Load Balancing Panzura CloudFS
Version 1.1.0
## Table of Contents

1. About this Guide ................................................................. 3
2. Loadbalancer.org Appliances Supported .................................. 3
3. Loadbalancer.org Software Versions Supported .......................... 3
4. Panzura CloudFS Software Versions Supported .......................... 3
5. Panzura CloudFS ................................................................. 3
6. Load Balancing Panzura CloudFS ........................................... 3
    Load Balancing & HA Requirements ....................................... 4
    Persistence (aka Server Affinity) ......................................... 4
    Virtual Service (VIP) Requirements ...................................... 4
    Port Requirements .......................................................... 4
7. Deployment Concept ............................................................. 4
8. Load Balancer Deployment Methods ......................................... 5
    Layer 4 NAT Mode .......................................................... 5
    Layer 7 SNAT Mode ......................................................... 7
    Our Recommendation ....................................................... 8
9. Configuring Panzura CloudFS for Load Balancing ......................... 8
    Configuring for Layer 4 NAT Mode ...................................... 8
    Configuring for Layer 7 SNAT Mode (recommended) .................. 8
10. Loadbalancer.org Appliance – the Basics .................................... 8
    Virtual Appliance ............................................................ 8
    Initial Network Configuration .............................................. 9
    Accessing the WebUI ........................................................ 9
    Main Menu Options ........................................................ 10
    HA Clustered Pair Configuration ....................................... 11
    Configuring the SMB Virtual Service (VIP) ............................ 11
    Defining the Real Servers (RIPs) ......................................... 12
    Configuring the NFS Virtual Service (VIP) ............................. 12
    Defining the Real Servers (RIPs) ......................................... 13
    Finalizing the Configuration .............................................. 14
    Creating a floating IP for the Panzura CloudFS gateway address ....... 14
    Configuring the SMB Virtual Service (VIP) ............................ 15
    Defining the Real Servers (RIPs) ......................................... 15
    Configuring the NFS Virtual Service (VIP) ............................. 16
    Defining the Real Servers (RIPs) ......................................... 17
    Finalizing the Configuration .............................................. 17
13. Testing & Verification ............................................................ 17
    Using System Overview ..................................................... 17
14. Technical Support ............................................................... 18
15. Further Documentation ......................................................... 18
16. Conclusion ........................................................................ 18
17. Appendix ........................................................................ 19
    Configuring HA - Adding a Secondary Appliance .................... 19
    Non-Replicated Settings ..................................................... 19
18. Document Revision History .................................................... 22
1. About this Guide

This guide details the steps required to configure a load balanced Panzura CloudFS environment utilizing Loadbalancer.org appliances. It covers the configuration of the load balancers and also any Panzura CloudFS 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 Panzura CloudFS. 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. Panzura CloudFS Software Versions Supported

- Panzura CloudFS V7.1.9x and later

5. Panzura CloudFS

The Panzura Cloud File System (PCFS) is a distributed cloud file system used for storing application data that spans the globe, granting users in various geographical locations fast and consistent access to that data.

Panzura CloudFS capabilities include:

- Providing instances at each site that connect to each other and to a master data source. These instances can be deployed as either a virtual machine (VM), or as an in-cloud instance
- Frequently used files are cached at each office for fast access
- Files are kept constantly synchronized across all sites
- Users can access the same file at the same time
- The master copy is kept synchronized with the public or private cloud provider of your choice
- Byte-range global locking technology protects files from being accidentally overwritten

6. Load Balancing Panzura CloudFS

Note: It's highly recommended that you have a working Panzura CloudFS environment first before implementing the load balancer. The Panzura instances should be configured on a Master/Subordinate configuration when being deployed behind a load balancer.
Load Balancing & HA Requirements
The function of the load balancer is to distribute inbound connections across a cluster of Panzura CloudFS nodes, to provide a highly available and scalable service. Two virtual services are used to load balance the different aspects of Panzura CloudFS.

Persistence (aka Server Affinity)
Persistence is not needed as the Panzura CloudFS Master and Subordinates synchronise configuration between themselves.

Virtual Service (VIP) Requirements
To provide load balancing for Panzura CloudFS, the following VIPs are required:

- **SMB**: for Windows print and file sharing cluster
- **NFS**: Network file system cluster

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

<table>
<thead>
<tr>
<th>Port</th>
<th>Protocols</th>
<th>Uses</th>
</tr>
</thead>
<tbody>
<tr>
<td>111</td>
<td>TCP/RPC</td>
<td>Remote Procedure Call / portmap traffic (RPC)</td>
</tr>
<tr>
<td>445</td>
<td>TCP/SMB</td>
<td>Windows File and print sharing</td>
</tr>
<tr>
<td>2049</td>
<td>TCP/NFS</td>
<td>NFS daemon process (nfsd)</td>
</tr>
</tbody>
</table>

7. Deployment Concept

VIPs = Virtual IP Addresses

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
8. Load Balancer Deployment Methods

The load balancer can be deployed in 4 fundamental ways: *Layer 4 DR mode*, *Layer 4 NAT mode*, *Layer 4 SNAT mode*, and *Layer 7 SNAT mode*.

For Panzura CloudFS, using either layer 4 NAT mode or layer 7 SNAT mode is recommended. *Layer 4 DR mode* is not recommended due to operating system restrictions on the Panzura CloudFS nodes.

These modes are described below and are used for the configurations presented in this guide. For configuring using NAT mode please refer to [Appliance Configuration for Panzura CloudFS – Using Layer 4 NAT Mode](#), and for configuring using layer 7 SNAT mode refer to [Appliance Configuration for Panzura CloudFS – Using Layer 7 SNAT Mode](#).

**Layer 4 NAT Mode**

Layer 4 NAT mode is a high performance solution, although not as fast as layer 4 DR mode. This is because real server responses must flow back to the client via the load balancer rather than directly as with DR mode.

- The load balancer translates all requests from the Virtual Service to the Real Servers.
- NAT mode can be deployed in the following ways:
  - **Two-arm (using 2 Interfaces)** (as shown above) - Here, 2 subnets are used. The VIP is located in one subnet and the load balanced Real Servers are located in the other. The load balancer requires 2 interfaces, one in each subnet.

**Note**

This can be achieved by using two network adapters, or by creating VLANs on a single adapter.

- Normally eth0 is used for the internal network and eth1 is used for the external network although this is not mandatory. If the Real Servers require Internet access, *Autonat* should be enabled using the
WebUI menu option: **Cluster Configuration > Layer 4 - Advanced Configuration**, the external interface should be selected.

- The default gateway on the Real Servers must be set to be an IP address on the load balancer.
- Clients can be located in the same subnet as the VIP or any remote subnet provided they can route to the VIP.

- **One-arm (using 1 Interface)** - Here, the VIP is brought up in the same subnet as the Real Servers.

![Diagram of one-arm (using 1 Interface)](image)

- To support remote clients, the default gateway on the Real Servers must be an IP address on the load balancer and routing on the load balancer must be configured so that return traffic is routed back via the router.

  **Note**
  
  For an HA clustered pair, a floating IP should be added to the load balancer and used as the Real Server’s default gateway. This ensures that the IP address can ‘float’ (move) between Primary and Secondary appliances.

- To support local clients, return traffic would normally be sent directly to the client bypassing the load balancer which would break NAT mode. To address this, the routing table on the Real Servers must be modified to force return traffic to go via the load balancer. For more information please refer to **One-Arm (Single Subnet) NAT Mode**.

  - If you want Real Servers to be accessible on their own IP address for non-load balanced services, e.g. SMTP or RDP, you will need to setup individual SNAT and DNAT firewall script rules for each Real Server or add additional VIPs for this.
  - Port translation is possible with Layer 4 NAT mode, e.g. VIP:80 → RIP:8080 is supported.
  - NAT mode is transparent, i.e. the Real Server will see the source IP address of the client.

### NAT Mode Packet re-Writing

In NAT mode, the inbound destination IP address is changed by the load balancer from the Virtual Service IP address (VIP) to the Real Server. For outbound replies the load balancer changes the source IP address of the Real Server to be the Virtual Services IP address.

The following table shows an example NAT mode setup:

<table>
<thead>
<tr>
<th>Protocol</th>
<th>VIP</th>
<th>Port</th>
<th>RIP</th>
<th>Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP</td>
<td>10.0.0.20</td>
<td>80</td>
<td>192.168.1.50</td>
<td>80</td>
</tr>
</tbody>
</table>

In this simple example all traffic destined for IP address 10.0.0.20 on port 80 is load-balanced to the real IP address 192.168.1.50 on port 80.
Packet rewriting works as follows:

1) The incoming packet for the web server has source and destination addresses as:

| Source | x.x.x.x:34567 | Destination | 10.0.0.20:80 |

2) The packet is rewritten and forwarded to the backend server as:

| Source | x.x.x.x:34567 | Destination | 192.168.1.50:80 |

3) Replies return to the load balancer as:

| Source | 192.168.1.50:80 | Destination | x.x.x.x:34567 |

4) The packet is written back to the VIP address and returned to the client as:

| Source | 10.0.0.20:80 | Destination | x.x.x.x:34567 |

Layer 7 SNAT Mode

Layer 7 SNAT mode uses a proxy (HAProxy) at the application layer. Inbound requests are terminated on the load balancer and HAProxy generates a new corresponding request to the chosen Real Server. As a result, Layer 7 is typically not as fast as the Layer 4 methods. Layer 7 is typically chosen when either enhanced options such as SSL termination, cookie based persistence, URL rewriting, header insertion/deletion etc. are required, or when the network topology prohibits the use of the layer 4 methods.

- Because layer 7 SNAT mode is a full proxy, any server in the cluster can be on any accessible subnet including across the Internet or WAN.
- Layer 7 SNAT mode is not transparent by default, i.e. the Real Servers will not see the source IP address of the client, they will see the load balancer’s own IP address by default, or any other local appliance IP address if preferred (e.g. the VIP address). This can be configured per layer 7 VIP. If required, the load balancer can be
configured to provide the actual client IP address to the Real Servers in 2 ways. Either by inserting a header that contains the client’s source IP address, or by modifying the Source Address field of the IP packets and replacing the IP address of the load balancer with the IP address of the client. For more information on these methods please refer to Transparency at Layer 7.

- Layer 7 SNAT mode can be deployed using either a one-arm or two-arm configuration. For two-arm deployments, eth0 is normally used for the internal network and eth1 is used for the external network although this is not mandatory.

- Requires no additional configuration changes to the load balanced Real Servers.

- Port translation is possible with Layer 7 SNAT mode, e.g. VIP:80 → RIP:8080 is supported.

- You should not use the same RIP:PORT combination for layer 7 SNAT mode VIPs and layer 4 SNAT mode VIPs because the required firewall rules conflict.

Our Recommendation
Where possible, we recommend that Layer 7 SNAT mode is used. This mode offers great performance with minimal to no changes required on the real servers and can be deployed in one-arm or two-arm mode. HAProxy is a high performance solution, but since it operates as a full proxy, it cannot perform as fast as the layer 4 solutions. Layer 7 SNAT mode is non-transparent by default, i.e. the Real Servers will see the source IP address of the load balancer.

9. Configuring Panzura CloudFS for Load Balancing

Configuring for Layer 4 NAT Mode
For layer 4 NAT mode to work, every Panzura CloudFS node must be configured so that its gateway points to a floating IP on the load balancer(s).

Configuring for Layer 7 SNAT Mode (recommended)
No changes are required on the Panzura CloudFS nodes for layer 7 SNAT mode.

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.

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.
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, 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
- **Reports** - View various appliance reports & graphs
- **Logs** - View various appliance logs
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.


Configuring the SMB Virtual Service (VIP)

1. Using the web user interface, navigate to Cluster Configuration > Layer 4– Virtual Services and click on Add a new Virtual Service.
2. Define the Label for the virtual service as required, e.g. Panzura-SMB.
3. Set the Virtual Service IP Address field to the required IP address, e.g. 192.168.86.140.
4. Set the Ports field to 445.
5. Set the Protocol to TCP.
6. Change the Forwarding Method to NAT.
7. Click Update to create the virtual service.

```
Layer 4 - Add a new Virtual Service

Label: Panzura-SMB
Virtual Service IP Address: 192.168.86.140
Ports: 445
Protocol:
    Protocol: TCP
Forwarding Method:
    Forwarding Method: NAT
```

8. Click Modify next to the newly created VIP.
9. Ensure that the Persistence Enable checkbox is unchecked.
10. Set the Health Checks Check Type to Connect to port.
11. Set the Check Port to 445.
12. Click **Update**.

**Defining the Real Servers (RIPs)**

1. Using the web user interface, navigate to *Cluster Configuration > Layer 4 – 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. **Panzura1**.
3. Set the **Real Server IP Address** field to the required IP address, e.g. **172.24.11.138**.
4. Click **Update**.
5. Repeat these steps to add additional Panzura servers as required.

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

**Configuring the NFS Virtual Service (VIP)**

1. Using the web user interface, navigate to *Cluster Configuration > Layer 4 – Virtual Services* and click on **Add a new Virtual Service**.
2. Define the **Label** for the virtual service as required, e.g. **Panzura-NFS**.
3. Set the **Virtual Service IP Address** field to the required IP address, e.g. **192.168.86.140**.
4. Set the **Ports** field to **111, 2049**.
5. Set the **Protocol** to **TCP**.
6. Change the **Forwarding Method** to **NAT**.
7. Click **Update** to create the virtual service.
8. Click **Modify** next to the newly created VIP.

9. Ensure that the **Persistence Enable** checkbox is unchecked.

10. Set the **Health Checks Check Type** to **Connect to port**.

11. Set the **Check Port** to **2049**.

12. Click **Update**.

**Defining the Real Servers (RIPs)**

1. Using the web user interface, navigate to **Cluster Configuration > Layer 4 – 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. **Panzura1**.

3. Set the **Real Server IP Address** field to the required IP address, e.g. **172.24.11.138**.

4. Click **Update**.

5. Repeat these steps to add additional Panzura servers as required.
Finalizing the Configuration

For layer 4 NAT mode to work every Panzura CloudFS node must be configured so that its gateway points to a floating IP of the load balancer.

Creating a floating IP for the Panzura CloudFS gateway address
1. Using the web user interface, navigate to Cluster Configuration > Floating IPs.

2. Specify the new floating IP.
3. Click Add Floating IP.

| Note | When using a clustered pair, ensure that the Secondary also has a static IP address assigned that’s in the same subnet as the floating IP being added. Failure to do so will result in heartbeat issues during a failover. |

| Note | Floating IPs are not deleted automatically when Virtual Services are removed or the IP address is changed, this must be done manually. |

Configuring the SMB 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. Panzura-SMB.

3. Set the Virtual Service IP Address field to the required IP address, e.g. 192.168.85.140.

4. Set the Ports field to 445.

5. Set the Layer 7 Protocol to TCP Mode.

6. Click Update to create the virtual service.

```
Layer 7 - Add a new Virtual Service

Label
Panzura-SMB

Virtual Service
IP Address
192.168.85.140
Ports
445

Protocol
Layer 7 Protocol
TCP Mode

Manual Configuration

```

7. Click Modify next to the newly created VIP.

8. Set Persistence Mode to None.

9. Set Health Checks to Connect to port.

10. In the Other section click Advanced to expand the menu.

11. Check the Timeout checkbox.

12. Set Client Timeout to 5m (the m is for minutes).

13. Set Real Server Timeout to 5m.

14. Click Update.

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. Panzura1.

3. Set the Real Server IP Address field to the required IP address, e.g. 172.24.11.138.

4. Click Update.

5. Repeat these steps to add additional Panzura CloudFS nodes as real servers as required.
Configuring the NFS 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. Panzura-NFS.

3. Set the Virtual Service IP Address field to the required IP address, e.g. 192.168.85.140.

4. Set the Ports field to 111, 2049.

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. Set Persistence Mode to None.

9. Set Health Checks to Connect to port.

10. In the Other section click Advanced to expand the menu.

11. Check the Timeout checkbox.
12. Set Client Timeout to 5m (the m is for minutes).

13. Set Real Server Timeout to 5m.

14. Click Update.

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. Panzura1.

3. Set the Real Server IP Address field to the required IP address, e.g. 172.24.11.138.

4. Click Update.

5. Repeat these steps to add additional Panzura CloudFS nodes as real servers as required.

Finalizing the Configuration

To apply the new settings, HAProxy must be reloaded. This can be done using the button in the blue 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.

13. Testing & Verification

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

Using System Overview

The System Overview can be viewed in the WebUI. It shows a graphical view of all VIPs & RIPs (i.e. the Panzura CloudFS nodes) 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 three HyperFile nodes are healthy and available to accept connections:
14. 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.

15. Further Documentation


16. Conclusion

Loadbalancer.org appliances provide a very cost effective solution for highly available load balanced Panzura CloudFS environments.
## 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 Configuration</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 Configuration</td>
<td>Various settings including Internet Proxy, Management Gateway, Firewall connection tracking table size, NIC offloading, SMTP relay, 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 Wizard</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:*
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**.
# 18. 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>8 November 2019</td>
<td>Initial version</td>
<td></td>
<td>IG</td>
</tr>
<tr>
<td>1.0.1</td>
<td>11 December 2019</td>
<td>Changed some instructions based on feedback from Panzura</td>
<td>Required updates</td>
<td>IG</td>
</tr>
<tr>
<td>1.0.2</td>
<td>2 September 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>1.1.0</td>
<td>1 November 2021</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.

United Kingdom
Loadbalancer.org Ltd.
Compass House, North Harbour Business Park, Portsmouth, PO6 4PS
UK:+44 (0) 330 380 1064
sales@loadbalancer.org
support@loadbalancer.org

Canada
Loadbalancer.org Appliances Ltd.
300-422 Richards Street, Vancouver, BC, V6B 2Z4, Canada
TEL:+1 866 998 0508
sales@loadbalancer.org
support@loadbalancer.org

United States
Loadbalancer.org, Inc.
4550 Linden Hill Road, Suite 201
Wilmington, DE 19808, USA
TEL: +1 833.274.2566
sales@loadbalancer.org
support@loadbalancer.org

Germany
Loadbalancer.org GmbH
Tengstraße 2780798,
München, Germany
TEL: +49 (0)89 2000 2179
sales@loadbalancer.org
support@loadbalancer.org

© Copyright Loadbalancer.org • www.loadbalancer.org