LEOSTREAM

Load Balancer

Installation and administration guide for spreading user connections across Leostream Connection Brokers.

Applies to	RHEL 9, Rocky 9, Alma 9 (64-bit)
Audience	System administrators
Requires	Two balancer servers and a Leostream Connection Broker

What it does

The Leostream Load Balancer spreads incoming user connections across several Leostream Connection Brokers.

You install it on two balancer servers. The two balancer servers share one IP address between them, called the virtual IP address. Your users connect to that one address. If the balancer server holding it fails, the other takes it over, usually within a few seconds.

Your users only ever see the virtual IP address. They do not see the balancer, and they do not need to know which Connection Broker they are using.

The balancer is made up of two parts you may see named in logs or service lists: HAProxy, which distributes the connections, and keepalived, which moves the virtual IP address between the two balancer servers.

What you need before you start

- **Two balancer servers** running RHEL 9, Rocky 9, or Alma 9, 64-bit. Both must be on the same subnet. They cannot be split across two sites.
- **One network interface per balancer server**, with a simple name such as `ens192`, and a default route on that interface. VLAN sub-interfaces, bonded interfaces, and bridges are not supported.
- **One unused IP address** on the same subnet as the two balancer servers. This becomes the virtual IP address.
- **At least two Leostream Connection Brokers**, reachable on port 443.
- **Root access** to both balancer servers.

Setup

Step 1. Reserve the virtual IP address and create a DNS name

Choose an IP address on the same subnet as your two balancer servers, and make sure nothing is using it:

```
ping -c2 <virtual IP address>
```

Nothing should answer.

Then create a DNS A record pointing your user-facing name at that address. This is the name your users will type. Check it from a user's machine:

```
dig +short <your DNS name>
```

It should return the virtual IP address.

Step 2. Check that your network allows the failover traffic

The two balancer servers pass VRRP between them to decide which one holds the virtual IP address. Ask your network team to confirm two things:

- IP protocol 112 is allowed between the two balancer servers.
- No other device on the same network segment is using VRRP router ID 51.

> IMPORTANT
>
> Firewalls and routers that run in pairs often use router ID 51 by default. If something else is already using it, the two balancer servers will not fail over correctly. The balancer always uses 51 and this cannot be changed, so the other device must be changed instead.

Step 3. Install the software on both balancer servers

Copy the balancer RPM to the first balancer server and install it:

```
sudo dnf install -y <balancer-rpm-filename>
```

Repeat on the second balancer server, then check the install on each:

```
sudo leostream-balancer --info
```

This reports the operating system, the version, and whether the balancer server is attached to a Connection Broker yet. At this stage it will say it is not attached. That is correct.

Step 4. Open the required ports

Open these:

- **Port 443**, from your users to the virtual IP address.
- **Port 443**, from each balancer server to each Connection Broker. The balancer checks each Connection Broker on this port. If it cannot reach one, it stops sending users to it.

Then close down port 8443. The installer opens it to every address, and you should narrow it:

- **Port 8443** should be reachable only from your Connection Brokers.

Port 8443 is how the Connection Broker configures the balancer. Your users never need it. Check from an ordinary user machine that port 8443 is not reachable.

Step 5. Broker setup

Both balancer servers and the virtual IP address are configured from the Connection Broker web interface.

Adding Balancers

High Availability › Load Balancers › Add Load Balancer › Save

Repeat for the second balancer server. Use each balancer server's own permanent IP address here, not the virtual IP address.

Adding Virtual IP in Broker

High Availability › Virtual IP › Add Virtual IP › Save

Enter the IP address, select the Connection Brokers, then select the balancers before saving.

> NO HIGH AVAILABILITY SECTION?
>
> If you do not see a High Availability section, your license may not include it. Contact Leostream Sales or Support to have it enabled.

Step 6. Check that it is working

On each balancer server:

```
sudo leostream-balancer --status
```

All three services should be running.

Find which balancer server currently holds the virtual IP address:

```
ip -4 addr show
```

The virtual IP address should appear on **one** of the two balancer servers, not both and not neither.

Finally, from a user machine, browse to your DNS name. A Connection Broker login page should load, and you should be able to log in. Setup is complete.

How users are assigned to a Connection Broker

The balancer decides which Connection Broker to use based on the IP address the user is coming from. The same address always goes to the same Connection Broker. This keeps a user on one Connection Broker for as long as their address does not change.

Two things follow from this, and both are worth checking before you go live.

Users are not spread evenly. Assignment is based on the address, not on a count of users. One Connection Broker may take more users than another. This is normal.

> CHECK THIS BEFORE YOU DEPLOY
>
> **Users sharing one address all go to the same Connection Broker.** If your users reach the balancer through a VPN, a NAT gateway, or a shared office internet connection, the balancer sees a single address for all of them and sends them all to the same Connection Broker.
>
> Check how your users reach the balancer before you deploy. If they all arrive from one address, the balancer cannot spread them.

Leostream Agent

The Leostream Agent runs on your desktops and talks to the Connection Broker. The two directions use different ports, and only one of them goes through the balancer.

DIRECTION	PORT	GOES THROUGH THE BALANCER?
Agent to Connection Broker	`443`	Yes
Connection Broker to Agent	`8080`	No. It goes straight to the desktop.

Point the Agent at the virtual IP address

In the Agent, set the Connection Broker address to your DNS name, the one that resolves to the virtual IP address. Do not set it to a single Connection Broker's own address.

The Agent connects on port 443, which the balancer handles. If the Connection Broker an Agent is using stops responding, the balancer sends that Agent to another one. An Agent pointed at a single Connection Broker has no way to recover if that Connection Broker goes down.

An Agent reaches the same Connection Broker each time, for the same reason users do. The balancer assigns it based on the address it is coming from.

Open port 8080 from each Connection Broker, not from the virtual IP address

The Connection Broker also contacts the Agent, on port 8080. This connection goes straight from the Connection Broker to the desktop. It does not pass through the balancer.

FIREWALL RULE

Port 8080 must be open to your desktops from **each Connection Broker's own IP address**. A rule that allows only the virtual IP address will not work, because the virtual IP address is never the source of this traffic.

Changing the list of Connection Brokers

You can add or remove Connection Brokers at any time from the Connection Broker web interface.

Applying the change restarts the load balancing service on the balancer. Users connected at that moment may be disconnected and may have to log in again. Because the assignment depends on how many Connection Brokers there are, users may also be moved to a different Connection Broker than before, including users who were not on the Connection Broker you changed.

Make these changes during a maintenance window.

Both balancer servers are active

Only one balancer server holds the virtual IP address at a time, but both are fully running. Both accept connections on their own IP addresses, and both check the health of every Connection Broker.

This means a user who browses directly to a balancer server's own address will reach a Connection Broker, bypassing the virtual IP address. If you do not want this, block the balancer servers' own addresses on port 443 at your network, and allow only the virtual IP address.

Commands

Run these as root on a balancer server.

COMMAND	WHAT IT DOES
`--info`	Operating system, version, and whether this balancer server is attached to a Connection Broker
`--status`	Whether each of the three services is running
`--start`	Start the services
`--stop`	Stop the services
`--logs`	Collect a log package to send to Leostream support
`--detach`	Detach this balancer server from the Connection Broker
`--help`	List the commands

For example: `sudo leostream-balancer --status`

If something is not working

Users cannot reach the login page

Check which balancer server holds the virtual IP address with `ip -4 addr show`. If neither has it, run `leostream-balancer --status` on both and start any service that is stopped.

Both balancer servers hold the virtual IP address

The two balancer servers cannot see each other's VRRP traffic. Re-check step 2 with your network team.

Everyone is sent to the same Connection Broker

First check that your users are not all arriving from one address, as described above. Then check the list of Connection Brokers the balancer is actually using:

```
cat /etc/haproxy/haproxy.cfg
```

Each Connection Broker should appear once, on its own `server` line, with the right IP address. Run this on the balancer server that holds the virtual IP address. If a Connection Broker is missing, apply the configuration again from the Connection Broker web interface.

One Connection Broker is getting no users

Check that the balancer can reach it on port 443. From the balancer server:

```
nc -vz -w3 <Connection Broker IP address> 443
```

If this fails, the balancer has marked that Connection Broker as unavailable and will not send users to it, even if the Connection Broker itself is running normally. The most common cause is a firewall rule that allows users to reach the Connection Broker but does not allow the balancer to reach it.

The Connection Broker cannot reach a desktop

Check that port 8080 is open to that desktop from the Connection Broker's own IP address. This traffic does not pass through the balancer, so a firewall rule written for the virtual IP address will not allow it.

Anything else

Run `leostream-balancer --logs` on both balancer servers and send the packages to Leostream support.