Load Balancing Ellucian Banner
Version 1.1.0
# Table of Contents

1. About this Brief .................................................. 3
2. Loadbalancer.org Appliances Supported ...................... 3
3. Software Versions Supported .................................. 3
   3.1. Loadbalancer.org Appliance ................................ 3
   3.2. Ellucian Banner ............................................. 3
4. Ellucian Banner .................................................. 3
5. Load Balancing Ellucian Banner ................................. 3
   5.1. Persistence (aka Server Affinity) ......................... 3
   5.2. Virtual Service (VIP) Requirements ..................... 4
   5.3. Port Requirements ......................................... 4
   5.4. TLS/SSL Termination ....................................... 4
6. Deployment Concept ............................................ 4
   6.1. Recommended Deployment Type (Without TLS Termination) ........................................ 4
   6.2. Alternative Deployment Type With TLS Termination .................. 4
7. Load Balancer Deployment Methods ............................. 5
   7.1. Layer 7 SNAT Mode .......................................... 5
8. Loadbalancer.org Appliance – the Basics ....................... 6
   8.1. Virtual Appliance ........................................... 6
   8.2. Initial Network Configuration .............................. 7
   8.3. Accessing the Appliance WebUI ........................... 7
      Main Menu Options ............................................ 8
   8.4. Appliance Software Update ................................ 9
      Determining the Current Software Version .................. 9
      Checking for Updates using Online Update .................. 9
      Using Offline Update ......................................... 9
   8.5. Ports Used by the Appliance ............................... 10
   8.6. HA Clustered Pair Configuration .......................... 11
9. Appliance Configuration for Ellucian Banner – Using Layer 7 SNAT Mode (Recommended) ..................... 11
   9.1. Configuring the Virtual Service (VIP) ................... 11
   9.2. Defining the Real Servers (RIPs) ......................... 11
   9.3. Finalizing the Configuration .............................. 12
10. Appliance Configuration for Ellucian Banner – Using Layer 7 SNAT Mode With TLS Termination .............. 12
   10.1. Configuring the Virtual Service (VIP) ................. 12
   10.2. Defining the Real Servers (RIPs) ....................... 13
   10.3. Uploading a Certificate .................................... 14
   10.4. Creating the TLS/SSL Termination ....................... 14
   10.5. Finalizing the Configuration ............................. 15
11. Testing & Verification ........................................ 15
   11.1. Using System Overview .................................... 15
12. Technical Support ............................................ 15
13. Further Documentation .......................................... 16
14. Appendix ...................................................... 17
   14.1. Configuring HA - Adding a Secondary Appliance ........ 17
      Non-Replicated Settings ..................................... 17
      Configuring the HA Clustered Pair ......................... 18
15. Document Revision History .................................... 20
1. About this Brief

This brief outlines the steps required to configure a load balanced Ellucian Banner environment utilizing Loadbalancer.org appliances. It covers the configuration of the load balancers and also any Ellucian Banner 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 Ellucian Banner. For full specifications of available models please refer to https://www.loadbalancer.org/products.

Some features may not be available or fully supported in all cloud platforms due to platform specific limitations. For more details, please refer to the “Main Differences to our Standard (Non-Cloud) Product” section in the appropriate cloud platform Quick Start Guide or check with Loadbalancer.org support.

3. Software Versions Supported

3.1. Loadbalancer.org Appliance

- V8.9.1 and later

Note: The screenshots used throughout this document aim to track the latest Loadbalancer.org software version. If you're using an older version, or the very latest, the screenshots presented here may not match your WebUI exactly.

3.2. Ellucian Banner

- All versions

4. Ellucian Banner

Banner from Ellucian is a complete student information system that lets you create an integrated digital campus. Banner makes it easier for all of your users to communicate, get the information they need, and accomplish their everyday tasks.

5. Load Balancing Ellucian Banner

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

5.1. Persistence (aka Server Affinity)

Session-based persistence is used via either source IP addresses or application cookies when load balancing an
5.2. Virtual Service (VIP) Requirements

To provide load balancing and HA for Ellucian Banner, only a single VIP is required:

- HTTP(S) (for all HTTP-based services)

5.3. 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>443</td>
<td>TCP/HTTPS</td>
<td>Ellucian Banner Web Application Traffic</td>
</tr>
</tbody>
</table>

5.4. TLS/SSL Termination

It is possible to terminate TLS connections on the load balancer. Performing TLS termination can add significant CPU overhead. As such, this deployment method should not be used unless the plaintext HTTP traffic must be inspected for some reason.

Unless there is a compelling reason not to do so, the recommended deployment method without TLS termination should be used.

6. Deployment Concept

Ellucian Banner can be deployed in two different ways:

6.1. Recommended Deployment Type (Without TLS Termination)

6.2. Alternative Deployment Type With TLS Termination
VIP = Virtual IP Address

7. 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 Ellucian Banner, using layer 7 SNAT mode is recommended. This mode is described below and is used for the configurations presented in this guide.

7.1. 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 mode-specific 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.

8. Loadbalancer.org Appliance – the Basics

8.1. 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 would be required.
8.2. Initial Network Configuration

After boot up, follow the instructions on the appliance console to configure the management IP address, subnet mask, default gateway, DNS servers and other network and administrative settings.

**Important** Be sure to set a secure password for the load balancer, when prompted during the setup routine.

8.3. Accessing the Appliance WebUI

The WebUI is accessed using a web browser. By default, users are authenticated using Apache authentication. Users can also be authenticated against LDAP, LDAPS, Active Directory or Radius - for more information, please refer to External Authentication.

**Note** There are certain differences when accessing the WebUI for the cloud appliances. For details, please refer to the relevant Quick Start / Configuration Guide.

1. Using a browser, navigate to the following URL:


   **Note** You’ll receive a warning about the WebUI’s SSL certificate. This is due to the default self signed certificate that is used. If preferred, you can upload your own certificate - for more information, please refer to Appliance Security Features.

   **Note** If you need to change the port, IP address or protocol that the WebUI listens on, please refer to Service Socket Addresses.

2. Log in to the WebUI using the following credentials:

   **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:

3. You’ll be asked if you want to run the Setup Wizard which can be used to configure layer 7 services. Click **Dismiss** if you’re following a guide or want to configure the appliance manually or click **Accept** to start the wizard.

**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
- **Support** - Create a support download, contact the support team & access useful links
8.4. Appliance Software Update

To ensure that the appliance(s) are running the latest software version, we recommend a software update check is performed.

Determining the Current Software Version

The software version is displayed at the bottom of the WebUI as shown in the example below:

Checking for Updates using Online Update

1. Using the WebUI, navigate to: Maintenance > Software Update.
2. Select Online Update.
3. If the latest version is already installed, a message similar to the following will be displayed:

   Information: Version v8.11.1 is the current release. No updates are available

4. If an update is available, you’ll be presented with a list of new features, improvements, bug fixes and security related updates.
5. Click Online Update to start the update process.

   Note Do not navigate away whilst the update is ongoing, this may cause the update to fail.

6. Once complete (the update can take several minutes depending on download speed and upgrade version) the following message will be displayed:

   Information: Update completed successfully.

7. If services need to be reloaded/restarted or the appliance needs a full restart, you’ll be prompted accordingly.

Using Offline Update

If the load balancer does not have access to the Internet, offline update can be used.
To perform an offline update:

1. Using the WebUI, navigate to: **Maintenance > Software Update**.
2. Select **Offline Update**.
3. The following screen will be displayed:

   **Software Update**

   **Offline Update**

   The following steps will lead you through offline update.

   1. Contact support@loadbalancer.org to obtain the offline update archive and checksum.
   2. Save the archive and checksum to your local machine.
   3. Select the archive and checksum files in the upload form below.
   4. Click Upload and Install to begin the update process.

     **Archive:** Choose File | No file chosen
     **Checksum:** Choose File | No file chosen

     **Upload and Install**

4. Select the **Archive** and **Checksum** files.
5. Click **Upload and Install**.
6. If services need to be reloaded/restarted or the appliance needs a full restart, you'll be prompted accordingly.

### 8.5. Ports Used by the Appliance

By default, the appliance uses the following TCP & UDP ports:

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Port</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP</td>
<td>22 *</td>
<td>SSH</td>
</tr>
<tr>
<td>TCP &amp; UDP</td>
<td>53 *</td>
<td>DNS / GSLB</td>
</tr>
<tr>
<td>TCP &amp; UDP</td>
<td>123</td>
<td>NTP</td>
</tr>
<tr>
<td>TCP &amp; UDP</td>
<td>161 *</td>
<td>SNMP</td>
</tr>
<tr>
<td>UDP</td>
<td>6694</td>
<td>Heartbeat between Primary &amp; Secondary appliances in HA mode</td>
</tr>
<tr>
<td>TCP</td>
<td>7778</td>
<td>HAPProxy persistence table replication</td>
</tr>
<tr>
<td>TCP</td>
<td>9000 *</td>
<td>Gateway service (Centralized/Portal Management)</td>
</tr>
<tr>
<td>TCP</td>
<td>9080 *</td>
<td>WebUI - HTTP (disabled by default)</td>
</tr>
<tr>
<td>TCP</td>
<td>9081 *</td>
<td>Nginx fallback page</td>
</tr>
<tr>
<td>Protocol</td>
<td>Port</td>
<td>Purpose</td>
</tr>
<tr>
<td>---------</td>
<td>------</td>
<td>----------------------------------------------</td>
</tr>
<tr>
<td>TCP</td>
<td>9443 *</td>
<td>WebUI - HTTPS</td>
</tr>
<tr>
<td>TCP</td>
<td>25565 *</td>
<td>Shuttle service (Centralized/Portal Management)</td>
</tr>
</tbody>
</table>

Note: The ports used for SSH, GSLB, SNMP, the WebUI, the fallback page, the gateway service and the shuttle service can be changed if required. For more information, please refer to Service Socket Addresses.

8.6. 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 the section Configuring HA - Adding a Secondary Appliance of the appendix.

9. Appliance Configuration for Ellucian Banner – Using Layer 7 SNAT Mode (Recommended)

9.1. 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. Ellucian Banner.
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 443.
5. Set the Layer 7 Protocol to TCP Mode.
6. Click Update to create the virtual service.

9.2. 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. **Banner Node 1**.

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 the remaining Banner nodes.

### 9.3. Finalizing the Configuration

To apply the new settings, HAProxy must be reloaded. This can be done using the button in the "Commit changes" 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**.

### 10. Appliance Configuration for Ellucian Banner – Using Layer 7 SNAT Mode With TLS Termination

This deployment method terminates TLS connections on the load balancer. Performing TLS termination can add significant CPU overhead. As such, this deployment method should not be used unless the plaintext HTTP traffic must be inspected for some reason.

Unless there is a compelling reason not to do so, refer to the recommended deployment method without TLS termination instead.

#### 10.1. 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. **Ellucian Banner**.

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 **80**.

5. Set the **Layer 7 Protocol** to **HTTP Mode**.
6. Click **Update** to create the virtual service.

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

8. Under the **SSL** section, enable the option **Enable Backend Encryption** and then click "OK" in the "enable re-encryption" confirmation box that appears.

9. Click **Update**.

### 10.2. 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. **Banner Node 1**.

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

4. Set the **Real Server Port** field to **443**.

5. Ensure that the option **Re-Encrypt to Backend** is enabled.

6. Click **Update**.

7. Repeat these steps to add the remaining Banner nodes.
10.3. Uploading a Certificate

The appropriate certificate for the service in question must be uploaded to the load balancer for TLS/SSL termination to work. The process for doing this is as follows:

1. Using the web user interface, navigate to **Cluster Configuration > SSL Certificate** and click on **Add a new SSL Certificate**.
2. Press the **Upload prepared PEM/PFX file** radio button.
3. Define the **Label** for the certificate as required. It may make sense to use the domain that the certificate is associated to, e.g. **example.com**.
4. Click on **Browse** and select the appropriate PEM or PFX style certificate.
5. If uploading a PFX certificate, enter the certificate’s password in the **PFX File Password** field.
6. Click **Upload certificate**.

For more information on creating PEM certificate files and converting between certificate formats please refer to [Creating a PEM File](#).

10.4. Creating the TLS/SSL Termination

1. Using the web user interface, navigate to **Cluster Configuration > SSL Termination** and click on **Add a new Virtual Service**.
2. From the **Associated Virtual Service** drop-down list, select the associated WAF gateway that was created previously, e.g. **Ellucian_Banner**.
3. Set the **Virtual Service Port** field to **443**.
4. From the **SSL Certificate** drop-down list, select the certificate for the service in question, which in this example is **example.com**.
5. Click **Update** to create the TLS/SSL termination service.
10.5. Finalizing the Configuration

To apply the new settings, HAProxy and stunnel must be reloaded. This can be done using the buttons in the "Commit changes" 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.
3. Click Reload STunnel.

11. Testing & Verification

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

11.1. Using System Overview

The System Overview can be viewed in the WebUI. It shows a graphical view of all VIPs & RIPS (i.e. the Ellucian Banner servers) and shows the state/health of each server as well as the state of the cluster as a whole. The example below shows a standard deployment where both Banner servers are healthy and available to accept connections:

12. 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.

13. Further Documentation

For additional information, please refer to the Administration Manual.
14. Appendix

14.1. 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 is fully configured first, then the Secondary appliance can be added to create an HA pair. Once the HA pair is configured, load balanced services must be configured and modified on the Primary appliance. The Secondary appliance will be automatically kept in sync.

Note: For Enterprise Azure, the HA pair should be configured first. For more information, please refer to the Azure Quick Start/Configuration Guide available in the documentation library.

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>Interface IP addresses, bonding configuration and VLANs</td>
</tr>
<tr>
<td>Local Configuration</td>
<td>Routing</td>
<td>Default gateways and static routes</td>
</tr>
<tr>
<td>Local Configuration</td>
<td>System Date &amp; time</td>
<td>Time and date related settings</td>
</tr>
<tr>
<td>Local Configuration</td>
<td>Physical – Advanced Configuration</td>
<td>Various appliance settings</td>
</tr>
<tr>
<td>Local Configuration</td>
<td>Portal Management</td>
<td>Portal management settings</td>
</tr>
<tr>
<td>Local Configuration</td>
<td>Security</td>
<td>Security settings</td>
</tr>
<tr>
<td>Local Configuration</td>
<td>SNMP Configuration</td>
<td>SNMP settings</td>
</tr>
<tr>
<td>Local Configuration</td>
<td>Graphing</td>
<td>Graphing settings</td>
</tr>
<tr>
<td>Local Configuration</td>
<td>License Key</td>
<td>Appliance licensing</td>
</tr>
<tr>
<td>Maintenance</td>
<td>Backup &amp; Restore</td>
<td>Local XML backups</td>
</tr>
<tr>
<td>Maintenance</td>
<td>Software Updates</td>
<td>Appliance software updates</td>
</tr>
<tr>
<td>Maintenance</td>
<td>Fallback Page</td>
<td>Fallback page configuration</td>
</tr>
<tr>
<td>Maintenance</td>
<td>Firewall Script</td>
<td>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 where any of the above have been configured on the Primary appliance, they're also configured on the Secondary.

Configuring the HA 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.

Create a Clustered Pair

3. Specify the IP address and the loadbalancer user's password for the Secondary (peer) appliance as shown in the example above.
4. Click Add new node.
5. The pairing process now commences as shown below:

Create a Clustered Pair

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 “Commit changes” message box at the top of the screen.

**Note**

Clicking the **Restart Heartbeat** button on the Primary appliance will also automatically restart heartbeat on the Secondary appliance.

**Note**

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

**Note**

For details on testing and verifying HA, please refer to **Clustered Pair Diagnostics**.
## 15. 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>3 March 2023</td>
<td>Initial version</td>
<td></td>
<td>VM, AH</td>
</tr>
<tr>
<td>1.0.1</td>
<td>7 March 2023</td>
<td>Removed conclusion section</td>
<td>Updates across all documentation</td>
<td>AH</td>
</tr>
<tr>
<td>1.1.0</td>
<td>24 March 2023</td>
<td>New document theme</td>
<td>Branding update</td>
<td>AH</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Modified diagram colours</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
About Loadbalancer.org

Loadbalancer.org’s mission is to ensure that its clients’ businesses are never interrupted. The load balancer experts ask the right questions to get to the heart of what matters, bringing a depth of understanding to each deployment. Experience enables Loadbalancer.org engineers to design less complex, unbreakable solutions - and to provide exceptional personalized support.