VMware vCenter Log Insight Manager

Deployment Guide

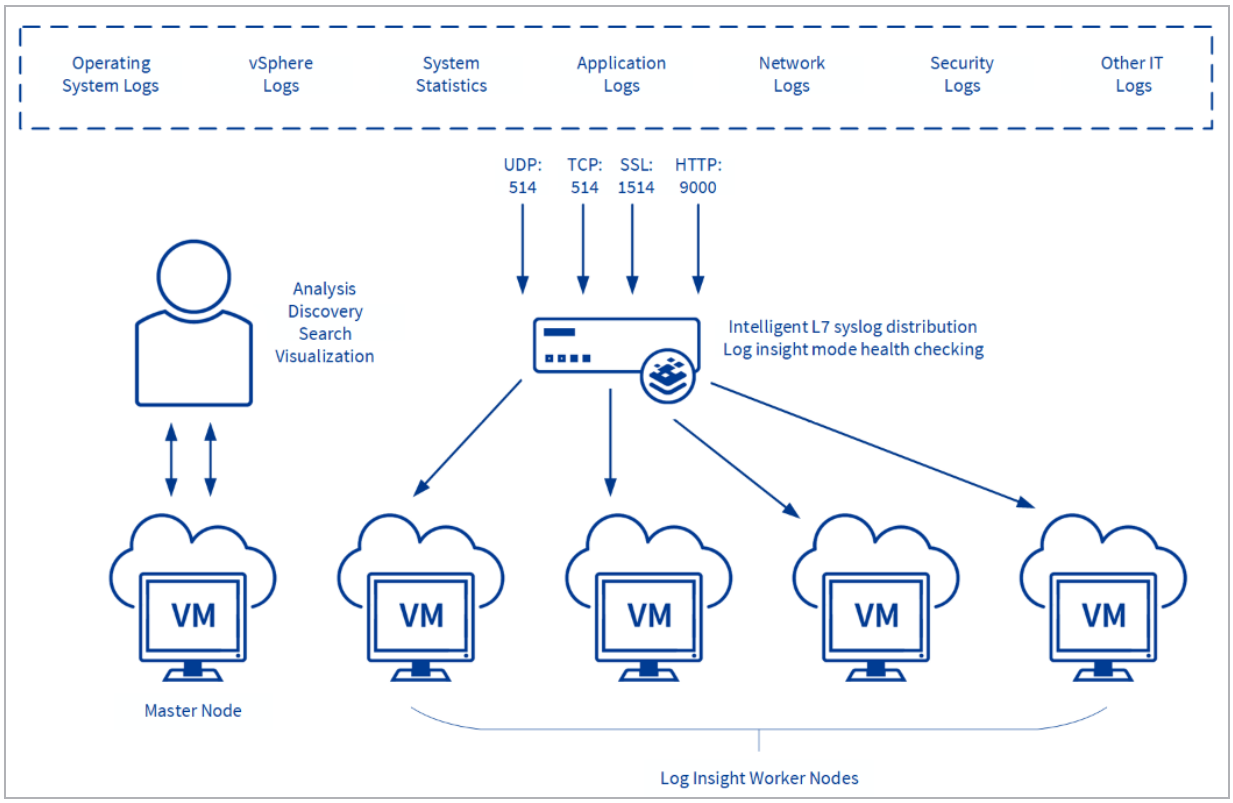
UPDATED: 19 March 2021

Copyright Notices

Table of Contents

1 Introduction

VMware vCenter Log Insight delivers real-time log management and log analysis with machine learning-based Intelligent Grouping, high performance search and better troubleshooting across physical, virtual and cloud environments.



The flow of traffic in the above diagram is as follows:

1. The syslog clients create logs
2. The syslog clients then send the messages to the Virtual IP address on the LoadMaster
3. The LoadMaster distributes these messages to the Log Insight nodes

Log Insight supports receipt and ingestion of syslog messages that are sent over UDP, TCP, TCP with SSL encryption and using the API. The LoadMaster provides specialized Log Insight-aware services to optimize high availability and scalability of Log Insight deployments. Users can then perform

deep analytics, discovery and search of the ingested data to get an enhanced operational view of their environment.

An inherent challenge that arises when syslog messages are sent using methods other than UDP, is that clients will often open long-lived connections that are then used for large amounts of messages. With this behavior, even when a scaled out architecture and application load balancer are implemented, traffic is not distributed in a close-to-even fashion across the pool of available nodes. The LoadMaster offers a solution that allows messages to be parsed within a connection to allow a more even distribution across servers in a pool, as well as simplified scalability of Log Insight environments.

1.1 Document Purpose

The purpose of this document is to explain how to configure the LoadMaster to optimize VMware Log Insight traffic flows.

1.2 Intended Audience

This document is intended to be read by anyone who is interested in configuring the LoadMaster to optimize VMware Log Insight deployments

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 Configure the LoadMaster

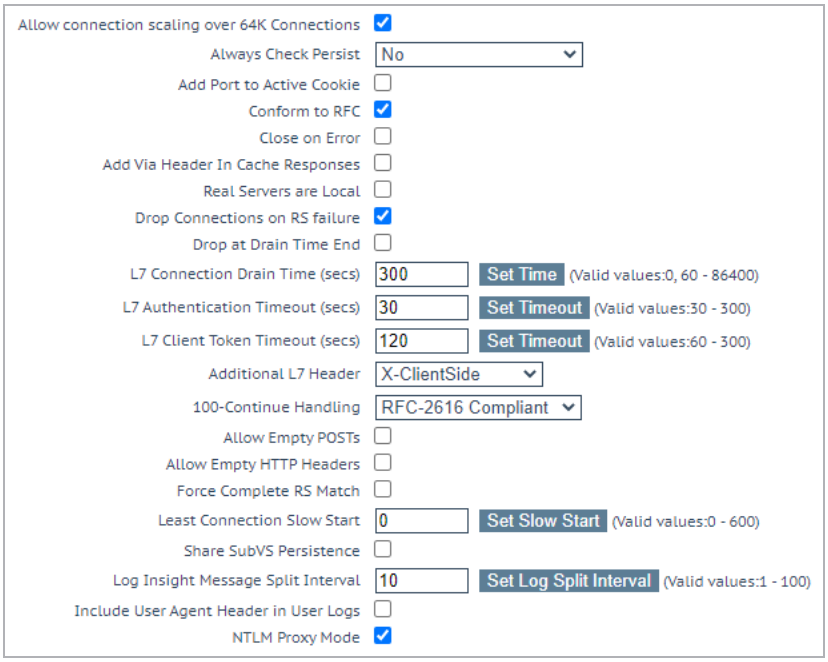
A number of Virtual Services will need to be created for the LoadMaster to work effectively with Log Insight. The services that is used depends on the methods that are used in the environment to send syslog messages to the Log Insight nodes. Refer to the sections below for detailed, step-by-step instructions.

2.1 Configure Log Insight Message Split Interval

The **Log Insight Message Split Interval** value controls how many syslog messages should be sent to each server in the pool before moving to the next server. For example, if there are three Log Insight nodes and the **Log Insight Message Split Interval** is set to **1** - a single message is sent to server A, and then to server B and then server C before again distributing a message to server A.

To set the **Log Insight Split Interval**, follow the steps below:

1. In the main menu of the WUI, go to **System Configuration > Miscellaneous Options > L7 Configuration**.



2. Set the **Log Insight Message Split Interval**.

The default value is 10. The range is 1-100.

2.2 Template

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.

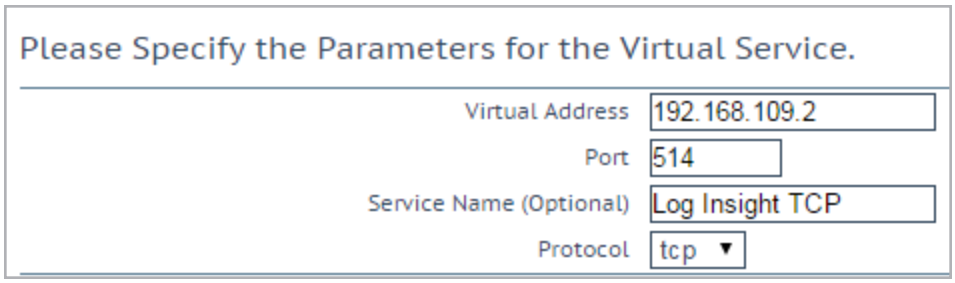
Download released templates from the **Templates** section on the Kemp Documentation page.

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.

2.3 Create the TCP Syslog Virtual Service

A TCP syslog Virtual Service must be created if clients will send syslog messages to Log Insight over TCP. To do this, follow the steps below:

1. In the main menu of the LoadMaster WUI, select **Virtual Services > Add New**.



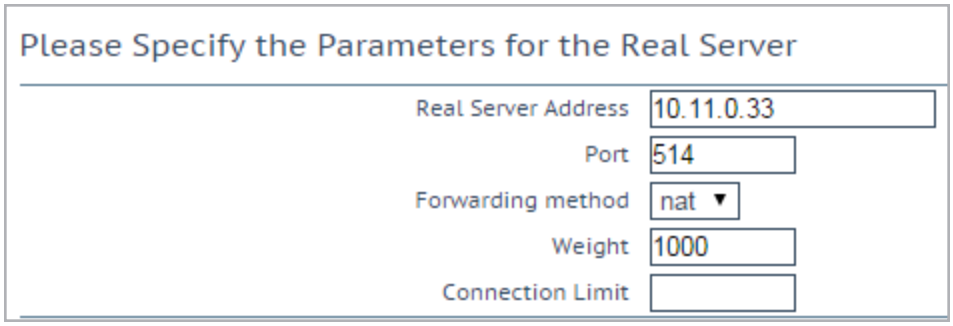
2. Enter a valid **Virtual Address**.
3. Enter **514** as the **Port**.
4. Enter a recognizable **Service Name**, for example **Log Insight TCP**.
5. Click **Add this Virtual Service**.
6. Configure the settings as shown in the following table:

Section	Option	Value	Comment
Basic Properties	Service Name	Log Insight	

Section	Option	Value	Comment
Standard Options	Scheduling Method	round robin *	
Real Servers	Checked Port	514	Click **Set Check Port.**

* Round robin is typically best to accomplish desired behavior of even traffic distribution. Least connection will result in an uneven distribution for syslog over TCP, especially when there is a low number of connections. If the **Scheduling Method** is set to least connection and there are a low number of connections, the **Log Insight Split Interval** (see below) will not behave as expected.

7. Click **Add New**.

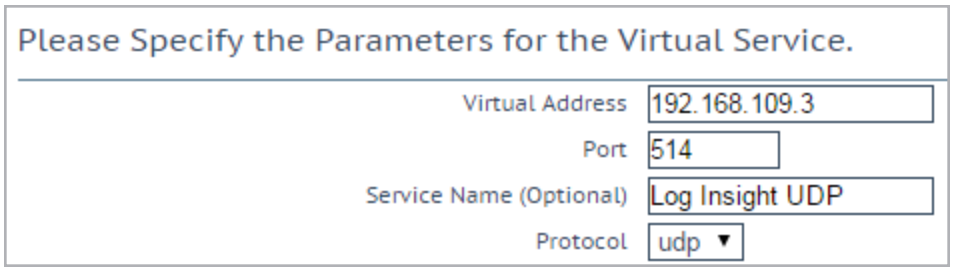


8. Enter the **Real Server Address**.
9. Click **Add This Real Server**.

2.4 Create the UDP Syslog Virtual Service

A UDP Syslog Virtual Service must be created if clients will send syslog messages to Log Insight over UDP. To do this, follow the steps below:

1. In the main menu of the LoadMaster WUI, select **Virtual Services > Add New**.

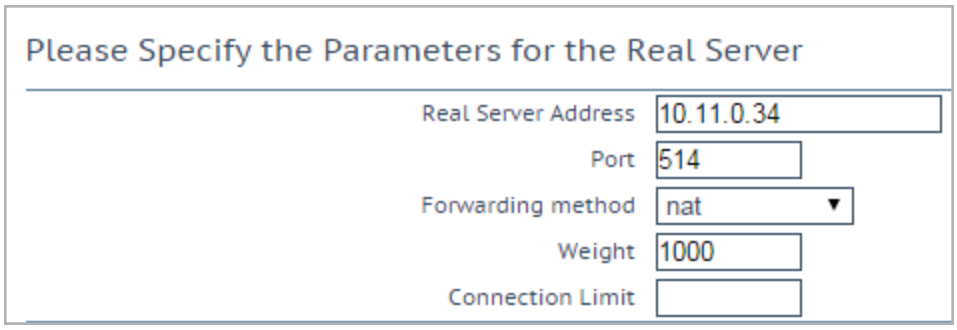


2. Enter a valid **Virtual Address**.
3. Enter **514** as the **Port**.
4. Enter a recognizable **Service Name**, for example **Log Insight UDP**.
5. Select **udp** as the **Protocol**.
6. Click **Add this Virtual Service**.
7. Configure the settings as shown in the following table:

Section	Option	Value	Comment
Standard Options	Transparency	Enabled *	
	Idle Connection Timeout	Enter a low value.	A value of **1**typically results in the best performance.
Real Servers	Real Server Check Method	ICMP Ping	

* This allows the client's IP address to be presented to the Log Insight servers. Depending on your network topology, transparency may not be supported. If this is the case, you can safely disable this **Transparency** option and the source IP presented to Log Insight is that of the Virtual Service. The hostname remains unchanged. Refer to the Transparency Feature Description for details on the caveats relating to transparency.

8. Click **Add New**.

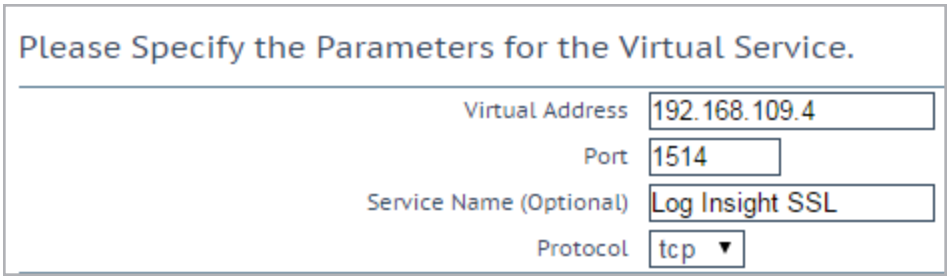


9. Enter the **Real Server Address**.
10. Click **Add This Real Server**.

2.5 Create the SSL Syslog Virtual Service

A SSL syslog Virtual Service must be created if clients will send syslog messages to Log Insight over TCP. To do this, follow the steps below:

1. In the main menu of the LoadMaster WUI, select **Virtual Services > Add New**.

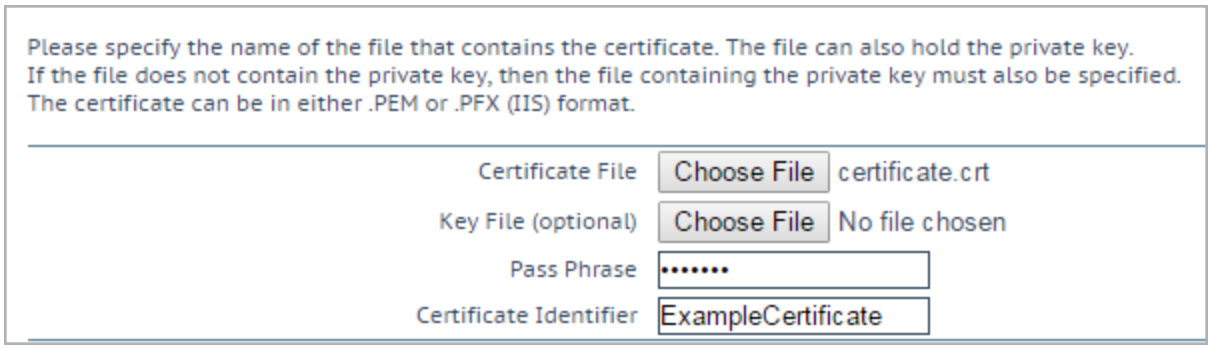


2. Enter a valid **Virtual Address**.
3. Enter **1514** as the **Port**.
4. Enter a recognizable **Service Name**, for example **Log Insight SSL**.
5. Click **Add this Virtual Service**.
6. Configure the settings as shown in the following table:

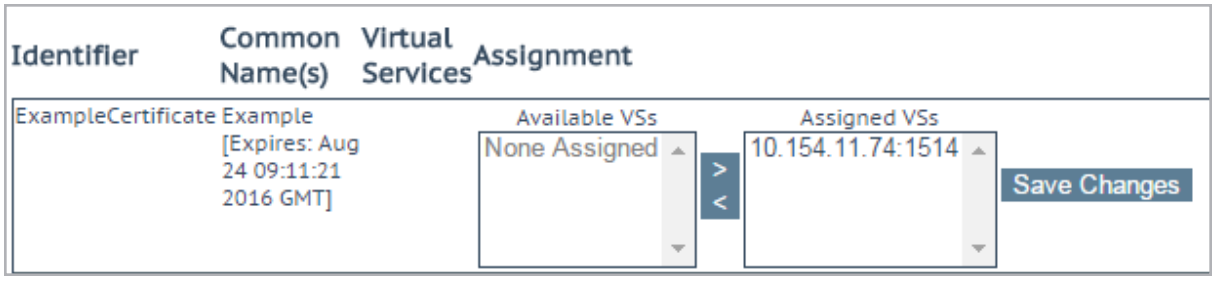
Section	Option	Value	Comment
Basic Properties	Service Type	Log Insight	
SSL Properties	SSL Acceleration	Enabled	Click **OK**.

7. Click **Manage Certificates**.

8. Click **Import Certificate**.



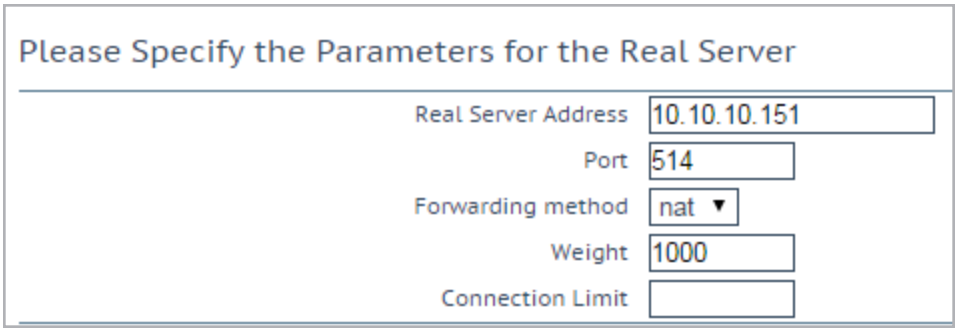
9. Click the first **Choose File** button.
10. Browse to and select the relevant certificate file.
11. If needed, upload a **Key File** and enter the **Pass Phrase**.
12. Enter a name in the **Certificate Identifier** text box.
13. Click **Save**.



14. Configure the Virtual Service settings as shown in the following table:

Section	Option	Value	Comment
SSL Properties	Certificates	Select the relevant certificate.	Click **>** to assign the certificate. Click **Set Certificates**.
Real Servers	Real Server Check Method	TCP Connection Only	

15. Click **Add New**.



16. Enter the **Real Server Address**.
17. Enter **514** as the **Port**.
18. Click **Add This Real Server**.
19. Add any other Real Servers as needed.

2.6 Log Insight API Ingest Service

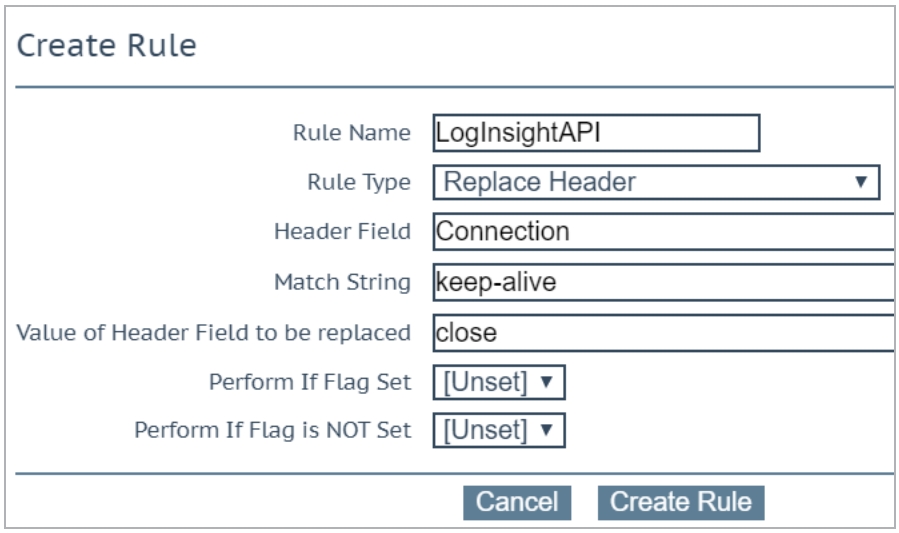
If HTTP POST requests are used to programmatically send log information to the Log Insight cluster, a "Log Split" content rule is required and an accompanying Virtual Service must be created. Content rules interrogate incoming client connections and make decisions as well as header modification based on the contents of the requests. Follow the steps in the two sections below for instructions on how to do this. This rule will ensure even distribution of messages across the cluster of Log Insight nodes when the API Ingest Service is utilized.

2.6.1 Create the Log Split Content Rule

A "Log Split" content rule is required to minimize "lumpiness" and accomplish a more even distribution of messages that are posted.

To create the content rule, follow the steps below:

1. In the main menu of the LoadMaster WUI, select **Rules & Checking > Content Rules**.
2. Click **Create New**.



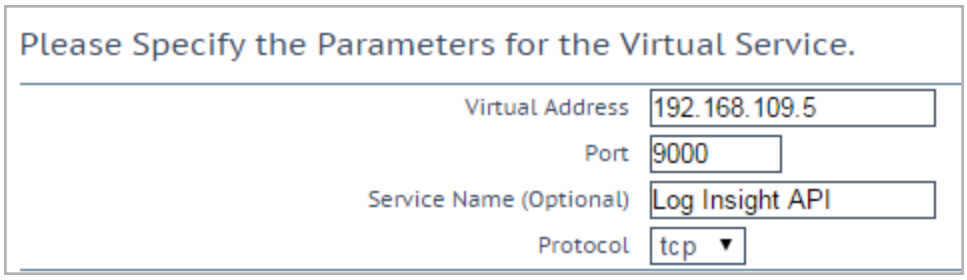
3. Enter a recognizable **Rule Name**, for example **LogInsightAPI**.
4. Select **Replace Header** as the **Rule Type**.
5. Enter **Connection** as the **Header Field**.
6. Enter **keep-alive** as the Match String.
7. Enter **close** as the **Value of Header Field to be replaced**.
8. Click **Create Rule**.

For more information, refer to the **Feature Description, Content Rules** document.

2.6.2 Create the API Ingest Virtual Service

Now, an API ingest Virtual Service must be created. To do this, follow the steps below:

1. In the main menu, select **Virtual Services > Add New**.



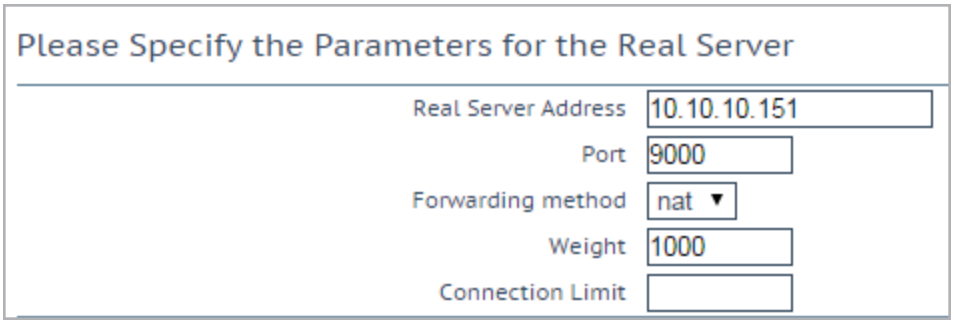
2. Enter a valid **Virtual Address**.
3. Enter **9000** as the **Port**.

4. Enter a recognizable **Service Name**, for example **Log Insight API**.
5. Click **Add this Virtual Service**.
6. Configure the settings as shown in the following table:

Section	Option	Value	Comment
Basic Properties	Service Type	HTTP/HTTPS	
Standard Options	Transparency	Enabled *	
Real Servers	Real Server Check Method	TCP Connection Only	

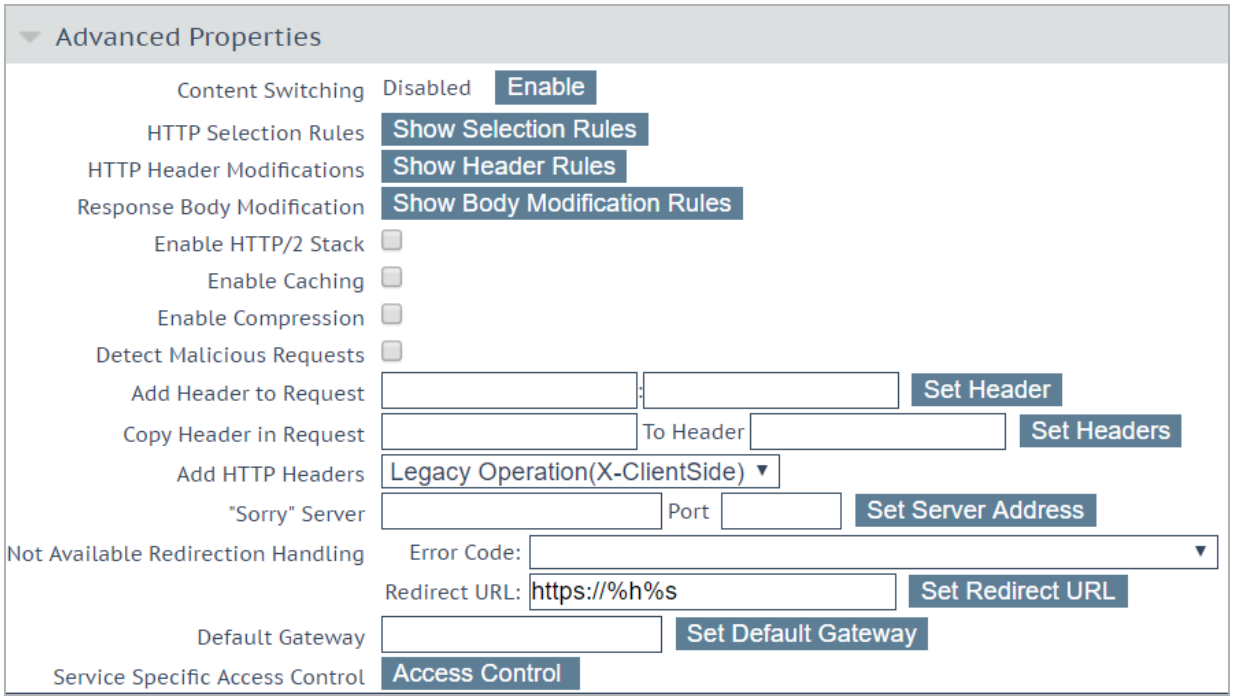
* This allows the client's IP address to be presented to the Log Insight servers. Depending upon your network topology, transparency may not be supported. If this is the case, you can safely disable this **Transparency** option and the source IP presented to Log Insight is that of the Virtual Service. The hostname will remain unchanged. Refer to the Transparency Feature Description for details on the caveats relating to transparency.

7. Click **Add New**.



8. Enter the **Real Server Address**.
9. Click **Add This Real Server**.
10. Click **OK**.
11. Add any other Real Servers as needed.
12. Click **Back**.

13. Expand the **Advanced Properties** section.



14. Click **Enable**.

15. Click **Show Header Rules**.

Name	Rule Type	Options	Header
LogInsightAPI	Replace Header		Connection

16. In the **Request Rules** section, select the relevant rule and click **Add**.

References

Unless otherwise specified, the following documents can be found at

http://kemptechnologies.com/documentation.

Feature Description, Content Rules

Web User Interface, Configuration Guide

Last Updated Date

This document was last updated on 19 March 2021.