

Load Balancing Fiserv DNA®connect

Version 1.2.0



Table of Contents

| | |
|--|----|
| 1. About this Guide | 3 |
| 2. Loadbalancer.org Appliances Supported | 3 |
| 3. Software Versions Supported | 3 |
| 3.1. Loadbalancer.org Appliance | 3 |
| 3.2. Fiserv DNAconnect | 3 |
| 4. Fiserv DNAconnect | 3 |
| 5. Load Balancing Fiserv DNAconnect | 3 |
| 5.1. Port Requirements | 3 |
| 6. Deployment Concept | 4 |
| 7. Load Balancer Deployment Methods | 4 |
| 7.1. Layer 4 DR Mode | 4 |
| 8. Configuring Fiserv DNAconnect for Load Balancing | 5 |
| 9. Loadbalancer.org Appliance – the Basics | 6 |
| 9.1. Virtual Appliance | 6 |
| 9.2. Initial Network Configuration | 6 |
| 9.3. Accessing the Appliance WebUI | 6 |
| 9.3.1. Main Menu Options | 8 |
| 9.4. Appliance Software Update | 9 |
| 9.4.1. Online Update | 9 |
| 9.4.2. Offline Update | 9 |
| 9.5. Ports Used by the Appliance | 10 |
| 9.6. HA Clustered Pair Configuration | 11 |
| 10. Configuration for Fiserv DNAconnect | 11 |
| 10.1. Appliance Configuration | 11 |
| 10.1.1. A) Setting up the Virtual Service | 11 |
| 10.1.2. B) Setting up the Real Servers | 11 |
| 10.2. Fiserv DNAconnect Configuration | 12 |
| 11. Testing & Verification | 12 |
| 11.1. Using the System Overview | 12 |
| 12. Technical Support | 13 |
| 13. Further Documentation | 13 |
| 14. Appendix | 14 |
| 14.1. Adding a Wildcard, "*", Instead of the Suggested Ports | 14 |
| 14.2. Configuring HA - Adding a Secondary Appliance | 14 |
| 14.2.1. Non-Replicated Settings | 15 |
| 14.2.2. Configuring the HA Clustered Pair | 15 |
| 15. Document Revision History | 18 |

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/enterprise>.

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 DNAconnect

- All versions

4. 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.

5. Load Balancing Fiserv DNAconnect

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

5.1. Port Requirements

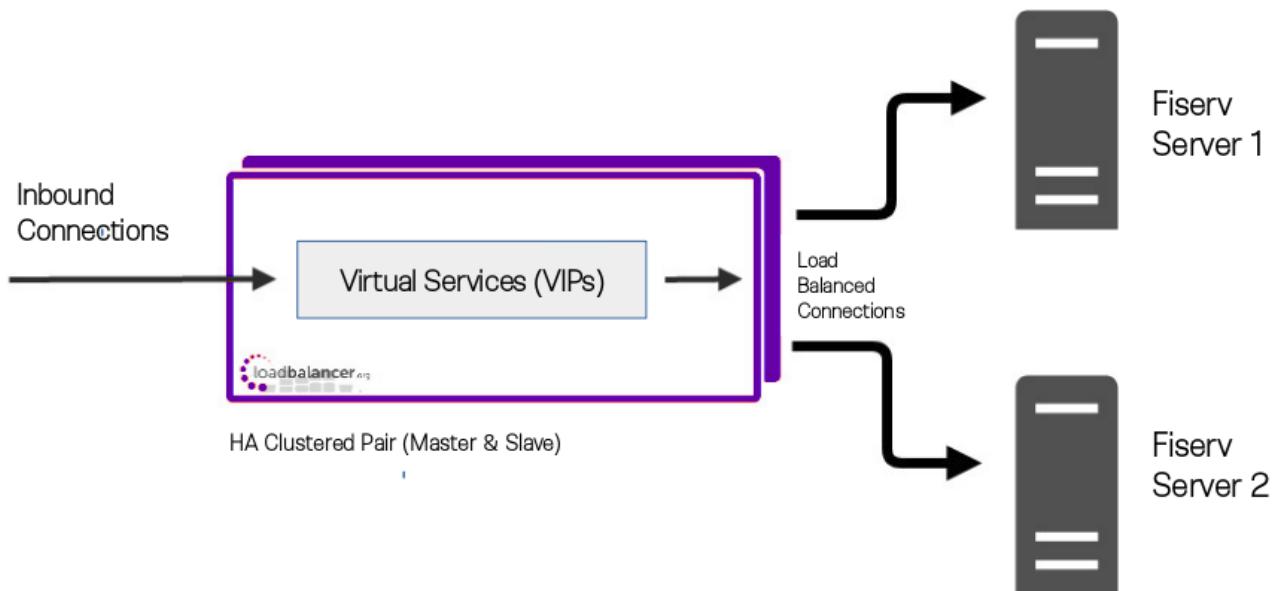
The following table shows the ports that are load balanced:



| Ports | Protocol | Use |
|--|----------|---------------------|
| 80 | TCP | HTTP - Fiserv |
| 2500, 2501, 2507, 2601, 2655, 2656, 2999 | TCP | DNAconnect - Fiserv |

6. 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.



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 [Configuring HA - Adding a Secondary Appliance](#) for more details on configuring a clustered pair.

7. Load Balancer Deployment Methods

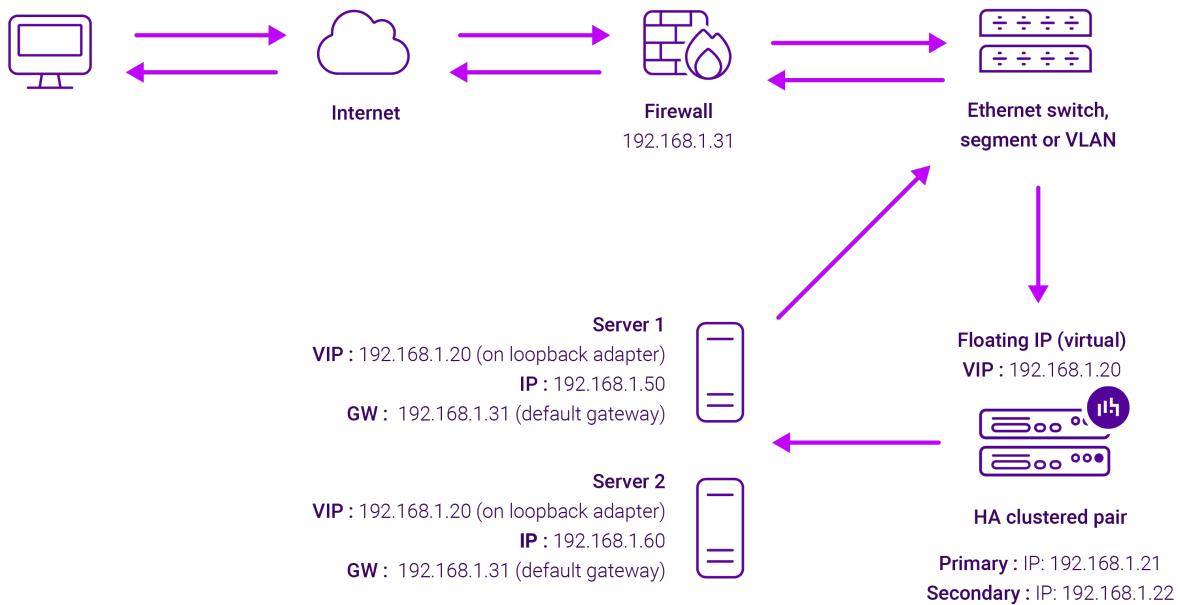
For Fiserv DNAconnect, using Layer 4 DR mode is the recommended deployment method.

7.1. Layer 4 DR Mode

Layer 4 DR (Direct Routing) mode is a very high performance solution that requires little change to your existing infrastructure. The image below shows an example network diagram for this mode.

Note

Kemp, Brocade, Barracuda & A10 Networks call this *Direct Server Return* and F5 call it *nPath*.

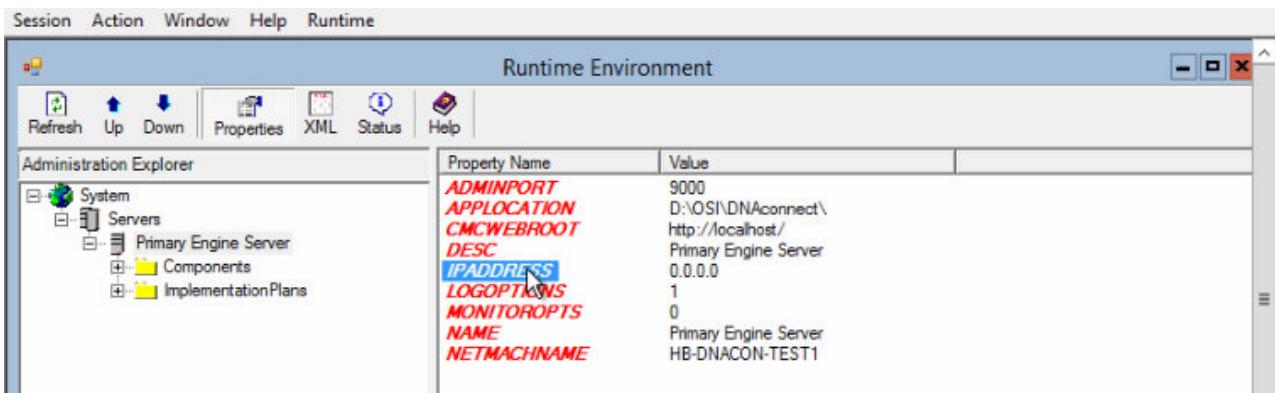


- DR mode works by changing the destination MAC address of the incoming packet to match the selected Real Server on the fly which is very fast.
- When the packet reaches the Real Server it expects the Real Server to own the Virtual Services IP address (VIP). This means that each Real Server (and the load balanced application) must respond to both the Real Server's own IP address and the VIP.
- The Real Server should not respond to ARP requests for the VIP. Only the load balancer should do this. Configuring the Real Server 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 mode for HTTP and much faster for other applications such as Remote Desktop Services, streaming media and FTP.
- The load balancer must have an interface in the same subnet as the Real Servers to ensure layer 2 connectivity which is required for DR mode to operate.
- 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.

8. 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.



9. Loadbalancer.org Appliance – the Basics

9.1. 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](#).

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 [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.

Note

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.

9.2. 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.

(!) Important

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

9.3. 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](#).

Note

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:

<https://<IP-address-configured-during-the-network-setup-wizard>:9443/lbadmin/>

 **Note** 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](#).

 **Note** 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>

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

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



Primary | Secondary Active | Passive Link 8 Seconds

System Overview

Local Configuration

Cluster Configuration

Maintenance

View Configuration

Reports

Logs

Support

Live Chat

WARNING: YOUR TRIAL IS DUE TO EXPIRE IN 30 DAYS.
Buy with confidence. All purchases come with a 90 day money back guarantee.
Already bought? Enter your license key [here](#)

Buy Now

System Overview 2025-05-08 12:37:21 UTC

Would you like to run the Setup Wizard?

Accept **Dismiss**

VIRTUAL SERVICE **IP** **PORTS** **CONN** **PROTOCOL** **METHOD** **MODE**

No Virtual Services configured.

Network Bandwidth

System Load Average

Memory Usage

3. You'll be asked if you want to run the Setup Wizard. Click **Dismiss** if you're following a guide or want to configure the appliance manually. Click **Accept** to start the Setup Wizard.



The Setup Wizard can only be used to configure Layer 7 services.

9.3.1. 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 creating 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

9.4. Appliance Software Update

We recommend that the appliance is kept up to date to ensure that you benefit from the latest bug fixes, security updates and feature improvements. Both online and offline update are supported.

 **Note**

For full details, please refer to [Appliance Software Update](#) in the Administration Manual.

 **Note**

Services may need to be restarted/reloaded after the update process completes or in some cases a full appliance restart may be required. We therefore recommend performing the update during a maintenance window.

9.4.1. Online Update

The appliance periodically contacts the Loadbalancer.org update server (**update.loadbalancer.org**) and checks for updates. This is the default behavior and can be disabled if preferred. If an update is found, a notification similar to the example below will be displayed at the top of the WebUI:

Information: Update 8.13.2 is now available for this appliance.

Online Update

Click **Online Update**. A summary of all new features, improvements, bug fixes and security updates included in the update will be displayed. Click **Update** at the bottom of the page to start the update process.

 **Important**

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

The update can take several minutes depending on download speed and upgrade version. Once complete, the following message will be displayed:

Information: Update completed successfully. Return to system overview.

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

9.4.2. Offline Update

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

To check for the latest version, please refer to our product roadmap page available [here](#). To obtain the latest offline update files contact support@loadbalancer.org.

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.

Archive: No file chosen

Checksum: No file chosen

Upload and Install

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.

9.5. Ports Used by the Appliance

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

| Protocol | Port | Purpose |
|-----------|---------|---|
| TCP | 22 * | SSH |
| TCP & UDP | 53 * | DNS / GSLB |
| TCP & UDP | 123 | NTP |
| TCP & UDP | 161 * | SNMP |
| UDP | 6694 | Heartbeat between Primary & Secondary appliances in HA mode |
| TCP | 7778 | HAProxy persistence table replication |
| TCP | 9000 * | Gateway service (Centralized/Portal Management) |
| TCP | 9080 * | WebUI - HTTP (disabled by default) |
| TCP | 9081 * | Nginx fallback page |
| TCP | 9443 * | WebUI - HTTPS |
| TCP | 25565 * | Shuttle service (Centralized/Portal Management) |

Note

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](#)



9.6. 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 [Configuring HA - Adding a Secondary Appliance](#).

10. Configuration for Fiserv DNAconnect

10.1. Appliance Configuration

10.1.1. 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:

| | | |
|------------------------|----------------------------|-----------------------------|
| Virtual Service | | |
| Label | Fiserv-DNAconnect | ? |
| IP Address | 192.168.1.30 | ? |
| Ports | 80,2500,2501,2507,2601,26! | ? |
| Protocol | | |
| Protocol | TCP | ? |
| Forwarding | | |
| Forwarding Method | Direct Routing | ? |
| | | Cancel Update |

3. Enter an appropriate *Label* for the VIP, e.g. **Fiserv-DNAconnect**.
4. Set the *IP Address* to the required IP address, e.g. **192.168.1.30**.
5. Set the *Ports* field to **80,2500,2501,2507,2601,2655,2656,2999**.
6. Leave the *Protocol* set to **TCP**.
7. Leave the *forwarding Method* set to **Direct Routing**.
8. Click **Update**.

Note

You can specify a wildcard (*) for all ports, instead on entering specific posts. This is covered in [Adding a Wildcard](#).

10.1.2. 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

| | | |
|------------------------|--------------|-----------------------------|
| Label | Server1 | ? |
| Real Server IP Address | 192.168.1.40 | ? |
| Weight | 100 | ? |
| Minimum Connections | 0 | ? |
| Maximum Connections | 0 | ? |
| | | Cancel Update |

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.

10.2. Fiserv DNAconnect Configuration

Layer 4 DR mode VIPs require the 'ARP problem' to be solved on each associated Fiserv server as mentioned in Load Balancer Deployment Methods. For full details on how this is done, please refer to [DR Mode Considerations](#).

11. Testing & Verification

Note

For additional guidance on diagnosing and resolving any issues you may have, please also refer to [Diagnostics & Troubleshooting](#).

11.1. Using the System Overview

The System Overview can be accessed via the WebUI. It shows a graphical view of all VIPs & RIPs (i.e. the Fiserv DNAConnect 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 all Fiserv servers are healthy (green) and available to accept connections:



System Overview

2023-01-05 14:18:01 UTC

| VIRTUAL SERVICE | IP | PORTS | CONN | PROTOCOL | METHOD | MODE |
|---|--------------|--------------|--------|----------|---------|------|
| REAL SERVER | IP | PORTS | WEIGHT | CONN | | |
|  Fiserv-DNAconnect.. | 192.168.1.30 | 80,2500,2.. | 0 | TCP | Layer 4 | DR |
|  Server1 | 192.168.1.40 | 80,2500,25.. | 100 | 0 | Drain | Halt |
|  Server2 | 192.168.1.41 | 80,2500,25.. | 100 | 0 | Drain | Halt |

If one of the servers within the cluster fails its health check, that server will be colored red and the cluster will be colored yellow as shown below:

System Overview

2023-01-05 14:18:01 UTC

| VIRTUAL SERVICE | IP | PORTS | CONN | PROTOCOL | METHOD | MODE |
|---|--------------|--------------|--------|----------|---------|------|
| REAL SERVER | IP | PORTS | WEIGHT | CONN | | |
|  Fiserv-DNAconnect.. | 192.168.1.30 | 80,2500,2.. | 0 | TCP | Layer 4 | DR |
|  Server1 | 192.168.1.40 | 80,2500,25.. | 100 | 0 | Drain | Halt |
|  Server2 | 192.168.1.41 | 80,2500,25.. | 100 | 0 | Drain | Halt |

Make sure that all servers are up (green) and verify that clients can connect to the VIP and access all load balanced services.

 Note

Make sure that DNS points at the VIP rather than individual servers.

12. 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.

13. Further Documentation

For additional information, please refer to the [Administration Manual](#).



14. Appendix

14.1. 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:

WARNING: With the current configuration, a port must be set for the Real Server health checks. A default Check Port of 80 has been chosen.

Layer 4 - Modify Virtual Service

Virtual Service

| | | |
|------------|-------------------|---|
| Label | Fiserv DNAconnect | ? |
| IP Address | 192.168.1.30 | ? |
| Ports | * | ? |

IP Protocol

| | | |
|----------|-----|---|
| Protocol | TCP | ? |
|----------|-----|---|

Forwarding

| | | |
|-------------------|----------------|---|
| Forwarding Method | Direct Routing | ? |
|-------------------|----------------|---|

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

| | | |
|------------|-----------------|---|
| Check Type | Connect to port | ? |
| Check Port | 2501 | ? |

14.2. 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.

14.2.1. 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:

| WebUI Main Menu Option | Sub Menu Option | Description |
|------------------------|-----------------------------------|---|
| Local Configuration | Hostname & DNS | Hostname and DNS settings |
| Local Configuration | Network Interface Configuration | Interface IP addresses, bonding configuration and VLANs |
| Local Configuration | Routing | Default gateways and static routes |
| Local Configuration | System Date & time | Time and date related settings |
| Local Configuration | Physical – Advanced Configuration | Various appliance settings |
| Local Configuration | Portal Management | Portal management settings |
| Local Configuration | Security | Security settings |
| Local Configuration | SNMP Configuration | SNMP settings |
| Local Configuration | Graphing | Graphing settings |
| Local Configuration | License Key | Appliance licensing |
| Maintenance | Backup & Restore | Local XML backups |
| Maintenance | Software Updates | Appliance software updates |
| Maintenance | Firewall Script | Firewall (iptables) configuration |
| Maintenance | Firewall Lockdown Wizard | Appliance management lockdown settings |

① Important

Make sure that where any of the above have been configured on the Primary appliance, they're also configured on the Secondary.

14.2.2. Configuring the HA Clustered Pair

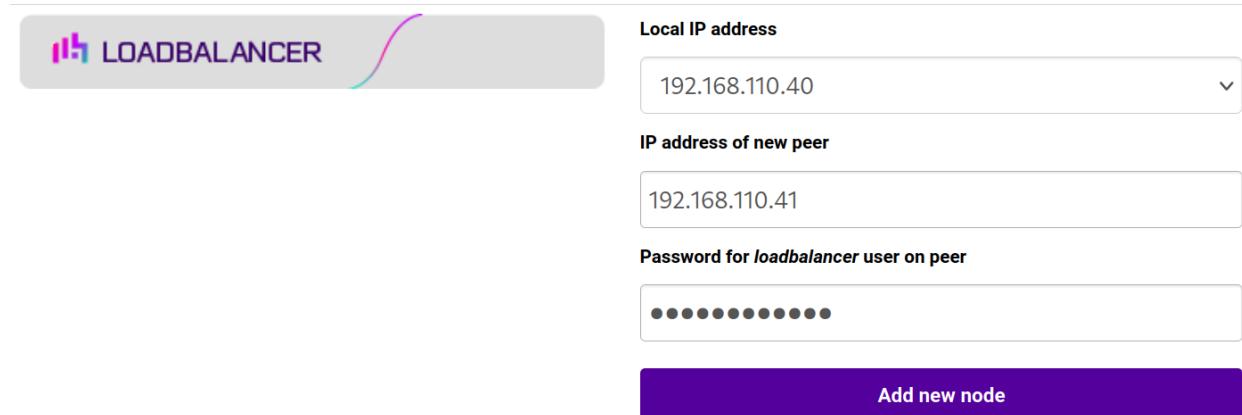
Note

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



Local IP address
192.168.110.40

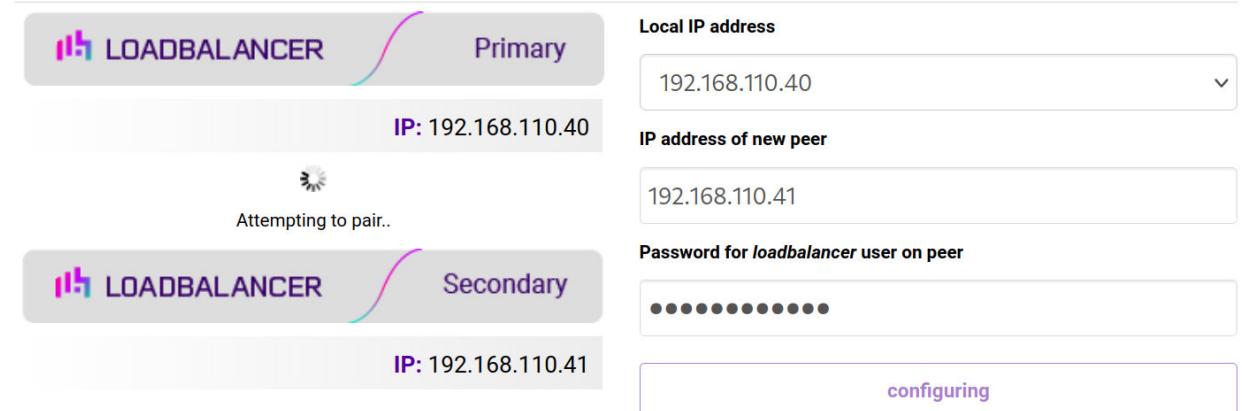
IP address of new peer
192.168.110.41

Password for *loadbalancer* user on peer
••••••••••••

Add new node

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



Primary

IP: 192.168.110.40

Attempting to pair..

Secondary

IP: 192.168.110.41

configuring

Local IP address
192.168.110.40

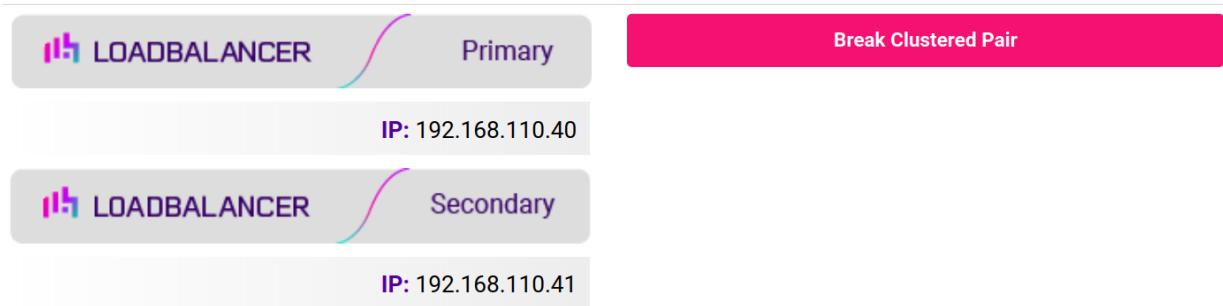
IP address of new peer
192.168.110.41

Password for *loadbalancer* user on peer
••••••••••••

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



High Availability Configuration - primary



7. 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](#).



15. Document Revision History

| Version | Date | Change | Reason for Change | Changed By |
|---------|-----------------|--|---------------------------------------|--------------|
| 1.0.0 | 3 July 2020 | Initial version | | RPC |
| 1.1.0 | 1 January 2022 | Converted the document to AsciiDoc | Move to new documentation system | AH, RJC, ZAC |
| 1.1.1 | 5 January 2023 | Updated Testing & Verification section | General Improvements | RJC |
| 1.1.2 | 5 January 2023 | Combined software version information into one section Added one level of section numbering Added software update instructions Added table of ports used by the appliance Reworded 'Further Documentation' section | Housekeeping across all documentation | AH |
| 1.1.3 | 2 February 2023 | Updated screenshots | Branding update | AH |
| 1.1.4 | 7 March 2023 | Removed conclusion section | Updates across all documentation | AH |
| 1.2.0 | 24 March 2023 | New document theme Modified diagram colours | Branding update | AH |





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](https://www.loadbalancer.org)

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.

