1. About this Guide

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

- Cloudian HyperFile – version 3.6.1 and later

5. Cloudian HyperFile

Cloudian HyperFile is a scale-out NAS platform that provides file system protocols for clients and transparent data tiering to object storage (Cloudian HyperStore). Client applications write data to HyperFile and then HyperFile manages the underlying storage tiers, leveraging its native information lifecycle management (ILM) capabilities.

HyperFile provides capabilities including:

- Local data caching and tiering to Cloudian HyperStore object storage
- Bi-modal access to data (data tiered from HyperFile to object storage can be read through HyperFile’s file protocols or directly through HyperStore’s S3 interface)
- Integrated data protection via snapshots
- Active Directory / LDAP integration and user quotas
- Multi-controller configurations
- High availability (HA) configurations
- Write Once Read Many (WORM) support, together with compliance features such as auditing and so on

6. Load Balancing Cloudian HyperFile
Load Balancing & HA Requirements
To allow a Cloudian HyperFile deployment to be load balanced, the HyperFile nodes must be deployed in a multi-controller configuration sharing an NFS volume.

Persistence (aka Server Affinity)
Source IP address persistence is required to successfully load balance Cloudian HyperFile. This is true for both the layer 4 DR mode and layer 7 load balancing scenarios described in this document.

Virtual Service (VIP) Requirements
To provide load balancing and HA for Cloudian HyperFile, a single VIP is used which covers all of the ports needed.

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>1110</td>
<td>TCP/NFS</td>
<td>Cluster status service</td>
</tr>
<tr>
<td>2049</td>
<td>TCP/NFS</td>
<td>NFS daemon process (nfsd)</td>
</tr>
<tr>
<td>4045</td>
<td>TCP/NFS</td>
<td>Network lock manager process (nlockmgr)</td>
</tr>
</tbody>
</table>

Additional high ports, as well as the above mentioned ports using UDP, are used for NFS version 3 and below.

As described later in this document, using * to cover all ports in a layer 4 setup is recommended for NFS version 3 and below.

7. Deployment Concept
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 Cloudian HyperFile, using either layer 4 DR mode or layer 7 SNAT mode is recommended. If using **NFS version 3 and below**, **layer 4 DR mode should be used** due to the wide range of ports that are used in these older versions of the NFS protocol.

These modes are described below and are used for the configurations presented in this guide. For configuring using DR mode please refer to **Appliance Configuration for Cloudian HyperFile - Using Layer 4 DR Mode**, and for configuring using layer 7 SNAT mode refer to **Appliance Configuration for Cloudian HyperFile - Using Layer 7 SNAT Mode**.

**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**.

**Layer 4 DR Mode Diagram**

- 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.

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 4 Direct Routing (DR) mode is used. This mode offers the best possible performance since replies go directly from the Real Servers to the client, not via the load balancer. It’s also relatively simple to implement. Ultimately, the final choice does depend on your specific requirements and infrastructure.

If DR mode cannot be used, for example if the real servers are located in remote routed networks, then SNAT mode is recommended.

If the load balancer is deployed in AWS or Azure, layer 7 SNAT mode must be used as layer 4 direct routing is not currently possible on these platforms.

9. Configuring Cloudian HyperFile for Load Balancing

**Configuring for Layer 4 DR Mode**

**Important**

Layer 4 DR mode should be used if NFS version 3 and below is used.

For layer 4 DR mode to work, **every HyperFile node** must be configured so that its loopback adaptor owns the VIP address.

1. The change to the loopback adaptor should be set from the command line by writing a script to ensure that the change is persistent across reboots.

   - The script should be put in the directory /etc/rc2.d and its filename must begin with a capital letter S. For example: /etc/rc2.d/Sloopbackscript
   - An example script that can be used is presented below - the example VIP address of 192.168.88.69 should be changed to match the VIP address being used:

```
#!/bin/sh
#
# This is to redirect ARP requests to the HyperFile VIP
#
ifconfig lo0:1 plumb
ifconfig lo0:1 192.168.88.69 netmask 255.255.255.255 up
```

**Configuring for Layer 7 SNAT Mode**

No changes are required on the HyperFile 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 The Virtual Appliance - Hypervisor Deployment and the ReadMe.txt text file included in the VA download for more detailed information on deploying the VA using various Hypervisors.

Note
For the VA, 4 NICs are included but only eth0 is connected by default at power up. If the other NICs are required, these should be connected using the network configuration screen within the Hypervisor.

Initial Network Configuration

After boot up, follow the instructions on the console to configure the IP address, subnet mask, default gateway, DNS 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 & 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
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 Clustered Pair Configuration - Adding a Secondary Unit.

11. Appliance Configuration for Cloudian HyperFile – Using Layer 4 DR Mode

Configuring the 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. HyperFile.
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 * (this wildcard sets the VIP to use all ports).
5. Set the Protocol to TCP/UDP.
7. Click Update to create the virtual service.

Layer 4 - Add a new Virtual Service

<table>
<thead>
<tr>
<th>Label</th>
<th>HyperFile</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address</td>
<td>192.168.85.140</td>
</tr>
<tr>
<td>Ports</td>
<td>*</td>
</tr>
<tr>
<td>Protocol</td>
<td>TCP/UDP</td>
</tr>
<tr>
<td>Forwarding Method</td>
<td>Direct Routing</td>
</tr>
</tbody>
</table>
8. Click **Modify** next to the newly created VIP.

9. Ensure that the **Persistence Enable** checkbox is checked and that the **Timeout** is set to **300** (this should already be configured by default).

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. **hyperfile-node1**.

3. Set the **Real Server IP Address** field to the required IP address, e.g. **192.168.85.200**.

4. Click **Update**.

5. Repeat these steps to add additional HyperFile servers as required.

### Layer 4 Add a new Real Server - HyperFile

<table>
<thead>
<tr>
<th>Label</th>
<th>hyperfile-node1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Real Server IP Address</td>
<td>192.168.85.200</td>
</tr>
<tr>
<td>Weight</td>
<td>100</td>
</tr>
<tr>
<td>Minimum Connections</td>
<td>0</td>
</tr>
<tr>
<td>Maximum Connections</td>
<td>0</td>
</tr>
</tbody>
</table>


#### Important

This load balancing method should not be used if NFS version 3 and below is to be used with HyperFile. Layer 4 DR mode should be used instead (see the previous section on how to set this up). This is because NFS versions 3 and below use additional high ports, as well as the standard ports but using UDP.

### Configuring the 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. **HyperFile**.
3. Set the **Virtual Service IP Address** field to the required IP address, e.g. `192.168.85.150`.
4. Set the **Ports** field to `111,1110,2049,4045`.
5. Set the **Layer 7 Protocol** to **TCP Mode**.
6. Click **Update** to create the virtual service.

### Layer 7 - Add a new Virtual Service

<table>
<thead>
<tr>
<th>Label</th>
<th>HyperFile</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Virtual Service</strong></td>
<td></td>
</tr>
<tr>
<td>IP Address</td>
<td><code>192.168.85.150</code></td>
</tr>
<tr>
<td>Ports</td>
<td><code>111,1110,2049,4045</code></td>
</tr>
<tr>
<td><strong>Protocol</strong></td>
<td></td>
</tr>
<tr>
<td>Layer 7 Protocol</td>
<td>TCP Mode</td>
</tr>
<tr>
<td>Manual Configuration</td>
<td>No</td>
</tr>
</tbody>
</table>

7. Click **Modify** next to the newly created VIP.
8. Set **Persistence Mode** to **Source IP**.
9. In the **Persistence** section click **Advanced** to expand the menu.
10. Set **Persistence Timeout** to **5** (the default units are minutes).
11. Set **Health Checks** to **Connect to port**.
12. In the **Health Checks** section click **Advanced** to expand the menu.
13. Set **Check Port** to **2049**.
14. In the **Other** section click **Advanced** to expand the menu.
15. Check the **Timeout** checkbox.
16. Set **Client Timeout** to **5m** (the `m` is for minutes).
17. Set **Real Server Timeout** to **5m**.
18. 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. `hyperfile-node1`.
3. Set the **Real Server IP Address** field to the required IP address, e.g. `192.168.85.200`.
4. Click **Update**.
5. Repeat these steps to add additional HyperStore nodes as real servers as required.

### Layer 7 Add a new Real Server - HyperFile

<table>
<thead>
<tr>
<th>Label</th>
<th>hyperfile-node1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Real Server IP Address</td>
<td>192.168.85.200</td>
</tr>
<tr>
<td>Real Server Port</td>
<td></td>
</tr>
<tr>
<td>Re-Encrypt to Backend</td>
<td>0</td>
</tr>
<tr>
<td>Weight</td>
<td>100</td>
</tr>
</tbody>
</table>

**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 general guidance please also refer to Testing Load Balanced Services.

**Using System Overview**

The System Overview can be viewed in the WebUI. It shows a graphical view of all VIPs & RIPs (i.e. the Cloudian HyperFile 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:

**Layer 4 DR mode specific test**

If the layer 4 DR mode load balancing method has been used then an additional check can be performed to
confirm that the load balanced HyperFile deployment as a whole is functioning correctly.

After sending some test traffic to the virtual service, from the WebUI, navigate to Reports > Layer 4 Current Connections. Ensure that the test connections are not shown to be in the SYN_RECV state under the third column, 'state'. Successful connections are shown as ESTABLISHED like so:

<table>
<thead>
<tr>
<th>IPVS connection entries</th>
<th>source</th>
<th>virtual</th>
<th>destination</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP 01:08 NONE 192.168.86.2:0</td>
<td>119.53.148.0:0 192.168.86.77:0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TCP 14:42 ESTABLISHED 192.168.86.2:669</td>
<td>192.168.86.69:2049 192.168.86.77:2049</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

If any of the connections are in the SYN_RECV state then it is very likely that the HyperFile nodes have not been correctly configured for layer 4 DR mode. Identify which nodes are affected, by looking at their IP address in the 'destination' column, and then refer to the section Configuring for Layer 4 DR Mode and ensure that all steps have been followed correctly.

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 Cloudian HyperFile environments.
17. Appendix

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.

Note
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>

To add a Secondary node - i.e. create a highly available clustered pair:
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](#).
## 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, AH</td>
</tr>
<tr>
<td>1.0.1</td>
<td>18 November 2019</td>
<td>Removed the instruction to change each node’s default gateway to the VIP address in section ‘Configuring Cloudian HyperFile for Load Balancing’</td>
<td>The step in question was not required and was removed for simplicity</td>
<td>AH</td>
</tr>
<tr>
<td>1.0.2</td>
<td>1 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 October 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.