

HAProxy

Load Balancer

1.5.11

Integration Guide

CryptoServer HSM

SecurityServer 3.21.0

Imprint

Copyright 2026	Utimaco IS GmbH Krefelder Straße 220 52070 Aachen Germany
Phone	AMERICAS +1-844-UTIMACO (+1 844-884-6226) EMEA +49 800-627-3081 APAC +81 800-919-1301
Internet	https://support.hsm.utimaco.com/
e-mail	support@utimaco.com
Document Version	1.0.0
Date	2026-07-27
Status	PUBLISHED
Document No.	IG-2026-0083
All rights reserved	No part of this documentation may be reproduced in any form (printing, photocopy or according to any other process) without the written approval of Utimaco IS GmbH or be processed, reproduced or distributed using electronic systems. Utimaco IS GmbH reserves the right to modify or amend the documentation at any time without prior notice. Utimaco IS GmbH assumes no liability for typographical errors and damages incurred due to them. All trademarks and registered trademarks are the property of their respective owners.

Table of Contents

1 Introduction.....4

2 Requirements5

3 Installation6

4 Configuration.....7

5 Further Information.....12

6 Contact and Support Information13

1 Introduction

HAProxy is a free, very fast and reliable solution offering high availability, load balancing, and proxying for TCP and HTTP-based applications. It is particularly suited for very high traffic websites and powers quite a number of the world's most visited ones. Over the years it has become the defacto standard open-source load balancer, it is included with most mainstream Linux distributions and is often deployed by default in cloud platforms.

2 Requirements

You should have prepared an installed Ubuntu 14.04 operating system. If you are using a PCI(e) card, you also have to compile and install the necessary driver for that card.

Operating System	Ubuntu 14.04.2 LTS
HSM Model	CryptoServer CS-Series/S-Series/Se-Series LAN
HSM Firmware	SecurityServer 3.21.0
Software	HAProxy 1.5.11

Table 1: Software and hardware requirements

3 Installation

HA Proxy can be downloaded and installed by the Ubuntu package system. The version used for the present integration guide was HA Proxy 1.5.11. This version or higher is required to support binary health monitoring of the CryptoServer.

›_ Console

```
# sudo apt-get install haproxy
```

4 Configuration

To configure HA Proxy to use with the CryptoServer create or adjust the `/etc/haproxy/haproxy.cfg` file. The next configuration includes a setup of web GUI (e.g. HTTP port 9090) and socket for the CryptoServer load sharing (e.g. TCP 3100). It is possible to run HAProxy without web GUI but the current transfer statistics and status of the CryptoServer can be seen here.

global

```
log /dev/log local0
log /dev/log local1 notice
chroot /var/lib/haproxy
user haproxy
group haproxy
daemon
```

defaults

```
log global
mode http
option tcplog
option dontlognull
timeout connect 5000
timeout client 50000
timeout server 50000
errorfile 400 /etc/haproxy/errors/400.http
errorfile 403 /etc/haproxy/errors/403.http
errorfile 408 /etc/haproxy/errors/408.http
errorfile 500 /etc/haproxy/errors/500.http
```

```
errorfile 502 /etc/haproxy/errors/502.http
```

```
errorfile 503 /etc/haproxy/errors/503.http
```

```
errorfile 504 /etc/haproxy/errors/504.http
```

```
listen stats :9090
```

```
    balance
```

```
    mode http
```

```
    stats enable
```

```
    stats auth admin:admin
```

```
listen CryptoServerCluster :3100
```

```
    balance leastconn
```

```
    mode tcp
```

```
    option tcp-check
```

```
    tcp-check send-binary 9C00001400830100436865636B204865616C7468
```

```
    tcp-check expect binary 9A00001068746C616548206B63656843
```

```
server Erebus 192.168.0.10:288 check
```

```
server Aphrodite 192.168.0.11:288 check
```

```
server Apollo 192.168.0.12:288 check
```

```
server Eros 192.168.0.13:288 check
```

The cluster of CryptoServer that is used here is defined in the section CryptoServerCluster. Besides the ip address of CryptoServer it is possible to assign a name for this device. This name

HAProxy version 1.5.11, released 2015/01/31

Statistics Report for pid 16470

> General process information

pid = 16470 (process #1, nproc = 1) uptime = 31d 20h5m2s system limits: memmax = unlimited; ulimit-n = 4019 maxsock = 4019; maxconn = 2000; maxpipes = 0 current conns = 1; current pipes = 0/0; conn rate = 0/sec Running tasks: 1/1/1; size = 100 %																																
active UP active UP, going down active DOWN, going up active or backup DOWN active or backup DOWN for maintenance (MAINT) active or backup SOFT STOPPED for maintenance backup UP backup UP, going down backup DOWN, going up not checked Note: "NOLB"/"DRAIN" = UP with load-balancing disabled.																																
Display option: ☐ Scope: Primary site Updates (v1.6) Online manual Hide DOWN servers Refresh now CSV export																																
state																																
		Queue			Session rate				Sessions				Bytes		Denied		Errors		Warnings		Server											
		Cur	Max	Limit	Cur	Max	Limit	Cur	Max	Limit	Total	LbTot	Last	In	Out	Req	Resp	Req	Conn	Resp	Retr	Redis	Status	LastChk	Wght	Act	Bck	Chk	Dwn	Dwntime	Thrft	
Frontend					0	3	-	1	2	2	0000	122		82 130	2 214 385	0	0	16					OPEN									
Backend		0	0		0	2		0	1	200	110	0	0s	82 130	2 214 385	0	0		110	0	0	0	31d2h UP		0	0	0					

There are also other strategies available like roundrobin, static-rr and first. After editing the `/etc/haproxy/haproxy.cfg` configuration file you need to restart HA Proxy to get new settings effective.

› Console

```
# /etc/init.d/haproxy restart
```

To monitor the health of a CryptoServer device you can use the tcp-check send-binary and tcp-check expect binary feature of HA Proxy. HA Proxy sends a binary tcp request to a CryptoServer with tcpcheck send-binary and checks the answer of the CryptoServer with tcp-check expect binary. If the answer of the CryptoServer does not match the pattern 9A00001068746C616548206B63656843, HA Proxy does recognize the device as a faulty device. In this case the load is shared with the available other CryptoServer devices. If the faulty device is coming back properly checks from HA Proxy does run successfully then it will be integrated again in the cluster.



Data (including cryptographic keys) that is created, generated or imported internally of the CryptoServer is not automatically shared between other CryptoServer devices with HA Proxy solution.

The cluster of CryptoServer device is presented as single CryptoServer device from HA Proxy to a calling API or application. To address the cluster for first test you can use *csadm* to check the availability of the cluster.

›_ Console

```
# csadm dev=3100@10.17.72.9 GetState
mode = Operational Mode
state = INITIALIZED (0x00100004)
temp = 31.2 [C]
alarm = OFF
bl_ver = 3.00.0.3 (Model: Se-Series)
uid = cc000011 0c519501 | Q
adm1 = 53653130 30302020 43533431 33303431 | Se1000 CS413041
adm2 = 5554494d 41434f20 43533431 33303431 | UTIMACO CS413041
adm3 = 4d455247 45440000 00000000 00000000 | MERGED
# csadm dev=3100@10.17.72.9 GetState
mode = Operational Mode
state = OPERATIONAL (0x00000005)
temp = 35.0 [C]
alarm = OFF
bl_ver = 2.00.2.5 (Model: C/S-Series (Classic))
hw_ver = 2.00.2.0
uid = 81000010 5ec05101 | ^ Q
adm1 = 53313020 20202020 43533331 32363733 | S10 CS312673
adm2 = 53656375 72697479 53657276 65720000 | SecurityServer
adm3 = 496e6974 2d446576 2d312d4b 65790000 | Init-Dev-1-Key
```

In this example we called csadm to show that HA Proxy is sharing the load accordingly to our chosen load sharing strategy.

5 Further Information

This document forms a part of the information and support which is provided by Utimaco IS GmbH. Additional documentation can be found on the product CD in the documentation directory.

6 Contact and Support Information

You can reach us from Monday to Friday, 09.00 a.m. to 05.00 p.m., Central European Time (CET).

Utimaco IS GmbH
Krefelder Str. 220
52070 Aachen
Germany

RMA Query

If you need to send the device back to Utimaco IS GmbH, please open a new RMA case (Return Merchandise Authorization). We request that you use the following web address. RMA cases cannot be opened by email or phone.

<https://support.hsm.utimaco.com/support/rma/new>

Other Support Queries

- Mail (preferred contact method)
support@utimaco.com
Attach the diagnostic information to your email.
- Web portal
<https://support.hsm.utimaco.com/support/cases/new/>
The diagnostic information will be requested in our response if necessary.
- By phone
AMERICAS +1-844-UTIMACO (+1 844-884-6226)
EMEA +49 800-627-3081
APAC +81 800-919-1301
The diagnostic information will be requested in our response if necessary.