM     CONNECTED     60456416
unix  3      [ ]         DGRAM                    10616
unix  3      [ ]         STREAM     CONNECTED     10700    @/com/ubuntu/upstart
unix  3      [ ]         STREAM     CONNECTED     10578    @/com/ubuntu/upstart
unix  2      [ ]         DGRAM                    60456413
unix  3      [ ]         STREAM     CONNECTED     9499
unix  3      [ ]         STREAM     CONNECTED     10698
unix  2      [ ]         DGRAM                    60455600
unix  3      [ ]         DGRAM                    10615
unix  3      [ ]         STREAM     CONNECTED     60456417
unix  2      [ ]         DGRAM                    11419
unix  2      [ ]         DGRAM                    60432351
unix  3      [ ]         STREAM     CONNECTED     10555    @/com/ubuntu/upstart
unix  2      [ ]         DGRAM                    60296865
unix  3      [ ]         STREAM     CONNECTED     10551
```

360037482051

nslookup

nslookup is used to query Internet name servers interactively. The command structure matches that of Windows, Mac, and Linux.

```
nslookup <domain>
```

Running a lookup using this syntax causes the VA to send the query to our public resolvers rather than to itself. In order to successfully perform a lookup for an internal domain, you need to specify your internal DNS server:

```
nslookup <Internal Domain> <Internal DNS Server IP>
```

To run an internal or external lookup from the VA against itself, you would run as follows:

```
nslookup <domain> 127.0.0.1
```

```
test-VA-1 ~ $ nslookup www.internetbadgirls.com.
Server:         127.0.0.1
Address:        127.0.0.1#53

Non-authoritative answer:
Name:   www.internetbadgirls.com
Address: 146.112.198.95
Name:   www.internetbadgirls.com
Address: ::ffff:146.112.198.95

test-VA-1 ~ $ nslookup www.examplemalwaredomain.com. 192.168.1.201
Server:         192.168.1.201
Address:        192.168.1.201#53

Non-authoritative answer:
Name:   www.examplemalwaredomain.com
Address: 146.112.61.107
Name:   www.examplemalwaredomain.com
Address: ::ffff:146.112.61.107

test-VA-1 ~ $ nslookup www.examplebotnetdomain.com. 127.0.0.1
Server:         127.0.0.1
Address:        127.0.0.1#53

Non-authoritative answer:
Name:   www.examplebotnetdomain.com
Address: 146.112.61.105
Name:   www.examplebotnetdomain.com
Address: ::ffff:146.112.61.105
```

4412413950484

For more information, see http://manpages.ubuntu.com/manpages/focal/en/man1/nslookup.1.html

passwd

passwd is used to reset the VA password. The syntax is as follows:

```
passwd
```

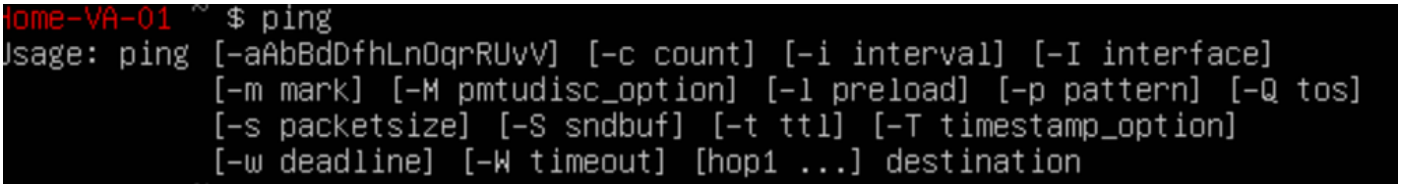
You are then be prompted for the old password, then the new one (twice). Alternatively, you can reset the password to the default via the Umbrella dashboard as detailed here.

```
test-VA-1 ~ $ passwd
Changing password for vmadmin.
Current password:
New password:
Retype new password:
passwd: password updated successfully
```

4412427409044

ping

The **ping** command is used to test connectivity, and the syntax again matches that found in Windows, Mac, and Linux. Available options are shown below.



360037482031

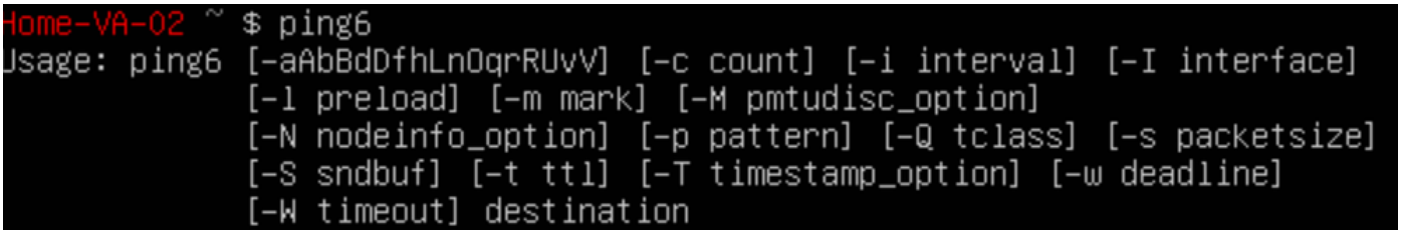
Most common usage would generally be as follows:

```
ping -c 4 <Domain or IP>
```

For more information, see http://manpages.ubuntu.com/manpages/focal/en/man1/ping.1.html

ping6

The **ping6** command is used to test connectivity to IPv6 endpoints, and the syntax again matches that found in Windows, Mac, and Linux. Available options are shown below.



360055639751

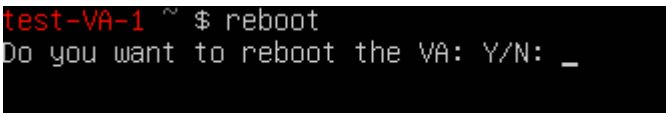
Most common usage would be as follows:

```
ping6 -c 4 <Domain or IPv6 address>
```

For more information, see http://manpages.ubuntu.com/manpages/focal/en/man1/ping6.1.html

reboot

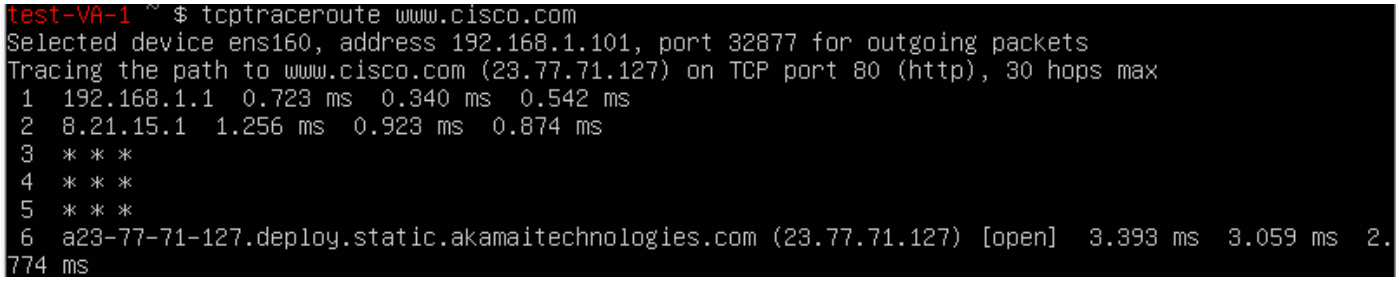
The **reboot** command reboots the VA. You are prompted to confirm the reboot (Y = yes) or cancel the reboot (N = no).



4412413584148

tcptraceroute

tcptraceroute send functions much the same as the standard traceroute command, however, it uses TCP packets instead of the standard UDP or ICMP packets.



4412426989332

For more information, see: https://manpages.ubuntu.com/manpages/focal/man1/tcptraceroute.mt.1.html

traceroute

traceroute can be used to test UDP and ICMP connectivity between two endpoints on different networks and provides information about each hop between them.
Most common usage would be as follows:

```
traceroute <domain or IP>
```

```
test-VA-1 ~ $ traceroute www.cisco.com
traceroute to www.cisco.com (23.77.71.127), 30 hops max, 60 byte packets
 1  * * *
 2  * * *
 3  * * *
 4  * * *
 5  * * *
 6  * * *
 7  * * *
 8  * * *
 9  * * *
10  * * *
11  * * *
12  * * *
13  * * *
14  * * *
15  * * *
16  * * *
17  * * *
18  * * *
19  * * *
20  * * *
21  * * *
22  * * *
23  * * *
24  * * *
25  * * *
26  * * *
27  * * *
28  * * *
29  * * *
30  * * *
test-VA-1 ~ $ _
```

4412413519508

For more information, see https://manpages.ubuntu.com/manpages/focal/en/man1/traceroute.db.1.html

traceroute6

traceroute6 can be used to test UDP and ICMP connectivity between two IPv6 endpoints on different networks and provides information about each hop between them.

For more information, see https://manpages.ubuntu.com/manpages/focal/man8/traceroute6.iputils.8.html

uptime

The **uptime** command shows the current time, how long the VA has been running, how many users are currently logged on, and the system load averages for the past 1, 5, and 15 minutes.

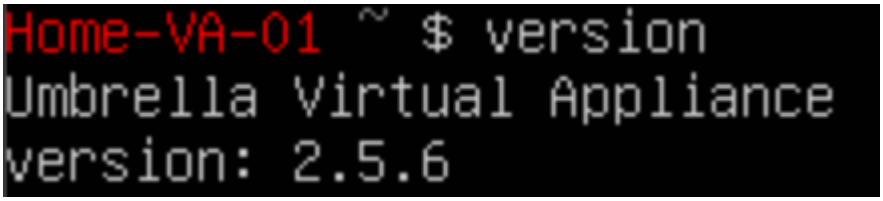
```
test-VA-1 ~ $ uptime
 23:25:33 up 42 days, 23:40,  2 users,  load average: 0.04, 0.20, 0.21
```

4412413617172

For more information, see https://manpages.ubuntu.com/manpages/focal/en/man1/uptime.1.html

version

version prints the current version of the VA software to the screen. This information is also available from the VA console.



360037481991