Load Balancing Fiserv DNA® SAF Server

v1.1.1
## Contents

1. About this Guide .......................................................................................................................... 3
2. Deployment .................................................................................................................................. 3
3. Initial Setup .................................................................................................................................. 4
   - Accessing the Loadbalancer.org Appliance ............................................................................. 4
   - Licensing Steps .......................................................................................................................... 4
   - Setup IP Addressing and Hostname ......................................................................................... 4
   - Setup Time Zone ....................................................................................................................... 5
4. Setting up the Virtual Service (VIP) ........................................................................................... 7
   - Define the Virtual Service .......................................................................................................... 7
   - Define the Associated Real Servers ......................................................................................... 8
5. Additional Information .................................................................................................................. 9
   - Health Checks ............................................................................................................................ 9
   - Built-in Layer 7 Checks .............................................................................................................. 9
   - ACL's ......................................................................................................................................... 10
   - Built-in ACL's ............................................................................................................................ 10
   - Built-in Actions .......................................................................................................................... 10
   - Use built-in ACL's via WebUI ..................................................................................................... 10
6. Testing HA Failover ........................................................................................................................ 12
   - Using the System Overview ....................................................................................................... 12
   - Using the HB_Takeover Command ........................................................................................... 12
7. Real Server Control ....................................................................................................................... 13
8. Recommended Product .................................................................................................................. 13
9. Supported Hypervisors .................................................................................................................. 14
10. Further Documentation ................................................................................................................ 15
11. Technical Support and Assistance ............................................................................................ 15
   - Accessing Technical Support ..................................................................................................... 15
   - Generating a Technical Support Download ............................................................................... 15
   - Uploading a Technical Support Download ............................................................................... 15
12. Document Revision History ......................................................................................................... 17

---

© Copyright Loadbalancer.org • www.loadbalancer.org • sales@loadbalancer.org
1. About this Guide
This guide details the steps required to configure a load balanced Fiserv DNA® SAF Server environment utilizing Loadbalancer.org appliances.

2. Deployment
The following section covers the most common deployment scenario.

SNAT mode is used as the default mode of operation. SNAT mode is achieved using a Layer 7 virtual service in TCP mode. In this deployment guide the load balancer and real servers are in the same subnet, although when using Layer 7 the real server can also be remote. When the Loadbalancer.org appliance receives a request from the client it will create a second connection to the real server with the source address becoming a load balancer IP. This creates two connections as described below:

Client ↔ VIP
LB ↔ Real Server

You can define the source address used for the connection between LB and Real Server or leave it blank (Default) allowing it to use the load balancer's base IP address.

Note: Should you choose to use a specific source address (SNAT Address) not already on the appliance then you will also need to add this IP address as an additional Floating IP to be used for this task.
3. Initial Setup

Note: We recommend using Firefox or Chrome web browsers for maximum compatibility.

Note: The load balancer will have a default IP address of 192.168.2.21/24.

Accessing the Loadbalancer.org Appliance

1. Login via the console using the following credentials to automatically start the Network Setup Wizard and configure the network settings:

   **Username**: setup
   **Password**: setup

2. Alternatively, open a web browser and use the default IP address:

   [https://192.168.2.21:9443/lbadmin](https://192.168.2.21:9443/lbadmin)

3. When prompted accept the self signed local SSL certificate.

4. Login to the WebUI using the following default credentials:

   **Username**: loadbalancer
   **Password**: loadbalancer

5. Once logged in, you can “Dismiss” the setup wizard prompt as it won't usually be used for this guide.

Licensing Steps

1. Navigate to **Local Configuration > License Key**

2. Now browse to and select the license key file provided

Setup IP Addressing and Hostname

Note: If you've already configured the base interface IP address using the setup utility (logged in as setup / setup) you may be able to skip these steps.
1. Navigate to Local Configuration > Network Interface Configuration in the WebUI
2. Optionally apply any interface bonding settings, configure VLAN tagging and set base interface IP addresses. You may configure multiple interfaces / VLAN’s if you desire a separate management network or more subnets.
3. Navigate to Local Configuration > Routing
4. Configure the IPv4 and/or IPv6 Default Gateway addresses and static routes (Optional)
5. Navigate to Local Configuration > Hostname and DNS to configure DNS servers and configure a hostname (Optional)

Setup Time Zone

1. Navigate to Local Configuration > System Time & Date
2. Select the System Timezone, provide any NTP servers and set the current Date and Time

Configuring a Highly Available Pair

Important:
- The HA pair (i.e. both Master and Slave) must be deployed at the same site.
- If you have more than one site, an HA pair should be deployed at each site.

1. Power up a second appliance that will be the slave and configure initial network settings as described earlier
2. In the WebUI of the master appliance, navigate to Cluster Configuration > High-Availability Configuration
3. Specify the IP address and the load balancer user's password (the default is 'loadbalancer') for the slave (peer) appliance
4. Click Add new node
5. A warning will be displayed indicating that the pairing process will overwrite the new slave appliance's existing configuration, click OK to continue
6. The pairing process now commences
7. Once complete, restart heartbeat as prompted in the blue message box

Note: The following settings are not replicated between master & slave appliances and must be configured on each appliance:
- Hostname & DNS settings
- Network settings including IP addresses, bonding configuration and VLANs
- Routing configuration including default gateways and static routes
- Date & time settings
• Physical – Advanced Configuration settings including Internet Proxy IP address & port, Firewall table size, SMTP relay and Syslog server
• SNMP settings
• Graphing settings
• Firewall Script & Firewall Lockdown Script settings
• Software updates

Note: The following network communication must be possible between appliances:

• The master and slave appliance must be able to perform an ICMP echo request (ping) to each other
• The master and slave appliance must be able to communicate with each other on TCP port 22
• The master and slave appliance must be able to communicate with each other on UDP port 6694 (or the selected custom port if this has been changed)

Set System Passwords/Protect Management Ports

Change System Passwords

WebUI
1. Navigate to Maintenance > Passwords in the WebUI.
2. Change the ‘loadbalancer’ user password.

CLI/SSH Password

1. Login via the CLI either directly or via SSH using the following default credentials:
   Username: root
   Password: loadbalancer

1. Run the following command to set the root password, enter the new password twice as prompted:
passwd

Firewall Lockdown Wizards

1. Navigate to Maintenance > Firewall Lockdown Wizard in the WebUI
2. Provide the management subnet or IP address, this will either be a subnet in CIDR format like 192.168.0.0/24 or
a single IP.

3. Click **Update**

**Running Lbsecure**
Alternatively, the appliance includes a security lockdown command (lbsecure) that enables passwords to be set, network access to be locked down and SSH key regeneration in one simple step. This command can be run on a single appliance or an HA pair. For more details please refer to page 67 of our full admin guide: [http://pdfs.loadbalancer.org/loadbalanceradministrationv8.pdf](http://pdfs.loadbalancer.org/loadbalanceradministrationv8.pdf)

**Ports Used By The Appliance**
The following TCP & UDP ports are used by the appliance:

**TCP:**
- 22 (SSH)
- 9080 (WUI – HTTP)
- 9081 (Nginx fallback page)
- 9443 (WUI – HTTPS)
- 7777 (HAProxy statistics page)
- 7778 (HAProxy persistence table replication)

**UDP:**
- 6694 (heartbeat between master/slave appliances in HA mode)

4. Setting up the Virtual Service (VIP)

**Define the Virtual Service**
1. Navigate to **Cluster Configuration > Layer 7 - Virtual Services**
2. Click **Add a new Virtual Service**
3. Enter the following details:
4. Enter an appropriate Label (name) for the Virtual Service, e.g. SAF-VIP
5. Enter an appropriate value for the Virtual Service IP address field, e.g. 192.168.156.5
6. Enter an appropriate value for the Virtual Service Ports field, e.g. 10001
7. Set Layer 7 Protocol to TCP Mode
8. Click Update to add the VIP
9. Click Modify next to the newly created VIP to set advanced options
10. Enable (tick) the Timeout option and supply the following values:
    - Client Timeout = 1h
    - Real Server Timeout = 1h
11. Click Update

Define the Associated Real Servers
1. Navigate to Cluster Configuration > Layer 7 - Real Servers
2. Click Add a new Real Server
3. Enter the following details:

4. Enter an appropriate Label (name) for the Real Server, e.g. Prodsaf01
5. Enter an appropriate value for the Real Server IP Address field, e.g. 192.168.156.10
6. Enter an appropriate value for the Real Server Port field, e.g. 10001
7. Click Update
8. Repeat as necessary until all Real Servers are added

Reload Haproxy
1. Once the Virtual Server and the associated Real Servers have been defined, HAProy must be reloaded to apply the new configuration. This can be done using the Reload HAProy button in the blue commit changes box at the top of the screen as shown below:
2. Once restarted, the VIP will be displayed in the system Overview as shown below:

![System Overview](image)

5. Additional Information

Health Checks

Note: By default a connect to port health check is used for newly created Virtual Services. You may however modify your Virtual Service to alter the default health check and use other options such as negotiate checks or external scripts.

Note: Custom external scripts can be used with the "external" check type. Scripts should be placed under "/var/lib/loadbalancer.org/check/" on the appliance and given world read and execute permissions. You can upload custom scripts using SCP (WinSCP for Windows) or write them directly on the appliance using an SSH session.

Built-in Layer 7 Checks

Layer 7 Health check options:

Connect to port – Just do a simple TCP connect to the specified port/service & verify that it’s able to accept a connection.

Negotiate HTTP (GET) – Sends an HTTP GET request and looks for a specific response. Also set the Request to Send & Response Expected fields.

Negotiate HTTPS (GET) – Sends an HTTP GET request using HTTPS and looks for a specific response. Also set the Request to Send & Response Expected fields. N.B. If a Negotiate check is selected and Response Expected is left blank, the appliance will check the location specified in Request to Send (if blank the root will be checked) and look for a 200
OK response from the real server.

**External Script** – use a custom file for the health check. Specify the script path in the Check Script field.

**MySQL** - The check consists of sending two MySQL packets, one Client Authentication packet, and one QUIT packet, to correctly close the MySQL session. It then parses the MySQL Handshake Initialization packet and/or Error packet. It is a basic but useful test and does not produce error nor aborted connect on the server. However, it does require adding an authorization in the MySQL table as follows: use mysql; INSERT INTO user (Host,User) values ('',''); flush privileges;
e.g. use mysql; INSERT INTO user (Host,User) values ('192.168.1.1','probe'); flush privileges;

No checks, always On – All Real Servers are on (i.e. no checking)

**ACL’s**

ACL’s can be used to redirect traffic to different URL’s and different backends. Some ACL’s are built into the WebUI while others are only accessible via a manual configuration. HTTP mode is needed for most ACL’s although IP based ACL’s such as “IP Block” can be used in TCP mode.

**Built-in ACL’s**

- **path_beg** - Identify traffic going to a specific URI, example: /static /images /css
- **path_end** - Identify traffic going to a specific URI, example: .gif .png .jpg
- **hdr_host** - Identify traffic going to a specific Host header, example: www.example.com
- **hdr_beg(Host)** - Identify traffic going to a specific subdomain, example: download. Test.
- **query** – Identify traffic by inspecting its query string, which starts after the first question mark. Example: uid=e33a0b&timestamp=1598615190
- **IP Block** - Identify traffic from a specific source IP or subnet, example: 192.168.0.1/24

**Built-in Actions**

- **Drop** - Drop the identified traffic by returning an HTTP 403 status code
- **URL Location** - Uses the exact value to redirect.
- **URL Prefix** - Uses the value to prefix the URL changing the domain posted but keeps the complete URI path intact.
- **Backend** - Matches an additional backend.
- **Use Server** - Send the identified traffic to the specified server by name (can also use the name of another layer 7 VIP)

**Use Built-in ACL’s Via WebUI**

1. Modify a VIP in HTTP mode then use the “Edit ACL Rules” button to access the ACL’s window.
2. Select “URL Select”, “Boolean”, “URL Text/IP”, “Redirect To” and “Redirect Location”
3. Click Add to add the rule and then “Save” to save the list.
4. Finally Click Update on the VIP and reload HAproxy to fully apply the configuration.

**Defining additional Manual Backends**

By default v8.2.3 and below only support a single pool of real servers per VIP unless you provide additional backends via manual configuration, from v8.3 and above the appliance will have better additional backend integration.
Setting Up Additional Backends

1. Add additional backends to the Layer 7 - Manual Configuration file in the WebUI.
2. Backends should look something like the following:

   ```
   backend test-additional-backend
   mode http
   balance leastconn
   cookie SERVERID insert nocache indirect
   server Server1 10.0.0.10:80 weight 100 cookie Server1 check inter 4000 rise 2 fall 2
   ```

3. Once the additional backend has been defined you can use ACL's in the WebUI or additional manual configuration to utilize the backend.

Retaining the Source IP, making things Source IP Transparent

As mentioned previously the default mode of operation is SNAT at Layer 7. In order to be source IP transparent you will require a two arm configuration. This means two subnets and having your real servers use the load balancer as their next hop (default gateway).

Setting Up L7 TPROXY

1. First be sure to have configured the load balancer in a two arm configuration, the VIP in one subnet and real servers in another
2. Add a floating IP on the real server subnet to be used as a floating default gateway using Cluster Configuration > Floating IP's
3. Set your real servers default gateway to the load balancer floating IP address

Option 1: To enable up TPROXY for a specific layer 7 virtual service on the load balancer:

1. Go to Cluster Configuration > Layer 7 Virtual Services and click Modify next to the virtual service in question
2. In the Other section, click Advanced to show more options
3. Enable the TPROXY service by checking the Transparent Proxy checkbox
4. Click Update to apply the change

Option 2: To enable up TPROXY globally on the load balancer:

1. Enable the TPROXY service by checking the Transparent Proxy checkbox from Cluster Configuration > Layer 7 - Advanced Configuration
2. Click Update to apply the change

SSL Offloading

Should you require SSL offloading at the load balancer you can do this using an SSL Termination. This is not our preferred config due to limitations with scaling but may be necessary to achieve Layer 7 manipulation of HTTP(s) traffic.
If required first make sure you have an HTTP (often port 80) Layer 7 VIP in place first then add an SSL Termination in front of it.

**Setting Up SSL Offloading**

1. Add a HTTP based VIP or modify an existing VIP removing port 443 to make it HTTP only. Optionally, also enable the “Enable Backend Encryption” checkbox if you want the connection to the backend to remain encrypted.
2. Upload your SSL Certificate from *Cluster Configuration > SSL Certificates*.
3. Add an SSL Termination from *Cluster Configuration > SSL Termination* selecting the certificate you uploaded earlier and setting the backend to the HTTP mode VIP configured in step 1.

**6. Testing HA Failover**

When configured as a clustered pair, the appliances work in Active-Passive mode. In this mode the active unit (normally the master) handles all traffic under normal circumstances. If the active unit fails, the passive unit (normally the slave) becomes active and handles all traffic. The failover process can be triggered on the passive device (normally the slave appliance) using the System Overview in the WebUI or by running the `hb_takeover` command.

**Using the System Overview**

To force the slave to become active & the master to become passive use the Take over button in the slave's System Overview:

Note: Click the [Advanced] link to show this button.

Once the slave is active, the same Take over button will be available on the passive master appliance and can be used in the same way to reverse the action.

**Using the HB_Takeover Command**

The following command can be used at the console, via SSH or via the WUI option: *Local Configuration > Execute Shell Command* to make the slave active and the master passive:
Once the salve is active, the same command can be used on the passive master appliance to reverse the action.

7. Real Server Control
The System Overview enables the state of each Real Server to be controlled. This is useful for performing Real Server maintenance tasks such as installing software updates. Real Servers can be put in the following modes:

- **Drain** – This option allows existing connections to close gracefully and prevents new connections
- **Halt** – This option prevents new connections and drops all existing connections immediately without waiting

The example below shows that server Prodsaf02 has been put into drain mode using the Drain option for that server.

![Real Server Control Example](image)

To bring Prodsaf02 back online, Online (drain) should be clicked. If the server had been halted rather than drained, then Online (halt) would be displayed rather than Online (drain).

Note: If a particular Real Server is used in multiple VIPs you can choose to apply the offline/online action to all relevant VIPs or only a single VIP. This simplifies taking Real Servers offline for maintenance purposes.

Note: Halting or draining all Real Servers in a cluster activates the fallback server.

8. Recommended Product
For deploying a load balanced highly-available DNA® SAF Server solution, Loadbalancer.org recommend a pair of Enterprise VA MAX, virtual load balancer licenses:


It is also advised that a 1 Years Premium 24/7 Support Contract is purchased with these licenses.
9. Supported Hypervisors
The Virtual Appliance is available for the following hypervisors:

<table>
<thead>
<tr>
<th>Hypervisor</th>
<th>Versions Supported</th>
</tr>
</thead>
<tbody>
<tr>
<td>VMware ESXi</td>
<td>v4.0 &amp; later</td>
</tr>
<tr>
<td>Microsoft Hyper-V</td>
<td>Windows 2012 &amp; later</td>
</tr>
<tr>
<td>XEN</td>
<td>v6.0 &amp; later</td>
</tr>
<tr>
<td>KVM</td>
<td>Kernel version 2.6.20 &amp; later</td>
</tr>
</tbody>
</table>

© Copyright Loadbalancer.org • www.loadbalancer.org • sales@loadbalancer.org
10. Further Documentation
The Administration Guide is available here: http://pdfs.loadbalancer.org/loadbalanceradministrationv8.pdf
Various Deployment Guides are available here: https://www.loadbalancer.org/resources/deployment-guides

11. Technical Support and Assistance

**Accessing Technical Support**
Loadbalancer.org have a team of very experienced support engineers who are available to assist with your load balancer deployments.

The best way to access technical support is via email: support@loadbalancer.org
Or or the support portal: https://support.loadbalancer.org/

We also offer phone support but due to the complexity of the appliance it's often best to start by opening a support case using email or our support portal and uploading a technical support download.

**Generating A Technical Support Download**
When contacting support you will usually be asked for a technical support download so they can review the configuration and logs, to create the Technical Support Download archive using the Web User Interface (WebUI):

1. In a web browser, open the WebUI of the Loadbalancer.org appliance
   (i.e. https://192.168.2.10:9443)
2. Navigate to the Support -> Technical Support Download page
3. Select the Generate Archive button, click the link which appears and save the file somewhere safe

**Uploading A Technical Support Download**
Should your Technical Support Download be too large to attach to an email you may use our site to upload and attach to your ticket. Please navigate to: https://support.loadbalancer.org/upload

When you email support@loadbalancer.org the automated system automatically replies with a ticket number in the format of "ABC-123-12345". You will need to use this ticket number along with the email address and help desk password that was used for the creation of your ticket. If you have never logged into our support portal before you will need to perform a password reset by using the link below.

Note: It is important that you do the password reset prior to attempting to upload the file as it will say there is no valid ticket if it can not match your email, password and ticket ID.

https://support.loadbalancer.org/index.php/?IBase/UserLostPassword/index

You will be asked for the password associated with your email address and if you have not previously logged into the help desk you will be prompted to perform a password reset before you are able to upload your support file.
You have the option to add a note to your upload, this should be something like "Master" or "Slave" to let us know what you have uploaded and where it came from.
12. Document Revision History

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Change</th>
<th>Reason for Change</th>
<th>Changed By</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1.0</td>
<td>30 August 2019</td>
<td>Styling and layout</td>
<td>General styling updates</td>
<td>AH</td>
</tr>
<tr>
<td>1.1.1</td>
<td>28 August 2020</td>
<td>New title page</td>
<td>Branding update</td>
<td>AH</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Updated Canadian contact details</td>
<td>Change to Canadian contact details</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Updated health check and ACL options</td>
<td>Changes to the appliance WebUI</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Amended instructions for enabling TPROXY to include new option for per-VIP TPROXY</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
About Loadbalancer.org

Loadbalancer.org's mission is to ensure that its clients' businesses are never interrupted. The load balancer experts ask the right questions to get to the heart of what matters, bringing a depth of understanding to each deployment. Experience enables Loadbalancer.org engineers to design less complex, unbreakable solutions - and to provide exceptional personalized support.