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 Administration Manual.

2. Loadbalancer.org Appliances Supported

All our products can be used for load balancing Fiserv DNA. For full specifications of available models please refer to https://www.loadbalancer.org/products. Some features may not be supported in all cloud platforms due to platform specific limitations, please check with Loadbalancer.org support for further details.

3. Loadbalancer.org Software Versions Supported

- V8.3.8 and later

Note: The screenshots used throughout this document aim to track the latest Loadbalancer.org software version. If using an older software version, note that the screenshots presented here may not match the WebUI exactly.

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, 2601, 2655, 2656, 2999</td>
<td>TCP</td>
<td>DNAconnect - Fiserv</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.
The load balancer can be deployed as a single unit, although Loadbalancer.org recommends a clustered pair for resilience & high availability. Please refer to Configuring HA - Adding a Secondary Appliance for more details on configuring a clustered pair.

8. Load Balancer Deployment Methods

For Fiserv DNAconnect, using Layer 4 DR mode is the recommended deployment method.

Layer 4 DR Mode

One-arm direct routing (DR) mode is a very high performance solution that requires little change to your existing infrastructure.

Note | Kemp, Brocade, Barracuda & A10 Networks call this Direct Server Return and F5 call it N-Path.

* DR mode works by changing the destination MAC address of the incoming packet to match the selected Real Server on the fly which is very fast.
• When the packet reaches the Real Server it expects the Real Server to own the Virtual Services IP address (VIP). This means that you need to ensure that the Real Server (and the load balanced application) respond to both the Real Server's own IP address and the VIP.

• The Real Servers should not respond to ARP requests for the VIP. Only the load balancer should do this. Configuring the Real Servers in this way is referred to as **Solving the ARP Problem**. For more information please refer to [DR Mode Considerations](#).

• On average, DR mode is 8 times quicker than NAT for HTTP, 50 times quicker for Terminal Services and much, much faster for streaming media or FTP.

• The load balancer must have an Interface in the same subnet as the Real Servers to ensure layer 2 connectivity required for DR mode to work.

• The VIP can be brought up on the same subnet as the Real Servers, or on a different subnet provided that the load balancer has an interface in that subnet.

• Port translation is not possible with DR mode, e.g. VIP:80 → RIP:8080 is not supported.

• DR mode is transparent, i.e. the Real Server will see the source IP address of the client.

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.

![Screenshot of Fiserv Runtime Environment console](image)

10. Loadbalancer.org Appliance – the Basics

**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](#).

<table>
<thead>
<tr>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>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.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>Please refer to <a href="#">Virtual Appliance Installation</a> and the ReadMe.txt text file included in the VA download for additional information on deploying the VA using the various Hypervisors.</td>
</tr>
</tbody>
</table>
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.

Initial Network Configuration

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

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

Accessing the WebUI

The WebUI is accessed using a web browser. By default, user authentication is based on local Apache .htaccess files. User administration tasks such as adding users and changing passwords can be performed using the WebUI menu option: Maintenance > Passwords.

Note
A number of compatibility issues have been found with various versions of Internet Explorer and Edge. The WebUI has been tested and verified using both Chrome & Firefox.

Note
If required, users can also be authenticated against LDAP, LDAPS, Active Directory or Radius. For more information please refer to External Authentication.

1. Using a browser, access the WebUI using the following URL:


2. Log in to the WebUI:

   **Username**: loadbalancer  
   **Password**: <configured-during-network-setup-wizard>

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

Once logged in, the WebUI will be displayed as shown below:
The WebUI for the VA is shown, the hardware and cloud appliances are very similar. The yellow licensing related message is platform & model dependent.

3. You'll be asked if you want to run the Setup Wizard. If you click Accept the Layer 7 Virtual Service configuration wizard will start. If you want to configure the appliance manually, simple click Dismiss.

Main Menu Options

- **System Overview** - Displays a graphical summary of all VIPs, RIPS 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 & RIPS
- **Maintenance** - Perform maintenance tasks such as service restarts and taking backups
- **View Configuration** - Display the saved appliance configuration settings
- **Reports** - View various appliance reports & graphs
- **Logs** - View various appliance logs
Support - Create a support download, contact the support team & access useful links
Live Chat - Start a live chat session with one of our Support Engineers

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 Configuring HA - Adding a Secondary Appliance.

11. Configuration for Fiserv DNAconnect

Appliance Configuration

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

   - **Label**: Fiserv DNAconnect
   - **IP Address**: 192.168.1.30
   - **Ports**: 80,2500,2501,2507,2601,2655
   - **Protocol**: TCP Mode
   - **Forwarding Method**: Direct Routing

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 ports. This is covered in Adding a Wildcard.

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)

3. Enter an appropriate *Label* for the RIP, e.g. *Server1*.

4. Set the *Real Server IP address* field to the required IP address, e.g. *192.168.1.40*.

5. Leave all other fields at their default values.

6. Click *Update*.

7. 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 solved on each Fiserv server as mentioned in *Load Balancer Deployment Methods*. For full details on how this is done, please refer to *DR Mode Considerations*.

12. Testing & Verification

   **Note**

   For additional guidance on diagnosing and resolving any issues you may have, please also refer to *Diagnostics & Troubleshooting*.

**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. *https://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 Primary & 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).

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, the Layer 7 statistics page can be used. To access the page, navigate to: Reports > Layer 7 Status - a new tabbed window will be displayed:

![Statistics Report](image)

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
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

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]

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]

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 should be configured first, then the Secondary should be added. Once the Primary and Secondary are paired, all load balanced services configured on the Primary are automatically...
replicated to the Secondary over the network using SSH/SCP.

Note
For Enterprise Azure, the HA pair should be configured first. In Azure, when creating a VIP using an HA pair, 2 private IPs must be specified – one for the VIP when it’s active on the Primary and one for the VIP when it’s active on the Secondary. Configuring the HA pair first, enables both IPs to be specified when the VIP is created.

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</td>
<td>All network settings including IP address(es), bonding configuration and VLANs</td>
</tr>
<tr>
<td>Local Configuration</td>
<td>Routing</td>
<td>Routing configuration including default gateways and static routes</td>
</tr>
<tr>
<td>Local Configuration</td>
<td>System Date &amp; time</td>
<td>All time and date related settings</td>
</tr>
<tr>
<td>Local Configuration</td>
<td>Physical – Advanced</td>
<td>Various settings including Internet Proxy, Management Gateway,</td>
</tr>
<tr>
<td></td>
<td>Configuration</td>
<td>Firewall connection tracking table size, NIC offloading, SMTP relay,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>logging and Syslog Server</td>
</tr>
<tr>
<td>Local Configuration</td>
<td>Security</td>
<td>Appliance security settings</td>
</tr>
<tr>
<td>Local Configuration</td>
<td>SNMP Configuration</td>
<td>Appliance SNMP settings</td>
</tr>
<tr>
<td>Local Configuration</td>
<td>Graphing</td>
<td>Appliance graphing settings</td>
</tr>
<tr>
<td>Local Configuration</td>
<td>License Key</td>
<td>Appliance licensing</td>
</tr>
<tr>
<td>Maintenance</td>
<td>Software Updates</td>
<td>Appliance software update management</td>
</tr>
<tr>
<td>Maintenance</td>
<td>Firewall Script</td>
<td>Appliance firewall (iptables) configuration</td>
</tr>
<tr>
<td>Maintenance</td>
<td>Firewall Lockdown</td>
<td>Appliance management lockdown settings</td>
</tr>
</tbody>
</table>

| Important              | Make sure that if these settings/updates have been configured on the Primary appliance, they’re also configured on the Secondary appliance. |

To add a Secondary node - i.e. create a highly available 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.
3. Specify the IP address and the loadbalancer user’s password for the Secondary (peer) appliance as shown above.

4. Click Add new node.

5. The pairing process now commences as shown below:

6. Once complete, the following will be displayed on the Primary appliance:

7. 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 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*. 


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>
<tr>
<td>1.1.0</td>
<td>1 January 2022</td>
<td>Converted the document to AsciiDoc</td>
<td>Move to new documentation system</td>
<td>AH, RJC, ZAC</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.