Load Balancing Storage Made Easy File Fabric

Version 1.1.0
Table of Contents

1. About this Guide ......................................................... 4
2. Loadbalancer.org Appliances Supported ................................. 4
3. Loadbalancer.org Software Versions Supported ....................... 4
4. File Fabric Software Versions Supported ............................... 4
5. Storage Made Easy File Fabric ......................................... 4
6. Load Balancing File Fabric ............................................. 4
   Load Balancing & HA Requirements .................................. 4
   Persistence (aka Server Affinity) ..................................... 5
   Virtual Service (VIP) Requirements .................................. 5
   Port Requirements .................................................... 5
7. Deployment Concept .................................................... 5
8. Load Balancer Deployment Methods .................................... 6
   Layer 4 DR Mode ..................................................... 6
   Layer 7 SNAT Mode .................................................. 7
   Our Recommendation .................................................. 8
9. Configuring File Fabric for Load Balancing ............................ 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
11. Appliance Configuration for File Fabric – Using Layer 4 DR Mode and Layer 7 SNAT Mode ........................................... 11
    Duplicate Service Function ........................................ 11
    Layer 4 Direct Routing Configuration ................................ 11
    Configuring VIP 1 – SME Web Portal ................................ 11
    Configuring VIP 2 – SME SFTP ...................................... 13
    Layer 7 SNAT Mode Configuration .................................... 14
    Duplicate Service Function ........................................ 15
    Configuring VIP 1 – SME Web Portal ................................ 15
    Configuring the Virtual Service (VIP) ............................... 15
    Defining the Real Servers (RIPs) ..................................... 16
    Configuring VIP 2 – SME SFTP ...................................... 17
    Configuring the Virtual Service (VIP) ............................... 17
    Defining the Real Servers (RIPs) ..................................... 18
    Configuring VIP 3 – SME SQL ...................................... 18
    Configuring the Virtual Service (VIP) ............................... 18
    Defining the Real Servers (RIPs) ..................................... 19
    Configuring VIP 4 – SME Memcache ................................ 20
    Configuring the Virtual Service (VIP) ............................... 20
    Defining the Real Servers (RIPs) ..................................... 21
    Finalizing the Configuration ......................................... 21
13. Testing & Verification .................................................. 22
    Using System Overview ............................................. 22
    Layer 4 Direct Routing Specific Check ................................ 22
    SFTP Service Check .................................................. 23
14. Technical Support .................................................... 23
15. Further Documentation ................................................ 23
1. About this Guide

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

- File Fabric – version 1906.00 and later

5. Storage Made Easy File Fabric

Storage Made Easy provides an on-premises Enterprise File Fabric solution which is storage agnostic and can be used either with a single storage back-end or multiple public/private storage systems. In the event of the latter, the File Fabric unifies the view across all access clients and implements a common control and governance policies through the use of its cloud control features.

The product is supplied as a software 'appliance' which is run inside of a hypervisor and consists of a pre-configured, 'hardened' operating system (CentOS) and the File Fabric Application provided by Storage Made Easy.

6. Load Balancing File Fabric

Note: It’s highly recommended that you have a working File Fabric environment first before implementing the load balancer.

Load Balancing & HA Requirements

To deploy File Fabric as an HA deployment, 4 SME File Fabric instances are needed. When configured as per the Storage Made Easy guides, the topology will be as follows:

- 2 SME Web servers
- 2 SME SQL servers
Persistence (aka Server Affinity)
Load balancing File Fabric requires source IP address affinity. This is true for both the layer 4 and layer 7 based load balancing methods described in this document.

Virtual Service (VIP) Requirements
To provide load balancing and HA for File Fabric, the following VIPs are required:

- Web portal access
- SQL
- Memcache
- SFTP

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

<table>
<thead>
<tr>
<th>Port</th>
<th>Protocols</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>80</td>
<td>TCP/HTTP</td>
<td>Web Portal Access over HTTP</td>
</tr>
<tr>
<td>443</td>
<td>TCP/HTTPS</td>
<td>Web Portal Access over HTTPS</td>
</tr>
<tr>
<td>3306</td>
<td>TCP/SQL</td>
<td>SQL Service</td>
</tr>
<tr>
<td>2200</td>
<td>TCP/SFTP</td>
<td>SFTP Service</td>
</tr>
<tr>
<td>11211</td>
<td>TCP/Memcache</td>
<td>Memcache Service</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
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 File Fabric, using a combination of layer 4 DR mode and layer 7 SNAT mode is recommended. It is also possible to only use layer 7 SNAT mode, however the performance of this setup is not as great and client source IP addresses are not passed through to the SME servers on the back end. Both of these setups are described below and are used for the configurations presented in this guide. For configuring using a combination of layer 4 DR mode and layer 7 SNAT mode please refer to **Appliance Configuration for File Fabric – Using Layer 4 DR Mode and Layer 7 SNAT Mode**. For configuring using only layer 7 SNAT mode refer to **Appliance Configuration for File Fabric – Using Only 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**.

- **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 \( \rightarrow \) 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 \( \rightarrow \) 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 the combination of Layer 4 Direct Routing (DR) mode and Layer 7 SNAT mode is used. This mode offers the best possible performance for the DR mode services, since replies go directly from the Real Servers to the client and 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. SNAT mode is also recommended if it is not possible to make network adaptor changes to the SME servers, for example if you do not own or do not control the infrastructure.

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

9. Configuring File Fabric for Load Balancing

Ensure that a working, HA File Fabric deployment is in place prior to deploying a load balancer.

Refer to the following Storage Made Easy documentation for guidance on how to achieve this:

Installation: Getting Started: File Fabric On-Premises

File Fabric HA Master - Master Database with Automatic Failover

SME How to configure SFTP

When using the load balancer setup that makes use of layer 4 DR mode, the ARP problem must be solved on each SME server. Please refer to Solving the ARP Problem for instructions on how to do this.

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:

   ![IP-address-configured-during-network-setup-wizard]:9443/lbadmin/

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:
Note: The WebUI for the VA is shown, the hardware and cloud appliances are very similar. The yellow licensing related message is platform & model dependent.

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

Main Menu Options

**System Overview** - Displays a graphical summary of all VIPs, RIPs and key appliance statistics

**Local Configuration** - Configure local host settings such as IP address, DNS, system time etc.

**Cluster Configuration** - Configure load balanced services such as VIPs & RIPs

**Maintenance** - Perform maintenance tasks such as service restarts and taking backups

**View Configuration** - Display the saved appliance configuration settings

**Reports** - View various appliance reports & graphs

**Logs** - View various appliance logs
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.


Duplicate Service Function

As of version 8.3.8 of the Loadbalancer.org appliance, the Duplicate Service button can be used to save time during initial configuration. This function duplicates the configuration of a given virtual service along with all of the associated back end real servers which have been defined. This is useful for deployments where multiple, very similar virtual services are used, with only minor changes between them. It saves time as the same settings and real servers do not need to be repeatedly defined.

First, fully create the initial virtual service as directed. Then click the Modify button for the virtual service in question, click the Duplicate Service button near the top, and make the necessary changes for the new, duplicated virtual service.

This feature is available for both layer 4 and layer 7 virtual services.

Layer 4 Direct Routing Configuration

Configuring VIP 1 – SME Web Portal

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. SME_WebPortal.

3. Set the Virtual Service IP Address field to the required IP address, e.g. 192.168.86.84.

4. Set the Ports field to 80,443.

5. Leave the Protocol set to TCP.


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 checked and that the **Timeout** is set to **1800**.

10. Leave the **Health Checks Check Type** set to **Connect to port**.

11. 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. **SMEWEB01**.

3. Set the **Real Server IP Address** field to the required IP address, e.g. **192.168.86.78**.

4. Click **Update**.

5. Repeat these steps to add additional SME servers as required.
Configuring VIP 2 – SME SFTP

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. SME_SFTP.

3. Set the Virtual Service IP Address field to the required IP address, e.g. 192.168.86.84.

4. Set the Ports field to 2200.

5. Leave the Protocol set to TCP.


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 checked and that the Timeout is set to 1800.
10. Leave the *Health Checks Check Type* set to *Connect to port*.

11. Click Update.

<table>
<thead>
<tr>
<th>Persistence</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable</td>
<td>✔</td>
</tr>
<tr>
<td>Timeout</td>
<td>1800 s</td>
</tr>
<tr>
<td>Granularity</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Health Checks</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Check Type</td>
<td>Connect to port</td>
</tr>
<tr>
<td>Check Port</td>
<td></td>
</tr>
</tbody>
</table>

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. **SMEWEB01**.

3. Set the *Real Server IP Address* field to the required IP address, e.g. **192.168.86.78**.

4. Click Update.

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

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Label</td>
<td>SMEWEB01</td>
</tr>
<tr>
<td>Real Server IP Address</td>
<td>192.168.86.78</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>

Layer 7 SNAT Mode Configuration

To load balance the SQL and Memcache services, layer 7 virtual services should be used. This is because layer 4 direct routing mode does not provide any real benefit or advantage for these services.

To set up layer 7 virtual services for SQL and Memcache, follow the appropriate instructions from the next section of this document, *Appliance Configuration for File Fabric – Using Only Layer 7 SNAT Mode*, i.e.:

- **Configuring VIP 3 – SME SQL**

Duplicate Service Function

As of version 8.3.8 of the Loadbalancer.org appliance, the Duplicate Service button can be used to save time during initial configuration. This function duplicates the configuration of a given virtual service along with all of the associated back end real servers which have been defined. This is useful for deployments where multiple, very similar virtual services are used, with only minor changes between them. It saves time as the same settings and real servers do not need to be repeatedly defined.

First, fully create the initial virtual service as directed. Then click the Modify button for the virtual service in question, click the Duplicate Service button near the top, and make the necessary changes for the new, duplicated virtual service.

This feature is available for both layer 4 and layer 7 virtual services.

Configuring VIP 1 – SME Web Portal

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. SME_WebPortal.
3. Set the Virtual Service IP Address field to the required IP address, e.g. 192.168.86.84.
4. Set the Virtual Service Ports field to 80,443.
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 **Source IP**.

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** (this is 5 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. Enter an appropriate name for the server in the **Label** field, e.g. **SMEWEB01**.

3. Change the **Real Server IP Address** field to the required IP address, e.g. **192.168.86.78**.

4. Click **Update**.

5. Repeat these steps to add additional servers as required.
Configuring VIP 2 – SME SFTP

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. SME_SFTP.

3. Set the Virtual Service IP Address field to the required IP address, e.g. 192.168.86.84.

4. Set the Virtual Service Ports field to 2200.

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 Source IP.

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 (this is 5 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. Enter an appropriate name for the server in the Label field, e.g. SMEWEB01.
3. Change the Real Server IP Address field to the required IP address, e.g. 192.168.86.78.
4. Click Update.
5. Repeat these steps to add additional servers as required.

Configuring VIP 3 – SME SQL

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. SME_SQL_VIP.
3. Set the Virtual Service IP Address field to the required IP address, e.g. 192.168.86.81.
4. Set the **Virtual Service Ports** field to **3306**.

5. Set the **Layer 7 Protocol** to **TCP Mode**.

6. Click **Update** to create the virtual service.

![Layer 7 - Add a new Virtual Service](image)

7. Click **Modify** next to the newly created VIP.

8. Set **Persistence Mode** to **Source IP**.

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** (this is 5 minutes).

13. Set **Real Server Timeout** to **5m**.

14. Click **Update**.

![Other configuration settings](image)

**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. Enter an appropriate name for the server in the **Label** field, e.g. **SMESQL01**.
3. Change the *Real Server IP Address* field to the required IP address, e.g. **192.168.86.82**.

4. Click **Update**.

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

### Configuring VIP 4 – SME Memcache

#### 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. **SME_MEMCACHE_VIP**.

3. Set the *Virtual Service IP Address* field to the required IP address, e.g. **192.168.86.86**.

4. Set the *Virtual Service Ports* field to **11211**.

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 **Source IP**.
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** (this is 5 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. Enter an appropriate name for the server in the **Label** field, e.g. *SMESQL01*.
3. Change the **Real Server IP Address** field to the required IP address, e.g. *192.168.86.82*.
4. Click **Update**.
5. Repeat these steps to add additional 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 SME 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 both SME servers are healthy, across all 5 virtual services, and available to accept connections:

![System Overview](image)

**Layer 4 Direct Routing Specific Check**

If using the setup that combines layer 4 DR mode and layer 7 SNAT mode, it is possible to specifically check that...
layer 4 DR mode has been correctly configured (including verifying that the real servers have been modified correctly in regards to the ARP problem).

After sending traffic to the layer 4 DR mode virtual services, check that connections are not in the SYN_RECV state and that they are ESTABLISHED. This can be done through the load balancer’s WebUI, by navigating to Reports > Layer 4 Current Connections.

If there are a significant number of connections in the SYN_RECV state then that implies that the ARP problem has not been correctly resolved on the back end real servers.

### Layer 4 Current Connections

<table>
<thead>
<tr>
<th>IPVS connection entries</th>
<th>source</th>
<th>virtual</th>
<th>destination</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP 08:44 FIN WAIT</td>
<td>192.168.86.2:56718</td>
<td>192.168.86.85:443</td>
<td>192.168.86.78:443</td>
</tr>
<tr>
<td>TCP 01:18 FIN WAIT</td>
<td>192.168.86.2:56842</td>
<td>192.168.86.85:443</td>
<td>192.168.86.78:443</td>
</tr>
<tr>
<td>TCP 01:28 FIN WAIT</td>
<td>192.168.86.2:56844</td>
<td>192.168.86.85:443</td>
<td>192.168.86.78:443</td>
</tr>
<tr>
<td>TCP 00:45 FIN WAIT</td>
<td>192.168.86.2:56765</td>
<td>192.168.86.85:443</td>
<td>192.168.86.78:443</td>
</tr>
<tr>
<td>TCP 08:38 FIN WAIT</td>
<td>192.168.86.2:56722</td>
<td>192.168.86.85:443</td>
<td>192.168.86.78:443</td>
</tr>
<tr>
<td>TCP 01:42 FIN WAIT</td>
<td>192.168.86.2:56912</td>
<td>192.168.86.85:443</td>
<td>192.168.86.78:443</td>
</tr>
<tr>
<td>TCP 08:45 FIN WAIT</td>
<td>192.168.86.2:56780</td>
<td>192.168.86.85:443</td>
<td>192.168.86.78:443</td>
</tr>
<tr>
<td>TCP 08:32 FIN WAIT</td>
<td>192.168.86.2:37500</td>
<td>192.168.86.85:80</td>
<td>192.168.86.70:80</td>
</tr>
<tr>
<td>TCP 01:49 FIN WAIT</td>
<td>192.168.86.2:56914</td>
<td>192.168.86.85:443</td>
<td>192.168.86.70:443</td>
</tr>
<tr>
<td>TCP 08:38 FIN WAIT</td>
<td>192.168.86.2:56744</td>
<td>192.168.86.85:443</td>
<td>192.168.86.70:443</td>
</tr>
<tr>
<td>TCP 08:38 FIN WAIT</td>
<td>192.168.86.2:56736</td>
<td>192.168.86.85:443</td>
<td>192.168.86.70:443</td>
</tr>
<tr>
<td>TCP 08:45 FIN WAIT</td>
<td>192.168.86.2:56780</td>
<td>192.168.86.85:443</td>
<td>192.168.86.70:443</td>
</tr>
<tr>
<td>TCP 01:18 FIN WAIT</td>
<td>192.168.86.2:56846</td>
<td>192.168.86.85:443</td>
<td>192.168.86.70:443</td>
</tr>
<tr>
<td>TCP 00:52 FIN WAIT</td>
<td>192.168.86.2:56752</td>
<td>192.168.86.85:443</td>
<td>192.168.86.70:443</td>
</tr>
<tr>
<td>TCP 08:59 FIN WAIT</td>
<td>192.168.86.2:56794</td>
<td>192.168.86.85:443</td>
<td>192.168.86.70:443</td>
</tr>
<tr>
<td>TCP 08:32 FIN WAIT</td>
<td>192.168.86.2:37496</td>
<td>192.168.86.85:80</td>
<td>192.168.86.70:80</td>
</tr>
<tr>
<td>IP 04:54 NONE</td>
<td>192.168.86.2:8</td>
<td>119.53.147.255:0</td>
<td>192.168.86.78:0</td>
</tr>
<tr>
<td>TCP 08:38 FIN WAIT</td>
<td>192.168.86.2:56720</td>
<td>192.168.86.85:443</td>
<td>192.168.86.70:443</td>
</tr>
<tr>
<td>TCP 08:38 FIN WAIT</td>
<td>192.168.86.2:56725</td>
<td>192.168.86.85:443</td>
<td>192.168.86.70:443</td>
</tr>
<tr>
<td>TCP 08:44 FIN WAIT</td>
<td>192.168.86.2:56755</td>
<td>192.168.86.85:443</td>
<td>192.168.86.70:443</td>
</tr>
<tr>
<td>TCP 14:57 ESTABLISHED</td>
<td>192.168.86.2:56932</td>
<td>192.168.86.85:443</td>
<td>192.168.86.70:443</td>
</tr>
</tbody>
</table>

**SFTP Service Check**

For details on how to perform a check of the SFTP service, see Testing the SFTP Service.

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 Storage Made
Easy File Fabric environments.
17. Appendix

Solving the ARP Problem

When using Layer 4 DR mode, the ARP problem must be solved. This involves configuring each Real Server to be able to receive traffic destined for the VIP, and ensuring that each Real Server does not respond to ARP requests for the VIP address – only the load balancer should do this. The steps below are for Windows 2012 and later.

Windows Server 2012 & Later

Windows Server 2012 and later support Direct Routing (DR) mode through the use of the Microsoft Loopback Adapter. The IP address allocated to the Loopback Adapter must be the same as the Virtual Service (VIP) address. If the Real Server is included in multiple DR mode VIPs, additional IP addresses can be added to the Loopback Adapter that correspond to each VIP. In addition, steps must be taken to set the strong/weak host behavior which is used to either block or allow interfaces to receive packets destined for a different interface on the same server.

Step 1 of 3: Install the Microsoft Loopback Adapter

1. Click Start, then run hdwwiz to start the Hardware Installation Wizard.
2. When the Wizard has started, click Next.
3. Select Install the hardware that I manually select from a list (Advanced), click Next.
4. Select Network adapters, click Next.
5. Select Microsoft & Microsoft KM-Test Loopback Adapter, click Next.
6. Click Next to start the installation, when complete click Finish.

Step 2 of 3: Configure the Loopback Adapter

1. Open Control Panel and click Network and Sharing Center.
2. Click **Change adapter settings**.

3. Right-click the new Loopback Adapter and select **Properties**.

4. Uncheck all items except **Internet Protocol Version 4 (TCP/IPv4)** and **Internet Protocol Version 6 (TCP/IPv6)** as shown below:

| Note | Leaving both checked ensures that both IPv4 and IPv6 are supported. Select one if preferred. |

5. If configuring IPv4 addresses select **Internet Protocol Version (TCP/IPv4)**, click **Properties** and configure the IP address to be the same as the Virtual Service (VIP) with a subnet mask of 255.255.255.255 , e.g. 192.168.2.20/255.255.255.255 as shown below:
6. If configuring IPv6 addresses select Internet Protocol Version (TCP/IPv6), click Properties and configure the IP address to be the same as the Virtual Service (VIP) and set the Subnet Prefix Length to be the same as your network setting, e.g. 2001:470:1f09:e72::15/64 as shown below:

7. Click OK on TCP/IP Properties, then click Close on Ethernet Properties to save and apply the new settings.

Note: For Windows 2012/2016/2019, it’s not necessary to modify the interface metric on the advanced tab and should be left set to Automatic.

Step 3 of 3: Configure the strong/weak host behavior

To configure the correct strong/weak host behavior for Windows 2012/2016/2019, the following commands must be
run on each Real Server:

For IPv4 addresses:

```
netsh interface ipv4 set interface "net" weakhostreceive=enabled
netsh interface ipv4 set interface "loopback" weakhostreceive=enabled
```

For these commands to work, the LAN connection NIC must be named "net" and the loopback NIC must be named "loopback" as shown below. If you prefer to leave your current NIC names, then the commands above must be modified accordingly. For example, if your network adapters are named "LAN" and "LOOPBACK", the commands required would be:

```
netsh interface ipv4 set interface "LAN" weakhostreceive=enabled
netsh interface ipv4 set interface "LOOPBACK" weakhostreceive=enabled
```

For IPv6 addresses:

```
netsh interface ipv6 set interface "net" weakhostreceive=enabled
netsh interface ipv6 set interface "loopback" weakhostreceive=enabled
```

For these commands to work, the LAN connection NIC must be named "net" and the loopback NIC must be named "loopback" as shown below. If you prefer to leave your current NIC names, then the commands above must be modified accordingly. For example, if your network adapters are named "LAN" and "LOOPBACK", the commands required would be:

```
netsh interface ipv6 set interface "LAN" weakhostreceive=enabled
netsh interface ipv6 set interface "LOOPBACK" weakhostreceive=enabled
```

Note

The names for the NICs are case sensitive, so make sure that the name used for the interface and the name used in the commands match exactly.

- Start PowerShell or use a command window to run the appropriate netsh commands as shown in the example below:
This shows an IPv6 example, use the IPv4 commands if you’re using IPv4 addresses.

Repeat steps 1 - 3 on all remaining Windows 2012/2016/2019 Real Server(s).

If preferred you can also use the following PowerShell Cmdlets:

The following example configures both IPv4 and IPv6 at the same time:

Set-NetIpInterface -InterfaceAlias loopback -WeakHostReceive enabled -WeakHostSend enabled -DadTransmits 0

Set-NetIpInterface -InterfaceAlias net -WeakHostReceive enabled

To configure just IPv4:

Set-NetIpInterface -InterfaceAlias loopback -WeakHostReceive enabled -WeakHostSend enabled -DadTransmits 0 -AddressFamily IPv4

Set-NetIpInterface -InterfaceAlias net -WeakHostReceive enabled -AddressFamily IPv4

To configure just IPv6:

Set-NetIpInterface -InterfaceAlias loopback -WeakHostReceive enabled -WeakHostSend enabled -DadTransmits 0 -AddressFamily IPv6

Set-NetIpInterface -InterfaceAlias net -WeakHostReceive enabled -AddressFamily IPv6

Testing the SFTP Service

When using SFTP, it should be possible to access the SFTP virtual service using pre-configured SME web portal credentials.

It should be possible to access the SFTP service via the VIP address, by using an SFTP client and appropriate credentials:
The test connection should appear on the System Overview page:

**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.
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:*

**Note**

If you have already run the firewall lockdown wizard on either appliance, you’ll need to ensure that it is temporarily disabled on both appliances whilst performing the pairing process.

1. Deploy a second appliance that will be the Secondary and configure initial network settings.
2. Using the WebUI on the Primary appliance, navigate to: Cluster Configuration > High-Availability Configuration.
3. Specify the IP address and the `loadbalancer` user’s password for the Secondary (peer) appliance as shown above.

4. Click Add new node.

5. The pairing process now commences as shown below:

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

7. To finalize the configuration, restart heartbeat and any other services as prompted in the blue message box at the top of the screen.
Clicking the **Restart Heartbeat** button on the Primary appliance will also automatically restart heartbeat on the Secondary appliance.

For more details on configuring HA with 2 appliances, please refer to *Appliance Clustering for HA*.

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>17 December 2019</td>
<td>Initial version</td>
<td></td>
<td>IBG, AH</td>
</tr>
<tr>
<td>1.0.1</td>
<td>3 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 December 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.