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 relevant Administration Manual:

- v7 Administration Manual
- v8 Administration Manual

2. Loadbalancer.org Appliances Supported

All our products can be used for load balancing Panzura CloudFS. 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

- V8.3.8 and later

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 section 1 in the appendix on page 22 for more details on configuring a clustered pair.

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 the section starting on page 13, and for configuring using layer 7 SNAT mode refer to the section starting on page 17.
Layer 4 NAT Mode

This mode is also a high performance solution but not as fast as DR mode. It requires the implementation of a two-arm infrastructure with an internal and external subnet to carry out the translation (the same way a firewall works). Also, each Real Server must use the load balancer as the default gateway. Layer 4 NAT mode is transparent, i.e. the Real Servers will see the source IP address of the client.

- The load balancer translates all requests from the external Virtual Service to the internal Real Servers.
- 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 option: Cluster Configuration > Layer 4 – Advanced Configuration, the external interface should be selected.
- NAT mode can be deployed in the following ways:
  1. **2-arm (using 2 Interfaces), 2 subnets** (as shown above) - One interface on the load balancer is connected to subnet1 and the second interface and Real Servers are connected to subnet2. The VIP is brought up in subnet1. The default gateway on the Real Servers is set to be an IP address in subnet2 on the load balancer. Clients can be located in subnet1 or any remote subnet provided they can route to the VIP.
  2. **2-arm (using 1 Interface), 2 subnets** - same as above except that a single interface on the load balancer is allocated 2 IP addresses, one in each subnet.
  3. **1-arm (using 1 Interface), 1 subnet** - Here, the VIP is brought up in the same subnet as the Real Servers. For clients located in remote networks the default gateway on the Real Servers must be set to be an IP address on the load balancer. For clients located on the same subnet, 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 details on ‘One-Arm NAT Mode’ refer to the administration manual.
- 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 - please refer to the administration manual for more details.
• NAT mode is transparent, i.e. the Real Server will see the source IP address of the client.

• Port translation is possible in NAT mode, i.e. VIP:80 --> RIP:8080 is possible.

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 request to the chosen Real Server. As a result, Layer 7 is a slower technique than DR or NAT mode at Layer 4. 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.

This mode can be deployed in a one-arm or two-arm configuration and does not require any changes to the Real Servers. However, since the load balancer is acting as a full proxy it doesn't have the same raw throughput as the layer 4 methods.

The load balancer proxies the application traffic to the servers so that the source of all traffic becomes the load balancer.

• SNAT mode is a full proxy and therefore load balanced Real Servers do not need to be changed in any way

• Because SNAT mode is a full proxy any server in the cluster can be on any accessible subnet including across the Internet or WAN

• 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 balancers 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 clients IP address can be passed through either by enabling TProxy on the load balancer, or for HTTP, using X-forwarded-For headers. Please refer to chapter 6 in the administration manual for more details

• SNAT mode can be deployed using either a 1-arm or 2-arm configuration
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 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 1 of the appendix on page 22.

**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](image)

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 point 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 slave 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.

**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

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

![Layer 7 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 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 as follows:

1. Using the WebUI, navigate to: Maintenance > Restart Services and click Reload HAProxy

13. Testing & Verification

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.
17. Appendix

1 – 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
• 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.
### 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>
</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