Progress®
Kemp® LoadMaster®

Technical Note Content Switching Exchange and Lync

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

Document Purpose 6

Intended Audience 6

Author Information 6

Chapter 2: Content Rules 7

Chapter 3: Challenges 9

Health Checking Exchange 10

Chapter 4: Configuring Content Rules 11

Scenario 1 11

Step 1: Create the Content Matching Rules 13

Step 2: Add the Certificate 14

Step 3: Create and Configure the Virtual Service 15

Step 4: Adding SubVSs 17

Scenario 2 20

Step 1: Create the Content Rules 20

Step 2: Add the Certificate 22

Step 3: Create and Configure a Virtual Service 23

Step 4: Adding SubVSs 24

Chapter 5: References 29

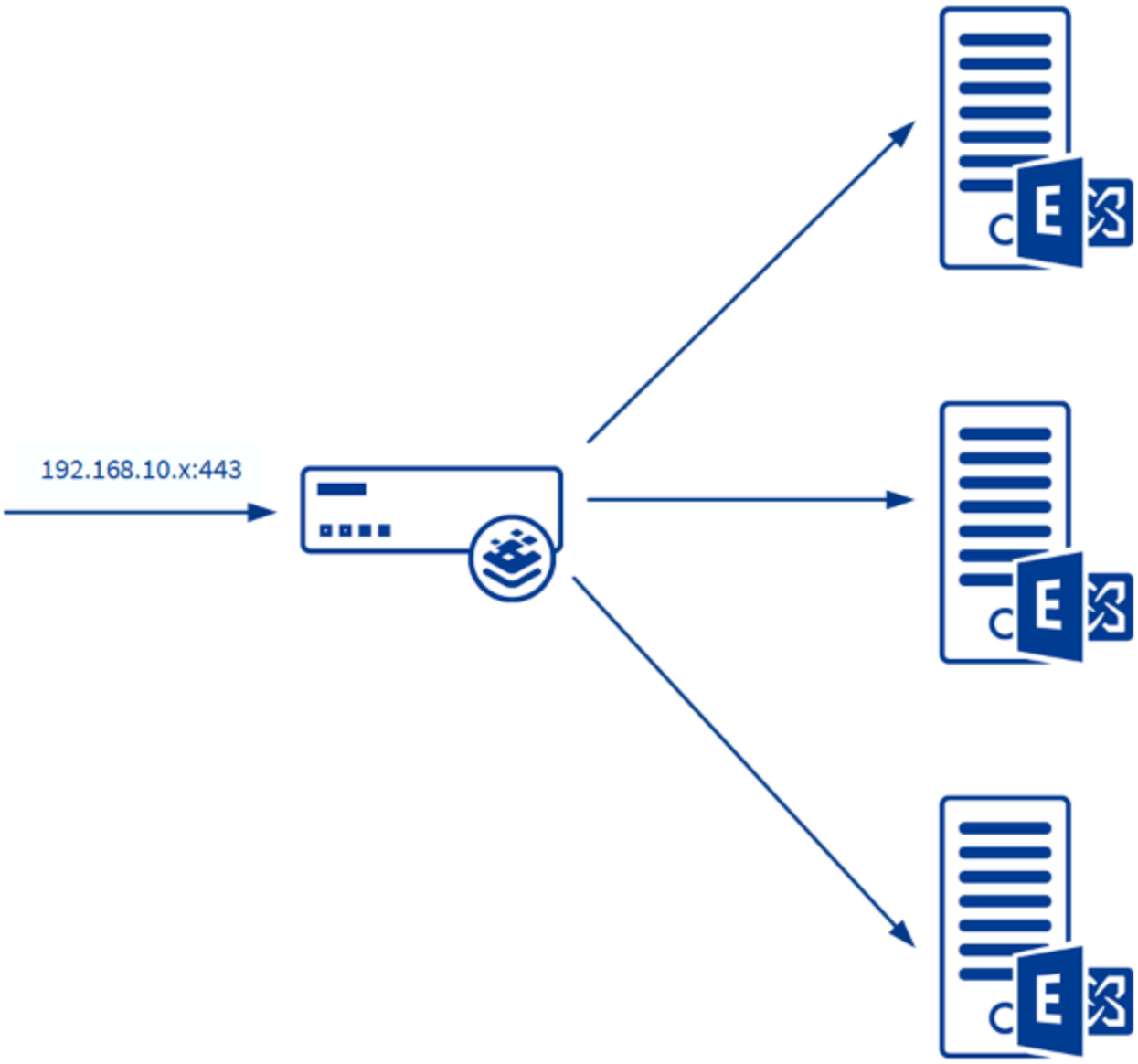
1

Introduction

Introduction

Sometimes customers face very specific networking requirements or they might be restricted in the amount of available IP addresses that can be allocated to Virtual Services which are used to publish or load balance applications. With the pool of available IPv4 addresses nearly being depleted, the latter scenario is not uncommon. These sort of problems highlight the need for a flexible solution which allows the use of a single IP address for multiple applications while maintaining the full flexibility of load balancing options that you would otherwise also have in a ‘typical’ setup.

Before we move on, it is important to understand how routing/load balancing decisions are being made.



Consider the scenario outlined in the diagram above: a Microsoft Exchange 2013 environment is load balanced on a single virtual IP address: 192.168.10.80.

Whenever traffic hits the virtual IP address – which is configured as a Virtual Service in the LoadMaster – the combination of the IP address and the specific – configured - TCP port will trigger the LoadMaster to use the settings defined in the Virtual Service and forward traffic to the Real Servers that are associated with that Virtual Service.

Without additional configuration, that Virtual Service would operate at Layer 4 and pass along any traffic that comes in through the aforementioned IP address and TCP port combination. The combination of an IP address with a specific TCP port is always unique. As such, once you have configured a Virtual Service, you cannot create another Virtual Service using the same IP address and TCP port.

Related Links

- Document Purpose

- Intended Audience
- Author Information

Document Purpose

Document Purpose

In the scenario above, Exchange is therefore the only application that can use the IP/port combination of 192.168.10.80:443. If you want to have another application use the same IP address and TCP port combination, routing decisions should be made based on the real destination of the traffic. In the world of web-based applications these destinations are typically revealed by Uniform Resource Locators (URLs).

As such, you would be able to use multiple (different) hostnames with a single IP address and TCP port combination and still use different routing/load balancing options for each of them:

Webmail.domain.com192.168.10.80:443LyncFE.domain.com192.168.10.80:443

The challenge here, however, is to get the LoadMaster to interpret the destination URL and act upon it. This document provides step-by-step instructions on how to achieve this.

Intended Audience

Intended Audience

This document is intended to be read by anyone who is interested in learning about how to use content switching to publish Exchange and Lync-related workloads.

Author Information

Author Information

Michael Van Horenbeeck is a Microsoft Certified Solutions Master (MCSM), Exchange Server Most Valuable Professional (MVP) and Microsoft Certified Trainer from Belgium. He has a strong focus on Microsoft Exchange, Office 365, Active Directory, and some Lync. Michael has been active in the industry for about 12 years and developed a love for Exchange back in 2000. He is a frequent blogger and a member of the Belgian Unified Communications User Group: Pro-Exchange - www.pro-exchange.be. Besides writing about technology, Michael is a regular contributor to The UC Architects podcast (www.theucarchitects.com) and speaker at various tech conferences around the world. You can follow Michael on Twitter (@mvanhorenbeeck) or his blog on http://michaelvh.wordpress.com.

2

Content Rules

Content Rules

The LoadMaster includes a feature called content rules. When content rules are enabled, the LoadMaster will evaluate incoming traffic against a set of rules and makes routing and load balancing decisions based on the results. These rules are typically based on regular expressions and can, for instance, be used to (partially) match the hostname string (URL) of incoming traffic. The result is that, now, that URL can be used to determine where the traffic should be forwarded to.

Let's clarify this with an example:

Name	Type	Options	Header	Pattern
OWA	RegEx	Ignore Case		/^\/owa*/

The above content rule would search the content of an incoming request for a pattern matching the regex expression: **/^\/owa.*/**.

Note: For more information on content rules in general, and further regex examples, refer to the Content Rules, Feature Description.

SubVSs

Id	Name	Weight	Limit	Status	Rules
1	OWA	1000	0	Enabled	1
2	ECP	1000	0	Enabled	1
3	RPC	1000	0	Enabled	1
4	EWS	1000	0	Enabled	1
5	EAS	1000	0	Enabled	1
6	OAB	1000	0	Enabled	1

When, for example, the hostname string (URL) matches this expression, the configuration parameters of the Virtual Service (or SubVS) to which the content rule is assigned, will be used for routing and load balancing decisions.

Rules assigned to subVS OWA on Virtual Service tcp/10.154.11.71:443 (Id:1)

OperationName	Match Type	Options	Header	Pattern
OWA	RegEx	Ignore Case		/^\/owa*/

SubVSs allow the creation of a flexible Virtual Service which leverages the use of multiple content matching rules to mix and match one or more applications.

3

Challenges

Challenges

In order for the LoadMaster to be able to evaluate incoming traffic, it must be able to read the traffic. For non-encrypted (HTTP) traffic, this would be no problem. However, many services - like Exchange or Lync - use encrypted traffic (HTTPS) by default and therefore the LoadMaster cannot read the incoming traffic without additional configuration. In order to do so, we need to configure the LoadMaster to decrypt SSL traffic first. Inherently, this changes the operating mode from Layer 4 to Layer 7.

While that opens up a wide range of possibilities, it does increase the load on the device and therefore should be taken into account when choosing the right model.

Note: In theory, there is no need to re-encrypt the traffic on its way out, but all examples hence forward will use re-encryption of the SSL traffic as it is being forwarded out of the LoadMaster to the published applications; in this case Exchange or Lync. For more information, including steps on how to configure SSL offloading and re-encryption, refer to the SSL Accelerated Services, Feature Description.

Related Links

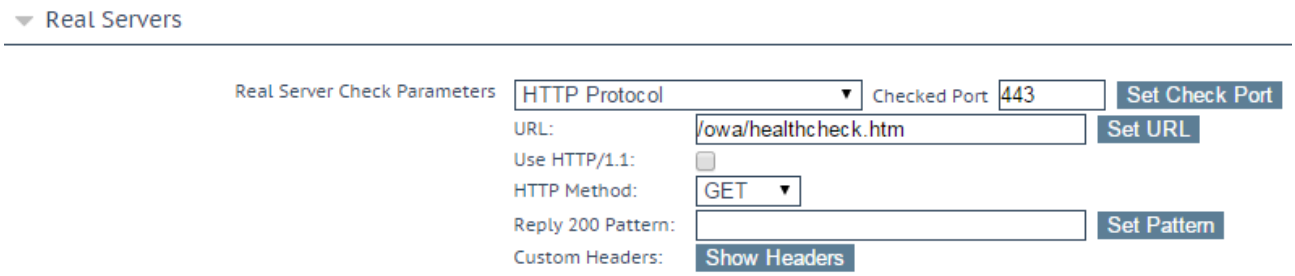
- Health Checking Exchange

Health Checking Exchange

Health Checking Exchange

A second challenge presents itself relating to the use of health checks. You can only define a single health check per Virtual Service. As a result, if you use a single Virtual Service to publish Exchange, the Virtual Service can only consider a single health parameter to determine whether an underlying Exchange server is healthy or not. Choosing the 'right' health check thus becomes very critical. But how does one determine what to health check? Depending on your own environment there might be one workload (for example OWA) which is used primarily and therefore it would make sense to use that specific workload. Unfortunately this does not offer much flexibility.

Luckily, the SubVSs would allow us to create multiple SubVSs (one per workload) and thus configure a health check for each of the workloads like OWA, Outlook Anywhere, Exchange Web Services, and so on.



Exchange 2013 introduced a new feature called Managed Availability which will perform in-box health checks of Exchange and uses that information to determine whether a workload is available for service or not. The result of these health checks are exposed in an HTML file called **healthcheck.htm** which is available per workload (for example OWA, MAPI/HTTP, Outlook Anywhere).

Using this information dramatically increases the flexibility and maximizes the utilization of an Exchange server by preventing a single workload failure to cause an entire server to be taken out of the pool of available servers.

4

Configuring Content Rules

Configuring Content Rules

In the following sections we will walk you through the configuration of a LoadMaster based on two specific scenarios.

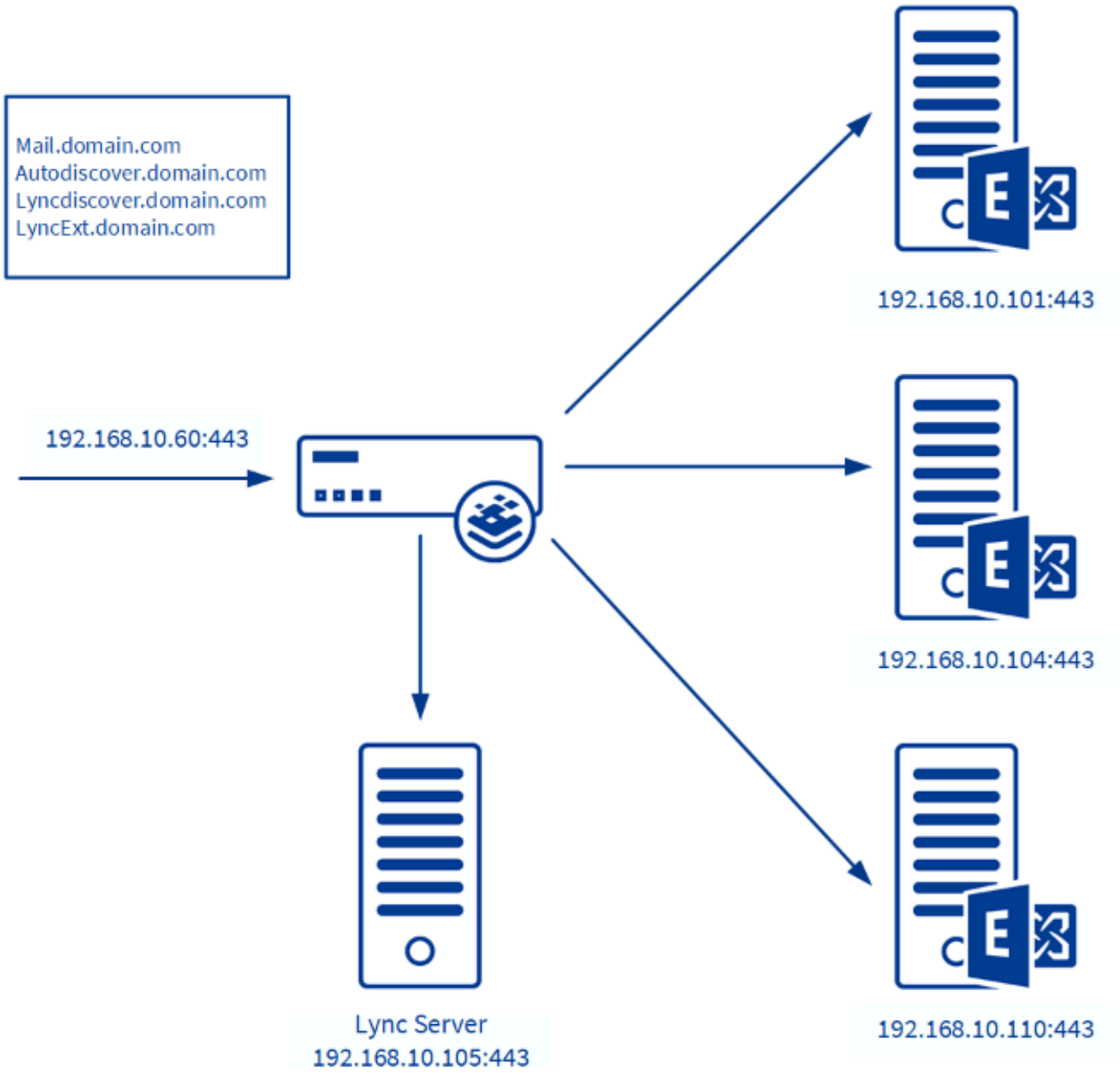
Related Links

- Scenario 1
- Scenario 2

Scenario 1

Scenario 1

A customer wants to publish and load balance both Exchange 2013 and Lync 2013. However, they can only spare a single IP address. To keep things simple, the customer does not require multiple health checks for Exchange.



The above image depicts the configuration of Exchange and Lync within the customer's network.

Related Links

- Step 1: Create the Content Matching Rules
- Step 2: Add the Certificate
- Step 3: Create and Configure the Virtual Service
- Step 4: Adding SubVSs

Step 1: Create the Content Matching Rules

Step 1: Create the Content Matching Rules

There are two type of content rules: Content Matching Rules and Header Modification Rules. The latter option is used to rewrite URLs ‘on the fly’ and are beyond the scope of this document. For more information on Header Modification Rules, refer to the Content Rules, Feature Description.

Content matching rules will be used to identify what traffic is currently entering the load balancer. Based on the scenario above, there are multiple ways we can approach the problem.

The first approach would be to have all traffic be forwarded to Exchange, unless there is a match for Microsoft Lync traffic. This means that we would only have to create two different content matching rules:

Lyncdiscover.domain.com

LyncExt.domain.com

The second approach would be to create a content matching rule per workload or hostname:

Mail.domain.com

Autodiscover.domain.com

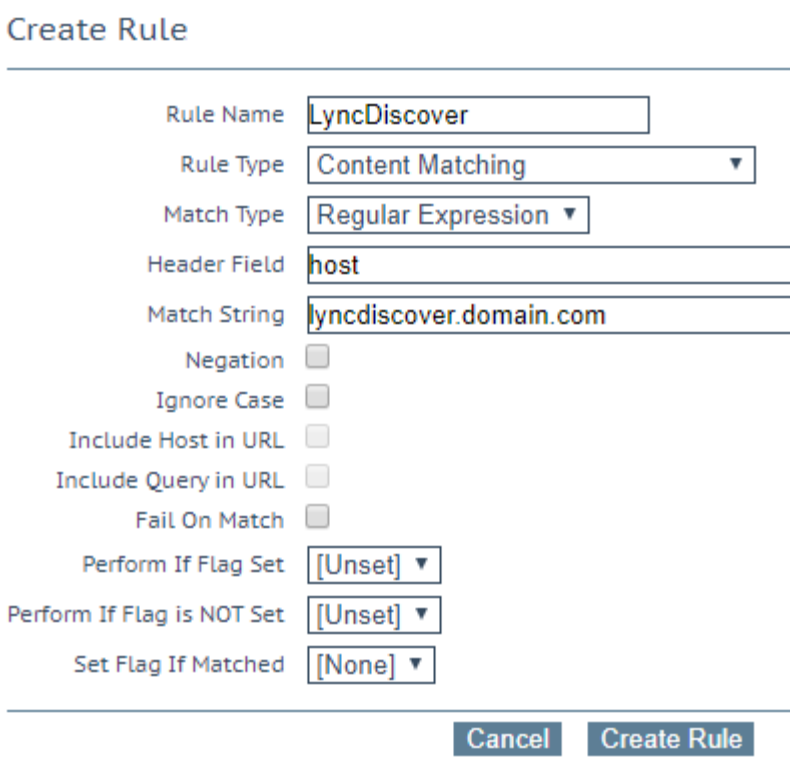
Lyncdiscover.domain.com

LyncExt.domain.com

For this scenario, we will use the latter option.

To create a new content matching rule, follow the steps below in the LoadMaster Web User Interface (WUI):

1. In the main menu, select **Rules & Checking**.
2. Select **Content Rules**.
3. Click **Create New**.



4. Enter a recognizable **Rule Name**, for example **LyncDiscover**.
5. Enter **host** in the **Header Field** text box.
6. Enter **lyncdiscover.domain.com** in the **Match String** text box.
7. Click **Create Rule**.
8. Repeat steps 3 to 7 above to add the other rules, but for step 6 - enter the following values in the **Match String** text box:

mail.domain.com

autodiscover.domain.com

LyncExt.domain.com

After completing these steps, you should have four distinct content rules. One for each of the hostnames we identified earlier.

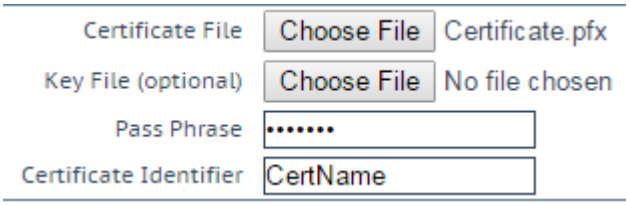
Step 2: Add the Certificate

Step 2: Add the Certificate

Before adding the Virtual Service, we first need to import the certificate to the LoadMaster so that we can use it later to decrypt incoming traffic. Follow the steps below, in the LoadMaster WUI, to import the certificate:

1. In the main menu, go to **Certificates & Security**.
2. Select **SSL Certificates**.

3. Click **Import Certificate**.



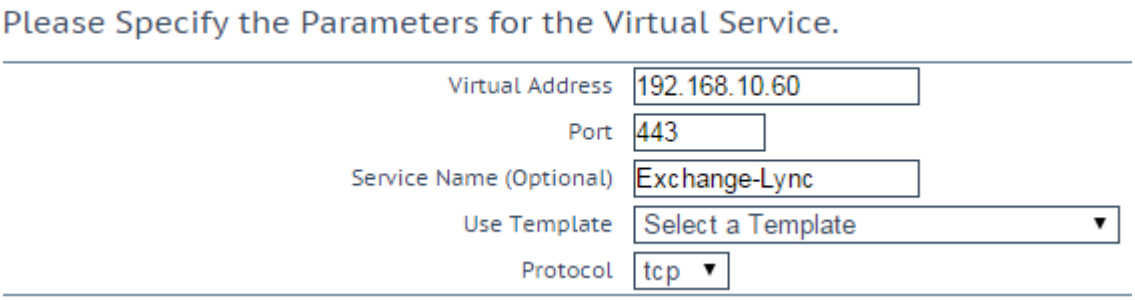
1. Click **Choose File**.
2. Browse to and select the certificate (.pfx file).
3. Enter the **Pass Phrase**.
4. Enter a name in the **Certificate Identifier** text box.
5. Click **Save**.

Step 3: Create and Configure the Virtual Service

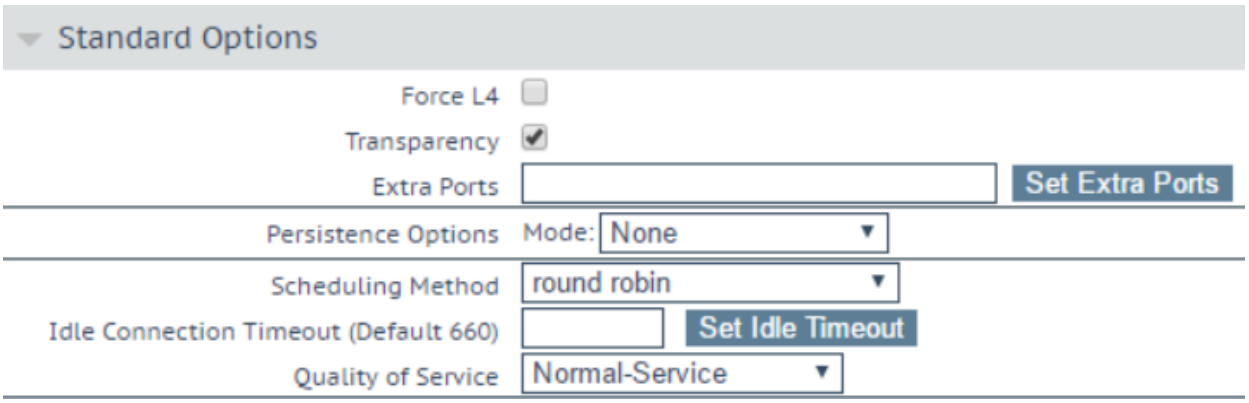
Step 3: Create and Configure the Virtual Service

The steps below describe how to configure a new Virtual Service which will be used as the parent Virtual Service. Follow these steps in the LoadMaster WUI:

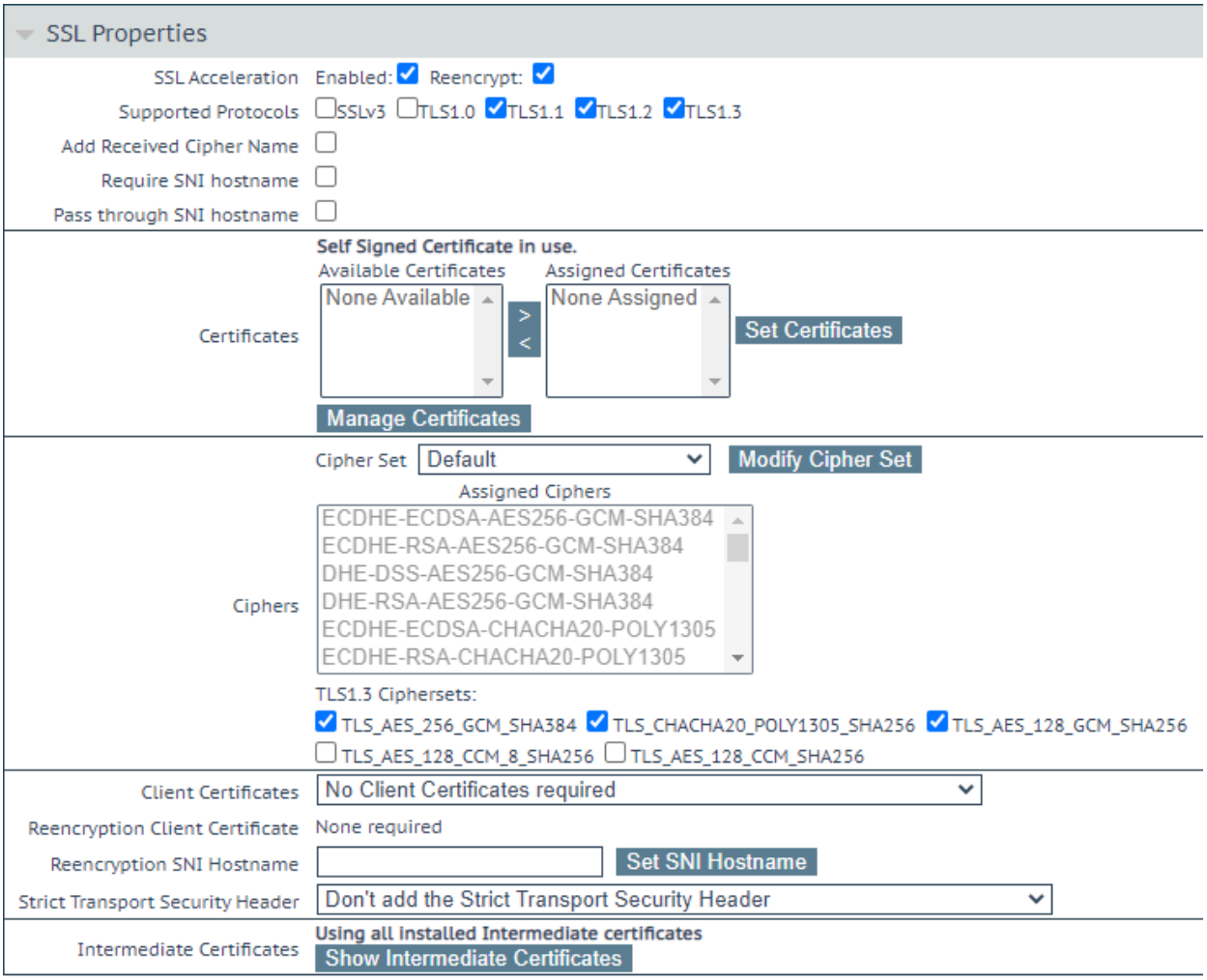
1. In the main menu, select **Virtual Services**.
2. Select **Add New**.



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



7. In the **Standard Options** section, ensure that **Force L4** is cleared.



8. Expand the **SSL Properties** section.
9. Select **Enabled**.
10. Click **OK** if a warning appears.
11. Select **Reencrypt**.
12. Select the relevant certificate in the **Available Certificates** box.

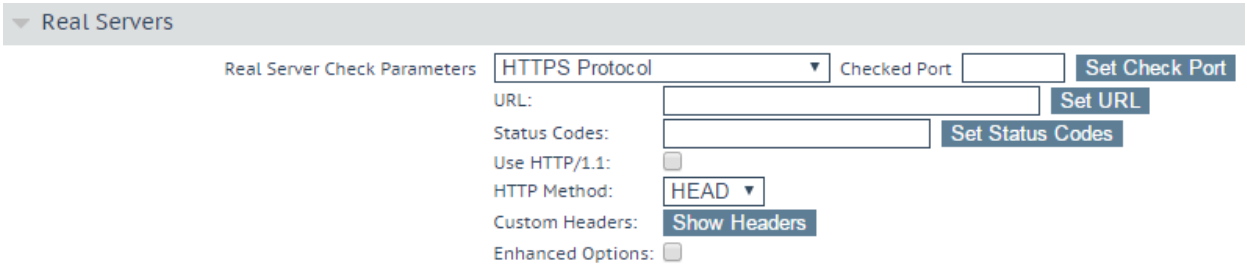
13. Click the right arrow to move the certificate into the **Assigned Certificates** box.
14. Click **Set Certificates**.

Step 4: Adding SubVSs

Step 4: Adding SubVSs

Now that the Virtual Service is configured, we can start adding SubVSs. A SubVS needs to be added for each of the workloads/applications defined earlier. Follow the steps below, in the LoadMaster WUI, to add these SubVSs:

1. In the modify screen for the Virtual Service, expand the **Real Servers** section.

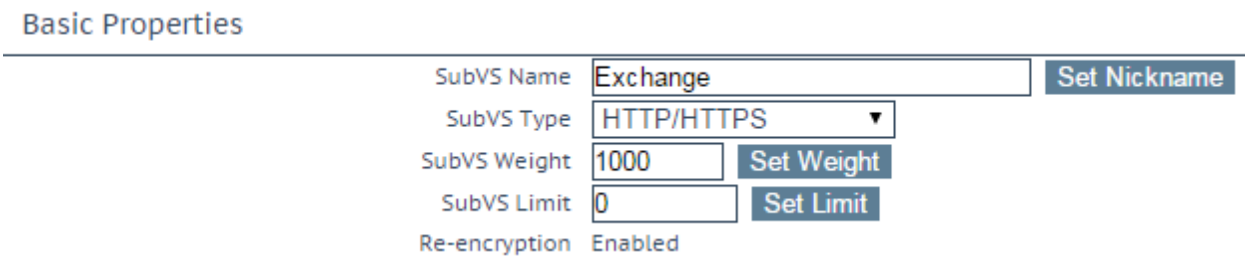


2. Click **Add SubVS**.
3. Click **OK** on the confirmation message.

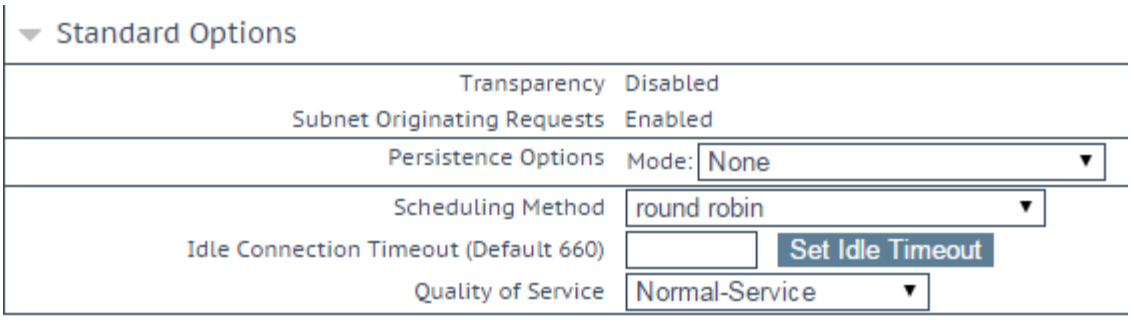
Note: Now that the first SubVS has been added, **Content Switching** can be enabled.



4. In the **SubVSs** section, click **Modify** to configure the SubVS.



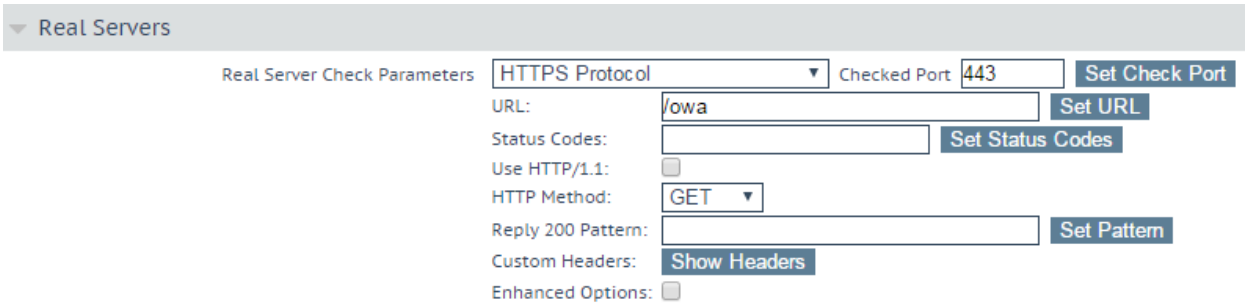
5. In the **Basic Properties** section, enter a recognizable **SubVS Name**, for example **Exchange**, and click **Set Nickname**.



6. In the **Standard Options** section, configure the required **Persistence Options** for the relevant application.

Note: There is no persistence required for Exchange 2013.

7. Select the relevant **Scheduling Method**.



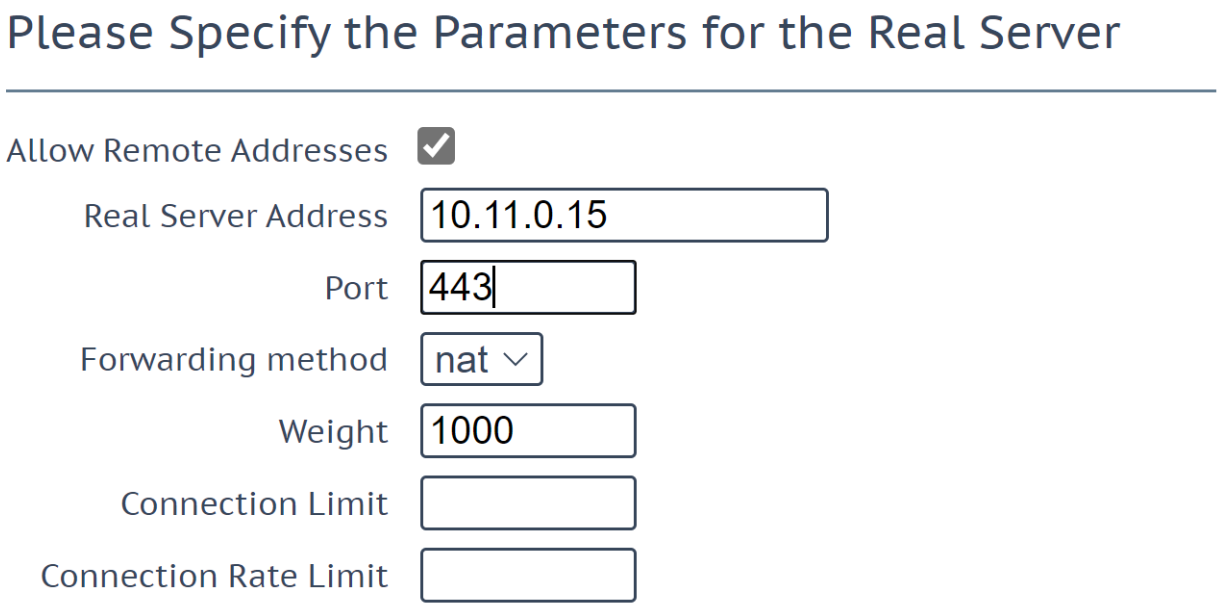
8. In the **Real Servers** section, configure the **Real Server Check Parameters**. This will define the health check that will be executed for this Virtual Service. For Exchange, the following options could be entered:

   Checked Port: 443

   URL: /owa/healthcheck.htm

   HTTP Method: GET

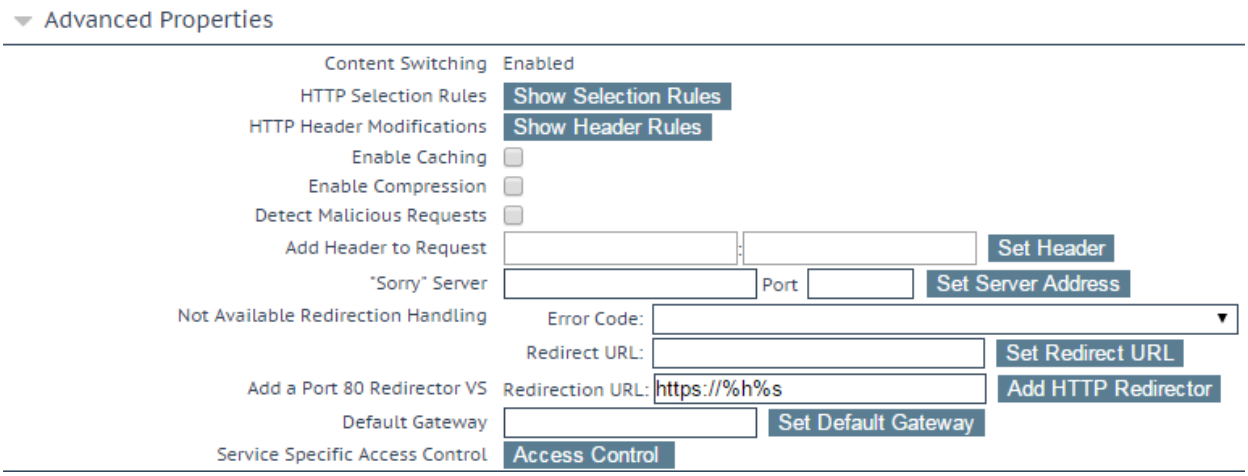
9. Click **Add New**.



10. Enter the Real Server's address in the **Real Server Address** text box.
11. Enter the relevant **Port**.

Note: For Lync, the **Port** may need to be changed to **4443**.

12. Click **Add This Real Server**.
13. Repeat the steps above for each of the servers that you want to add to this SubVS.
14. When finished adding all of the Real Servers, click **Back** to return to the SubVS properties screen. Then, click **Back** to return to the parent Virtual Service properties screen.
15. Expand the **Advanced Properties** section.



16. Click **Enable**.



17. In the **SubVSs** section, click **None**.



18. Select the relevant rule and click **Add**.
19. Create a SubVS for Lync by repeating steps above. However, **Content Switching** has already been enabled for the parent Virtual Service and in the last step, select the content rule which applies to Lync instead of Exchange.

Scenario 2

Scenario 2

The previous scenario might be used if you want to leverage the Managed Availability feature in Exchange 2013 which allows a health check per Exchange workload.

The process for scenario 2 is similar to the one described earlier. Only this time, a content rule will be created for each Exchange workload:

- Outlook Web App (OWA)
- Exchange Admin Center (EAC/ECP)
- Exchange Web Services (EWS)
- Outlook Anywhere (OA)
- MAPI/HTTP (MAPI)
- Offline Address Book (OAB)
- Exchange ActiveSync (EAS)
- Autodiscover (AutoD)

Related Links

- Step 1: Create the Content Rules
- Step 2: Add the Certificate
- Step 3: Create and Configure a Virtual Service
- Step 4: Adding SubVSs

Step 1: Create the Content Rules

Step 1: Create the Content Rules

In many cases, all of the above workloads will share a common domain name – except for Autodiscover. Therefore, we need to find another way of determining the difference between each workload. Consider the

following:

When a client connects with Outlook, the URL which it will try to connect will look like this:

https://autodiscover.domain.com/mapi/...

Similarly, if an ActiveSync client is trying to connect, it will do so using the following URL:

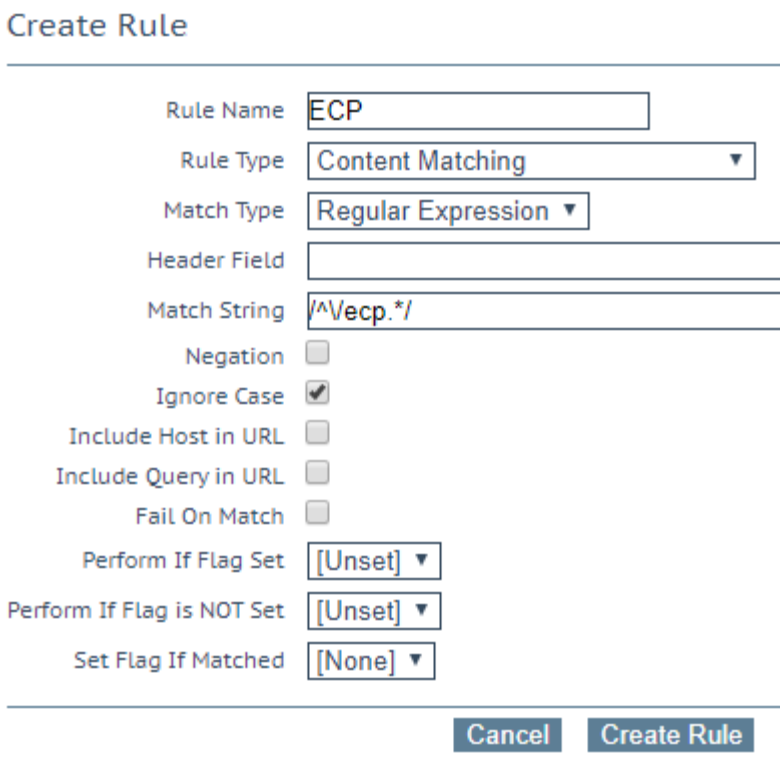
https://mail.domain.com/Microsoft-Server-ActiveSync/....

Because Exchange uses a different virtual directory for each of the workloads, we can use that to differentiate traffic from one another. The following table summarizes how this can be achieved:

Workload	RegEx	Health check page – Exchange 2013
OWA	/^\/owa.*/	/owa/healthcheck.htm
EAC/ECP	/^\/ecp.*/	/ecp/healthcheck.htm
EWS	/^\/ews.*/	/ews/healthcheck.htm
OA	/^\/rpc.*/	/rpc/healthcheck.htm
MAPI	/^\/mapi.*/	/mapi/healthcheck.htm
OAB	/^\/oab.*/	/oab/healthcheck.htm
EAS	/^\/Microsoft-server-activesync.*/	/Microsoft-server-activesync/ healthcheck.htm
AutoD	/^\/autodiscover.*/	/autodiscover/healthcheck.htm

To create these content matching rules, follow the steps below in the LoadMaster WUI:

1. In the main menu, select **Rules & Checking**.
2. Select **Content Rules**.
3. Click **Create New**.



4. Add a recognizable **Rule Name**, for example **ECP**.
5. Enter **/^\/ecp.*/** in the **Match String** text box.
6. Select **Ignore Case**.
7. Click **Create Rule**.
8. Repeat steps 1 to 7 for each of the rules in the table above. Enter the relevant **RegEx** in the **Match String** text box for step 5.

Step 2: Add the Certificate

Step 2: Add the Certificate

Before moving on to the configuration of this Virtual Service, we first need to import the certificate to the LoadMaster so that we can use it later to decrypt incoming traffic. To add the certificate, follow the steps below in the LoadMaster WUI:

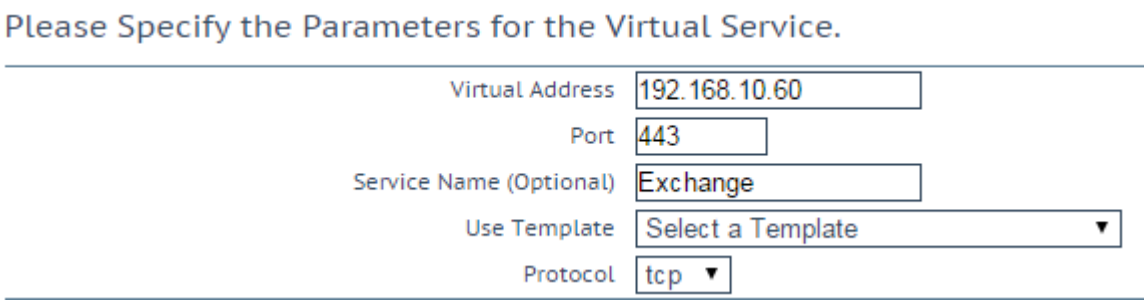
1. In the main menu, go to **Certificates > SSL Certificates**.
2. Select **SSL Certificates**.
3. Click **Import Certificate**.

Step 3: Create and Configure a Virtual Service

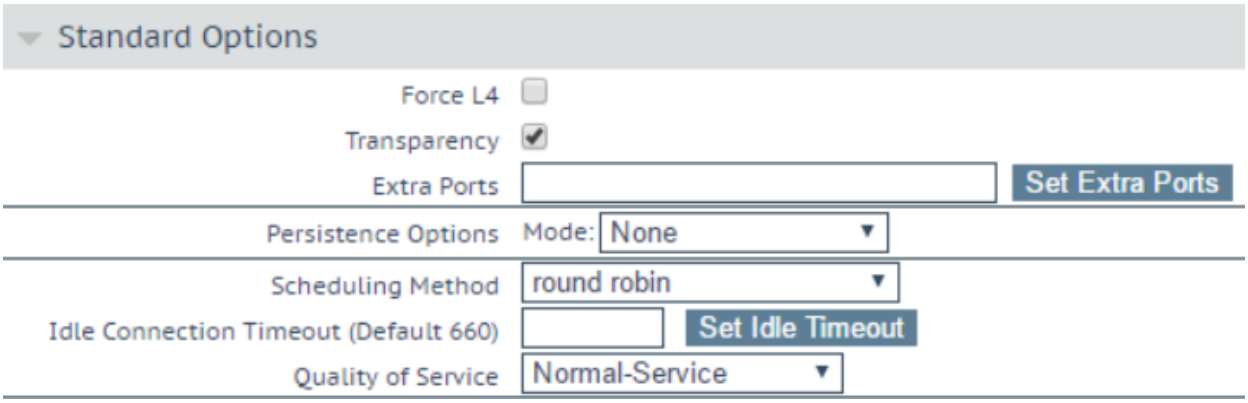
Step 3: Create and Configure a Virtual Service

Follow the steps below, in the LoadMaster WUI, to create the parent Virtual Service:

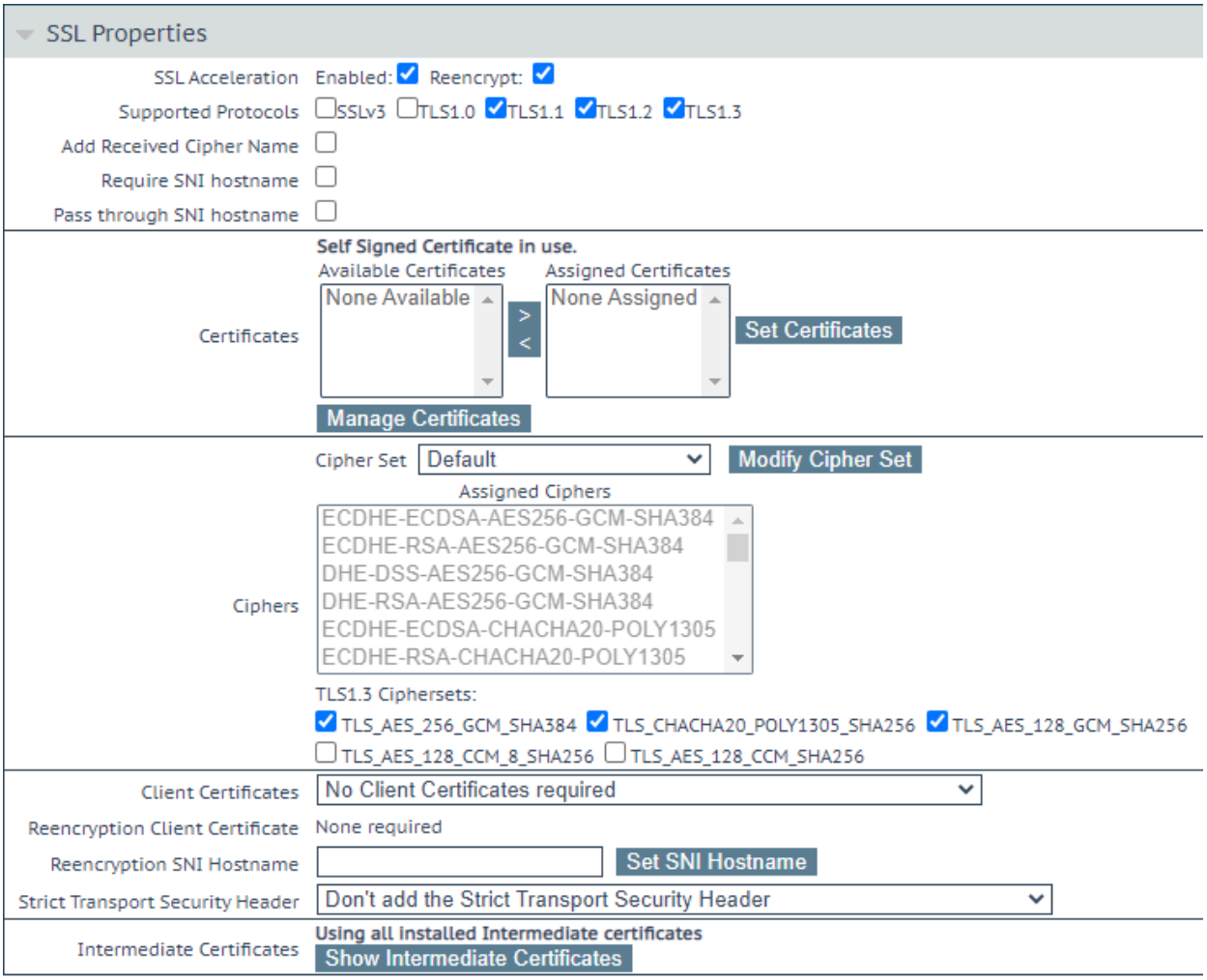
1. In the main menu, select **Virtual Services**.
2. Select **Add New**.



3. Enter a valid IP address in the **Virtual Address** text box.
4. Enter **443** as the **Port**.
5. Enter a recognizable **Service Name**, for example **Exchange**.
6. Click **Add this Virtual Service**.
7. Expand the **Standard Options** section.



8. Ensure **Force L4** is cleared.



9. Expand the **SSL Properties** section.
10. Select **Enabled**.
11. Click **OK**.
12. Select **Reencrypt**.
13. Select the relevant certificate in the **Available Certificates** box.
14. Click the right arrow to move the certificate into the **Assigned Certificates** box.
15. Click **Set Certificates**.

Step 4: Adding SubVSs

Step 4: Adding SubVSs

Now that the parent Virtual Service is configured, the SubVSs can be added. We will need to add a SubVS for each of the workloads/applications defined earlier. To add the SubVSs, follow the steps below in the LoadMaster WUI.

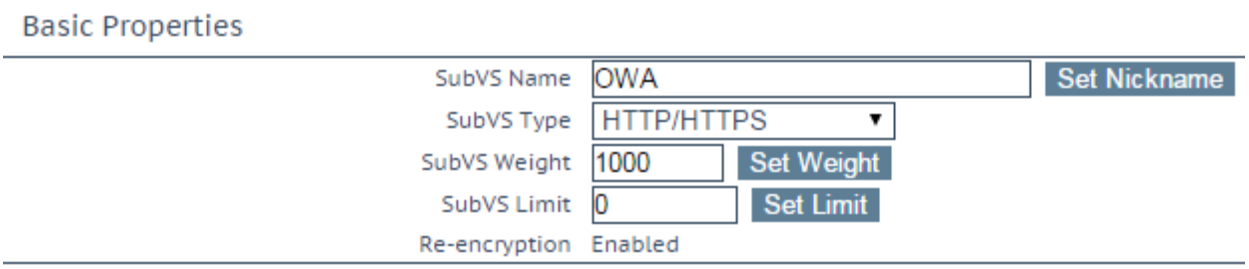
1. In the Virtual Service modify screen, expand the **Real Servers** section.



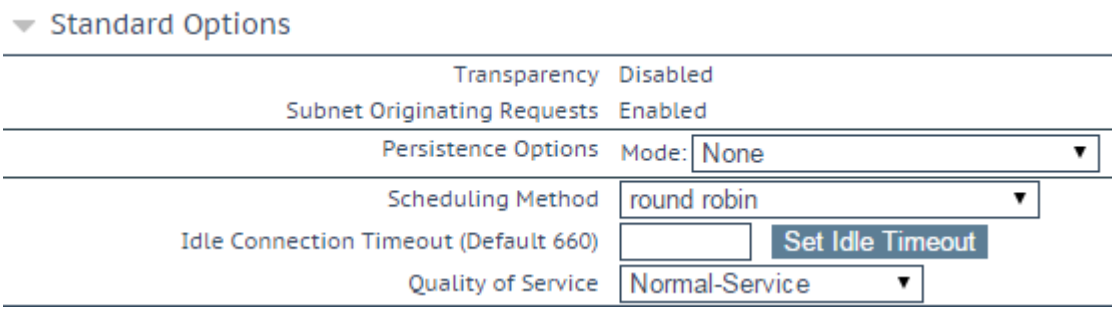
2. Click **Add SubVS**.
3. Click **OK**.

Note: As the first SubVS has been added, it is now possible to enable **Content Switching**.

4. In the **SubVSs** section, click **Modify** to configure the SubVS.



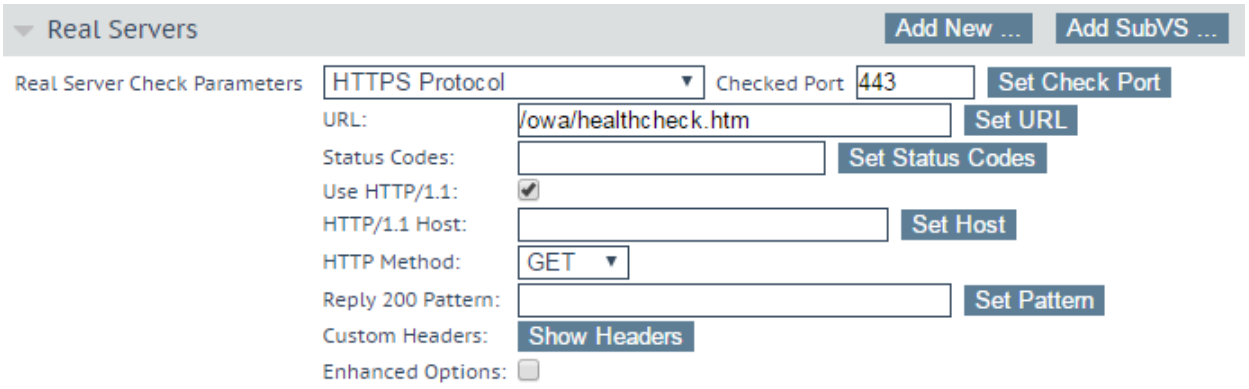
5. In the **Basic Properties** section, enter a recognizable **SubVS Name**, for example **OWA** and click **Set Nickname**.



6. In the **Standard Options** section, configure the required **Persistence Options** for the relevant application.

Note: There is no persistence required for Exchange 2013.

7. Select the relevant **Scheduling Method**.



8. In the **Real Servers** section, configure the **Real Server Check Parameters**. This defines the health

check that is executed for this Virtual Service. For Exchange, the following settings could be entered:

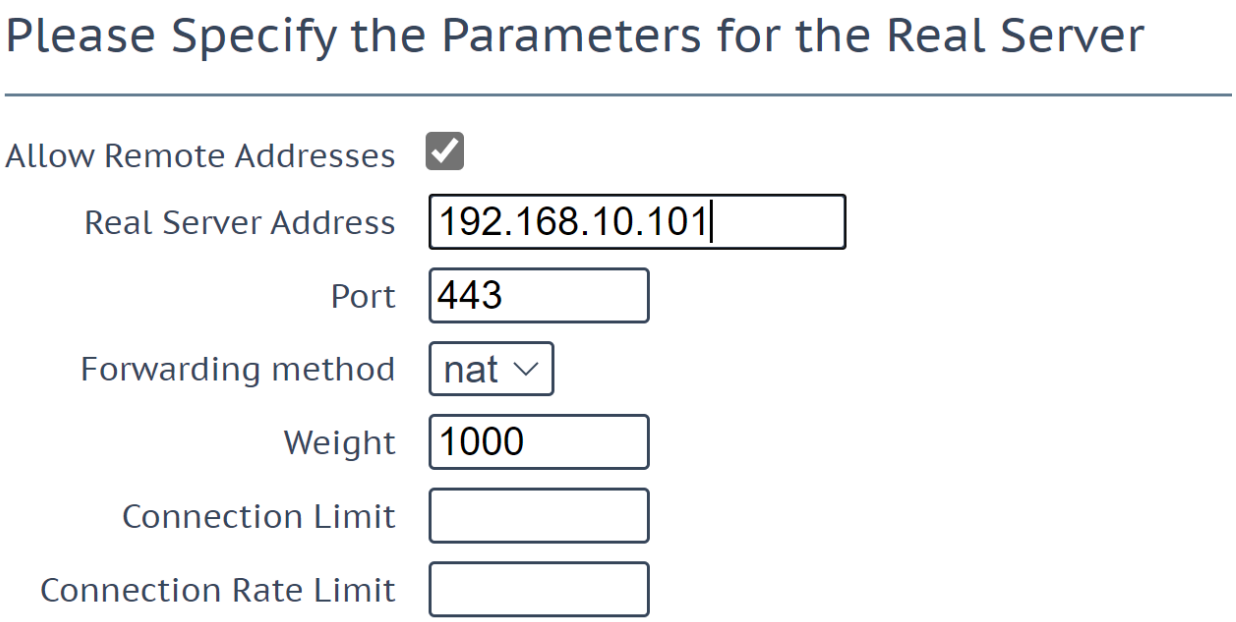
Checked Port: 443

URL: /owa/healthcheck.htm

Use HTTP/1.1: Enabled

HTTP Method: GET

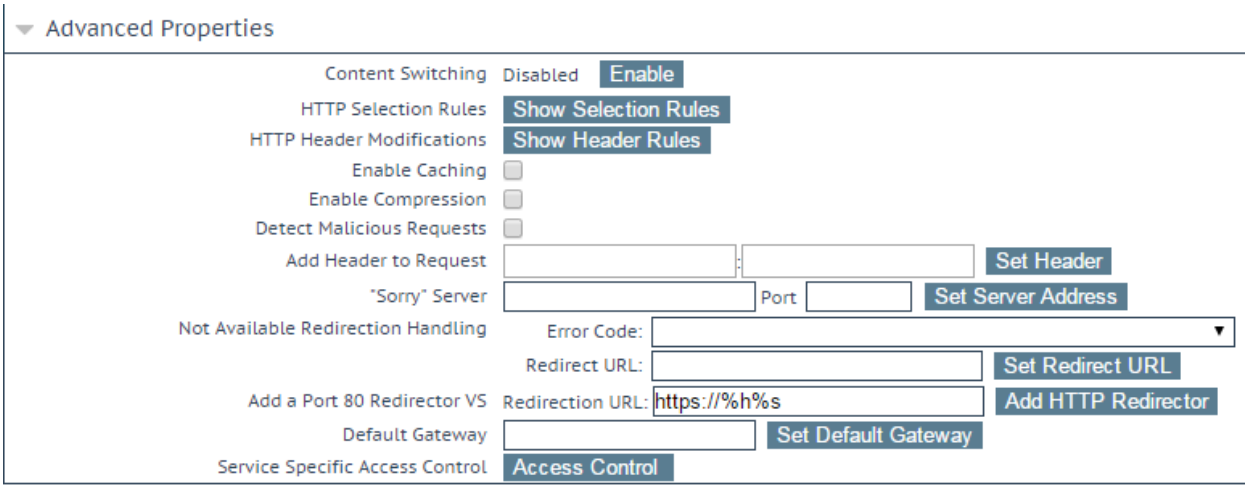
9. Click **Add New**.



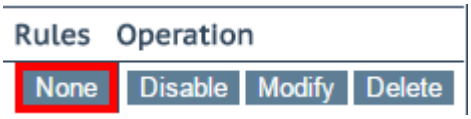
10. Enter the Real Server's address in the **Real Server Address** text box.
11. Enter the relevant **Port**.

Note: For Lync, the **Port** might need to be changed to **4443**.

12. Click **Add This Real Server**.
13. Repeat steps 12 to 14 above for each Real Server that needs to be added to this SubVS.
14. When all of the Real Servers have been added, click **Back** to return to the SubVS properties screen.
15. Click **Back** to return to the parent Virtual Service properties screen.
16. Expand the **Advanced Properties** section.



17. Click **Enable**.

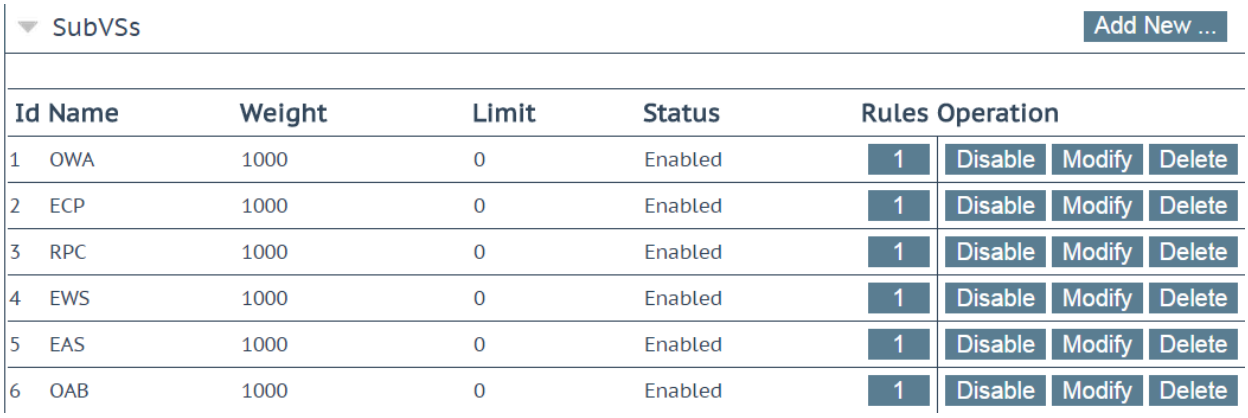


18. Click **None**.



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

Note: If the SubVS is for Exchange, select the **OWA** rule.



20. Now, create a SubVS for each of the other workloads by repeating steps 1 to 19 above. Steps 4 and 5 are no longer required as **Content Switching** has already been enabled for the parent Virtual Service.

Up	OWA ECP RPC EWS EAS OAB	Modify Delete

Once everything is set up, the overview of the Virtual Services will show something similar to the screenshot above.

Status	Real Servers	Operation
Up	OWA ECP RPC EWS EAS OAB	Modify Delete
Up	10.154.201.2	Modify
Up	10.154.201.2	Modify
Up	10.154.201.2	Modify
Up	10.154.201.2	Modify
Up	10.154.201.2	Modify
Up	10.154.201.2	Modify

When you click the blue IP address, a breakdown of the different SubVSs will be displayed; one for each workload with each having its specific health check.

5

References

References

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

SSL Accelerated Services, Feature Description

Content Rules, Feature Description

Web User Interface (WUI), Configuration Guide