BHUTAN TELECOM

Last Updated: 20th Jan 2026

Prepared By -

Tetra Information Team

CAUTION

HA proxy Installation and configuration

BHUTAN TELECOM

SAME STEPS FOR BOTH SERVERS

10.10.100.137 mta1.bt.bt
10.10.100.141 mta2.bt.bt
10.10.100.132 haproxy1.bt.bt
10.10.100.133 haproxy2.bt.bt
10.10.100.132 (202.144.128.132) Public IP
10.10.100.133 (202.144.128.133) Public IP

202.144.128.134 Virtual IP

Reference Doc -
https://wiki.zimbra.com/wiki/Zimbra_Proxy_HA

Add the below entry in /etc/hosts

10.10.100.137 mta1.bt.bt
10.10.100.141 mta2.bt.bt
10.10.100.132 haproxy1.bt.bt
10.10.100.133 haproxy2.bt.bt

Install the HA proxy package

1. **apt install haproxy**

Install the keepalived package

1. **apt install keepalived**

Move the existing haproxy file to .bkp

1. **mv /etc/haproxy/haproxy.conf /etc/haproxy/haproxy.conf.bkp**

Create new file

1. **vi /etc/haproxy/haproxy.conf**

Add below configuration

```
global
        log /dev/log local0
        log /dev/log local1 notice
        chroot /var/lib/haproxy
        stats socket /run/admin.sock mode 660 level admin
        stats timeout 30s
        user haproxy
        group haproxy
        daemon
        tune.ssl.default-dh-param 2048

##############################
# HTTP DEFAULTS
##############################
defaults http
        log global
        mode http
        option httplog
        option dontlognull
        option http-server-close
```

```
        option forwardfor
        timeout connect 5s
        timeout client 50s
        timeout server 50s

##############################
# TCP DEFAULTS
##############################
defaults tcp
        log global
        mode tcp
        option tcplog
        timeout connect 5s
        timeout client 1m
        timeout server 1m

##############################
# HTTPS
##############################
frontend https-in
        bind *:443 ssl crt /etc/haproxy/certs/bundle.pem
        default_backend nginx-backend

backend nginx-backend
        mode http
        balance roundrobin
        http-request add-header X-Forwarded-Proto https
        http-request add-header X-Forwarded-Port 443
        cookie SERVER_USED insert indirect nocache
        server nginx1 10.10.100.137:443 check ssl verify none
        server nginx2 10.10.100.141:443 check ssl verify none

##############################
# SMTP SUBMISSION
##############################
```

```
frontend submission
        bind *:587
        default_backend bk_submission

backend bk_submission
        balance leastconn
        server submit1 10.10.100.137:587 check
        server submit2 10.10.100.141:587 check

##############################
# SMTPS
##############################
frontend smtps
        bind *:465
        default_backend bk_smtps

backend bk_smtps
        balance leastconn
        server smtps1 10.10.100.137:465 check
        server smtps2 10.10.100.141:465 check

##############################
# IMAP
##############################
frontend imap
        bind *:143
        default_backend bk_imap

backend bk_imap
        balance leastconn
        server imap1 10.10.100.137:143 check
        server imap2 10.10.100.141:143 check

##############################
# IMAPS
```

```
#############################
frontend imaps
        bind *:993
        default_backend bk_imaps

backend bk_imaps
        balance leastconn
        server imaps1 10.10.100.137:993 check
        server imaps2 10.10.100.141:993 check

#############################
# POP3S
#############################
frontend pop3s
        bind *:995
        default_backend bk_pop3s

backend bk_pop3s
        balance leastconn
        stick-table type ip size 200k expire 30m
        stick store-request src
        server pop3s1 10.10.100.137:995 check
        server pop3s2 10.10.100.141:995 check
```

—----------

mv existing keepalived configuration file to .bkp

1. mv /etc/keepalived/keepalived.conf /etc/keepalived/keepalived.conf.bkp

Create new conf file

1. **vi /etc/keepalived/keepalived.conf**

Add below configuration

```
global_defs {
   router_id ha1
   enable_script_security
}

vrrp_script haproxy_healthcheck {
   script "/usr/bin/pgrep haproxy"
   interval 2
   weight -2
   fall 2
   rise 2
}

vrrp_instance VI_1 {
   state MASTER
   interface ens13
   virtual_router_id 51
   priority 150
   advert_int 1

   authentication {
      auth_type PASS
      auth_pass redhat
   }

   virtual_ipaddress {
      202.144.128.134/25
   }
```

```
    track_script {
        haproxy_healthcheck
    }
}
```

Import the SSL file and change the path in the HAProxy configuration file

Restart service

```
systemctl  restart keepalived haproxy
systemctl  status keepalived haproxy
```

```
root@haproxy1:~# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
2: ens13: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether aa:00:00:54:88:e2 brd ff:ff:ff:ff:ff:ff
    altname enp0s13
    inet 202.144.128.132/25 brd 202.144.128.255 scope global ens13
       valid_lft forever preferred_lft forever
    inet 202.144.128.134/25 scope global secondary ens13
       valid_lft forever preferred_lft forever
3: ens14: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether aa:00:00:25:54:5a brd ff:ff:ff:ff:ff:ff
    altname enp0s14
    inet 10.10.100.132/24 brd 10.10.100.255 scope global ens14
       valid_lft forever preferred_lft forever
```