Load Balancing Fiserv DNA SAF Server

Version 2.1.0
# Table of Contents

1. About this Guide ........................................................................................................... 3
2. Loadbalancer.org Appliances Supported ........................................................................ 3
3. Software Versions Supported
   3.1. Loadbalancer.org Appliance .................................................................................. 3
   3.2. Fiserv DNA SAF Server ....................................................................................... 3
4. Fiserv DNA SAF Server ................................................................................................. 3
5. Load Balancing Fiserv DNA SAF Server
   5.1. Persistence (aka Server Affinity) ........................................................................... 3
   5.2. Virtual Service (VIP) Requirements ..................................................................... 4
   5.3. Port Requirements .............................................................................................. 4
6. Deployment Concept ..................................................................................................... 4
7. Loadbalancer.org Appliance – the Basics
   7.1. Virtual Appliance .................................................................................................. 4
   7.2. Initial Network Configuration ............................................................................... 5
   7.3. Accessing the Appliance WebUI
      Main Menu Options ................................................................................................. 6
   7.4. Appliance Software Update
      Determining the Current Software Version ............................................................. 7
      Checking for Updates using Online Update ............................................................... 7
      Using Offline Update ............................................................................................... 8
   7.5. Ports Used by the Appliance ............................................................................... 8
   7.6. HA Clustered Pair Configuration ......................................................................... 9
8. Appliance Configuration for Fiserv DNA SAF Server
   8.1. Configuring the Virtual Service (VIP) ................................................................ 9
   8.2. Defining the Real Servers (RIPs) ...................................................................... 10
   8.3. Finalizing the Configuration ................................................................................ 10
9. Testing & Verification .................................................................................................... 10
   9.1. Using System Overview ....................................................................................... 11
10. Technical Support ........................................................................................................ 11
11. Further Documentation ................................................................................................. 11
12. Appendix ...................................................................................................................... 12
   12.1. Configuring HA - Adding a Secondary Appliance
      Non-Replicated Settings ......................................................................................... 12
      Configuring the HA Clustered Pair ....................................................................... 13
13. Document Revision History ......................................................................................... 15
1. About this Guide

This guide details the steps required to configure a load balanced Fiserv DNA SAF Server environment utilizing Loadbalancer.org appliances. It covers the configuration of the load balancers and also any Fiserv DNA SAF Server configuration changes that are required to enable load balancing.

For more information about initial appliance deployment, network configuration and using the Web User Interface (WebUI), please also refer to the Administration Manual.

2. Loadbalancer.org Appliances Supported

All our products can be used with Fiserv DNA SAF Server. For full specifications of available models please refer to https://www.loadbalancer.org/products.

Some features may not be available or fully supported in all cloud platforms due to platform specific limitations. For more details, please refer to the "Main Differences to our Standard (Non-Cloud) Product" section in the appropriate cloud platform Quick Start Guide or check with Loadbalancer.org support.

3. Software Versions Supported

3.1. Loadbalancer.org Appliance

- V8.9.1 and later

Note: The screenshots used throughout this document aim to track the latest Loadbalancer.org software version. If you’re using an older version, or the very latest, the screenshots presented here may not match your WebUI exactly.

3.2. Fiserv DNA SAF Server

- All versions

4. Fiserv DNA SAF Server

Fiserv is a provider of financial services and technologies. Fiserv’s DNA SAF server is one part of their product offering. In order to make the service highly available and to ensure uptime, it is recommended to deploy multiple SAF servers and place a highly available pair of load balancers in front of them.

5. Load Balancing Fiserv DNA SAF Server

Note: It’s highly recommended that you have a working Fiserv DNA SAF Server environment first before implementing the load balancer.

5.1. Persistence (aka Server Affinity)

Source IP affinity is required for a load balanced Fiserv DNA SAF Server deployment to function correctly. This is
enabled by default when creating the virtual service as described in this document.

5.2. Virtual Service (VIP) Requirements
To provide load balancing and HA for Fiserv DNA SAF Server, only a single VIP is required:

- SAF

5.3. Port Requirements
The following table shows information regarding the port that is load balanced:

<table>
<thead>
<tr>
<th>Port</th>
<th>Protocols</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>10001</td>
<td>TCP</td>
<td>DNA SAF service</td>
</tr>
</tbody>
</table>

6. Deployment Concept

VIP = Virtual IP Address

VIP = Virtual IP Address

**Note**
The load balancer can be deployed as a single unit, although Loadbalancer.org recommends a clustered pair for resilience & high availability. Please refer to the section Configuring HA - Adding a Secondary Appliance in the appendix for more details on configuring a clustered pair.

7. Loadbalancer.org Appliance – the Basics

7.1. Virtual Appliance
A fully featured, fully supported 30 day trial is available if you are conducting a PoC (Proof of Concept) deployment. The VA is currently available for VMware, Virtual Box, Hyper-V, KVM, XEN and Nutanix AHV and has been optimized for each Hypervisor. By default, the VA is allocated 2 vCPUs, 4GB of RAM and has a 20GB virtual disk. The Virtual Appliance can be downloaded here.
The same download is used for the licensed product, the only difference is that a license key file (supplied by our sales team when the product is purchased) must be applied using the appliance’s WebUI.

Please refer to Virtual Appliance Installation and the ReadMe.txt text file included in the VA download for additional information on deploying the VA using the various Hypervisors.

The VA has 4 network adapters. For VMware only the first adapter (eth0) is connected by default. For HyperV, KVM, XEN and Nutanix AHV all adapters are disconnected by default. Use the network configuration screen within the Hypervisor to connect the required adapters.

7.2. Initial Network Configuration
After boot up, follow the instructions on the appliance console to configure the management IP address, subnet mask, default gateway, DNS servers and other network and administrative settings.

Be sure to set a secure password for the load balancer, when prompted during the setup routine.

7.3. Accessing the Appliance WebUI
The WebUI is accessed using a web browser. By default, users are authenticated using Apache authentication. Users can also be authenticated against LDAP, LDAPS, Active Directory or Radius - for more information, please refer to External Authentication.

There are certain differences when accessing the WebUI for the cloud appliances. For details, please refer to the relevant Quick Start / Configuration Guide.

1. Using a browser, navigate to the following URL:


You'll receive a warning about the WebUI’s SSL certificate. This is due to the default self signed certificate that is used. If preferred, you can upload your own certificate - for more information, please refer to Appliance Security Features.

If you need to change the port, IP address or protocol that the WebUI listens on, please refer to Service Socket Addresses.

2. Log in to the WebUI using the following credentials:

Username: loadbalancer
Password: <configured-during-network-setup-wizard>
To change the password, use the WebUI menu option: **Maintenance > Passwords.**

Once logged in, the WebUI will be displayed as shown below:

3. You’ll be asked if you want to run the Setup Wizard which can be used to configure layer 7 services. Click **Dismiss** if you’re following a guide or want to configure the appliance manually or click **Accept** to start the wizard.

**Main Menu Options**

- **System Overview** - Displays a graphical summary of all VIPs, RIPv and key appliance statistics
- **Local Configuration** - Configure local host settings such as IP address, DNS, system time etc.
- **Cluster Configuration** - Configure load balanced services such as VIPs & RIPv
- **Maintenance** - Perform maintenance tasks such as service restarts and taking backups
- **View Configuration** - Display the saved appliance configuration settings
7.4. Appliance Software Update

To ensure that the appliance(s) are running the latest software version, we recommend a software update check is performed.

Determining the Current Software Version

The software version is displayed at the bottom of the WebUI as shown in the example below:

![Version Example](image)

Checking for Updates using Online Update

1. Using the WebUI, navigate to: Maintenance > Software Update.
2. Select Online Update.
3. If the latest version is already installed, a message similar to the following will be displayed:
   
   **Information:** Version v8.11.1 is the current release. No updates are available

4. If an update is available, you'll be presented with a list of new features, improvements, bug fixes and security related updates.
5. Click Online Update to start the update process.

   **Note** Do not navigate away whilst the update is ongoing, this may cause the update to fail.

6. Once complete (the update can take several minutes depending on download speed and upgrade version) the following message will be displayed:
   
   **Information:** Update completed successfully.

7. If services need to be reloaded/restarted or the appliance needs a full restart, you'll be prompted accordingly.
Using Offline Update

If the load balancer does not have access to the Internet, offline update can be used.

Note

Please contact support@loadbalancer.org to check if an update is available and obtain the latest offline update files.

To perform an offline update:

1. Using the WebUI, navigate to: Maintenance > Software Update.
2. Select Offline Update.
3. The following screen will be displayed:

   Software Update

   Offline Update

   The following steps will lead you through offline update:
   1. Contact Loadbalancer.org support to obtain the offline update archive and checksum.
   2. Save the archive and checksum to your local machine.
   3. Select the archive and checksum files in the upload form below.
   4. Click Upload and Install to begin the update process.

4. Select the Archive and Checksum files.
5. Click Upload and Install.
6. If services need to be reloaded/restarted or the appliance needs a full restart, you'll be prompted accordingly.

7.5. Ports Used by the Appliance

By default, the appliance uses the following TCP & UDP ports:

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Port</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP</td>
<td>22 *</td>
<td>SSH</td>
</tr>
<tr>
<td>TCP &amp; UDP</td>
<td>53 *</td>
<td>DNS / GSLB</td>
</tr>
<tr>
<td>TCP &amp; UDP</td>
<td>123</td>
<td>NTP</td>
</tr>
<tr>
<td>TCP &amp; UDP</td>
<td>161 *</td>
<td>SNMP</td>
</tr>
<tr>
<td>UDP</td>
<td>6694</td>
<td>Heartbeat between Primary &amp; Secondary appliances in HA mode</td>
</tr>
<tr>
<td>TCP</td>
<td>7778</td>
<td>HAProxy persistence table replication</td>
</tr>
<tr>
<td>TCP</td>
<td>9000 *</td>
<td>Gateway service (Centralized/Portal Management)</td>
</tr>
</tbody>
</table>

© Copyright Loadbalancer.org • Documentation • Load Balancing Fiserv DNA SAF Server
## 7.6. HA Clustered Pair Configuration

Loadbalancer.org recommend that load balancer appliances are deployed in pairs for high availability. In this guide a single unit is deployed first, adding a secondary unit is covered in the section Configuring HA - Adding a Secondary Appliance of the appendix.

## 8. Appliance Configuration for Fiserv DNA SAF Server

### 8.1. Configuring the Virtual Service (VIP)

1. Using the web user interface, navigate to **Cluster Configuration > Layer 7 – Virtual Services** and click on **Add a new Virtual Service**.

2. Define the **Label** for the virtual service as required, e.g. **SAF_VIP**.

3. Set the **Virtual Service IP Address** field to the required IP address, e.g. **192.168.85.150**.

4. Set the **Ports** field to **10001**.

5. Set the **Layer 7 Protocol** to **TCP Mode**.

6. Click **Update** to create the virtual service.

7. Click **Modify** next to the newly created VIP.

8. In the **Other** section click **Advanced** to expand the menu.

---

### Service Socket Addresses

The ports used for SSH, GSLB, SNMP, the WebUI, the fallback page, the gateway service and the shuttle service can be changed if required. For more information, please refer to **Service Socket Addresses**.

```
<table>
<thead>
<tr>
<th>Protocol</th>
<th>Port</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP</td>
<td>9080</td>
<td>WebUI - HTTP (disabled by default)</td>
</tr>
<tr>
<td>TCP</td>
<td>9081</td>
<td>Nginx fallback page</td>
</tr>
<tr>
<td>TCP</td>
<td>9443</td>
<td>WebUI - HTTPS</td>
</tr>
<tr>
<td>TCP</td>
<td>25565</td>
<td>Shuttle service (Centralized/Portal Management)</td>
</tr>
</tbody>
</table>
```
9. Check the **Timeout** checkbox.

10. Set **Client Timeout** to **1h** (one hour).

11. Set **Real Server Timeout** to **1h** (one hour).

12. Click **Update**.

### 8.2. Defining the Real Servers (RIPs)

1. Using the web user interface, navigate to **Cluster Configuration > Layer 7 – Real Servers** and click on **Add a new Real Server** next to the newly created VIP.

2. Define the **Label** for the real server as required, e.g. **Prod_SAF_01**.

3. Set the **Real Server IP Address** field to the required IP address, e.g. **192.168.85.200**.

4. Click **Update**.

5. Repeat these steps to add additional servers as required.

### 8.3. Finalizing the Configuration

To apply the new settings, HAProxy must be reloaded. This can be done using the button in the "Commit changes" box at the top of the screen or by using the **Restart Services** menu option:

1. Using the WebUI, navigate to: **Maintenance > Restart Services**.

2. Click **Reload HAProxy**.

### 9. Testing & Verification
9.1. Using System Overview

The System Overview can be viewed in the WebUI. It shows a graphical view of all VIPs & RIPv (i.e. the Fiserv DNA SAF servers) and shows the state/health of each server as well as the state of the cluster as a whole. The example below shows that both DNA SAF servers are healthy and available to accept connections:

![System Overview Image]

10. Technical Support

For more details about configuring the appliance and assistance with designing your deployment please don’t hesitate to contact the support team using the following email address: support@loadbalancer.org.

11. Further Documentation

For additional information, please refer to the Administration Manual.
12. Appendix

12.1. Configuring HA - Adding a Secondary Appliance

Our recommended configuration is to use a clustered HA pair of load balancers to provide a highly available and resilient load balancing solution. We recommend that the Primary appliance is fully configured first, then the Secondary appliance can be added to create an HA pair. Once the HA pair is configured, load balanced services must be configured and modified on the Primary appliance. The Secondary appliance will be automatically kept in sync.

Note

For Enterprise Azure, the HA pair should be configured first. For more information, please refer to the Azure Quick Start/Configuration Guide available in the documentation library.

The clustered HA pair uses Heartbeat to determine the state of the other appliance. Should the active device (normally the Primary) suffer a failure, the passive device (normally the Secondary) will take over.

Non-Replicated Settings

A number of settings are not replicated as part of the Primary/Secondary pairing process and therefore must be manually configured on the Secondary appliance. These are listed by WebUI menu option in the table below:

<table>
<thead>
<tr>
<th>WebUI Main Menu Option</th>
<th>Sub Menu Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local Configuration</td>
<td>Hostname &amp; DNS</td>
<td>Hostname and DNS settings</td>
</tr>
<tr>
<td>Local Configuration</td>
<td>Network Interface Configuration</td>
<td>Interface IP addresses, bonding configuration and VLANs</td>
</tr>
<tr>
<td>Local Configuration</td>
<td>Routing</td>
<td>Default gateways and static routes</td>
</tr>
<tr>
<td>Local Configuration</td>
<td>System Date &amp; time</td>
<td>Time and date related settings</td>
</tr>
<tr>
<td>Local Configuration</td>
<td>Physical – Advanced Configuration</td>
<td>Various appliance settings</td>
</tr>
<tr>
<td>Local Configuration</td>
<td>Portal Management</td>
<td>Portal management settings</td>
</tr>
<tr>
<td>Local Configuration</td>
<td>Security</td>
<td>Security settings</td>
</tr>
<tr>
<td>Local Configuration</td>
<td>SNMP Configuration</td>
<td>SNMP settings</td>
</tr>
<tr>
<td>Local Configuration</td>
<td>Graphing</td>
<td>Graphing settings</td>
</tr>
<tr>
<td>Local Configuration</td>
<td>License Key</td>
<td>Appliance licensing</td>
</tr>
<tr>
<td>Maintenance</td>
<td>Backup &amp; Restore</td>
<td>Local XML backups</td>
</tr>
<tr>
<td>Maintenance</td>
<td>Software Updates</td>
<td>Appliance software updates</td>
</tr>
<tr>
<td>Maintenance</td>
<td>Fallback Page</td>
<td>Fallback page configuration</td>
</tr>
<tr>
<td>Maintenance</td>
<td>Firewall Script</td>
<td>Firewall (iptables) configuration</td>
</tr>
<tr>
<td>Maintenance</td>
<td>Firewall Lockdown Wizard</td>
<td>Appliance management lockdown settings</td>
</tr>
</tbody>
</table>
Important Make sure that where any of the above have been configured on the Primary appliance, they’re also configured on the Secondary.

Configuring the HA Clustered Pair

Note If you have already run the firewall lockdown wizard on either appliance, you’ll need to ensure that it is temporarily disabled on both appliances whilst performing the pairing process.

1. Deploy a second appliance that will be the Secondary and configure initial network settings.
2. Using the WebUI on the Primary appliance, navigate to: Cluster Configuration > High-Availability Configuration.

Create a Clustered Pair

3. Specify the IP address and the loadbalancer user’s password for the Secondary (peer) appliance as shown in the example above.
4. Click Add new node.
5. The pairing process now commences as shown below:

Create a Clustered Pair

6. Once complete, the following will be displayed on the Primary appliance:
To finalize the configuration, restart heartbeat and any other services as prompted in the "Commit changes" message box at the top of the screen.

**Note**
Clicking the **Restart Heartbeat** button on the Primary appliance will also automatically restart heartbeat on the Secondary appliance.

**Note**
For more details on configuring HA with 2 appliances, please refer to **Appliance Clustering for HA**.

**Note**
For details on testing and verifying HA, please refer to **Clustered Pair Diagnostics**.
<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>
<tr>
<td>2.0.0</td>
<td>7 February 2022</td>
<td>Completely reworked document into more typical format</td>
<td>Move to new documentation system</td>
<td>AH</td>
</tr>
<tr>
<td>2.0.1</td>
<td>28 September 2022</td>
<td>Updated layer 7 VIP and RIP creation screenshots</td>
<td>Reflect changes in the web user interface</td>
<td>AH</td>
</tr>
<tr>
<td>2.0.2</td>
<td>5 January 2023</td>
<td>Combined software version information into one section</td>
<td>Housekeeping across all documentation</td>
<td>AH</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Added one level of section numbering</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Added software update instructions</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Added table of ports used by the appliance</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Reworded 'Further Documentation' section</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Removed references to the colour of certain UI elements</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.0.3</td>
<td>2 February 2023</td>
<td>Updated screenshots</td>
<td>Branding update</td>
<td>AH</td>
</tr>
<tr>
<td>2.0.4</td>
<td>7 March 2023</td>
<td>Removed conclusion section</td>
<td>Updates across all documentation</td>
<td>AH</td>
</tr>
<tr>
<td>2.1.0</td>
<td>24 March 2023</td>
<td>New document theme</td>
<td>Branding update</td>
<td>AH</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Modified diagram colours</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.

Visit us: www.loadbalancer.org
Phone us: +44 (0)330 380 1064
Phone us: +1 833 274 2566
Email us: info@loadbalancer.org
Follow us: @loadbalancer.org