Aequitas

Deployment Guide

UPDATED: 24 March 2021

Copyright Notices

Table of Contents

1 Introduction

Aequitas Solutions, Inc. is a leader in innovative K-12 Student Information Systems (SIS). One of their products is Q, which is a next generation Enterprise Student Management Solution. It uses state of the art technology to deliver a fast, interactive and intuitive fully web-based application experience to end-users. Q includes modules on basic administration, scheduling, attendance, and grade reporting.

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 Kemp LoadMaster can load balance the Aequitas 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 Aequitas with a Kemp LoadMaster. The Kemp Support Team is available to provide solutions for scenarios not explicitly defined.

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

1.1 Document Purpose

This documentation is intended to provide guidance on how to configure Kemp LoadMaster products to provide high availability for an Aequitas environment. As this documentation is not intended to cover every possible deployment scenario, it may not address your unique setup or requirements. The Kemp Support Team is always available to provide solutions for scenarios not explicitly defined.

1.2 Intended Audience

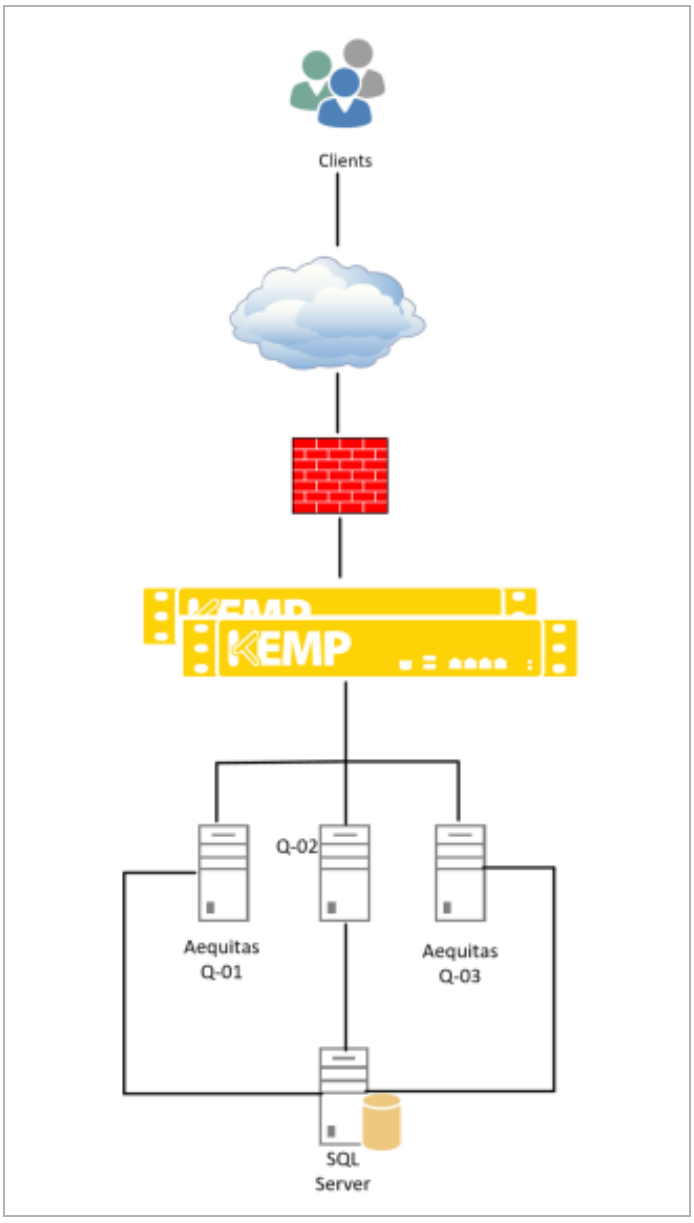
This document is for anyone deploying Aequitas with a Kemp LoadMaster.

1.3 Related Firmware Version

Published with LMOS version 7.2.48.4 LTS. This document has not required substantial changes since 7.2.48.4 LTS. However, the content is in sync with the latest LoadMaster LTS firmware.

2 Architecture

Use the following set up to load balance your environment.



3 Aequitas Template

Kemp has developed a template containing our recommended settings for Aequitas. You can install this template to help when creating Virtual Services, as it automatically populates the settings. This is quicker and easier than manually configuring each Virtual Service. If needed, changes can be made to any of the Virtual Service settings after using the template.

Download released templates from the Templates section on the Kemp documentation page: http://kemptechnologies.com/documentation.

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

For steps on how to manually add and configure each of the Virtual Services using the recommended settings, refer to the steps in this document.

4 Configure the LoadMaster

The deployed Aequitas environment determines which of the following setups is used.

4.1 Configure the Global Settings

The sections below provide instructions on configuring some recommended global settings.

4.1.1 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:

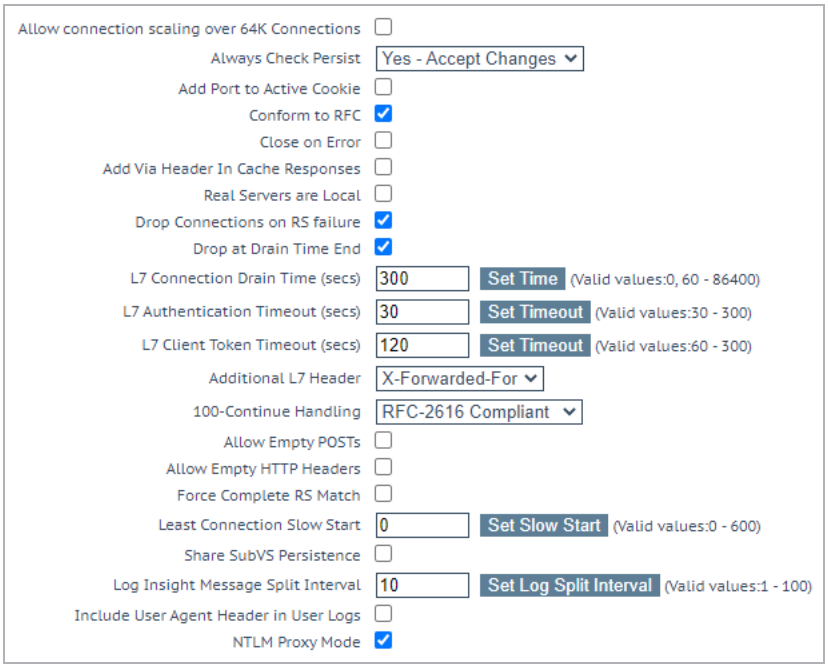
1. In the main menu of the LoadMaster User Interface (UI), go to **System Configuration > Miscellaneous Options > Network Options**.

2. Select the **Subnet Originating Requests** check box.

4.1.2 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**.

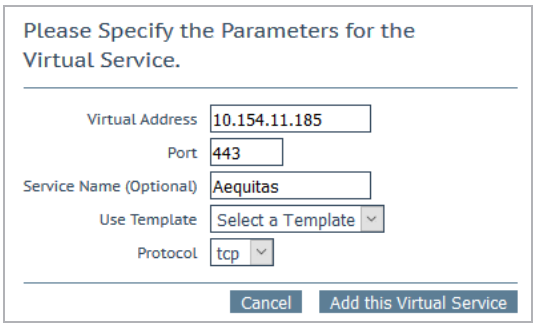


2. Click the **Always Check Persist** drop-down arrow and select **Yes – Accept Changes**.

5 Create the Aequitas HTTPS Offloaded Virtual Service

Follow the steps below to create and configure the recommended settings for the Aequitas Virtual Service:

1. In the main menu of the LoadMaster Web User Interface (WUI), go to **Virtual Services > Add New**.



2. Type a valid IP address in the **Virtual Address** text box.
3. Type **443** in the **Port** text box.
4. Enter a recognizable **Service Name** such as **Aequitas**.
5. Ensure **tcp** is selected as the **Protocol**.
6. Click **Add this Virtual Service**.
7. Configure the settings as shown in the following table:

Section	Option	Value	Comment
SSL Properties	SSl Acceleration	Enabled	
	Reencrypt	Disabled	
	Supported Protocols	TLS1.0; TLS1.1; TLS1.2; TLS1.3	While this workload may not support TLS1.3 yet, Kemp recommend enabling it for future

Section	Option	Value	Comment
			proofing.
	Cipher Set	BestPractices	
Standard Options	Persistence Mode	Active Cookie	
	Timeout	1 Hour	
	Cookie name	LM_Aequitas	
	Scheduling Method	least connection	
Advanced Properties	Add a Port 80 Redirector VS	https://%h%s	Click **Add HTTP Redirector**. This automatically creates a redirect on port 80.

8. Add the Real Servers:

   a) Expand the **Real Servers** section.

   b) Click **Add New**.

   c) Type the address of the Real Server.

   d) Type **80443** as the **Port**.

   e) Click **Add This Real Server**.

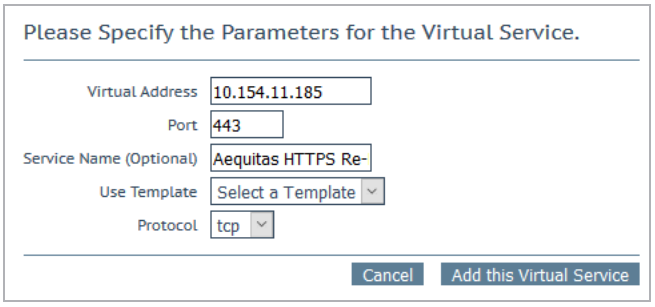
   f) Repeat the steps above to add more Real Servers as needed, based on the environment.

Create an Aequitas HTTPS Offloaded Redirect Virtual Service

Clicking the **Add HTTP Redirector** button automatically creates a port 80 redirect Virtual Service. This is optional, but the purpose of this Virtual Service is to redirect any clients who have connected using HTTP to the HTTPS Virtual Service. Kemp also recommends changing the **Persistence Mode** and the **Real Server Check Method** to **None**.

6 Create the Aequitas HTTPS Re-Encrypt Virtual Service

Follow the steps below to create and configure the recommended settings for the Aequitas HTTPS Re-Encrypt Virtual Service:



1. In the main menu of the LoadMaster Web User Interface (WUI), go to **Virtual Services > Add New**.
2. Type a valid IP address in the **Virtual Address** text box.
3. Type **443** in the **Port** text box.
4. Enter a recognizable **Service Name** such as **Aequitas Re-Encrypt Virtual Service**.
5. Ensure **tcp** is selected as the **Protocol**.
6. Click **Add this Virtual Service**.
7. Configure the settings as shown in the following table:

Section	Option	Value	Comment
SSL Properties	SSl Acceleration	Enabled	
	Reencrypt	Enabled	
	Supported Protocols	TLS1.0; TLS1.1; TLS1.2; TLS1.3	While this workload may not support TLS1.3 yet, Kemp recommend enabling it for future

Section	Option	Value	Comment
			proofing.
	Cipher Set	BestPractices	
Standard Options	Persistence Mode	Active Cookie	
	Timeout	1 Hour	
	Cookie name	LM_Aequitas	
	Scheduling Method	least connection	
Advanced Properties	Add a Port 80 Redirector VS	https://%h%s	Click **Add HTTP Redirector**. This automatically creates a redirect on port 80.

8. Add the Real Servers:

   a) Expand the **Real Servers** section.

   b) Click **Add New**.

   c) Type the address of the Real Server.

   d) Type **443** as the **Port**.

   e) Click **Add This Real Server**.

   f) Repeat the steps above to add more Real Servers as needed, based on the environment.

Create an Aequitas HTTPS Offloaded Redirect Virtual Service

Clicking the **Add HTTP Redirector** button automatically creates a port 80 redirect Virtual Service. This is optional, but the purpose of this Virtual Service is to redirect any clients who have connected using HTTP to the HTTPS Virtual Service. Kemp also recommends changing the **Persistence Mode** and the **Real Server Check Method** to **None**.

Last Updated Date

This document was last updated on 24 March 2021.