Load Balancing Fujifilm SYNAPSE

Version 1.3.0
Table of Contents

1. About this Guide ................................................................. 4
2. Loadbalancer.org Appliances Supported ................................ 4
3. Loadbalancer.org Software Versions Supported ...................... 4
4. Fujifilm Synapse Software Versions Supported ...................... 4
5. Load Balancing Fujifilm Synapse ......................................... 4
   Port Requirements ............................................................. 4
   Deployment Concept ........................................................ 5
   Virtual Service (VIP) Requirements ..................................... 5
   Synapse PACS ................................................................. 5
   Synapse VNA ................................................................. 5
   Synapse Mobility ............................................................ 5
   Synapse CWM ............................................................... 6
   Synapse Server Configuration Requirements .......................... 6
      SNAT Mode ............................................................... 6
      DR Mode ................................................................. 6
6. Loadbalancer.org Appliance – the Basics ............................... 6
   Virtual Appliance ............................................................. 6
   Initial Network Configuration ............................................. 7
   Accessing the WebUI ....................................................... 7
      Main Menu Options .................................................... 8
   HA Clustered Pair Configuration ....................................... 9
7. Load Balancing Fujifilm Synapse PACS ................................ 9
   Appliance Configuration ................................................... 9
      Configuring VIP1 - synapsePacsHTTP ............................. 9
      Configuring VIP2 - synapsePacsDICOM ........................... 10
   Synapse PACS Configuration ......................................... 11
8. Load Balancing Fujifilm Synapse VNA ................................ 12
   Appliance Configuration ................................................... 12
      Configuring VIP1 - synapsePacsHTTP ............................. 12
      Configuring VIP2 - synapsePacsDICOM ........................... 13
   Synapse VNA Configuration ......................................... 14
9. Load Balancing Fujifilm Synapse Mobility ............................ 14
   Appliance Configuration ................................................... 14
      Configuring VIP1 - synapseMobility ............................... 14
   Synapse Mobility Configuration ..................................... 16
10. Load Balancing Fujifilm Synapse CWM ................................ 16
   Appliance Configuration .................................................. 16
      Configuring VIP1 - SynapseCwm .................................. 16
   Synapse CWM Configuration ....................................... 17
11. Additional Configuration Options & Settings ........................ 17
   SSL Termination ............................................................ 17
   SSL Termination on the load balancer - SSL Offloading .......... 17
      Certificates ............................................................. 18
   Configuring SSL Termination on the Load Balancer ................. 20
      1) Configuring SSL Offloading for Synapse Mobility using a Layer 7 HTTP mode VIP .............................. 20
      2) Configure SSL termination ..................................... 21
   Finalizing the Configuration ......................................... 22
12. Testing & Verification ......................................................... 22
   Using the System Overview ............................................. 22
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client Connection Tests</td>
<td>23</td>
</tr>
<tr>
<td>13. Technical Support</td>
<td>23</td>
</tr>
<tr>
<td>14. Additional Documentation</td>
<td>23</td>
</tr>
<tr>
<td>15. Conclusion</td>
<td>23</td>
</tr>
<tr>
<td>16. Appendix</td>
<td>24</td>
</tr>
<tr>
<td>Configuring HA - Adding a Secondary Appliance</td>
<td>24</td>
</tr>
<tr>
<td>DR Mode Server Configuration</td>
<td>26</td>
</tr>
<tr>
<td>Windows Server 2012, 2016 &amp; 2019</td>
<td>26</td>
</tr>
<tr>
<td>17. Document Revision History</td>
<td>32</td>
</tr>
</tbody>
</table>
1. About this Guide

This guide details the steps required to configure a load balanced Fujifilm Synapse environment utilizing Loadbalancer.org appliances. It covers Synapse PACS, Synapse VNA, Synapse Mobility and Synapse CWM and details the configuration of the load balancers and also any Synapse server configuration changes that are required to enable load balancing.

For more information about initial appliance deployment, network configuration and using the Web User Interface (WebUI), please also refer to the Administration Manual.

2. Loadbalancer.org Appliances Supported

All our products can be used with Fujifilm Synapse. 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

4. Fujifilm Synapse Software Versions Supported

- Fujifilm Synapse PACS – All versions
- Fujifilm Synapse VNA – All versions
- Fujifilm Synapse Mobility – All versions
- Fujifilm Synapse CWM – All versions

5. Load Balancing Fujifilm Synapse

For high availability and scalability, Fujifilm recommend that multiple Synapse Servers are deployed in a load balanced cluster.

Port Requirements

The following table shows the ports used by the various Synapse systems. The load balancer must be configured to listen on the same ports.

<table>
<thead>
<tr>
<th>Port</th>
<th>Protocols</th>
<th>System</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>80</td>
<td>TCP</td>
<td>PACS</td>
<td>HTTP</td>
</tr>
<tr>
<td>104</td>
<td>TCP</td>
<td>PACS</td>
<td>DICOM</td>
</tr>
<tr>
<td>80</td>
<td>TCP</td>
<td>VNA</td>
<td>HTTP</td>
</tr>
<tr>
<td>104</td>
<td>TCP</td>
<td>VNA</td>
<td>DICOM</td>
</tr>
<tr>
<td>8080</td>
<td>TCP</td>
<td>Mobility</td>
<td>HTTP</td>
</tr>
<tr>
<td>8443</td>
<td>TCP</td>
<td>Mobility</td>
<td>HTTPS</td>
</tr>
<tr>
<td>80</td>
<td>TCP</td>
<td>CWM</td>
<td>HTTP</td>
</tr>
</tbody>
</table>
Deployment Concept

When Fujifilm systems are deployed with the load balancer, clients connect to the Virtual Service (VIP) on the load balancer rather than connecting directly to one of the Fujifilm servers. The load balancer then distributes these connection to the load balanced servers according to the algorithm selected.

**Note**
The load balancer can be deployed as a single unit, although Loadbalancer.org recommends a clustered pair for resilience & high availability. Please refer to Configuring HA - Adding a Secondary Appliance for more details on configuring a clustered pair.

Virtual Service (VIP) Requirements

The following tables summarize the VIPs required for each Synapse system and how they are configured.

**Synapse PACS**

2 VIPs are required:

<table>
<thead>
<tr>
<th>Ref.</th>
<th>VIP Name</th>
<th>Operating Mode</th>
<th>Protocol</th>
<th>Port(s)</th>
<th>Persistence</th>
<th>Health check Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>VIP1</td>
<td>SynapsePacsHTTP</td>
<td>Layer 7 SNAT mode</td>
<td>TCP</td>
<td>80</td>
<td>Source IP</td>
<td>Connect to Port</td>
</tr>
<tr>
<td>VIP2</td>
<td>SynapsePacsDICOM</td>
<td>Layer 4 DR mode</td>
<td>TCP</td>
<td>104</td>
<td>Source IP</td>
<td>External Script – DICOM-C-ECHO</td>
</tr>
</tbody>
</table>

**Synapse VNA**

2 VIPs are required:

<table>
<thead>
<tr>
<th>Ref.</th>
<th>VIP Name</th>
<th>Operating Mode</th>
<th>Protocol</th>
<th>Port(s)</th>
<th>Persistence</th>
<th>Health check Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>VIP1</td>
<td>SynapseVnaHTTP</td>
<td>Layer 7 SNAT mode</td>
<td>TCP</td>
<td>80</td>
<td>Source IP</td>
<td>Connect to Port</td>
</tr>
<tr>
<td>VIP2</td>
<td>SynapseVnaDICOM</td>
<td>Layer 4 DR mode</td>
<td>TCP</td>
<td>104</td>
<td>Source IP</td>
<td>External Script – DICOM-C-ECHO</td>
</tr>
</tbody>
</table>

**Synapse Mobility**

1 VIP is required:
Synapse CWM
1 VIP is required:

<table>
<thead>
<tr>
<th>Ref.</th>
<th>VIP Name</th>
<th>Operating Mode</th>
<th>Protocol</th>
<th>Port(s)</th>
<th>Persistence</th>
<th>Health check Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>VIP1</td>
<td>SynapseCwm</td>
<td>Layer 7 SNAT mode</td>
<td>HTTP</td>
<td>80</td>
<td>HTTP Cookie</td>
<td>Connect to Port</td>
</tr>
</tbody>
</table>

Synapse Server Configuration Requirements
As mentioned in the tables above, Layer 7 SNAT mode and Layer 4 DR mode are used when load balancing Fujifilm Synapse.

SNAT Mode
When using Layer 7 SNAT mode, no additional Synapse server configuration changes are required.

DR Mode
When using DR mode, the ‘ARP problem’ must be solved on each Synapse server for DR mode to work. For detailed steps on solving the ARP problem, please refer to DR Mode Server Configuration for more information.

6. 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. Appliance authentication is based on Apache .htaccess files. User admin 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:
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
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.

7. Load Balancing Fujifilm Synapse PACS

Appliance Configuration

Configuring VIP1 - synapsePacsHTTP

a) Setting up the Virtual Service

1. Using the WebUI, navigate to: Cluster Configuration > Layer 7 – Virtual Service and click Add a New Virtual Service.

2. Enter the following details:

   - **Label**: SynapsePacsHTTP
   - **IP Address**: 10.50.20.10
   - **Ports**: 80
   - **Layer 7 Protocol**: TCP Mode

3. Enter an appropriate label for the VIP, e.g. SynapsPacsHTTP.

4. Set the Virtual Service IP address field to the required IP address, e.g. 10.50.20.10.

5. Set the Virtual Service Ports field to 80.


7. Click Update.

b) Setting up the Real Servers

1. Using the WebUI, navigate to: Cluster Configuration > Layer 7 – Real Servers and click Add a new Real Server next to the newly created VIP.

2. Enter the following details:
3. Enter an appropriate label for the RIP, e.g. **Server1**.

4. Set the **Real Server IP Address** field to the required IP address, e.g. **10.50.20.20**.

5. Set the **Real Server Port** field to **80**.

6. Click **Update**.

7. Repeat the above steps to add your other server(s).

**Configuring VIP2 - synapsePacsDICOM**

**a) Setting up the Virtual Service (VIP)**

1. Using the WebUI, navigate to: **Cluster Configuration > Layer 4 – Virtual Services** and click **Add a new Virtual Service**.

2. Enter the following details:

   - **Label**: SynapsePacsDICOM
   - **Virtual Service IP address**: 10.50.20.11
   - **Virtual Service Ports**: 104
   - **Protocol**: TCP
   - **Forwarding Method**: Direct Routing

3. Enter an appropriate label (name) for the VIP, e.g. **SynapsePacsDICOM**.

4. Set the **Virtual Service IP address** field to the required IP address, e.g. **10.50.20.11**.

5. Set the **Virtual Service Ports** field to **104**.

   **Note**  
   For layer 4 DR mode a star ( * ) can be specified instead of **104** to mean "all ports" if required.

6. Leave **Protocol** set to **TCP**.
7. Leave the *Forwarding Method* to Direct Return.
8. Click Update.
9. Now click Modify next to the newly created Virtual Service.
10. Scroll down to the *Health Checks* section and set the *Health Check* to **External Script**.
11. Set the *Check Port* to 104.

```
For v8.6 and later, you’ll first need to add the DICOM-C-ECHO check from template:

1. Using the WebUI, navigate to *Cluster Configuration > Health Check Scripts* and click *Add New Health Check*.
2. Specify an appropriate *Name* for the health check, e.g. **DICOM-C-ECHO**.
3. Set *Type* to **Virtual Service**.
4. Set the *Template* dropdown to **DICOM-C-ECHO**.
5. Click *Update*.
```

12. Set *External script* to **DICOM-C-ECHO**.

b) Setting up the Real Server (RIP)
1. Using the WebUI, navigate to: *Cluster Configuration > Layer 4 – Real Servers* and click *Add a new Real Server* next to the newly created VIP.
2. Enter the following details:

```
3. Enter an appropriate label (name) for the RIP, e.g. **Server1**.
4. Change the *Real Server IP Address* field to the required IP address, e.g. **10.50.20.21**.
5. Click *Update*.
6. Repeat the above steps to add your other server(s).
```

**Synapse PACS Configuration**

Since VIP2 is configured using layer 4 DR (Direct Return) mode, the "ARP Problem" must be solved on each Synapse server as mentioned in **DR Mode**. For full details on how this is done, please refer to **DR Mode Server Configuration**.
8. Load Balancing Fujifilm Synapse VNA

Appliance Configuration
Configuring VIP1 - synapsePacsHTTP

a) Setting up the Virtual Service
1. Using the WebUI, navigate to: Cluster Configuration > Layer 7 – Virtual Service and click Add a New Virtual Service.
2. Enter the following details:

<table>
<thead>
<tr>
<th>Label</th>
<th>SynapseVnaHTTP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual Service</td>
<td></td>
</tr>
<tr>
<td>IP Address</td>
<td>10.50.20.12</td>
</tr>
<tr>
<td>Ports</td>
<td>80</td>
</tr>
<tr>
<td>Protocol</td>
<td></td>
</tr>
<tr>
<td>Layer 7 Protocol</td>
<td>TCP Mode</td>
</tr>
</tbody>
</table>

3. Enter an appropriate label for the VIP, e.g. SynapseVnaHTTP.
4. Set the Virtual Service IP address field to the required IP address, e.g. 10.50.20.12.
5. Set the Virtual Service Ports field to 80.
7. Click Update.

b) Setting up the Real Servers
1. Using the WebUI, navigate to: Cluster Configuration > Layer 7 – Real Servers and click Add a new Real Server next to the newly created VIP.
2. Enter the following details:

<table>
<thead>
<tr>
<th>Label</th>
<th>Server1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Real Server IP Address</td>
<td>10.50.20.22</td>
</tr>
<tr>
<td>Real Server Port</td>
<td>80</td>
</tr>
<tr>
<td>Re-Encrypt to Backend</td>
<td></td>
</tr>
<tr>
<td>Weight</td>
<td>100</td>
</tr>
</tbody>
</table>

3. Enter an appropriate label for the RIP, e.g. Server1.
4. Set the *Real Server IP Address* field to the required IP address, e.g. 10.50.20.22.
5. Set the *Real Server Port* field to 80.
6. Click *Update*.
7. Repeat the above steps to add your other server(s).

### Configuring VIP2 - synapsePacsDICOM

a) Setting up the Virtual Service (VIP)

1. Using the WebUI, navigate to: *Cluster Configuration > Layer 4 – Virtual Services* and click *Add a new Virtual Service*.
2. Enter the following details:

   ![Virtual Service Configuration](image)

   3. Enter an appropriate label (name) for the VIP, e.g. *SynapseVnaDICOM*.
   4. Set the *Virtual Service IP address* field to the required IP address, e.g. 10.50.20.13.
   5. Set the *Virtual Service Ports* field to 104.

   **Note**

   For layer 4 DR mode a star ( * ) can be specified instead of 104 to mean "all ports" if required.

6. Leave *Protocol* set to TCP.
7. Leave the *Forwarding Method* to Direct Return.
8. Click *Update*.
9. Now click *Modify* next to the newly created Virtual Service.
10. Scroll down to the *Health Checks* section and set the *Health Check* to External Script.
11. Set the *Check Port* to 104.
For v8.6 and later, you'll first need to add the DICOM-C-ECHO check from template:

1. Using the WebUI, navigate to Cluster Configuration > Health Check Scripts and click Add New Health Check.

2. Specify an appropriate Name for the health check, e.g. DICOM-C-ECHO.
3. Set Type to Virtual Service.
4. Set the Template dropdown to DICOM-C-ECHO.
5. Click Update.

12. Set External script to DICOM-C-ECHO.

b) Setting up the Real Server (RIP)

1. Using the WebUI, navigate to: Cluster Configuration > Layer 4 – Real Servers and click Add a new Real Server next to the newly created VIP.
2. Enter the following details:

   - Label: Server1
   - Real Server IP Address: 10.50.20.23
   - Weight: 100
   - Minimum Connections: 0
   - Maximum Connections: 0

3. Enter an appropriate label (name) for the RIP, e.g. Server1.
4. Change the Real Server IP Address field to the required IP address, e.g. 10.50.20.23.
5. Click Update.
6. Repeat the above steps to add your other server(s).

Synapse VNA Configuration

Since VIP2 is configured using layer 4 DR (Direct Return) mode, the "ARP Problem" must be solved on each Synapse server as mentioned in DR Mode. For full details on how this is done, please refer to DR Mode Server Configuration.

9. Load Balancing Fujifilm Synapse Mobility

Appliance Configuration
Configuring VIP1 - synapseMobility

a) Setting up the Virtual Service

1. Using the WebUI, navigate to: Cluster Configuration > Layer 7 – Virtual Service and click Add a New Virtual Service.
2. Enter the following details:

<table>
<thead>
<tr>
<th>Label</th>
<th>SynapseMobility</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address</td>
<td>10.50.20.14</td>
</tr>
<tr>
<td>Ports</td>
<td>8080,8443</td>
</tr>
<tr>
<td>Layer 7 Protocol</td>
<td>TCP Mode</td>
</tr>
</tbody>
</table>

3. Enter an appropriate label for the VIP, e.g. **SynapseMobility**.

4. Set the **Virtual Service IP address** field to the required IP address, e.g. **10.50.20.14**.

5. Set the **Virtual Service Ports** field to **8080,8443**.

6. Set **Layer 7 Protocol** set to **TCP Mode**.

7. Click **Update**.

8. Scroll down to the **Health Checks** section and set the **Health Check** to **Negotiate HTTP (GET)**.

9. Set **Request to Send** to **https://syncavmob:8080/pureweb/server/login.jsp**.

10. Leave **Response Expected** blank (this will configure the load balancer to look for a 200 OK response).

b) Setting up the Real Servers

1. Using the WebUI, navigate to: **Cluster Configuration > Layer 7 – Real Servers** and click **Add a new Real Server** next to the newly created VIP.

2. Enter the following details:

<table>
<thead>
<tr>
<th>Label</th>
<th>Server1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Real Server IP Address</td>
<td>10.50.20.24</td>
</tr>
<tr>
<td>Real Server Port</td>
<td></td>
</tr>
<tr>
<td>Re-Encrypt to Backend</td>
<td></td>
</tr>
<tr>
<td>Weight</td>
<td>100</td>
</tr>
</tbody>
</table>

3. Enter an appropriate label for the RIP, e.g. **Server1**.

4. Set the **Real Server IP Address** field to the required IP address, e.g. **10.50.20.24**.
5. Leave the Real Server Port field blank.

6. Click Update.

7. Repeat the above steps to add your other server(s).

**Synapse Mobility Configuration**

As mentioned in SNAT Mode, when using Layer 7 SNAT mode no additional Synapse server configuration changes are required.

**10. Load Balancing Fujifilm Synapse CWM**

**Appliance Configuration**

**Configuring VIP1 - SynapseCwm**

a) Setting up the Virtual Service

1. Using the WebUI, navigate to: Cluster Configuration > Layer 7 – Virtual Service and click Add a New Virtual Service.

2. Enter the following details:

   ![Virtual Service Configuration](image)

3. Enter an appropriate label for the VIP, e.g. SynapseCwm.

4. Set the Virtual Service IP address field to the required IP address, e.g. 10.50.20.15.

5. Set the Virtual Service Ports field to 80.


7. Click Update.

b) Setting up the Real Servers

1. Using the WebUI, navigate to: Cluster Configuration > Layer 7 – Real Servers and click Add a new Real Server next to the newly created VIP.

2. Enter the following details:
3. Enter an appropriate label for the RIP, e.g. **Server1**.

4. Set the **Real Server IP Address** field to the required IP address, e.g. **10.50.20.25**.

5. Set the **Real Server Port** field to **80**.

6. Click **Update**.

7. Repeat the above steps to add your other server(s).

**Synapse CWM Configuration**

As mentioned in **SNAT Mode**, when using Layer 7 SNAT mode no additional Synapse server configuration changes are required.

11. Additional Configuration Options & Settings

**SSL Termination**

SSL termination can be handled in the following ways:

1. On the Real Servers - aka **SSL Pass-through**
2. On the load balancer – aka **SSL Offloading**
3. On the load balancer with re-encryption to the backend servers – aka **SSL Bridging**

**Note**

SSL termination on the load balancer can be very CPU intensive.

By default, a self-signed certificate is used for the new SSL VIP. Certificates can be requested on the load balancer or uploaded as described in the section below. The default self-signed certificate can be regenerated if needed using the WebUI menu option: SSL Certificate and clicking the **Regenerate Local SSL Certificate button**.

The backend for the SSL VIP can be either a Layer 7 SNAT mode VIP or a Layer 4 NAT or SNAT mode VIP. Layer 4 DR mode cannot be used since stunnel acts as a proxy, and the VPSA node servers see requests with a source IP address of the VIP. However, since the VPSA node servers believe that they own the VIP (due to the loopback adapter configured to handle to ARP problem) they are unable to reply to stunnel.

**SSL Termination on the load balancer - SSL Offloading**
In this case, an SSL VIP utilizing stunnel is configured on the appliance and an SSL certificate is uploaded and associated to the Virtual Service. Data is encrypted from the client to the load balancer, but is un-encrypted from the load balancer to the backend servers as shown above.

Certificates

If you already have an SSL certificate in either PFX or PEM file format, this can be uploaded to the Load balancer using the certificate upload option as explained in Uploading Certificates. Alternatively, you can create a Certificate Signing Request (CSR) and send this to your CA to create a new certificate.

Generating a CSR on the Load Balancer

CSR’s can be generated on the load balancer to apply for a certificate from your chosen CA.

To generate a CSR:

1. Using the WebUI, navigate to: Cluster Configuration > SSL Certificates.
2. Click Add a new SSL Certificate & select Create a New SSL Certificate (CSR).
3. Enter a suitable label (name) for the certificate, e.g. **Cert1**.

4. Populate the remaining fields according to your requirements.

5. Once all fields are complete click **Create CSR**.

6. To view the CSR click **Modify** next to the new certificate, then expand the Certificate Signing Request (CSR) section.

7. Copy the CSR and send this to your chosen CA.

8. Once received, copy/paste your signed certificate into the Your Certificate section.

9. Intermediate and root certificates can be copied/pasted into the Intermediate Certificate and Root Certificate sections as required.

10. Click **Update** to complete the process.

### Uploading Certificates

If you already have a certificate in either PEM or PFX format, this can be uploaded to the load balancer.

To upload a Certificate:

1. Using the WebUI, navigate to: **Cluster Configuration > SSL Certificates**.

2. Click **Add a new SSL Certificate** & select **Upload prepared PEM/PFX file**.
3. Enter a suitable Label (name) for the certificate, e.g. **Cert1**.

4. Browse to and select the certificate file to upload (PEM or PFX format).

5. Enter the password if applicable.

6. Click **Upload Certificate**, if successful, a message similar to the following will be displayed:

   ![Information: cert1 SSL Certificate uploaded successfully.]

   **Note**

   It’s important to back up all of your certificates. This can be done via the WebUI from **Maintenance > Backup & Restore > Download SSL Certificates**.

### Configuring SSL Termination on the Load Balancer

To configure an SSL VIP the steps are outlined below:

1. Configure a layer 7 HTTP mode VIP
2. Configure SSL termination

1) Configuring SSL Offloading for Synapse Mobility using a Layer 7 HTTP mode VIP

a) Setting up the Virtual Service (VIP)

1. Using the WebUI, navigate to **Cluster Configuration > Layer 7 – Virtual Services** and click **Add a new Virtual Service**.
2. Enter the following details:

   ![Layer 7 - Add a new Virtual Service]

   3. Enter an appropriate label for the VIP, e.g. **SynapseMobility**.
4. Set the **Virtual Service IP address** field to the required IP address, e.g. **10.50.20.14**.
5. Set the **Virtual Service Ports** field to **8080**.
6. Set **Layer 7 Protocol** to **HTTP Mode**.
7. Click Update.
8. Click Modify.
9. Scroll down to the Health Checks section and set the Health Check to Negotiate HTTP (GET).
11. Leave Response Expected blank (this will configure the load balancer to look for a 200 OK response).

b) Setting up the Real Servers
1. Using the WebUI, navigate to: Cluster Configuration > Layer 7 – Real Servers and click Add a new Real Server next to the newly created VIP.
2. Enter the following details:

<table>
<thead>
<tr>
<th>Label</th>
<th>Server1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Real Server IP Address</td>
<td>10.50.20.24</td>
</tr>
<tr>
<td>Real Server Port</td>
<td></td>
</tr>
<tr>
<td>Re-Encrypt to Backend</td>
<td></td>
</tr>
<tr>
<td>Weight</td>
<td>100</td>
</tr>
</tbody>
</table>

3. Enter an appropriate label for the RIP, e.g. Server1.
4. Set the Real Server IP Address field to the required IP address, e.g. 10.50.20.24.
5. Leave the Real Server Port field blank.
6. Click Update.
7. Repeat the above steps to add your other server(s).

2) Configure SSL termination
1. Using the WebUI, navigate to Cluster Configuration > SSL Termination and click Add a new Virtual Service.
2. Set **Associated Virtual Service** to the appropriate VIP, e.g. **SynapseMobility**. This will automatically fill in the label as the VIP name with SSL inserted in front of the VIP name e.g. **SSL-SynapseMobility**.

**Note**

The Associated Virtual Service drop-down is populated with all single port, standard (i.e. non-manual) Layer 7 VIPs available on the load balancer. Using a Layer 7 VIP for the backend is the recommended method although as mentioned earlier, Layer 4 NAT mode and layer 4 SNAT mode VIPs can also be used if required. To forward traffic from the SSL VIP to these type of VIPs, you’ll need to set Associated Virtual Service to **Custom**, then configure the IP address & port of the required VIP.

3. Leave **Virtual Service Port** set to **443**.

4. Leave **SSL operation Mode** set to **High Security**.

5. Select the required certificate from the **SSL Certificate** drop-down.

6. Click **Update**.

7. Click **Reload STunnel** when prompted to apply the new settings using the button provided in the blue box.

Once configured, HTTP traffic will be load balanced by the Layer 7 SNAT mode VIP and HTTPS traffic will be terminated by the SSL VIP, then passed on to the Layer 7 SNAT mode VIP as unencrypted HTTP for load balancing.

**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**.

**12. Testing & Verification**

**Using the System Overview**

The System Overview shows a graphical view of all VIPs & RIPs (i.e. the Synapse servers) and shows the state/health of each server as well as the state of the each cluster as a whole. The example below shows that all Synapse servers are healthy and available to accept connections:
Client Connection Tests

Ensure that clients can connect via the load balancer to the Synapse servers. You’ll probably need to create new DNS records or modify your existing DNS records, replacing the IP addresses of individual servers or the cluster with the IP address of the Virtual Service on the load balancer.

**Note**

For more details on testing & diagnosing load balanced services please refer to [Testing Load Balanced Services](#).

13. 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.

14. Additional Documentation


15. Conclusion

Loadbalancer.org appliances provide a very cost effective solution for a highly available load balanced Fujifilm Synapse environments.
16. 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</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, 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:
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**.

### DR Mode Server Configuration

When using Layer 4 DR mode the ARP problem must be solved. This involves configuring each Synapse Server to accept traffic destined for the VIP in addition to it’s own IP address, and ensuring that each server does not respond to ARP requests for the VIP address – only the load balancer should do this. The following section covers Windows 2012 and later, for earlier versions of Windows please refer to the **Administration Manual**.

#### Windows Server 2012, 2016 & 2019

The basic concept is the same as for Windows 2000/2003. However, additional steps are required to set the strong/weak host behavior. This is used to either block or allow interfaces receiving packets destined for a different interface on the same server. As with Windows 2000/2003/2008, if the Real Server is included in multiple VIPs, you can add additional IP addresses to the Loopback Adapter that correspond to each VIP.

#### 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:**

```bash
netsh interface ipv4 set interface "net" weakhostreceive=enabled
netsh interface ipv4 set interface "loopback" weakhostreceive=enabled
netsh interface ipv4 set interface "loopback" weakhostsend=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:

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

**For IPv6 addresses:**
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:

```plaintext
netsh interface ipv6 set interface "LAN" weakhostreceive=enabled
netsh interface ipv6 set interface "LOOPBACK" weakhostreceive=enabled
netsh interface ipv6 set interface "LOOPBACK" weakhostsend=enabled
netsh interface ipv6 set interface "LOOPBACK" dadtransmits=0
```

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:

Note: 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).

For Windows 2012/2016/2019 you can also use the following PowerShell Cmdlets:

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

```powershell
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
## 17. 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 April 2018</td>
<td>Initial version</td>
<td></td>
<td>AH</td>
</tr>
<tr>
<td>1.0.1</td>
<td>6 December 2018</td>
<td>Added the new &quot;Company Contact Information&quot; page</td>
<td>Required updates</td>
<td>AH</td>
</tr>
<tr>
<td>1.2.0</td>
<td>18 September 2019</td>
<td>Multiple updates</td>
<td>Revised load balancing design</td>
<td>RJC</td>
</tr>
<tr>
<td>1.2.1</td>
<td>17 January 2020</td>
<td>Updated the health check settings for the Synapse Mobility VIP</td>
<td>To improve the accuracy of the health check</td>
<td>RJC</td>
</tr>
<tr>
<td>1.2.2</td>
<td>8 April 2020</td>
<td>Added SSL Termination</td>
<td>Revised load balancing design</td>
<td>IBG</td>
</tr>
<tr>
<td>1.2.3</td>
<td>27 July 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>1.3.0</td>
<td>1 January 2022</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.