Progress®
Kemp® LoadMaster®

Deployment Guide Ellucian Banner

Generated on: 16 September 2024

Copyright

Visit the following page online to see Progress Software Corporation's current Product Documentation Copyright Notice/Trademark Legend: Product Documentation Copyright Notice & Trademarks | Progress

Table of Contents

Chapter 1: Introduction 4

Chapter 2: Template 6

Chapter 3: LoadMaster Global Settings 7

Enable Subnet Originating Requests Globally 7

Enable Check Persist Globally 8

Chapter 4: Virtual Service - Ellucian Banner 9

Create Ellucian Banner HTTPS Re-Encrypted Virtual Service 9

Banner HTTPS Re-encrypted Virtual Service Recommended API Settings (optional) 10

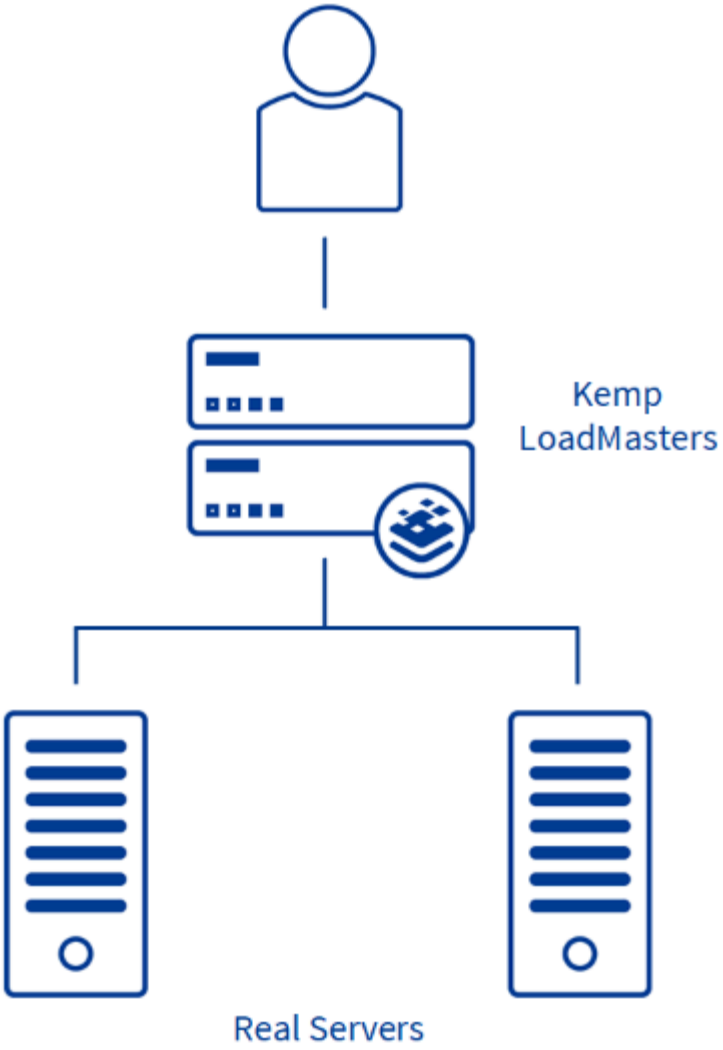
Banner HTTPS Re-encrypted Redirect Virtual Service Recommended API Settings (optional). 11

1

Introduction

Introduction

Banner® by Ellucian is the world's leading higher education Enterprise Resource Planning (ERP) system —the solution of choice for almost 1,400 institutions in 40 countries. With the industry's most comprehensive set of features and future-ready technology, Banner strengthens every major workflow in higher education, from student recruiting and retention to talent attraction and management.



The LoadMaster offers advanced Layer 4 and Layer 7 server load balancing, SSL Acceleration and a multitude of other advanced Application Delivery and Optimization (ADC) features. The LoadMaster can load balance the Ellucian Banner workload. The LoadMaster intelligently and efficiently distributes user traffic among the application servers so that users get the best experience possible.

This document provides guidance and recommended settings on how to load balance Ellucian Banner with a LoadMaster. The Progress Kemp Support Team is available to provide solutions for scenarios not explicitly defined.

The Progress Kemp support site can be found at: https://support.kemptechnologies.com.

2

Template

Template

Progress Kemp has developed a template containing our recommended settings for this workload. You can install this template to help create Virtual Services (VSs) because it automatically populates the settings. You can use the template to easily create the required VSs with the recommended settings. For some workloads, additional manual steps may be required such as assigning a certificate or applying port following. These steps are covered in the document, if needed.

You can remove templates after use and this will not affect deployed services. If needed, you can make changes to any of the VS settings after using the template.

Download released templates from the following page: LoadMaster Templates.

For more information and steps on how to import and use templates, refer to the Virtual Services and Templates, Feature Description.

3

LoadMaster Global Settings

LoadMaster Global Settings

Follow the steps in the sections below to configure the LoadMaster with the recommended settings to load balance the Ellucian Banner workload.

Related Links

- Enable Subnet Originating Requests Globally
- Enable Check Persist Globally

Enable Subnet Originating Requests Globally

Enable Subnet Originating Requests Globally

It is best practice to enable the **Subnet Originating Requests** option globally.

In a one-armed setup (where the Virtual Service and Real Servers are on the same network/subnet) **Subnet Originating Requests** is usually not needed. However, enabling **Subnet Originating Requests** should not affect the routing in a one-armed setup.

In a two-armed setup where the Virtual Service is on network/subnet A, for example, and the Real Servers are on network B, **Subnet Originating Requests** should be enabled on LoadMasters with firmware version 7.1-16 and above.



When **Subnet Originating Requests** is enabled, the Real Server sees traffic originating from 10.20.20.21 (LoadMaster eth1 address) and responds correctly in most scenarios.

With **Subnet Originating Requests** disabled, the Real Server sees traffic originating from 10.0.0.15 (LoadMaster Virtual Service address on **eth0**) and responds to **eth0** which could cause asymmetric routing.

When **Subnet Originating Requests** is enabled globally, it is automatically enabled on all Virtual Services. If the **Subnet Originating Requests** option is disabled globally, you can choose whether to enable **Subnet Originating Requests** on a per-Virtual Service basis.

To enable **Subnet Originating Requests** globally, follow the steps below:

1. In the main menu of the LoadMaster User Interface (UI), go to **System Configuration > Miscellaneous Options > Network Options**.
2. Select the **Subnet Originating Requests** check box.

Enable Check Persist Globally

Enable Check Persist Globally

It is recommended that you change the **Always Check Persist** option to **Yes – Accept Changes**. Use the following steps:

1. Go to **System Configuration > Miscellaneous Options > L7 Configuration**.
2. Click the **Always Check Persist** drop-down arrow and select **Yes – Accept Changes**.

4

Virtual Service - Ellucian Banner

Virtual Service - Ellucian Banner

This step-by-step set up of VSs leverages the Progress Kemp application template for Ellucian Banner.

The table in each section outlines the settings configured by the application template. You can use this information to manually configure VSs or using the LoadMaster API and automation tools.

Related Links

- Create Ellucian Banner HTTPS Re-Encrypted Virtual Service

Create Ellucian Banner HTTPS Re-Encrypted Virtual Service

Create Ellucian Banner HTTPS Re-Encrypted Virtual Service

To configure a VS using the application template, perform the following steps:

1. In the main menu of the LoadMaster WUI, go to **Virtual Services > Add New**.
2. Type a valid **Virtual Address**.

3. Select **Ellucian Banner HTTPS Re-Encrypted** in the **Use Template** drop-down list.
4. Click **Add this Virtual Service**.
5. In the left-hand navigation select **View/Modify Services**.
6. Click **Modify** on the Virtual Service **Ellucian Banner HTTPS Re-encrypted** on port TCP 443.
7. Expand the **SSL Properties** section.
8. Select the certificate to use from **Available Certificates** and click the arrow (>) to move it to **Assigned Certificates**.
9. Expand the **Real Servers** section.
10. Click **Add New**.
11. Type the **Real Server Address**.
12. Confirm that port **443** is entered.
13. Click **Add This Real Server**.
    1. Repeat this step to add more Real Servers as needed.

Related Links

- Banner HTTPS Re-encrypted Virtual Service Recommended API Settings (optional)
- Banner HTTPS Re-encrypted Redirect Virtual Service Recommended API Settings (optional)

Banner HTTPS Re-encrypted Virtual Service Recommended API Settings (optional)

Banner HTTPS Re-encrypted Virtual Service Recommended API Settings (optional)

This table outlines the API parameters and values set using the Progress Kemp application template. You can use these settings with scripts and automation tools.

API Parameter	API Value
port	443
prot	tcp
SubnetOriginating	1
Persist	active-cookie
Cookie	jsessionid

API Parameter	API Value
PersistTimeout	3600
Schedule	lc
Idletimeout	660
SSLAcceleration	1
SSLReencrypt	1
CipherSet	BestPractices
ClientCert	0
CheckUseGet	0

Banner HTTPS Re-encrypted Redirect Virtual Service Recommended API Settings (optional)

Banner HTTPS Re-encrypted Redirect Virtual Service Recommended API Settings (optional)

This table outlines the API parameters and values set using the Progress Kemp application template. You can use these settings with scripts and automation tools.

API Parameter	API Value
port	80
prot	tcp
Transparent	0
Persist	none

API Parameter	API Value
Schedule	rr