Progress®
Kemp® LoadMaster®

Feature Description Content Rules

Generated on: 18 December 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 5

Chapter 2: Advantages of Content Rules. 7

Chapter 3: Configure a Virtual Service to use Content Rules 10

Setting up Content Rules 11

Configuring Virtual Services 11

Content Rules WUI Options 14

Content Matching 15

Add Header 19

Delete Header 20

Replace Header 21

Modify URL. 23

Replace String in Response Body 24

Force Complete RS Match 25

Limitations of Using Regular Expressions in the LoadMaster WUI 26

Content Matching Rules 26

Adding Content Matching Rules 26

Associating Content Matching Rules to a Virtual Service. 27

Header Modification 29

Adding Header Modification Rules 29

Associating Header Rules to a Virtual Service 30

SSL Information in Client Request Headers. 31

Response Body String Replacement 32

Adding Response Body String Replacement Rules 33

Associating Response Body String Replacement Rules to a Virtual Service. 34

Chapter 4: Perl Compatible Regular Expressions 37
PCRE Examples 38

Chapter 5: Shell Regular Expressions 40
Shell Regular Expression Examples 41

Chapter 6: Content Rules Cookbook 42
Match Host or Domain 43
Change Domain or Host 43
Match URL or Directory 45
Change URL or Directory 45
Naked Domain Rewrite 46
Rewrite Clients from "/" to "/testpage" 47
Redirect Content to a Different URL While Keeping the Directory or Path 47
Redirecting Clients from HTTP to HTTPS 48
Change the Host Seen by the Real Server 49
Match on Source IP 49
URL Rewrite Based on Source IP 50
Add the SSL Secure Flag and HTTPonly Flag to Cookies from the Real Server 51
User-Agent String 51
Changing the User-Agent String 52
Content Match on a Query 52
Content Matching Rule Example 53
Content Matching Rules 53
Virtual Services 53

Chapter 7: References 58

1

Introduction

The LoadMaster supports content switching, which is sometimes referred to as URL switching. This enables the LoadMaster to direct specific requests to specific Real Servers based on the contents of the requested URL.

For example, if there are two groups of servers - one to serve images and the other to serve all other content - you can create rules to separate these two types of request. Any URL that includes **/images** in it, for example **http://example.com/images/demo.jpg**, is directed to the image server(s). Anything else is directed to the other server(s).

Content switching enables the LoadMaster to break up traffic based on the content of the request. Traffic can be examined by the:

- Request URL
- HTTP Header
- Source IP address
- Body of a request

Note: Content rules only apply to HTTP or HTTPS traffic. If you want to match or edit the traffic, you must offload/re-encrypt SSL traffic.

Note: The maximum number of content rules that a LoadMaster can have is 1024.

Note: In this document, the term content switching does not refer to the process involved with Layer 2 switching. Instead, content switching refers to the switching of traffic between different servers, depending upon what content was requested.

Document Purpose

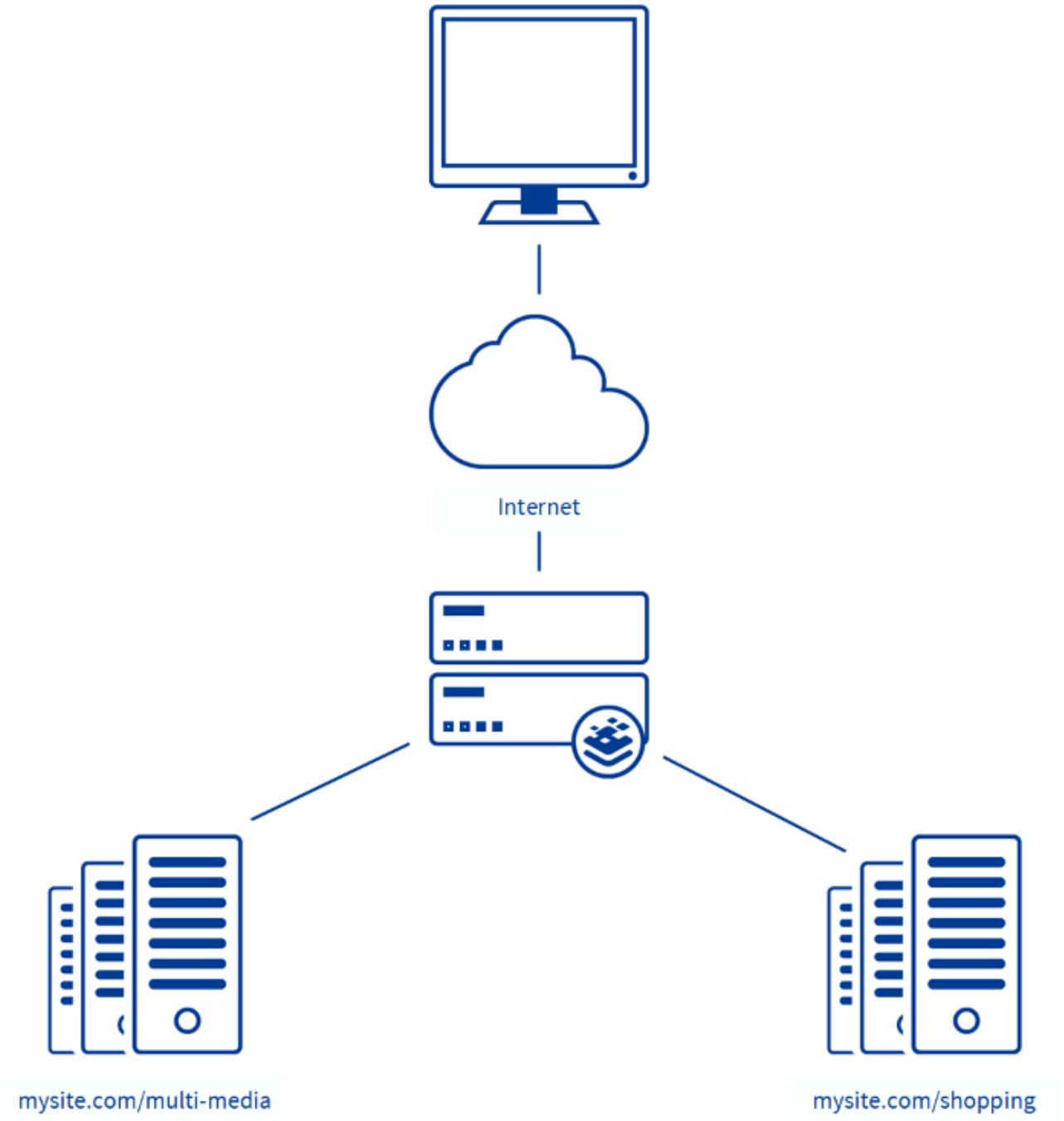
This document describes various aspects of the Content Rules feature of the LoadMaster. It describes in detail how to configure the Content Rules feature using the LoadMaster Web User Interface (WUI).

Intended Audience

Anyone who wishes to learn about or implement Content Rules with the LoadMaster.

2

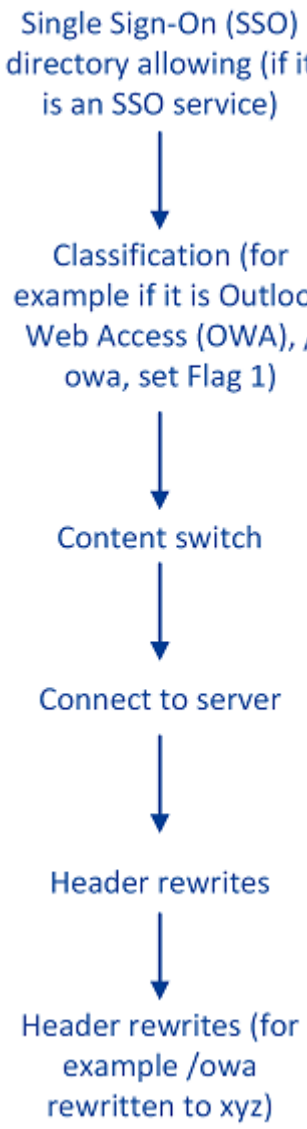
Advantages of Content Rules



Content rules enable you to:

- Strip out server information
- Rewrite requests for the root of a server
- Rewrite redirections from HTTP to HTTPS
- Force connections to close
- Secure cookies

Content switching can be very useful if there are dedicated server types that perform different functions. Examples include: image servers, static content servers, mapping servers, specialized content servers, application servers, and media servers that must all be served from the same general hostname, for example, **www.mysite.com**. Content switching also allows for hostname-specific servers and source IP-specific servers.



The above diagram outlines the order in which content rule operations are performed.

3

Configure a Virtual Service to use Content Rules

There are two parts to configuring content switching: the content rules and the Virtual Service configuration. The content rules are configured globally on the LoadMaster and various rules are applied to specific Real Servers operating under a Virtual Service.

The sections below describe the steps required to configure a Virtual Service that makes use of content switching.

Related Links

For details, see the following topics:

- Setting up Content Rules
- Configuring Virtual Services
- Content Rules WUI Options
- Content Matching Rules
- Header Modification
- Response Body String Replacement

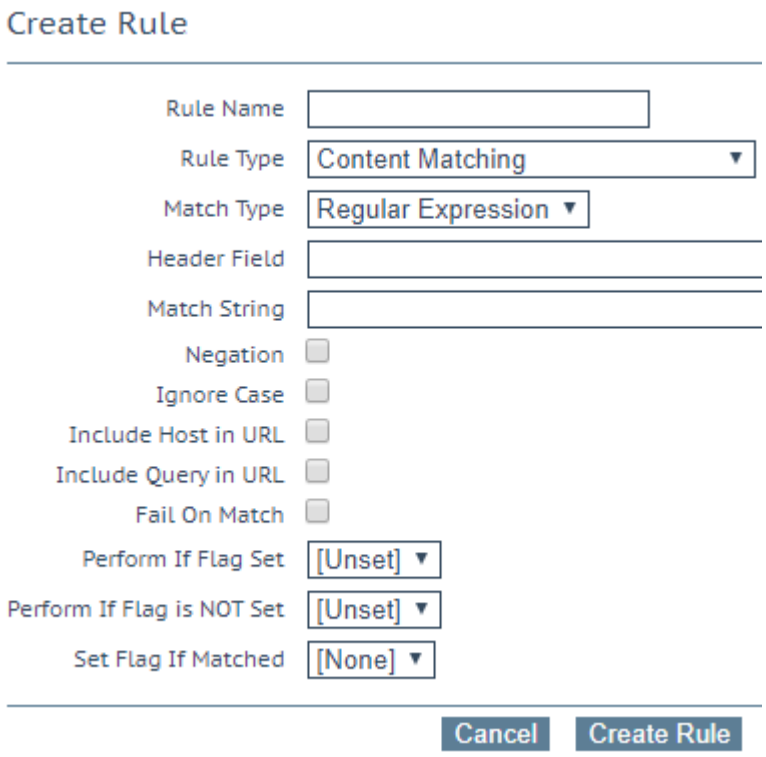
Setting up Content Rules

To set up a content rule, follow the steps below on the LoadMaster WUI:

1. In the main menu, select **Rules & Checking** and then **Content Rules**.

   Note: There is a default (catch-all) rule that matches everything and is not editable. If this rule is applied to the Real Server or SubVS, it is always the last one to match if Content Switching is enabled in a Virtual Service.

2. Click **Create New...**.



3. Fill out the form as needed. For details on what each of the options mean, refer to the Content Rules WUI Options section.
4. Click **Create Rule**.

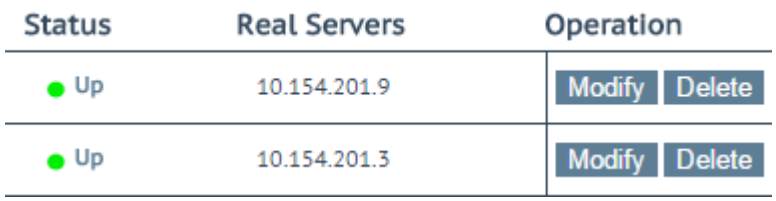
The rule is added but does not affect any Virtual Service. After the rules have been added, they must be applied to Real Servers within individual Virtual Services.

Configuring Virtual Services

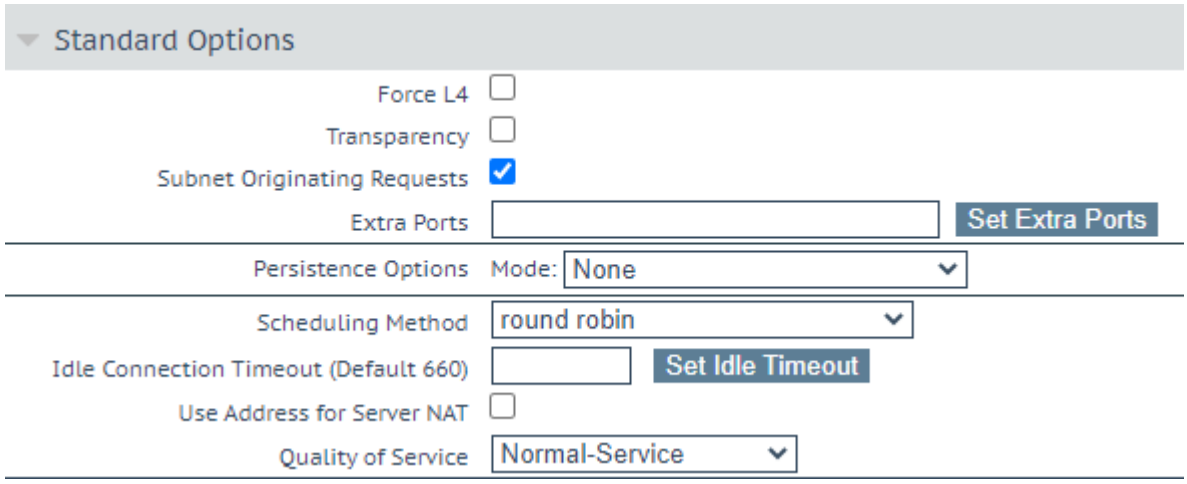
To configure a Virtual Service to use content switching, follow the steps below:

1. Log in to the relevant LoadMaster WUI.

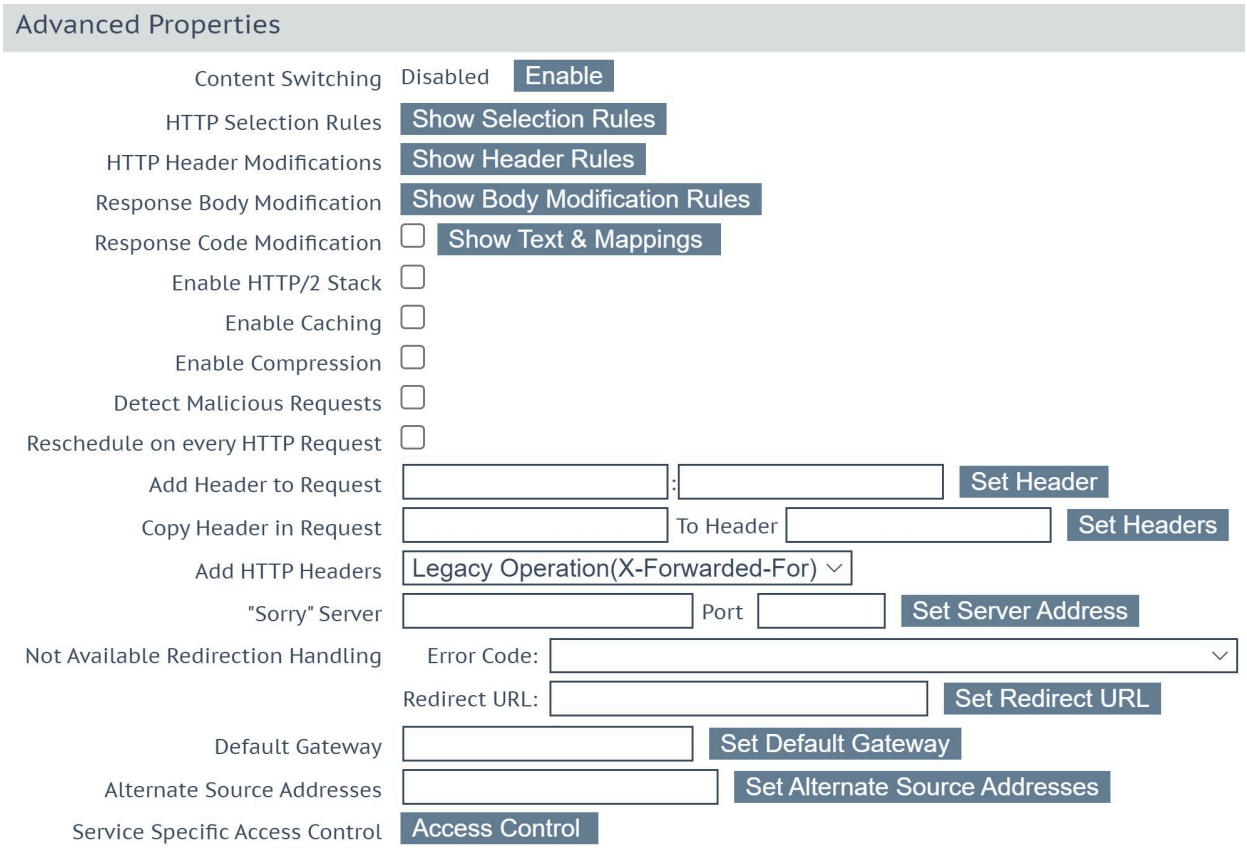
2. In the main menu, select **Virtual Services** and **View/Modify Services**.



3. Click **Modify** on the relevant Virtual Service.
4. Expand the **Standard Options** section.



5. Select **None** in the **Persistence Options** drop-down menu.
6. Expand the **Advanced Properties** section.



7. Click **Enable** in the **Content Switching** row.



Note: The enable button is only available if there is a Real Server set up on this Virtual Service.

Note: If you exit the Virtual Service modify screen without adding a content rule to a Real Server, you will need to re-enable **Content Switching**.

8. Expand the **Real Servers** section.

Note: There is a column called **Rules**. Content switching has just been enabled so no rules are active.

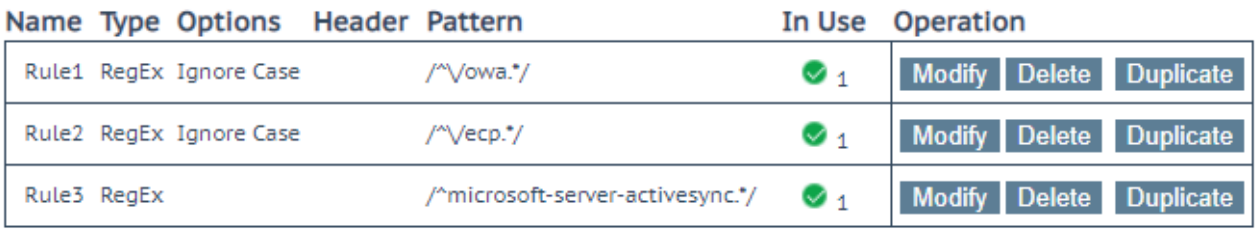
9. Click the **None** button.
10. Select the relevant rule in the drop-down list and click **Add**.

Note: The maximum number of content rules that a LoadMaster can have is 1024. There is no limit on a per-Real Server basis regarding how many of these rules can be assigned.

The rule is added to the Real Server. Multiple rules can be added to each Real Server.

Content Rules WUI Options

The various fields associated with Content Rules in the LoadMaster WUI are described below.



The **Content Rules** screen displays the rules that have been configured and gives the option to **ModifyDelete** or **Duplicate**.

In LoadMaster firmware 7.2.52 and above, it is possible to **Duplicate** content rules. There is also an **In Use** column on the Content Rules page that indicates if the content rule is in use or not:

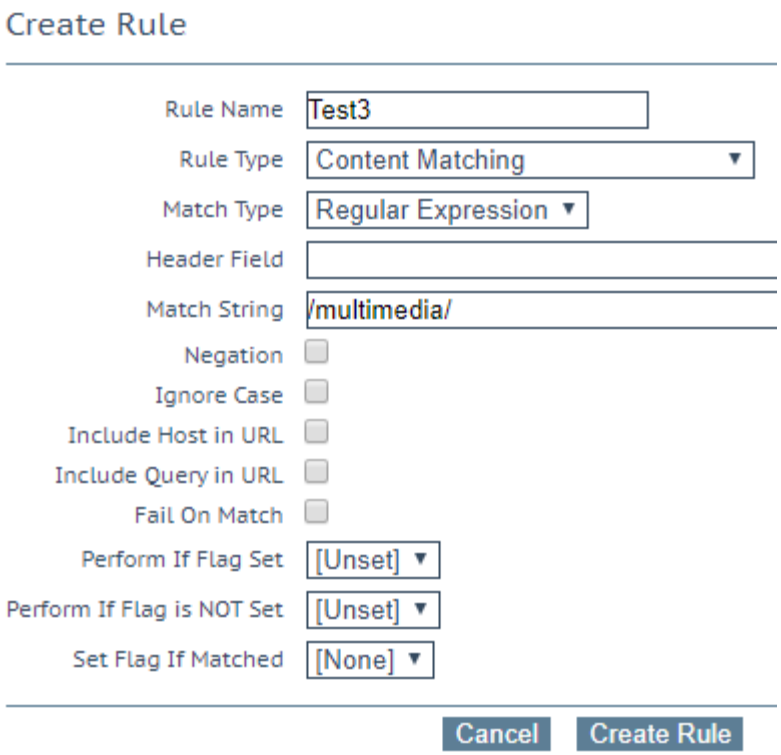
- The star icon means the content rule is not assigned to any Virtual Services.



- The tick icon means the content rule is assigned to at least one Virtual Service. The number of assigned Virtual Services is displayed next to the tick icon. Hover over the tick icon to get details about the Virtual Services this content rule is assigned to. The hover text only displays the first 20 assigned Virtual Services.



To define a new rule, click **Create New**.



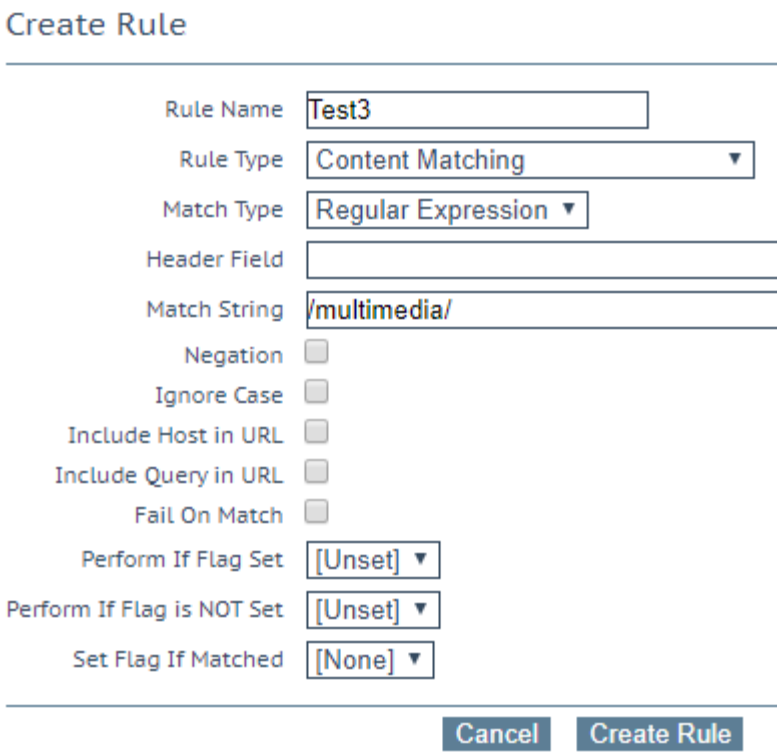
The **Rule Name** must be alphanumeric, unique, and cannot contain spaces. Rules are case sensitive, thus two different rules can exist in the form of **Rule1** and **rule1**. It is not possible to name a content rule **default**.

The options that are available depend on the **Rule Type** that is selected. The available rules are as follows:

- **Content Matching**: Matches the content of the URL, header or body of a request. For example, to rewrite requests for the root of a server, set the **Content Matching** rule type to match and send to a SubVS that is set to 301/302 (You can also use **Modfiy URL** rules to rewrite requests for the root of a server.)
- **Add Header**: Adds a header according to the rule. For example, to force connections to close, use an **Add Header** named **Connection** with the value set to close.
- **Del Header**: Deletes the header according to the rule and enables you to strip out server information
- **Replace Header**: Replaces the header according to the rule. For example, to rewrite redirects from HTTP to HTTPS, use the **Replace Header** rule type to rewrite the location header. To secure cookies, use the **Replace Header** rule type to replace/modify the contents of cookies that are set by the Real Server in the **set-cookie** header.
- **Modify URL**: Changes the URL according to the rule.
- **Replace String in Response Body**: Replaces text in the body according to the content in the rule.

Content Matching

When the **Rule Type** selected is **Content Matching**, the following options are available.



Rule Name

This is the name of the rule.

Match Type:

- **Regular Expression:** A powerful way of creating complex matching and replacement rules. Regular expressions can also be used to reference parts of the original string.

Note: If you use quotes in regular expressions in the LoadMaster WUI, there are limitations. For more information, refer to the section Limitations of Using Regular Expressions in the LoadMaster WUI.

- **Prefix:** Matches from the beginning of the string only.
- **Postfix:** Matches from the end of the string only.

Note: When **Prefix** or **Postfix** is selected, the **Match String** should be in the form of a pure string, not a regular expression.

Header Field

The header field name must be matched. If no header field name is set, the default is to match the string within the URL.

Rules can be matched based on the Source IP of the client by entering **src-ip** within the **Header Field** input field. The header field is populated by the source IP of the client.

The **Header Field** can be set to **method** to match on the HTTP method field.

The body of a request can also be matched by typing **body** in the **Header Field** text box. When matching on the **body**, up to the first 50K of the input stream is read.

Match String

Enter the pattern to match. Both Shell Regular Expressions and Perl Compatible Regular Expressions (PCRE) are supported.

Note: We recommend using PCRE expressions instead of Shell.

Both are the same in terms of performance. Performance is affected if a highly complex expression is used. The maximum number of characters allowed is 250.

To create a rule that sends all URL requests that have **/images*** as the root path to a group of servers, the **Match String** value should be **/^\/images.*/**

It is possible to perform content switching on URL, HTTP Header, Source IP, or the body of a request. The default behavior is to test the URL, however, a **Header Field** may be specified instead. To use Source IP content switching, use the pseudo-header **src-ip** — the source IP of the client is then available as a text field. The HTTP method can be matched upon by filling out the **Header Field** text box and the method. The body can be matched upon by entering **body** in the **Header Field** text box.

Negation

Negation inverts the sense of the match. Without negation, all requests that include **/images/** for example, would match an applicable rule. With negation, all requests except **/images/** would match the rule.

Ignore Case

If enabled, case is ignored when comparing strings.

Include Host in URL

If selected, this option prepends the hostname, for example, **support.progress.com**, to the request URL before performing the match.

Note: You may achieve better results by using flagging instead of using the **Include Host in URL** option. For more information, refer to the Use of Flags to Create Dependent Rules section.

Include Query in URL

Selecting this option enables the match string to include the text generated after the **?** in a URL. This part of the URL is the URL query. For example, in the URL **http://example.com/images/imagid.jsp?item=1**, the query is **item=1**.

Fail on Match

If this rule is matched, then always fail to connect. If an error code or error URL is set, the code/URL is sent back to the client.

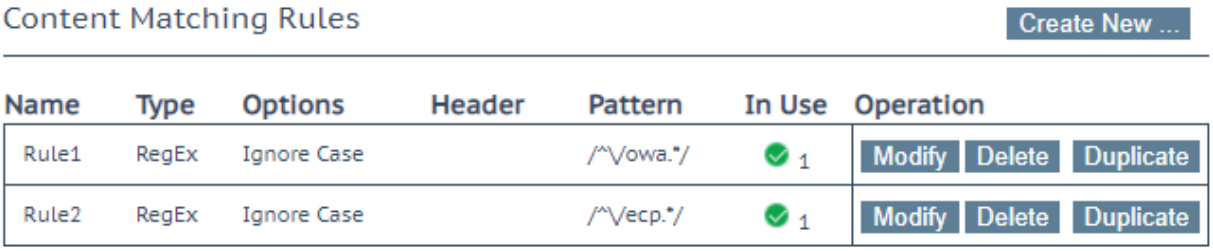
Use of Flags to Create Dependent Rules

By using the **Perform If Flag Set** and **Set Flag If Matched** options it is possible to make rules dependent on each other, therefore, only execute a particular rule(s) if another rule(s) has been successfully matched.

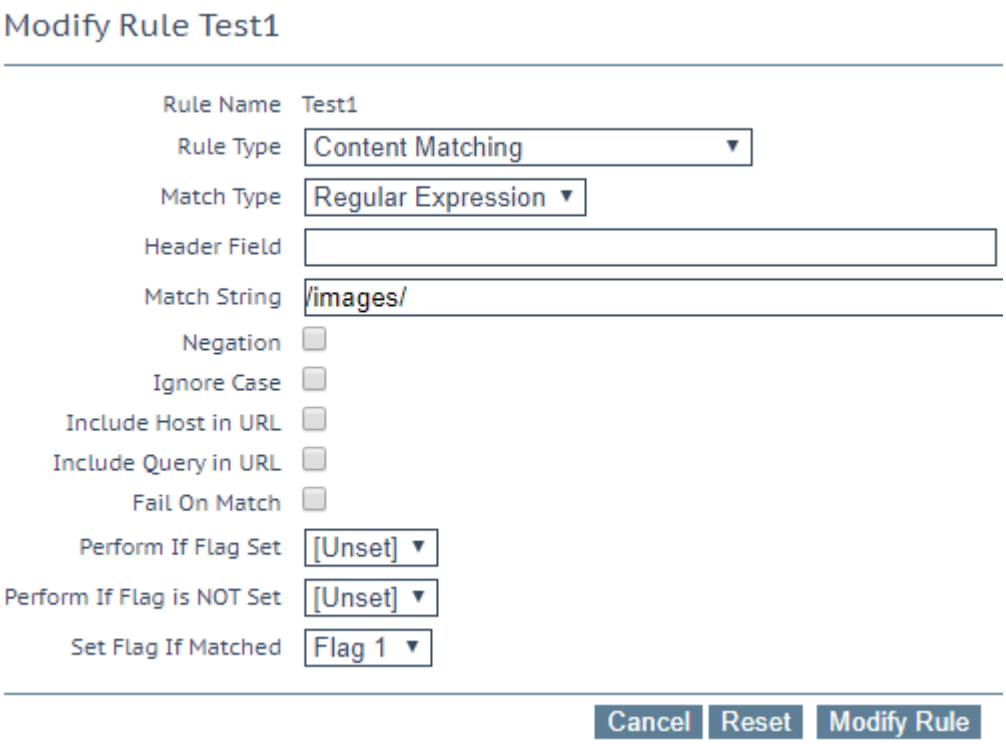
Note: You can also use the **Perform If Flag is NOT Set** field to only execute a rule if the specified flag is not set.

For example, if a rule called **Test2** should execute only if a rule called **Test1** was matched successfully, complete the following steps:

1. Log in to the LoadMaster WUI.
2. In the main menu, select **Rules & Checking** and **Content Rules**.

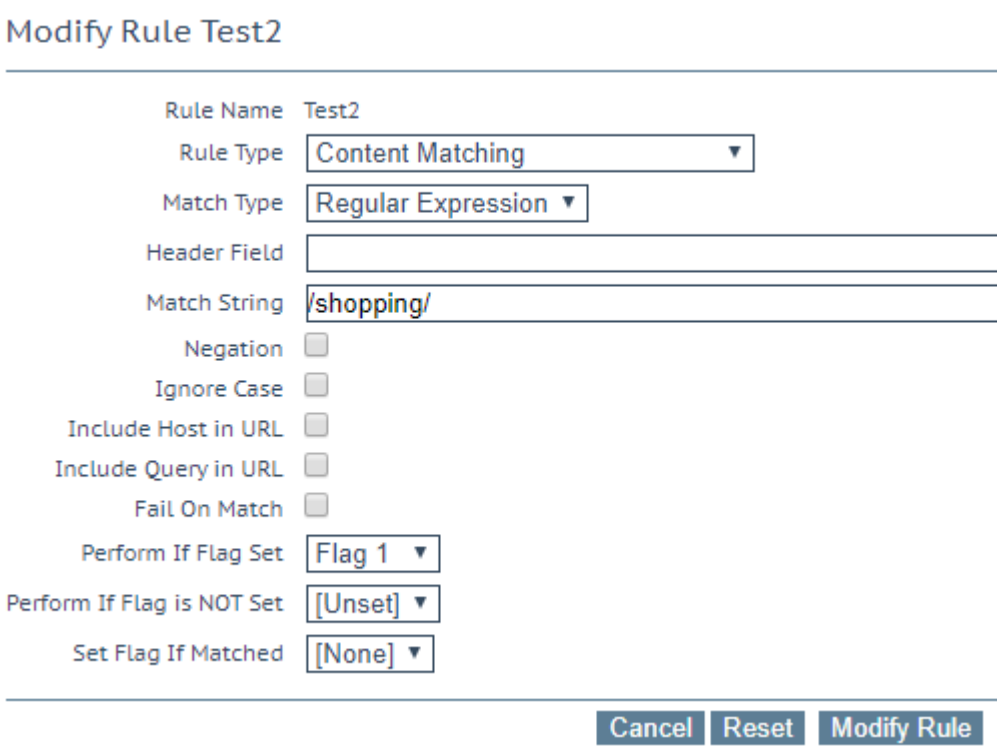


3. Click **Modify** on the **Test1** rule.



4. Select **Flag 1** from the **Set Flag If Matched** drop-down list.

5. Click **Modify Rule**.
6. Click **Modify** on the **Test2** rule.



7. Select **Flag 1** from the **Perform If Flag Set** drop-down list.
8. Click **Modify Rule**.

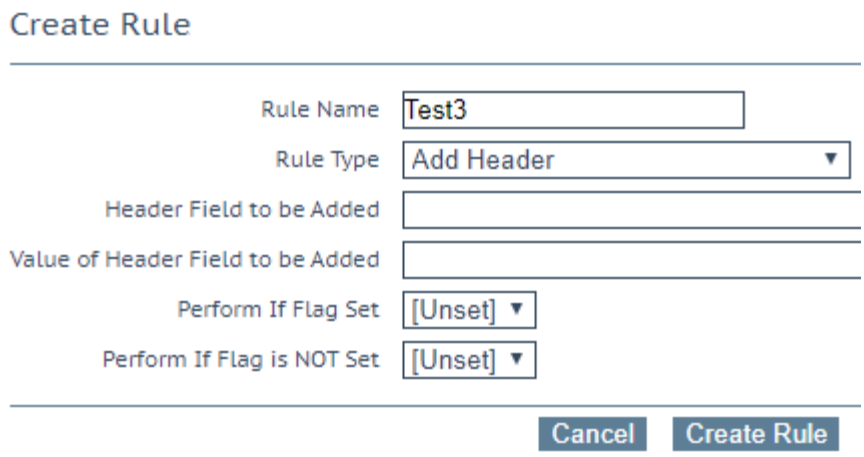
When the **Test1** rule is successfully matched, a flag (**Flag 1**) is set. The **Test2** rule will not execute unless **Flag 1** is set. So, **Test2** cannot run unless **Test1** has been successfully matched.

If a flag is set during the matching of a request, it can be queried when processing response header modifications. Therefore, if the request sets a given flag, when the server responds, any response rules that are dependent on the flag will only execute if it is set.

Note: Up to nine rule dependencies can be set up (as there are nine flags available to set) which can create a chain of dependent rules.

Add Header

The **Add Header** option adds a static header to the request. This can be used on the client header going to the server, or on the server header going to the client.



Rule Name

This field is used for identification and should be named to help remember what the rule does in the Virtual Service.

Header Field to be Added

This is the name of the field inserted in the header.

Note: Do not add the trailing colon.

Value of Header Field to be added

This is the value that will be associated with the inserted header.

Perform if Flag is Set

Only execute this rule if the specified flag is set.

The flag will have been set by a different rule.

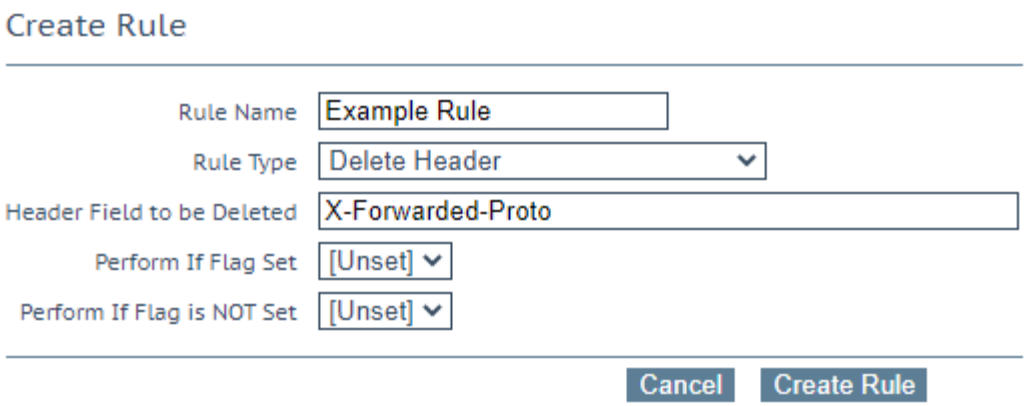
Perform If Flag is NOT Set

Only try to execute this rule if the specified flag is not set.

Delete Header

The **Delete Header** option removes a header from the request. This can be used on the client header going to the server, or on the server header going to the client.

The **Delete Header** option uses a Regex over the whole header and the value of the header. The header will only be deleted if it all matches.



For example, in the screenshot above the **Server** header is being deleted to hide the web server details from the client. If the header name **Server** is matched, the header is deleted. If you want to change or delete the value of a header, use the **Replace Header** rule instead.

Rule Name

This field is used for identification and should be named to help remember what the rule does in the Virtual Service.

Header Field to be Deleted

The LoadMaster removes the header field with this name from the request/response**.**

Note: Do not add the trailing colon.

Perform if Flag is Set

Only execute this rule if the specified flag is set.

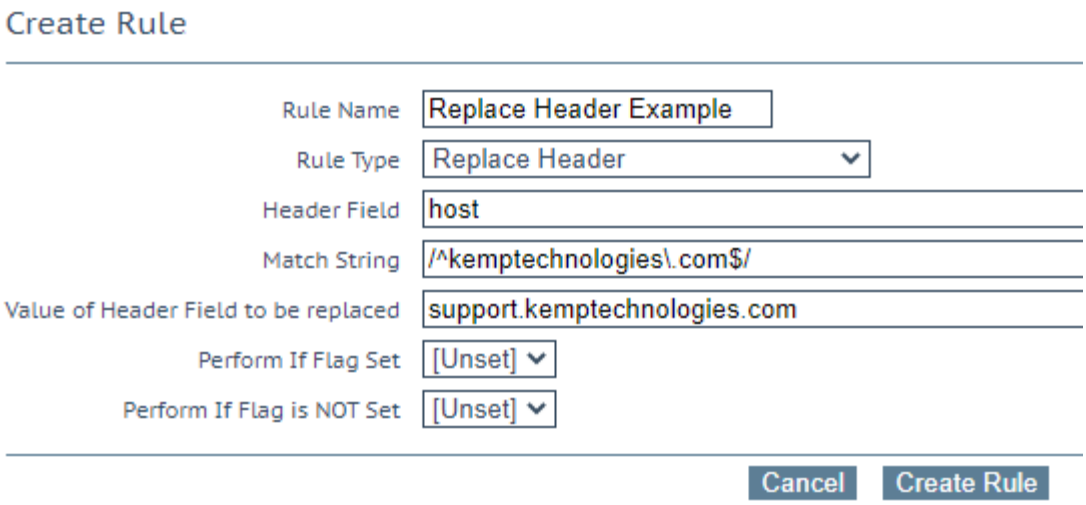
The flag will have been set by a different rule.

Perform If Flag is NOT Set

Only try to execute this rule if the specified flag is not set.

Replace Header

The **Replace Header** option matches a header based on its value and replaces its value with the one specified. This can be used on the client header going to the server, or on the server header going to the client.



Rule Name

This field is used for identification and should be named to help remember what the rule does in the Virtual Service.

Header Field

This is the name of the field that the substitution will be performed on.

Note: Do not add the trailing colon.

Match String

Enter a pattern to match against the content of this header. If the content matches the pattern, the header value will be replaced. This follows regular expression rules.

Value of Header Field to be replaced

When the rule is matched, the value of the header will be replaced with this text. Regular expressions and back references can be used here to reuse part of the existing value.

\1 and **\2** can be used as back reference marks in PCRE expressions. For example:

Match: /(path1)\/(path2)/

Edit: new-path-is-\2/\1

Expected output: new-path-is-path2/path1

Perform if Flag is Set

Only execute this rule if the specified flag is set.

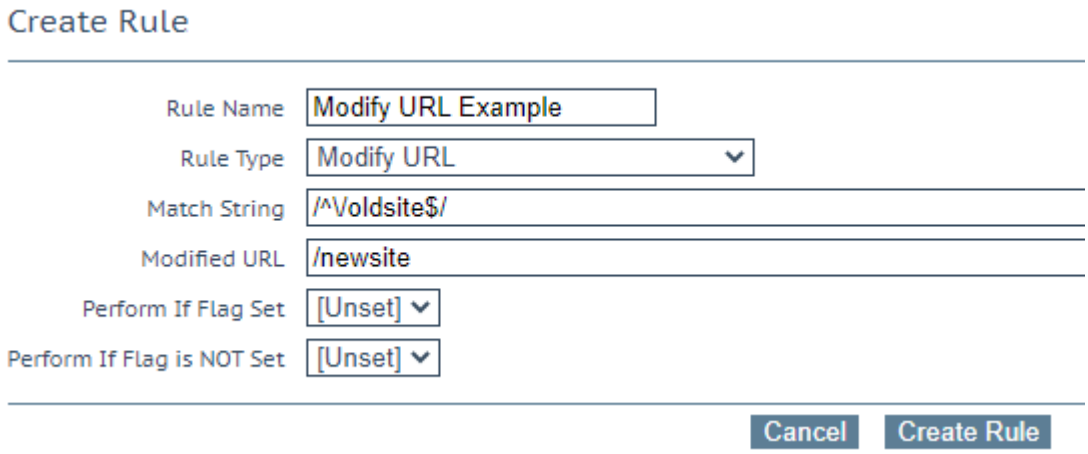
The flag will have been set by a different rule.

Perform If Flag is NOT Set

Only try to execute this rule if the specified flag is not set.

Modify URL

The **Modify URL** option is a specialized header replacement that only matches the URL in the HTTP headers and replaces it with the one specified. This can be used on the client header going to the server.



Rule Name

This field is used for identification and should be named to help remember what the rule does in the Virtual Service.

Match String

Enter a pattern to match against the URL. If the URL matches the pattern, the URL value will be replaced. This follows regular expression rules.

Modified URL

Enter the new URL to be sent to the server. Regular expressions and back references can be used here to reuse part of the existing value.

Perform if Flag is Set

Only execute this rule if the specified flag is set.

The flag will have been set by a different rule.

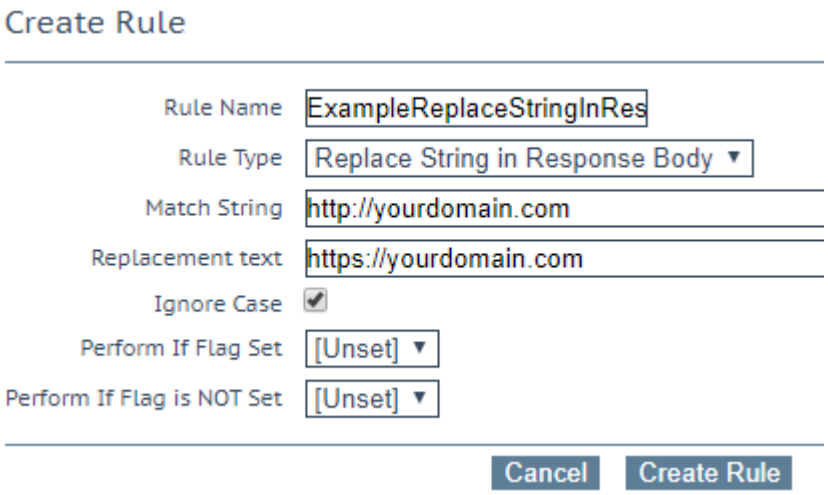
Perform If Flag is NOT Set

Only try to execute this rule if the specified flag is not set.

Note: As of LoadMaster firmware version 7.2.51, you can assign URL modification rules to a response.

Replace String in Response Body

When the **Rule Type** selected is **Replace String in Response Body**, the following options available.



Rule Name

The name of the rule. The rule name must be unique.

Match String

The string to match.

Replacement text

The replacement string.

Ignore Case

Enable this check box to ignore the case of the strings when comparing.

Perform If Flag Set

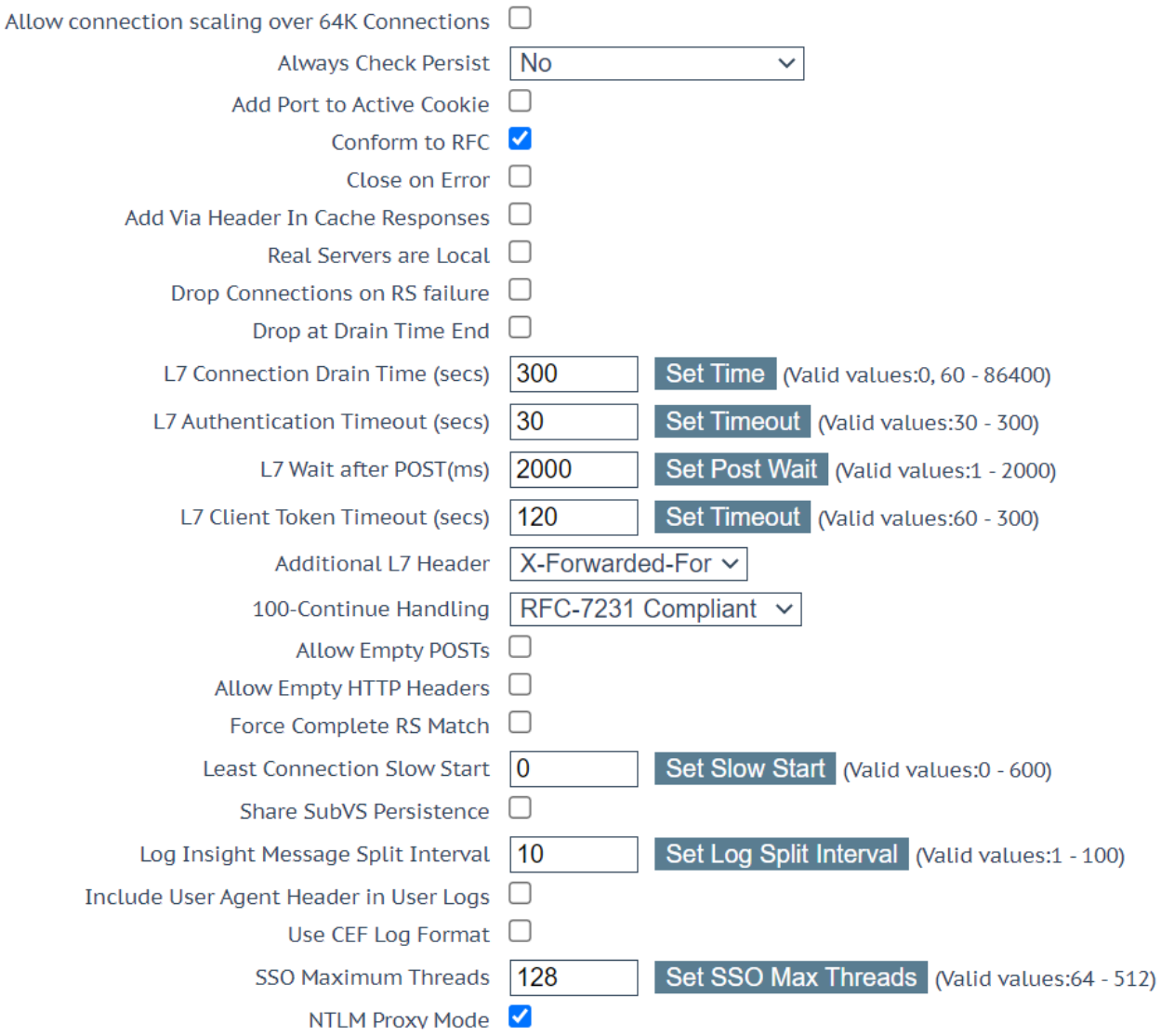
Only execute this rule if the specified flag is set.

The flag will have been set by a different rule.

Perform If Flag is NOT Set

Only try to execute this rule if the specified flag is not set.

Force Complete RS Match



By default, when the LoadMaster tries to locate a Real Server for use with content switching, it tries to use the same Real Server as currently selected, even if the port is not the same. Enabling this option forces the port to also be compared. To enable this option, go to **System Configuration > Miscellaneous Options > L7 Configuration** and select the **Force Complete RS Match** check box.

You may need to enable this option in the event that you are trying to content match to the same Real Server but on different ports, for example:

Virtual Service 1:

- Real Server 1: 10.140.22.146:80 - content match on X
- Real Server 2: 10.140.22.146:8080 - content match on Y

Content Matching is enabled on each SubVS. If the destination for a content rule is checked (the Real

Server) but not the port, the LoadMaster tries to reuse the current connection instead of opening a new connection to save on performance. Enabling this option should force the LoadMaster to also check the port.

Limitations of Using Regular Expressions in the LoadMaster WUI

When using regular expressions in the LoadMaster WUI, you must use an even number of quotes (single or double). The quotes must also nest correctly, for example, if you use single quotes within double quotes, the single quotes must be matched inside the double-quotes. To use a single " (double-quote) character in a regex, use **%22** instead (or **%27** for a single quote).

If you want to use an uneven number of quotes in a regular expression, use the API instead of the WUI.

For example, trying to set the following **Match String** in the WUI results in an error that says **Please specify a pattern to be matched**:

/\<img([^\>\/]*)\ssrc\=\"([^\"]*)\"([^\>\/]*)\/?>/

However, it is possible to set this using the API, for example:

```
/access/
addrule?name=Example&pattern=/\<img([^\>\/]*)\ssrc\=\"([^\"]*)\"([^\>\/]*)\/?>/
```

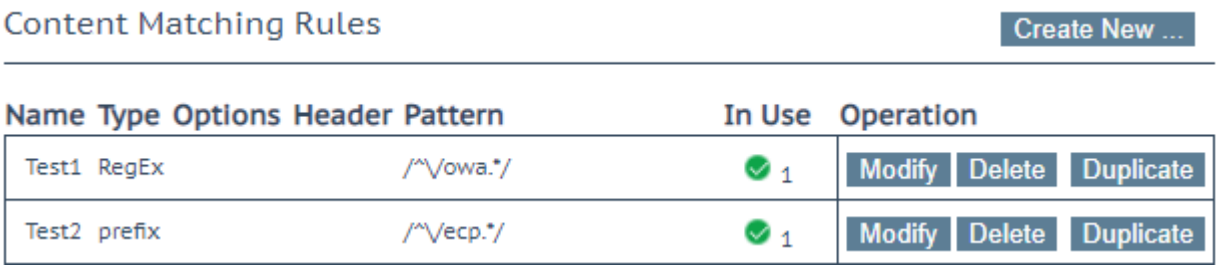
Content Matching Rules

Content Matching rules are also known as selection rules. These rules allow you to match all or some of a **Header Field** or URL string and then set flags if there is a match.

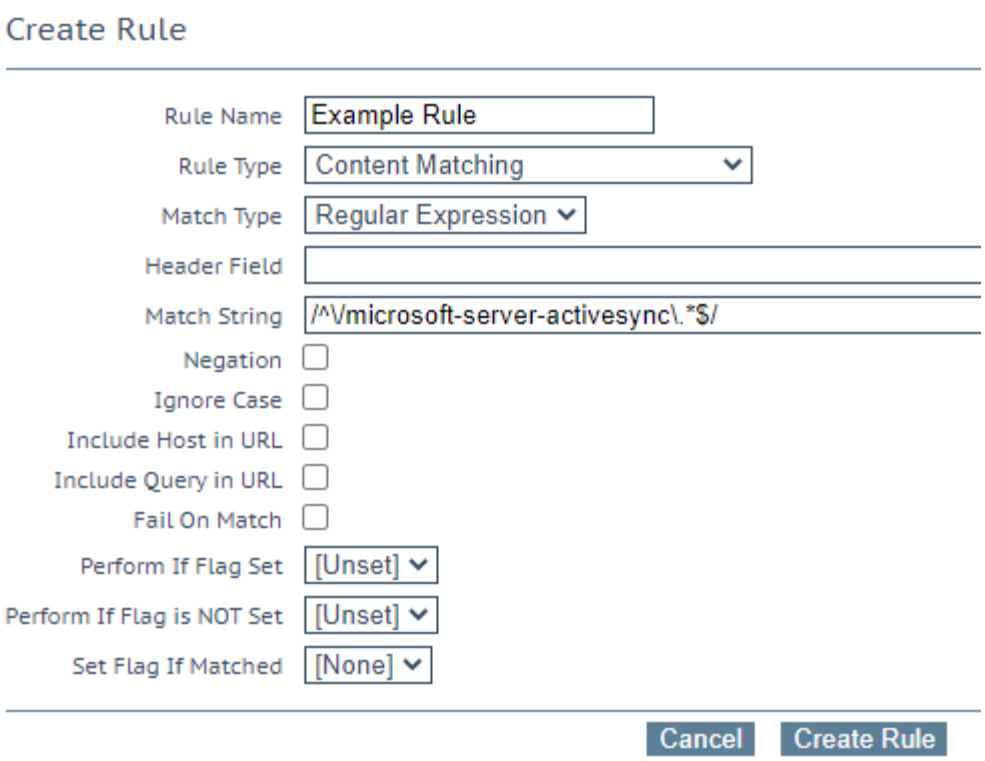
Adding Content Matching Rules

To add a content matching rule, follow the steps below:

1. Log in to the relevant LoadMaster WUI.
2. In the menu on the left, select **Rules & Checking** and **Content Rules**.



3. Click **Create New…**.



4. Enter a recognizable **Rule Name**.
5. Ensure **Content Matching** is selected as the **Rule Type**.
6. Select which **Match Type** to use.

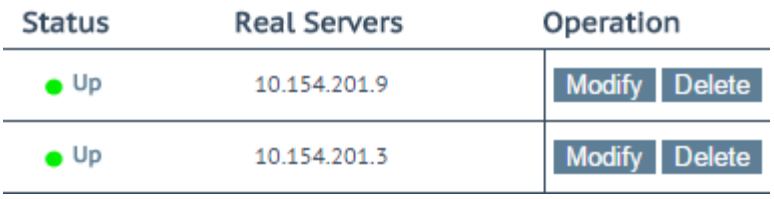
   Note: For more information on the **Match Type** options, or any of the fields on this form, refer to the Content Matching section.

7. Enter the relevant **Header Field**, or enter **body** to match on the body of a request.
8. Enter the **Match String**.
9. Enable/disable any of the check boxes as required.
10. Select any flags as needed in the **Perform If Flag Set**, **Perform If Flag is NOT Set**, and **Set Flag If Matched** drop-down lists.
11. Click **Create Rule**.

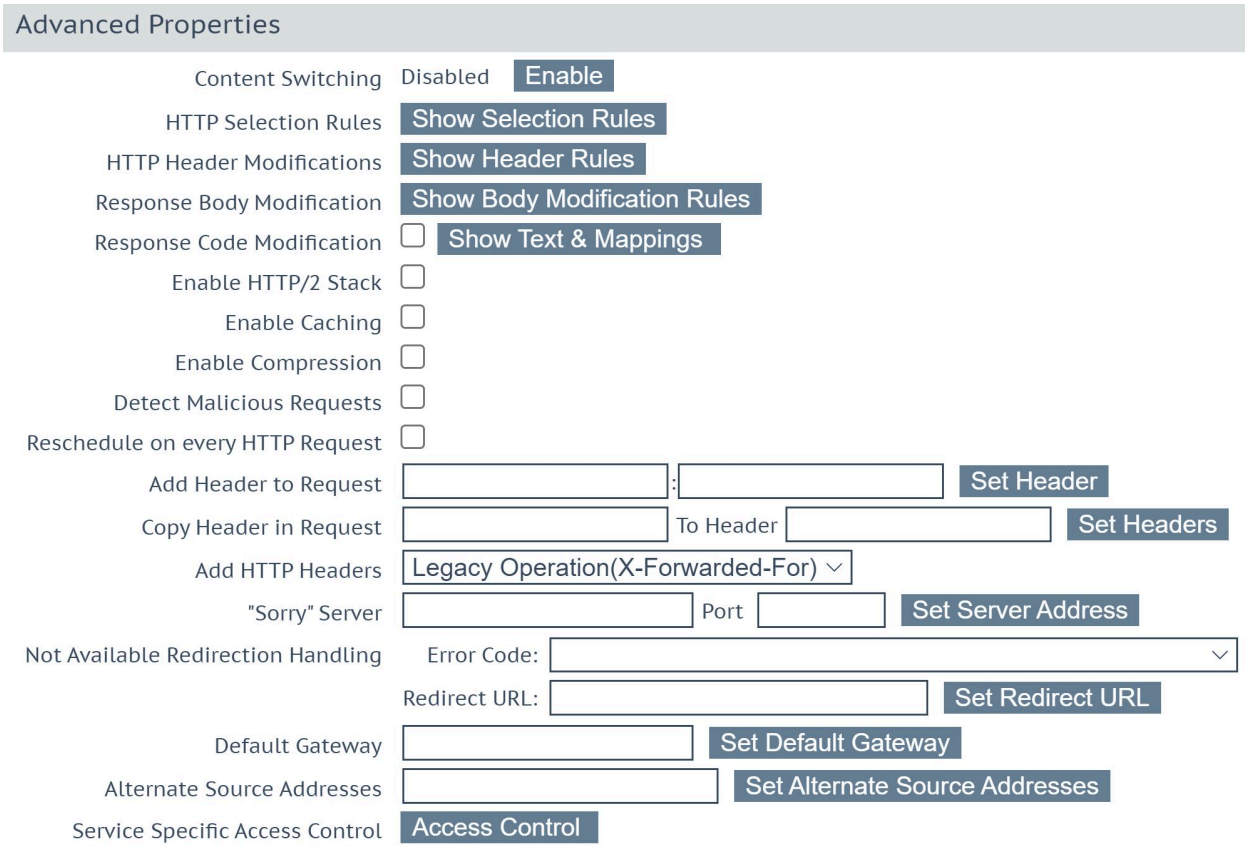
Associating Content Matching Rules to a Virtual Service

After a rule is created, you can associate it to a Virtual Service. To do this, follow the steps below:

1. In the main menu of the LoadMaster WUI, select **Virtual Services** and **View/Modify Virtual Services**.



2. Click **Modify** on the relevant Virtual Service.
3. Expand the **Advanced Properties** section.



4. Click **Show Selection Rules**.

Note: If any content matching rules exist on this LoadMaster, they will be visible here.

5. Select the relevant rule and click **Add** .



If there is more than one rule in a section, the priority at which a rule is applied can be adjusted using the

Move button.

Note: In LoadMaster firmware 7.2.52 and above, it is easier to reorder the priority of rules in a Virtual Service - there is a move option that allows you to specify the position to move the rule to.

Header Modification

Modifying headers gives control over how HTTP functions. The LoadMaster can add, delete, and replace HTTP headers, including URL modification. This is done on a per Virtual Service basis and can be used for request and/or response headers.

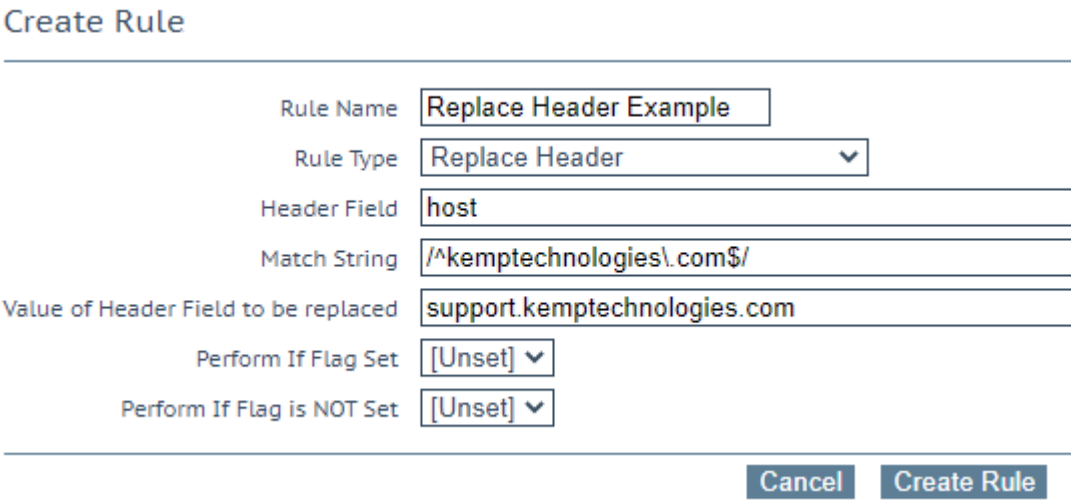
Header modification can be used to add identifying information to incoming requests. For example, if the LoadMaster is offloading SSL, the traffic back to the server is usually HTTP plain text. Normally, the server does not know that this had come in on SSL originally. To help identify this traffic as SSL originating, a header such as **SSL_Offload: Yes** can be added.

Another reason you may use a header modification rule is to delete/modify sensitive information returning from the server, such as operating system or web server version.

Adding Header Modification Rules

To add a header modification rule, follow the steps below:

1. Log in to the relevant LoadMaster WUI.
2. In the menu on the left, select **Rules & Checking** and **Content Rules**.
3. Click **Create New**.



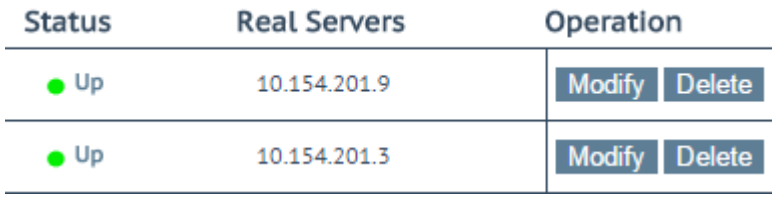
A number of rule types can be added. The **Add Header**, **Delete Header**, **Replace Header**, and **Modify URL Rule Type** options all modify the HTTP stream in some way. For information about what each of the fields mean, refer to the Content Rules WUI Options section. For **Replace Header** and **Modify URL** rules, shell syntax or Perl Compatible Regular Expressions (PCRE) style regular expressions can be used. For

information on regular expressions, refer to the PCRE section.

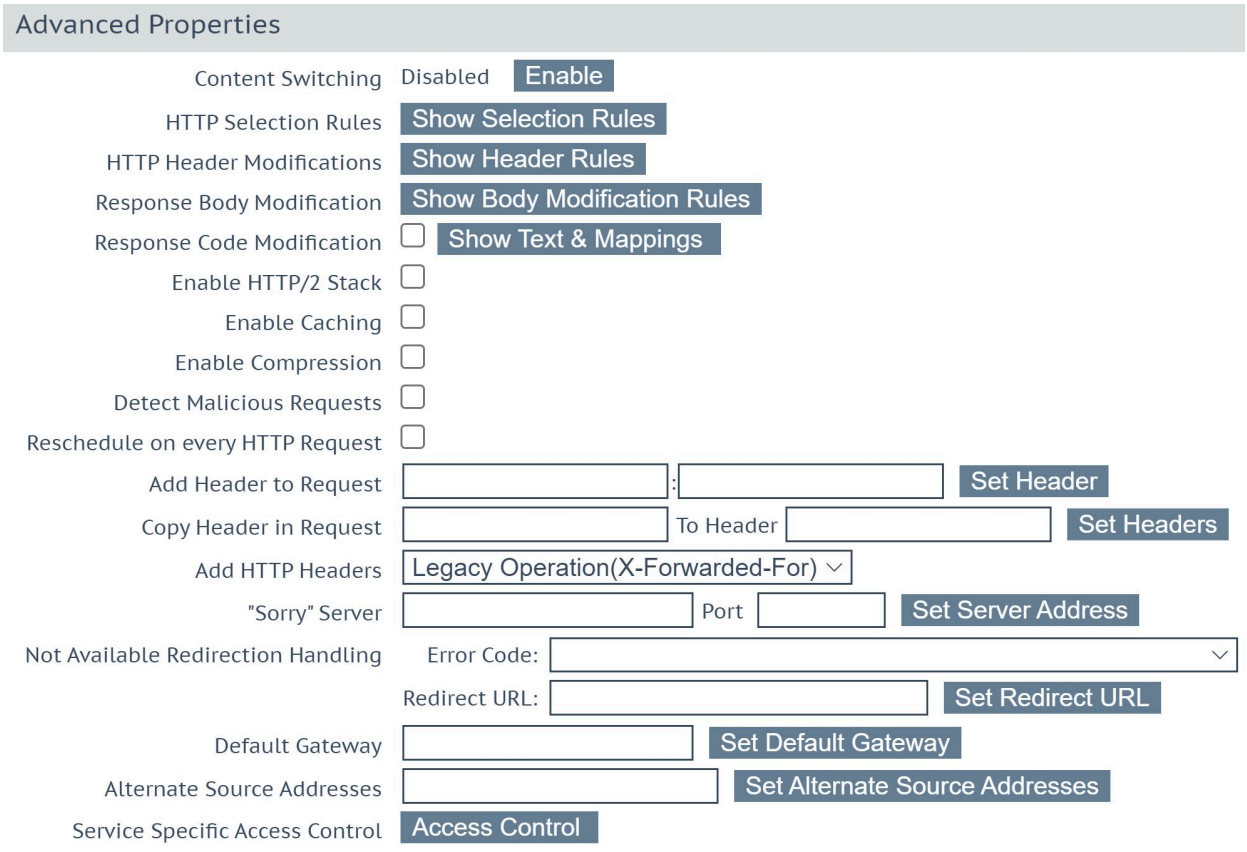
Associating Header Rules to a Virtual Service

Once a rule has been created, it can be associated to a Virtual Service. To do this, follow the steps below:

1. Log in to the relevant LoadMaster WUI.
2. In the main menu, select **Virtual Services** and **View/Modify Services**.



3. Click **Modify** on the relevant Virtual Service.
4. Expand the **Advanced Properties** section.



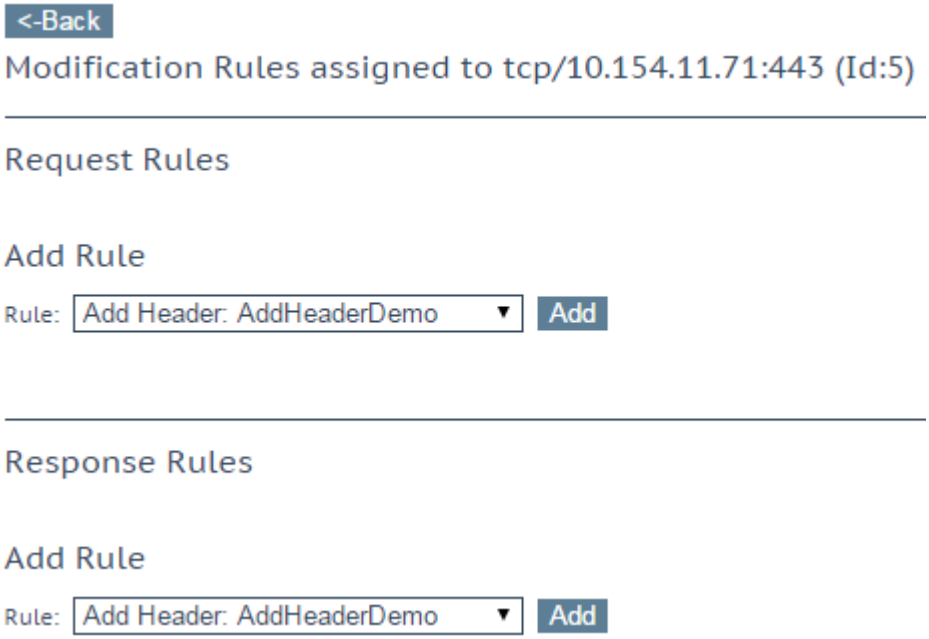
5. Click **Show Header Rules**.

   Response Rules: These are modifications to the server headers going back to the client or the URL.

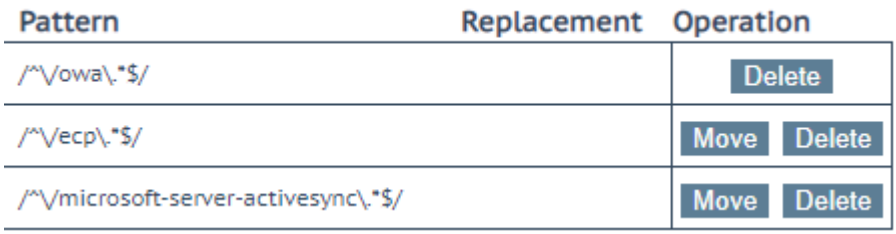
   Request Rules: These are modifications to the client headers going to the server.

Here, either **Request Rules** or **Response Rules** can be added.

If any header modification rules exist for this LoadMaster, they will be visible here.



6. Select the relevant rule in the relevant section and click **Add** .



If there is more than one rule in a section, the priority at which a rule is applied can be adjusted using the **Promote** button.

In LoadMaster firmware 7.2.52 and above, it is easier to reorder the priority of rules in a Virtual Service - there is a move option that allows you to specify the position to move the rule to.

SSL Information in Client Request Headers

In LoadMaster version 7.2.52 and above, a new check box called **Add Received Cipher Name** was added. This option is disabled by default. when this option is enabled, the LoadMaster adds X-SSL headers containing client SSL information such as TLS version, TLS cipher, client certificate serial number, and SNI host as described in below table.

The information contained in these headers can be used in content rules by referencing the appropriate header name in the rule (see the table below). This allows you to make load balancing decisions based on, for example, the cipher used.

This information can also be useful, for example, as you maintain cipher sets over time; it allows you to see which ciphers are being used and can help you plan what ciphers to change or delete in the cipher sets. The **Add Received Cipher Name** check box must be enabled to use the headers in the table below in content rules.

Header	Description	Example Value
X-SSL-Cipher	The cipher used.	X-SSL-Cipher: ECDHE-RSA-AES256-GCM-SHA384
X-SSL-Protocol	The SSL protocol version used.	X-SSL-Protocol: TLSv1.2
X-SSL-Serialid	The Virtual Service certificate serial number.	X-SSL-Serialid: 4900000006A2ABDC165ACEAD55000000000006
X-SSL-ClientSerialid	The client certificate serial number.	X-SSL-ClientSerialid: 490000005D6898F3C7E590536100010000005D
X-SSL-SNIHost	The value of the received SNI name.	X-SSL-SNIHost: sni.test.com

Response Body String Replacement

Response body string replacement rules can be used to reduce cost and time-to-market when in-transit traffic handling requirements change for applications. For example, you may want to rewrite URLs that are in the BODY of the response and change them from HTTP to HTTPS. This may be needed if there is a third-party application that has a number of hyperlinks embedded. It may be easier to mitigate this with a proxy type feature than it is to have the third party rework the application. The LoadMaster may be used to SSL offload a Virtual Service in front of the application. Because of this configuration, responses need to return to the LoadMaster as HTTPS. These response body string replacement rules can be used to modify the URLs embedded in the BODY.

These rules can also be used to switch domain names, for example, replace **test.yourdomain.com** with **yourdomain.com**.

Rules can be assigned to process the response body. These rules are run over the response body before it is sent to the client.

These rules do not work on binary files or compressed files. Something to be aware of is that it is very common for a browser to send the file compressed. To stop compression from occurring, remove the "Accept-Encoding" header (or remove any gzip information from that field) from each request. It is possible to do this using a content rule. You can also configure your server to not compress specific files (the steps to configure this are server-dependent). Contact Progress Kemp Support for further help, if needed.

If you try to perform body modification rules on file types listed in **Virtual Services > Compression Options** in the **File extensions that should not be compressed** field, this will not work. File types that you want to perform body modification rules on should not be listed in the **File extensions that should not be compressed** field.

The whole response is read into the LoadMaster before it is processed.

Each file is treated as a set of lines. The rules (multiple rules are allowed) are run over each line, one at a time. If a match is found, the text is replaced.

The file size must be greater than 512 bytes for the rule to be applied. If the file size is equal to or less than 512 bytes, the rule is not applied.

Body rules are case dependent. They can be made case independent by selecting the **Ignore Case** check box when creating the rule.

The system performs a "global replace" on each line. If more than one rule matches at a particular location, the first rule in the list is performed (rule precedence can be managed by using the **Move** button in the Virtual Service **Body Modification Rules** screen).

In LoadMaster firmware 7.2.52 and above, it is easier to reorder the priority of rules in a Virtual Service - there is a move option that allows you to specify the position to move the rule to.

Rules starting with a "beginning of line (^)" only match the start of the line.

Responses can only be handled if they fit in the configured cache memory. Input lines/resulting lines can have a maximum length of approximately 64K bytes in length (before or after - depending on how much data is added and taken away in the modifications). If an input line is more than 64K, it is processed as if it was a line of 64K. If the resulting line after the modification is more than 64K, only the first 64K is included in the output, the rest is ignored.

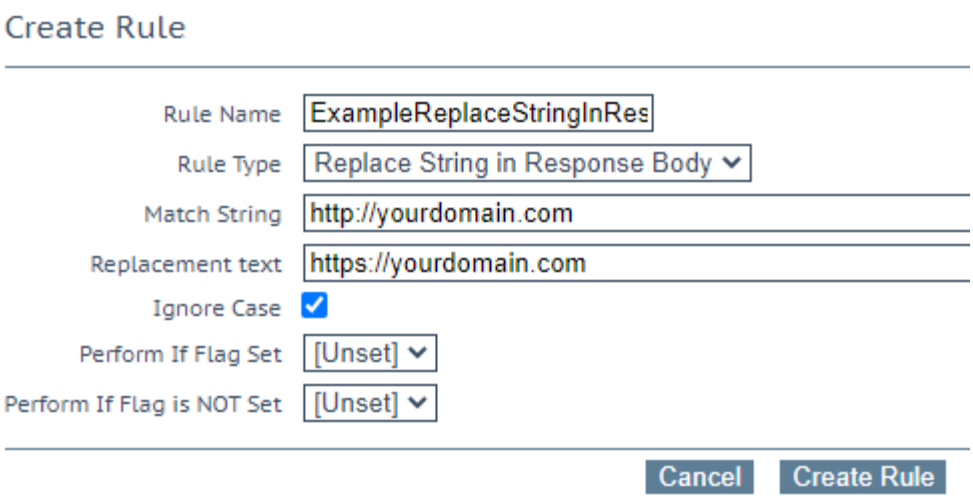
Response body rules are not compatible with Kerberos Constrained Delegation (KCD). If KCD is enabled on a Virtual Service, it is not possible to assign a body rule to it.

Response body modification rules are only executed on the body of the server response if the HTTP response code received along with the response from the server is 200 OK. If any other HTTP response code is received, no response body modifications are performed on that server response.

Adding Response Body String Replacement Rules

To add a response body string replacement rule, follow the steps below in the LoadMaster WUI:

1. In the menu on the left, go to **Rules & Checking > Content Rules**.
2. Click **Create New**.

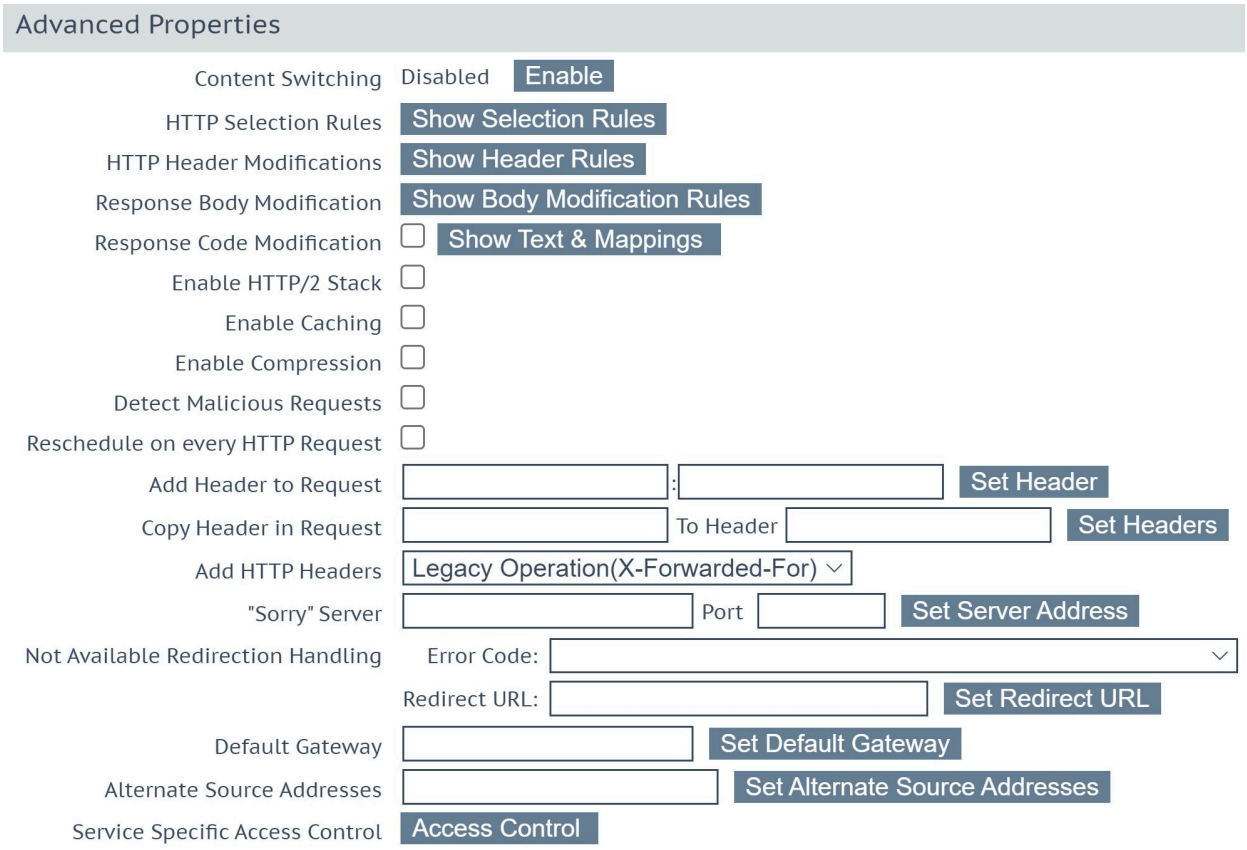


3. Enter the **Rule Name**.
4. Select **Replace String in Response Body** as the **Rule Type**.
5. Enter the string to be matched in the **Match String** text box.
6. Enter the replacement string in the **Replacement text** text box.
7. Select the **Ignore Case** check box if you want case to be ignored during the comparison.
8. Select any flags as needed in the **Perform If Flag Set** and **Perform If Flag is NOT Set** drop-down lists.

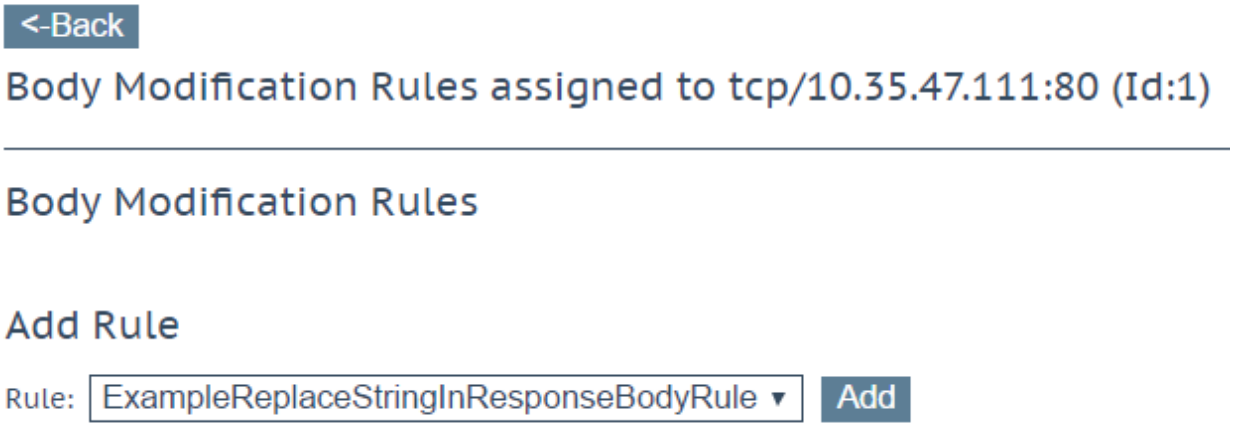
Associating Response Body String Replacement Rules to a Virtual Service

Once a rule has been created, you can associate it with a Virtual Service. To do this, follow the steps below in the LoadMaster WUI:

1. In the main menu, go to **Virtual Services > View/Modify Services**.
2. Click **Modify** on the relevant Virtual Service.
3. Expand the **Advanced Properties** section.



4. Click **Show Body Modification Rules**.



5. Existing body modification rules are shown here. Select the relevant rule and click **Add**.

Pattern	Replacement	Operation
http://kemptechnologies.com		Delete
https://support.kemptechnologies.com		Move Delete
http://progress.com		Move Delete

If there is more than one rule in a section, you can adjust the priority of the rule by using the **Move** button.

Note: In LoadMaster firmware 7.2.52 and above, it is easier to reorder the priority of rules in a Virtual Service - there is a move option that allows you to specify the position to move the rule to.

4

Perl Compatible Regular Expressions

Perl Compatible Regular Expressions (PCRE) implements regular expression pattern matching. It uses the same syntax and semantics as Perl 5. For further information regarding PCRE, refer to www.PCRE.org

When using special characters in PCRE, it is best practice to use the character's ASCII or HTML equivalent rather than the actual character. For example, to match the percentage symbol, instead of writing **/%/,** for the HTML version, use **/&#37/**, and for the ASCII version use **/\x25/.**

To ensure that an expression is treated as a PCRE, the expression must be enclosed by the forward-slash character (/) or it will be treated as a Shell Regular Expression. For example, a PCRE expression would look like this: **/^[Tt]est$/.**

Character	Meaning
.	Matches any character but a line-break
\d	Matches any numeric digit
\w	Matches any alpha character

Character	Meaning
[]	Matches a set of characters
?	Optionally matches the previous expression
*	Matches the previous expression zero or more times
+	Matches the previous expression one or more times
{x}	Matches the previous expression x times
{x, y}	Matches the previous expression x to y times
^	Matches the beginning of the string/line
$	Matches the end of the string/line
(x)	Allows grouping of expressions
a|b	Alternative expressions, matches a OR b

Related Links

For details, see the following topics:

- PCRE Examples

PCRE Examples

Some PCRE examples are below:

- **^/$** matches **/** and **/** only
- **^.*test.*$** matches the whole line of any line where test is mentioned

- **[A-F0-9]{8}** matches a string of eight hex characters
- **Gr[ae]y** matches both spellings of gray/grey
- **^(www\.example\.com|example.com)$** matches www.example.com and example.com
- **^[^~].*$** matches any line that does not start with **~**
- **\s\s+** matches multiple consecutive line breaks

5

Shell Regular Expressions

Regular expressions can be used to craft complex matching and replacing rules. The **Match String** can be a Shell Regular Expression, which is a type of statement that matches or excludes based on the strings. An asterisk (*****) in a Shell Regular Expression means “match all”.

A Shell Regular Expression is a sequence of characters. Any character, which is not a special character, matches itself. The following special characters are defined.

Character	Meaning
^	This can only be placed at the start of the string and means that the string must match at the start of the URL
$	This can only be placed at the end of the string and means that the string must match at the end of the URL
?	This matches any single character
*****	This matches zero or more characters

Character	Meaning
[	This starts the set notation. This matches a single character which is contained within a set. If the set starts with **^**, then this matches a single character which is not within the set

Related Links

For details, see the following topics:

- Shell Regular Expression Examples

Shell Regular Expression Examples

Some examples of Shell Regular Expressions are below:

- **[0-9]** matches any single digit
- **[^abf]** matches any character, which is not “a”, “b” or “f”
- **^/[^a-z]** matches any first character in the URL which is not a small letter
- **home/*.gif** matches any URL which points to a **.gif** file in the **/home** directory
- **[gG][il][fF]** matches any URL which contains the string “gif”, “GIF”, “gIF”, “giF”, “GiF”, and so on.

Note: Given an input URL such as **/home/cgi-bin/XXX.cmd?value=hello**, the end of the string used in matching is terminated by the **?** character, therefore, a postfix string of **cmd** matches this URL, while a postfix of **hello** does not. To include the end of the string, enable the **Include Query in URL** option.

6

Content Rules Cookbook

Some example rules that can be used in real life scenarios are below. For further information on content rules and to see further examples, refer to http://kemptechnologies.com/load-balancing-support/kemp-support.

Note: The examples provided here are for guidance purposes only. They may not work in all configurations.

Related Links

For details, see the following topics:

- Match Host or Domain
- Change Domain or Host
- Match URL or Directory
- Change URL or Directory
- Naked Domain Rewrite
- Rewrite Clients from "/" to "/testpage"
- Redirect Content to a Different URL While Keeping the Directory or Path
- Redirecting Clients from HTTP to HTTPS
- Change the Host Seen by the Real Server
- Match on Source IP

- URL Rewrite Based on Source IP
- Add the SSL Secure Flag and HTTPonly Flag to Cookies from the Real Server
- User-Agent String
- Changing the User-Agent String
- Content Match on a Query
- Content Matching Rule Example

Match Host or Domain

Use the following rule to match a host or a domain, for example, **https://www.domain.com**

Rule type: Content Matching

Match Type: Regular Expression

Header Field: Host

Match String: /^www\.domain\.com$/

Ignore Case: enabled

Match field

Start Regex: /

Start Match: ^

Regular text: www

Literal character: \.

Regular text: domain

Literal character: \.

Regular text: com

End Match: $

End Regex: /

Change Domain or Host

Option 1: 302 Redirects

302 Redirect Logic

When the client connects to **www.domain.com**, the LoadMaster sends a 302 redirect to the client and tells the client to connect to the new domain. This is also used for redirecting HTTP to HTTPS. With this option, the client sees the change in the browser.

Syntax

In the Virtual Service modify screen: **Advanced Properties -> Not Available Redirection Handling**.

Error code: 302 found

Redirect URL: http://www.newdomain.com

or for HTTP to HTTPS: **https://%h%s**

Replace with Host/Domain: %h

Replace with URL/Directory/Path: %s

Example: %h and **%s** are replaced with **http://www.newdomain.com/test/index.html**

Option 2: Rewrite the URL

Logic

Match on host and replace host with new host details. With this option, the client does not see the change in the browser.

Syntax

Rule: Replace Header

Header: Host

Match String: /^www\.domain\.com$/

Replace with: www.newdomain.com

Match field

Start Regex: /

Start Match: ^

Regular text: www

Literal character: \.

Regular text: domain

Literal character: \.

Regular text: com

End Match $

End Regex /

Match URL or Directory

Use the following rule to match a URL or a directory, for example, **https://www.domain.com/support/newsite/testpage**

Rule type: Content Matching

Match Type: Regular Expression

Header Field: blank

Match String: /^\/support.*/

Ignore Case: enabled

Match field

Start Regex: /

Start Match: ^

Literal character: .*

Regular text: support

End Regex: /

Change URL or Directory

Option 1: 302 Redirects

Logic

When the client connects to **www.domain.com/test**, the LoadMaster sends a 302 redirect to the client and tells the client to connect to the new domain. This is also used for redirecting HTTP to HTTPS. With this option, the client sees the change in the browser.

Syntax

In the Virtual Service modify screen: **Advanced Properties -> Not Available Redirection Handling**.

Error code: 302 found

Redirect URL: http://www.newdomain.com/newtestpage

or for HTTP to HTTPS: **https://%h/newtestpage**

Replace with Host/Domain: %h

Example: %h is replaced with **http://www.newdomain.com**

Option 2: Rewrite the URL

Logic

Match on the URL and replace it with a new URL. With this option, the client does not see the change in the browser.

For example, if a client is requesting **http://www.newdomain.com/test** and you want to change this to **http://www.newdomain.com/newpage**..

Syntax

Rule Type: Modify URL

Match String: /^test$/

Modified URL: newpage

Match field

Start Regex: /

Start Match: ^

Regular text: test

End Match: $

End Regex: /

Naked Domain Rewrite

There may be scenarios where a **www** prefix needs to be added to the original request, for example, if the original request is **mydomain.com**, this will be rewritten to **www.mydomain.com**

Solution

Using the **Naked_Domain_Rewrite** rule below, requests automatically have **www** appended to the original request.

Example - Static Version

Rule Name: Naked_Domain_Rewrite

Rule Type: Replace Header

Match Type: Regular Expression

Header Field: host

Match string: /^mydomain\.com$/

Modified URL: www.mydomain.com

Example - Dynamic Version

Rule Name: Naked_Domain_Rewrite

Rule Type: Replace Header

Match Type: Regular Expression

Header Field: host

Match string: /^(.*)$/

Modified URL: www.\1

Rewrite Clients from "/" to "/testpage"

Logic

Match on the URL/directory “/” and replace it with “/testpage”.

Example: www.domain.com/ changed to **www.domain.com/testpage/**

Syntax

Rule type: Modify URL

Match String: /^\/$/

Replace with: /testpage

Start Regex: /

Start Match: ^

**Literal character: **

End Match: $

End Regex: /

Redirect Content to a Different URL While Keeping the Directory or Path

Rule type: Modify URL

Match String: /^Directory1(.*)/

Modified URL: /Directory2\1/

Match String: /^Directory1(.*)/

Start Regex: /

Start Match: ^

Regular text: **Directory1**

Wildcard- capture everything in () and save it as capture group 1: (.*)

End Match: $

End Regex: /

Modify URL String: /Directory2\1/

Start Regex: /

Start Match: ^

Replace with saved data in capture group 1: \1

End Match: $

End Regex: /

Redirecting Clients from HTTP to HTTPS

302 Redirect Logic

When the client connects to http://www.domain.com, the LoadMaster sends a 302 redirect to the client and tells the client to connect to the new domain. This is also used for redirecting HTTP to HTTPS.

Syntax

In the Virtual Service modify screen: **Advanced Properties -> Not Available Redirection Handling**.

Error code: 302 found

Redirect URL: https://www.newdomain.com

Replace with Host/Domain: %h

Replace with URL/Directory/Path: %s

Example: http://www.newdomain.com/test/index.html where **%h** is replaced with **www.newdomain.com/** and **%s** is replaced with **test/index.html**.

Change the Host Seen by the Real Server

If the client connects to a URL which has a different hostname to the Real Server, the Real Server may reject the request. This rule changes the host that is seen by the Real Server.

Rule type: Replace Header

Header Field: Host

Match String: /^.*/

Value to be replaced: domain.com

Start Regex: /

Start Match: ^

Wildcard: .*

End Match: $

End Regex: /

Match on Source IP

Use the following rule to match on Source IP. This can be used to allow a single IP or a range. If you select the option **Fail On Match** it behaves as a block list.

Rule Type: Content Matching

Match Type: Regular Expression

Header Field: src-ip

If single address 192.168.10.10

Match String: /^192.168.10.10$/

If address range 192.168.0.0/16

Match String: /^192.168.\d{1,3}.\d{1,3}$/

Match field:
/^192.168.(25[0-5]|2[0-4][0-9]|1[0-9]{2}|[0-9][0-9]?).(25[0-4]|2[0-4][0-9]|1[0-9]{2}|[1-9][0-9]?)$/

Start Regex: /

Start Match: ^

Match: 192.168.

192.168.0 – 192.168.255

192.168.0.1 – 192.168.255.254

End Match: $

End Regex: /

URL Rewrite Based on Source IP

In some cases it may be required to rewrite a rule based on a source IP subnet. For example, if there are two different websites (A and B) on one webserver and, depending on the source subnet, the user should be redirected to either website A or B. The user is using the same external URL, for example **aaa.bbb.com**, but will get a different website based on the source IP.

Solution

This can be done one of two ways, but either will start the same. First, set up a conditional rule using the following parameters:

Rule Name: Subnet_A

Rule Type: Content Matching

Match Type: Regular Expression

Header Field: src-ip

Match String: /^10\.0\..*/

Set Flag If Matched: Flag 1

The subnet that needs to be rewritten should be entered in the **Match String**. It must be done as a “classful” address as the LoadMaster is using a pseudo-header “src-ip” to do a text match against the source IP of the request. That means that something like 192.168.0/17 cannot be used – instead, use something like /192\.168\.10\..*/ to match an entire Class A, B, or C subnet.

Flag 1 is set if the above rule is matched. This can invoke another rule when matched. The rewrite can be done in two ways. Both are below.

Rule Name: Rewrite_Host

Rule Type: Replace Header

Header Field: Host

Match String: /.*/

Replace String: new.host.com

Perform If Flag Set: Flag 1

OR

Rule Name: Rewrite_URL

Rule Type: Modify URL

Match String: /.*/

Replace String: /new\0

Perform If Flag Set: Flag 1

Either of the two rewrite rules above can be used to either change the host header or the URL depending on how it needs to be changed on the server. We recommend using the hostname option because it usually results in fewer issues.

Once the two rules have been created, navigate to the Virtual Service modify screen. In the **Advanced Properties** section, click **Show Selection Rules** and apply the **Subnet_A** rule. Then, click **Show Header Rules** and apply the rewrite rule. Now, the rewrite should be applied only to requests from the designated subnet.

Add the SSL Secure Flag and HTTPonly Flag to Cookies from the Real Server

To add flags to a cookie being generated by the Real Server, the content switching engine must be used.

Rule Name: SetSecure

Rule Type: Replace Header

Header Field: set-cookie

Match String: /(.*?);?$/

Replace String: \1; secure; httponly

Perform If Flag Set: [Unset]

User-Agent String

Use the following rule to match on User-Agent String.

User-Agent String: Content Match

Rule type: Content Matching

Match Type: Regular Expression

Header Field: User-Agent

Match String: Mozilla/5.0 (Windows; U; MSIE 9.0; Windows NT 9.0; en-US)

You can view examples of User-Agent Strings at the following link: http://www.useragentstring.com/pages/useragentstring.php

Changing the User-Agent String

Rule type: Replace Header

Header Field: User-Agent

Match String: /^.*$/

Replace with: Mozilla/5.0 (Windows; U; MSIE 9.0; WIndows NT 9.0; en-US)

You can view examples of User-Agent strings at the following link: http://www.useragentstring.com/pages/useragentstring.php

Start Regex: /

Start Match: ^

Wildcard: .*

End Match: $

End Regex: /

Content Match on a Query

Use this rule to perform a content match on a query string.

To query a match on https://www.domain.com/orders/f?p=100, use the following settings:

Rule type: Content Matching

Match Type: Regular Expression

Header Field: <blank>

Match String: /^\/orders\/f\?p=100.*/

Ignore Case: enabled

Include Query in URL: enabled

Start Regex: /

Start Match: ^

Literal Character: \/

Regular text: orders

Literal Character: \f

Literal Character: \?

Regular text: p=100

Wildcard: .*

End Regex: /

Content Matching Rule Example

Address	LoadMaster	SubVS
http://kemp.mail.com	One Virtual Service	OWA
		ECP

This table shows an example architecture that can be achieved using content matching rules and SubVSs. The following example shows how to add another SubVS and content rule. You can repeat these steps add needed to add more SubVSs and content rules..

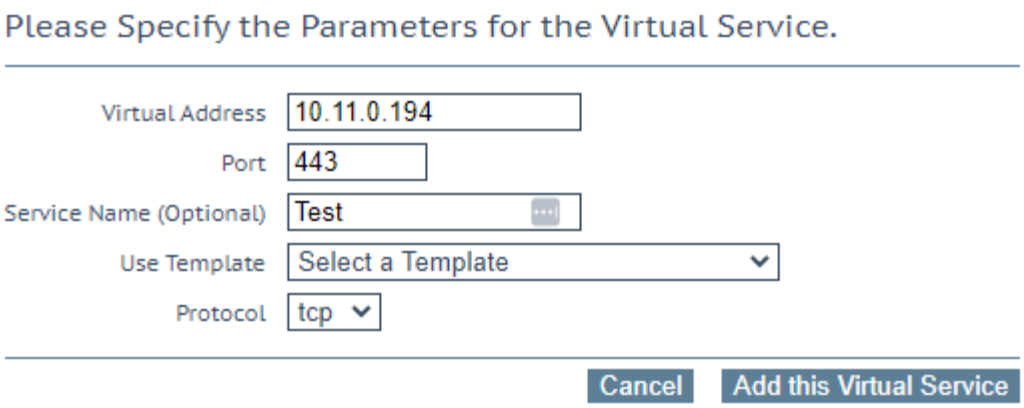
Content Matching Rules

Content Matching rules are also known as selection rules. These rules allow you to match all or some of a **Header Field** or URL string and then set flags if there is a match.

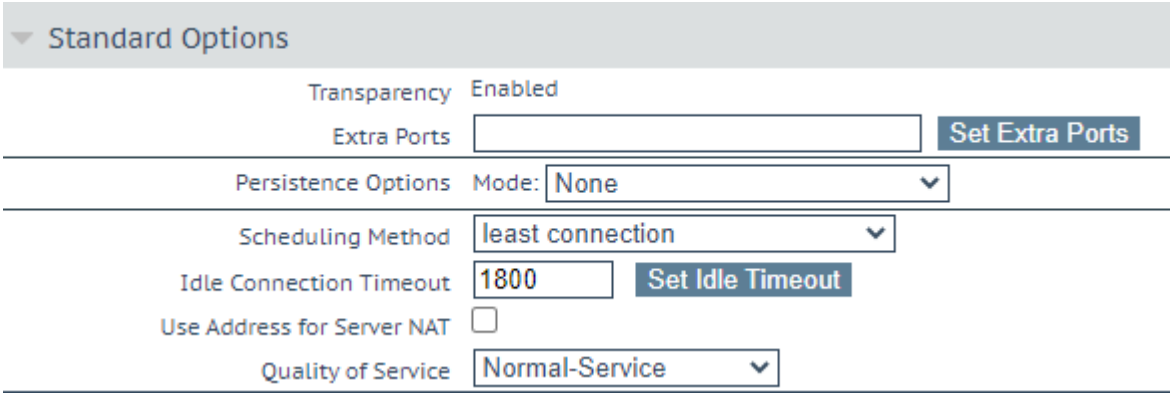
Virtual Services

To add the parent Virtual Service, follow the steps below in the LoadMaster WUI:

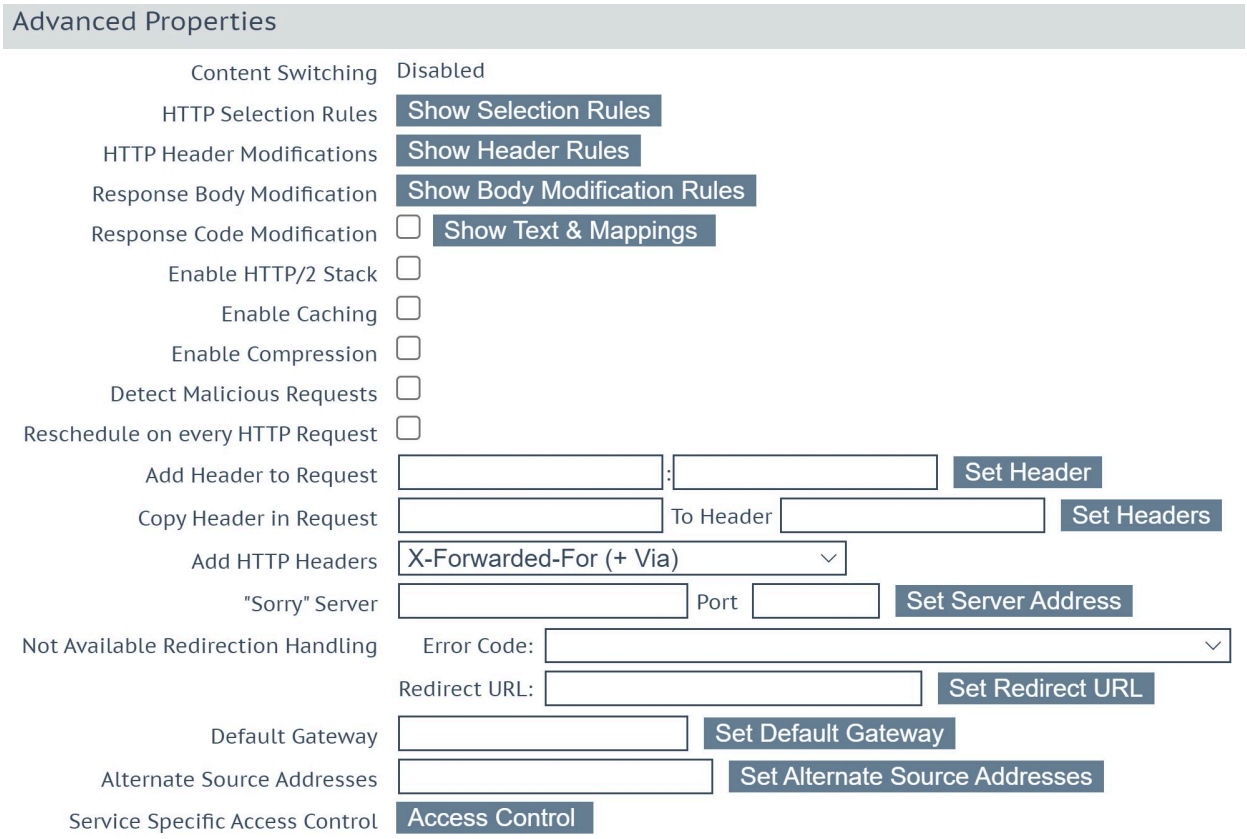
1. In the main menu, select **Virtual Services**.
2. Select **Add New**.



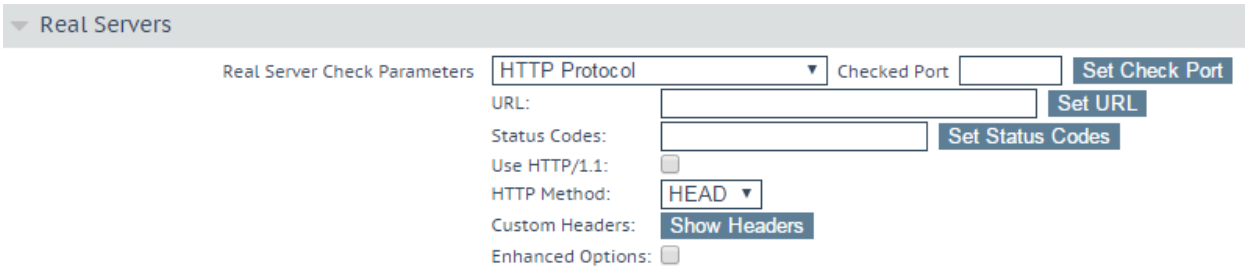
3. Enter a valid IP address.
4. Enter **443** as the **Port**.
5. Enter a recognizable **Service Name**.
6. Click **Add this Virtual Service**.



7. Expand the **SSL Properties** section.
8. Select the **Enabled** check box.
9. Expand the **Advanced Properties** section.



10. Click **Enable** next to **Content Switching**.
11. Expand the **Real Servers** section.



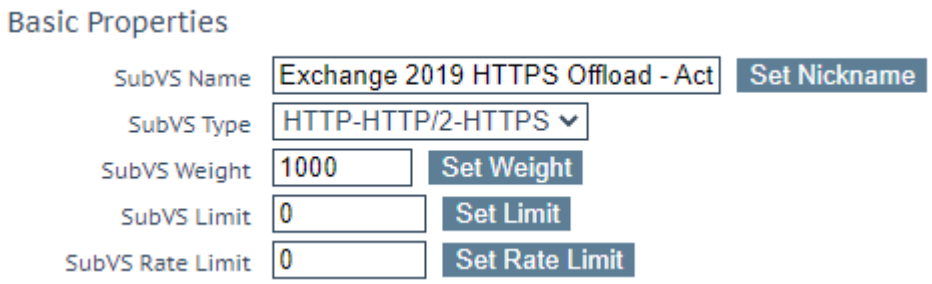
12. Click **Add SubVS**.
13. Click **OK**.
14. Click **None** in the **Rules** column in the **SubVSs** section.
15. Select the rule to be added (for example, **API**) and click **Add**.

Note: Repeat the steps as needed to assign more rules.

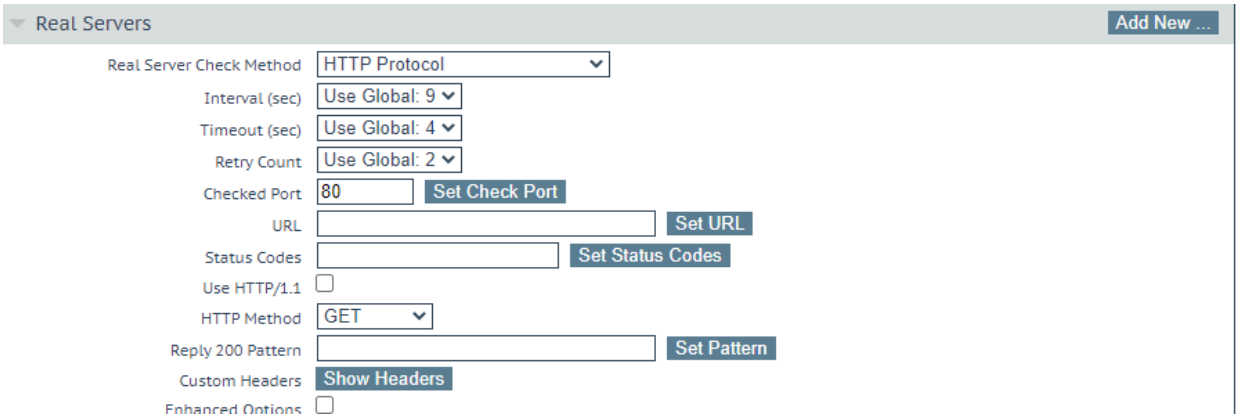
16. Click **Back**.



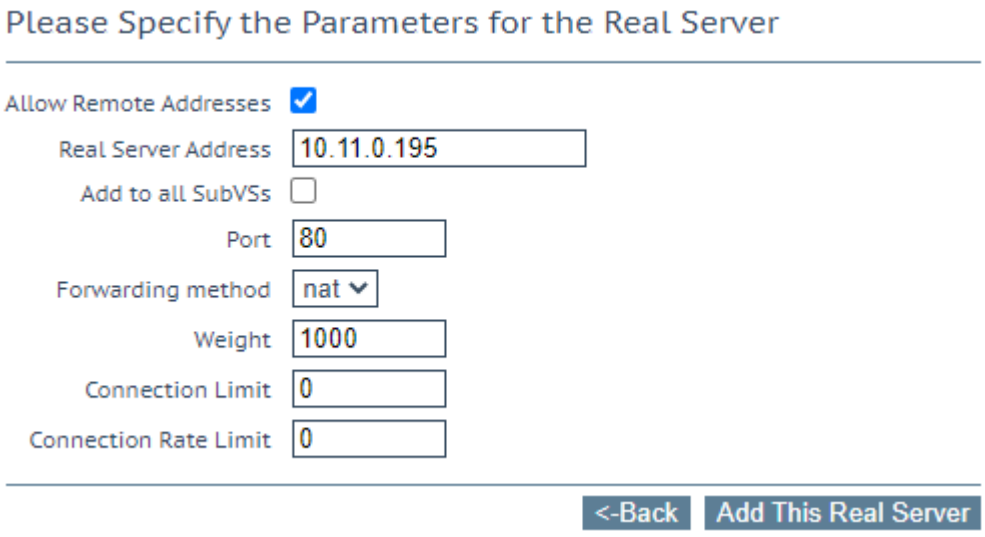
17. Click **Modify**.



18. Enter the **SubVS Name**, for example, **Exchange 2019 HTTPS Offload - API**.
19. Expand the **Real Servers** section.



20. Click **Add New**.



21. Enter the relevant address in the **Real Server Address** text box.
22. Enter **80** as the **Port**.
23. Click **Add This Real Server**.

The steps above describe how to add one SubVS. There are three SubVSs in this example. For documents on how to deploy various supported workloads, refer to the Deployment Guide section on the documentation page.

SubVS Name	Request Rules
Exchange 2019 HTTPS Offload - OWA (steps above)	OWA
Exchange 2019 HTTPS Offload - ECP	ECP
Exchange 2019 HTTPS Offload - API	API

7

References

Unless otherwise specified, the following documents can be found at https://docs.progress.com/.

WUI, Configuration Guide

LoadMaster, Product Overview

Virtual Services and Templates, Feature Description