Load Balancing Fiserv DNA®connect
v1.0.0

Deployment Guide
1. About this Guide

This guide details the steps required to configure a load balanced Fiserv DNAconnect environment utilizing Loadbalancer.org appliances. It covers the configuration of the load balancers and also any Fiserv 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 relevant Administration Manual:

- [v7 Administration Manual](#)
- [v8 Administration Manual](#)

2. Loadbalancer.org Appliances Supported

All our products can be used for load balancing Fiserv DNA. The complete list of models is shown below:

<table>
<thead>
<tr>
<th>Discontinued Models</th>
<th>Current Models *</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enterprise R16</td>
<td>Enterprise R20</td>
</tr>
<tr>
<td>Enterprise VA R16</td>
<td>Enterprise MAX</td>
</tr>
<tr>
<td>Enterprise VA</td>
<td>Enterprise 10G</td>
</tr>
<tr>
<td>Enterprise R320</td>
<td>Enterprise 40G</td>
</tr>
<tr>
<td></td>
<td>Enterprise Ultra</td>
</tr>
<tr>
<td></td>
<td>Enterprise VA R20</td>
</tr>
<tr>
<td></td>
<td>Enterprise VA MAX</td>
</tr>
<tr>
<td></td>
<td>Enterprise AWS **</td>
</tr>
<tr>
<td></td>
<td>Enterprise AZURE **</td>
</tr>
<tr>
<td></td>
<td>Enterprise GCP **</td>
</tr>
</tbody>
</table>

* For full specifications of these models please refer to: [http://www.loadbalancer.org/products/hardware](http://www.loadbalancer.org/products/hardware)

** Some features may not be supported, please check with Loadbalancer.org support

3. Loadbalancer.org Software Versions Supported

- V76.4 and later

4. Fiserv DNAconnect Software Versions Supported

- Fiserv DNAconnect – All versions
5. Fiserv DNAconnect
DNAconnect – a suite of applications and services that facilitate the creation and processing of interfaces between different systems you can use to support communication between a source system and one or more target systems.

6. Load Balancing Fiserv DNAconnect
For high availability and scalability, Fiserv recommends that DNAconnect is deployed in load balanced clusters.

Port Requirements
The following table shows the ports that are load balanced:

<table>
<thead>
<tr>
<th>Ports</th>
<th>Protocol</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>80</td>
<td>TCP</td>
<td>HTTP - Fiserv</td>
</tr>
<tr>
<td>2500, 2501, 2507,</td>
<td>TCP</td>
<td>DNAconnect - Fiserv</td>
</tr>
<tr>
<td>2601, 2655, 2656,</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2999</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

7. Deployment Concept
When Fiserv services are deployed with the load balancer, clients connect to the Virtual Service (VIP) on the load balancer rather than connecting directly to one of the Fiserv servers. The load balancer then distributes these connections to the load balanced servers according to the algorithm selected.
8. Load Balancer Deployment Methods

For Fiserv DNAconnect, using Layer 4 DR mode is the recommended deployment method. When Using DR mode, the ‘ARP problem’ must be solved on each of the Fiserv servers for DR mode to work. For detailed steps please refer to the Administration manual, for your software version, under the section Configuring Load Balanced Services, The ARP Problem.

9. Configuring Fiserv DNAconnect for Load Balancing

Please refer to the Fiserv DNAconnect documentation for the configuration of the application. The following screenshot is an example from the Fiserv Runtime Environment console and shows the listening IP and associated settings.
Virtual Appliance Download & Deployment

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 and XEN and has been optimized for each Hypervisor. By default, the VA is allocated 1 CPU, 2GB of RAM and has an 8GB virtual disk. The Virtual Appliance can be downloaded here.

Note: 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.

Note: Please refer to the Administration Manual and the ReadMe.txt text file included in the VA download for more detailed information on deploying the VA using various Hypervisors.

Initial Network Configuration

The IP address, subnet mask, default gateway and DNS settings can be configured in several ways as detailed below:

**Method 1 - Using the Network Setup Wizard at the console**

After boot up, follow the instructions on the console to configure the IP address, subnet mask, default gateway and DNS settings.

**Method 2 - Using the WebUI**

Using a browser, connect to the WebUI on the default IP address/port: **https://192.168.2.21:9443**

To set the IP address & subnet mask, use: Local Configuration > Network Interface Configuration

To set the default gateway, use: Local Configuration > Routing

To configure DNS settings, use: Local Configuration > Hostname & DNS
**Accessing the Web User Interface (WebUI)**

The WebUI can be accessed via HTTPS at the following URL: **https://192.168.2.21:9443/lbadmin**

* Note the port number → **9443**

*(replace 192.168.2.21 with the IP address of your load balancer if it’s been changed from the default)*

Login using the following credentials:

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

Note: To change the password, use the WebUI menu option: Maintenance > Passwords.

Once logged in, the WebUI will be displayed as shown on the following page:
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 slave unit is covered in section 2 of the appendix on page 14.
Appliance Configuration

A) Setting Up The Virtual Service

1. Using the WebUI, navigate to Cluster Configuration > Layer 4 – Virtual Service and click Add a New Virtual Service
2. Enter the following details:

3. Enter an appropriate Label for the VIP, e.g. Fiserv DNAconnect
4. Set the Virtual Service IP Address to the required IP address, e.g. 192.168.1.30
5. Set the Virtual Service Ports field to 80,2500,2501,2507,2601,2655,2656,2999
6. Set layer 7 Protocol to TCP Mode
7. Click Update

Note: You can specify a wildcard (*) for all ports, instead on entering specific posts. This is covered in section 1 of the appendix, Adding a Wildcard, “*”, Instead of the Suggested Ports, on page 14.
B) Setting Up The Real Servers

1. Using the WebUI, navigate to Cluster Configuration > Layer 4 - Real Servers and click **Add a New Real Server**
2. Enter the following details:

   ![Layer 4 Add a new Real Server - Fiserv_DNAconnect](image)

   - Enter an appropriate **Label** for the RIP, e.g. **Server1**
   - Set the **Real Server IP address** field to the required IP address, e.g. **192.168.1.40**
   - Leave all other fields at their default values
   - Click **Update**
   - Repeat these steps to add the remaining servers

**Fiserv DNAconnect Configuration**

Since the VIP is configured using Layer 4 DR (Direct Return) mode, the ‘ARP Problem’ must be resolved on each Fiserv server, as mentioned in Section 8. For full details on how this is done, please refer to the Administration manual, for your software version, under the section Configuring Load Balanced Services, The ARP Problem.
12. Testing & Verification

Testing Load Balanced Services

As an example, to test a web server based configuration, add a page to each web server's root directory, e.g. test.html, and then put the server name on this page for easy identification during the tests.

Use two or more clients to carry out the testing. Open up a web browser on each test client and enter the URL for the VIP, e.g. http://104.40.133.119.

Provided that persistence is disabled, each client should see a different server name because of the load balancing algorithm in use, i.e. they are being load balanced across the cluster.

Why test using two clients? If you use a single client it will most likely keep hitting the same server for multiple requests. This is to do with the way that the load balancing algorithms are optimized.

Diagnosing VIP Connection Problems

1. Make sure that the device is active – This can be checked in the WebUI. For a single appliance, the status bar should report Master & Active as shown below:

   ![Status Bar Image]

2. Check that the Real Servers are up – Using System Overview make sure that none of your VIPs are colored red. If they are, the entire cluster is down (i.e. all Real Servers). Green indicates a healthy cluster, yellow indicates that your cluster may need attention (one or more of the Real Servers may be down), and blue indicates all Real Server have been deliberately taken offline (by using either Halt or Drain).

   ![System Overview Image]

3. Check the connection state - For layer 4 (NAT mode) VIPs, check Reports > Layer 4 Current Connections to view the current traffic in detail. Any packets with state SYN_RECV often implies a return traffic routing issue, so make sure that the routing rules for the real server subnet have been configured correctly.

   For Layer 7 VIPs, check Reports > Layer 7 Status. The default credentials required are:
username: loadbalancer
password: loadbalancer

This will open a second tab in the browser and display a statistics/status report as shown in the example below (this is accessed on port TCP/7777 so make sure that the inbound rules allow connections on this port):

Taking Real Servers Offline

1) Using the System Overview, check that when you Halt one of the Real Servers the connections are redirected to the other server in the cluster.

2) Stop the web service/process on one of the servers, wait a few seconds (for the load balancer to detect the change) and then refresh the browsers on both clients. They should now both switch to the same server (since one has been removed from the load balancing list). Also check that the server is shown red (down) in the system overview.

3) Start the web service/process on the server, wait a few seconds and then refresh the browsers again. After a few refreshes they should again show different web servers. Also check that the server is shown green (up) in the system overview.

The System Overview shows the status as these tests are performed:

In this example:

- **RIP1** is green, this indicates that it’s operating normally
- **RIP2** is blue, this indicates that it has been either Halted or Drained. In this example Halt has been used as indicated by **Online (Halt)** being displayed. If it had been drained it would show as **Online (Drain)**
- **RIP3** is red, this indicates that it has failed a health check
Using Reports & Log Files
The appliance includes several logs and reports that are very useful when diagnosing issues. Both are available as main menu options in the WebUI. Details of both can be found in the administration manual.

13. 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.

14. Further Documentation

15. Conclusion
Loadbalancer.org appliances provide a very cost effective solution for highly available load balanced Fiserv DNA environments.
16. Appendix

1 - Adding a Wildcard, “*”, Instead of the Suggested Ports

The specified ports (80, 2500, 2501, 2507, 2600, 2601, 2655, 2656, 2999) may vary between customer installations, so it is possible to allow all ports through the Layer 4 VIP by using the wildcard (*) in the ports section.

So, the VIP edited for the wildcard would look like this:

![Layer 4 - Modify Virtual Service](image)

Please note the warning at the top of the WebUI. As we now use the wildcard to access the VIP, the load balancer needs to choose a port for health-checking and automatically chooses the first one, 80.

If the automatically chosen port is unsuitable to use for health checking then please choose another port that can be checked against. To change the health checking port, modify the VIP like shown in this example which uses port 2501:

![Health Checks](image)

2 - Clustered Pair Configuration – Adding a Slave Unit

If you initially configured just the master unit and now need to add a slave - our recommended procedure, please refer to the relevant section below for more details:
Note: A number of settings are not replicated as part of the master/slave pairing process and therefore must be manually configured on the slave appliance. These are listed below:

- 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

Version 7:
Please refer to Chapter 8 – Appliance Clustering for HA in the v7 Administration Manual.

Version 8:
To add a slave node – i.e. create a highly available clustered pair:

- Deploy a second appliance that will be the slave and configure initial network settings
- Using the WebUI, navigate to: Cluster Configuration > High-Availability Configuration

```
Create a Clustered Pair

Local IP address
192.168.1.20

IP address of new peer
192.168.1.21

Password for loadbalancer user on peer

Add new node
```

- Specify the IP address and the loadbalancer users password (the default is 'loadbalancer') for the slave (peer) appliance as shown above
- Click Add new node
- The pairing process now commences as shown below:
Once complete, the following will be displayed:

To finalize the configuration, restart heartbeat and any other services as prompted in the blue message box at the top of the screen.

Note: Clicking the Restart Heartbeat button on the master appliance will also automatically restart heartbeat on the slave appliance.

Note: Please refer to chapter 9 – Appliance Clustering for HA in the Administration Manual for more detailed information on configuring HA with 2 appliances.
17. 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>1.0.0</td>
<td>3 July 2020</td>
<td>Initial version</td>
<td></td>
<td>RPC</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.