



Content Switching Exchange and Lync

Technical Note

UPDATED: 27 July 2023

Copyright Notices

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

These materials and all Progress® software products are copyrighted and all rights are reserved by Progress Software Corporation. The information in these materials is subject to change without notice, and Progress Software Corporation assumes no responsibility for any errors that may appear therein. The references in these materials to specific platforms supported are subject to change.

#1 Load Balancer in Price/Performance, 360 Central, 360 Vision, Chef, Chef (and design), Chef Habitat, Chef Infra, Code Can (and design), Compliance at Velocity, Corticon, Corticon.js, DataDirect (and design), DataDirect Cloud, DataDirect Connect, DataDirect Connect64, DataDirect XML Converters, DataDirect XQuery, DataRPM, Defrag This, Deliver More Than Expected, DevReach (and design), Driving Network Visibility, Flowmon, Inspec, Ipswitch, iMacros, K (stylized), Kemp, Kemp (and design), Kendo UI, Kinvey, LoadMaster, MessageWay, MOVEit, NativeChat, OpenEdge, Powered by Chef, Powered by Progress, Progress, Progress Software Developers Network, SequeLink, Sitefinity (and Design), Sitefinity, Sitefinity (and design), Sitefinity Insight, SpeedScript, Stylized Design (Arrow/3D Box logo), Stylized Design (C Chef logo), Stylized Design of Samurai, TeamPulse, Telerik, Telerik (and design), Test Studio, WebSpeed, WhatsConfigured, WhatsConnected, WhatsUp, and WS_FTP are registered trademarks of Progress Software Corporation or one of its affiliates or subsidiaries in the U.S. and/or other countries.

Analytics360, AppServer, BusinessEdge, Chef Automate, Chef Compliance, Chef Desktop, Chef Workstation, Corticon Rules, Data Access, DataDirect Autonomous REST Connector, DataDirect Spy, DevCraft, Fiddler, Fiddler Classic, Fiddler Everywhere, Fiddler Jam, FiddlerCap, FiddlerCore, FiddlerScript, Hybrid Data Pipeline, iMail, InstaRelinker, JustAssembly, JustDecompile, JustMock, KendoReact, OpenAccess, PASOE, Pro2, ProDataSet, Progress Results, Progress Software, ProVision, PSE Pro, Push Jobs, SafeSpaceVR, Sitefinity Cloud, Sitefinity CMS, Sitefinity Digital Experience Cloud, Sitefinity Feather, Sitefinity Thunder, SmartBrowser, SmartComponent, SmartDataBrowser, SmartDataObjects, SmartDataView, SmartDialog, SmartFolder, SmartFrame, SmartObjects, SmartPanel, SmartQuery, SmartViewer, SmartWindow, Supermarket, SupportLink, Unite UX, and WebClient are trademarks or service marks of Progress Software Corporation and/or its subsidiaries or affiliates in the U.S. and other countries. Java is a registered trademark of Oracle and/or its affiliates. Any other marks contained herein may be trademarks of their respective owners.

Please refer to the NOTICE.txt or Release Notes – Third-Party Acknowledgements file applicable to a particular Progress product/hosted service offering release for any related required third-party acknowledgements.

Table of Contents

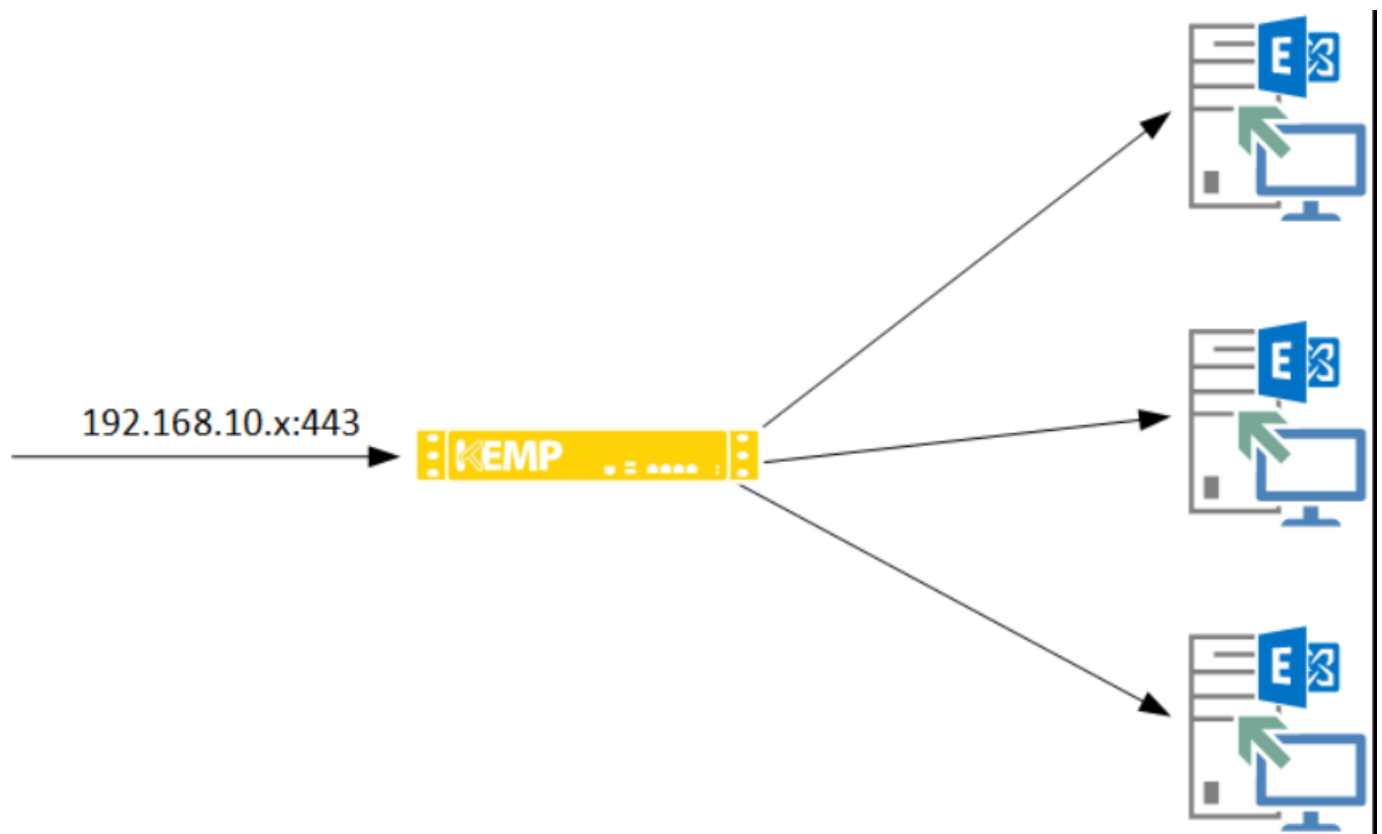
| | |
|--|-----------|
| 1 Introduction | 5 |
| 1.1 Document Purpose | 6 |
| 1.2 Intended Audience | 6 |
| 1.3 Author Information | 6 |
| 2 Content Rules | 7 |
| 3 Challenges | 9 |
| 3.1 Health Checking Exchange | 9 |
| 4 Configuring Content Rules | 11 |
| 4.1 Scenario 1 | 11 |
| 4.1.1 Step 1: Create the Content Matching Rules | 12 |
| 4.1.2 Step 2: Add the Certificate | 13 |
| 4.1.3 Step 3: Create and Configure the Virtual Service | 14 |
| 4.1.4 Step 4: Adding SubVSs | 16 |
| 4.2 Scenario 2 | 19 |
| 4.2.1 Step 1: Create the Content Rules | 19 |
| 4.2.2 Step 2: Add the Certificate | 21 |
| 4.2.3 Step 3: Create and Configure a Virtual Service | 21 |
| 4.2.4 Step 4: Adding SubVSs | 23 |
| References | 29 |
| SSL Accelerated Services, Feature Description | 29 |
| Content Rules, Feature Description | 29 |

| | |
|---|-----------|
| Web User Interface (WUI), Configuration Guide | 29 |
| Last Updated Date | 30 |

1 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.

1.1 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.com192.168.10.80:443

LyncFE.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.

1.2 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.

1.3 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

The Kemp 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.*\/`.

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*/ |

2 Content Rules

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

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.

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](#).

3.1 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.

3 Challenges

▼ Real Servers

Real Server Check Parameters

HTTP Protocol

Checked Port

443

Set Check Port

URL:

/owa/healthcheck.htm

Set URL

Use HTTP/1.1:

☐

HTTP Method:

GET

Set Pattern

Reply 200 Pattern:

Custom Headers:

Show Headers

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).

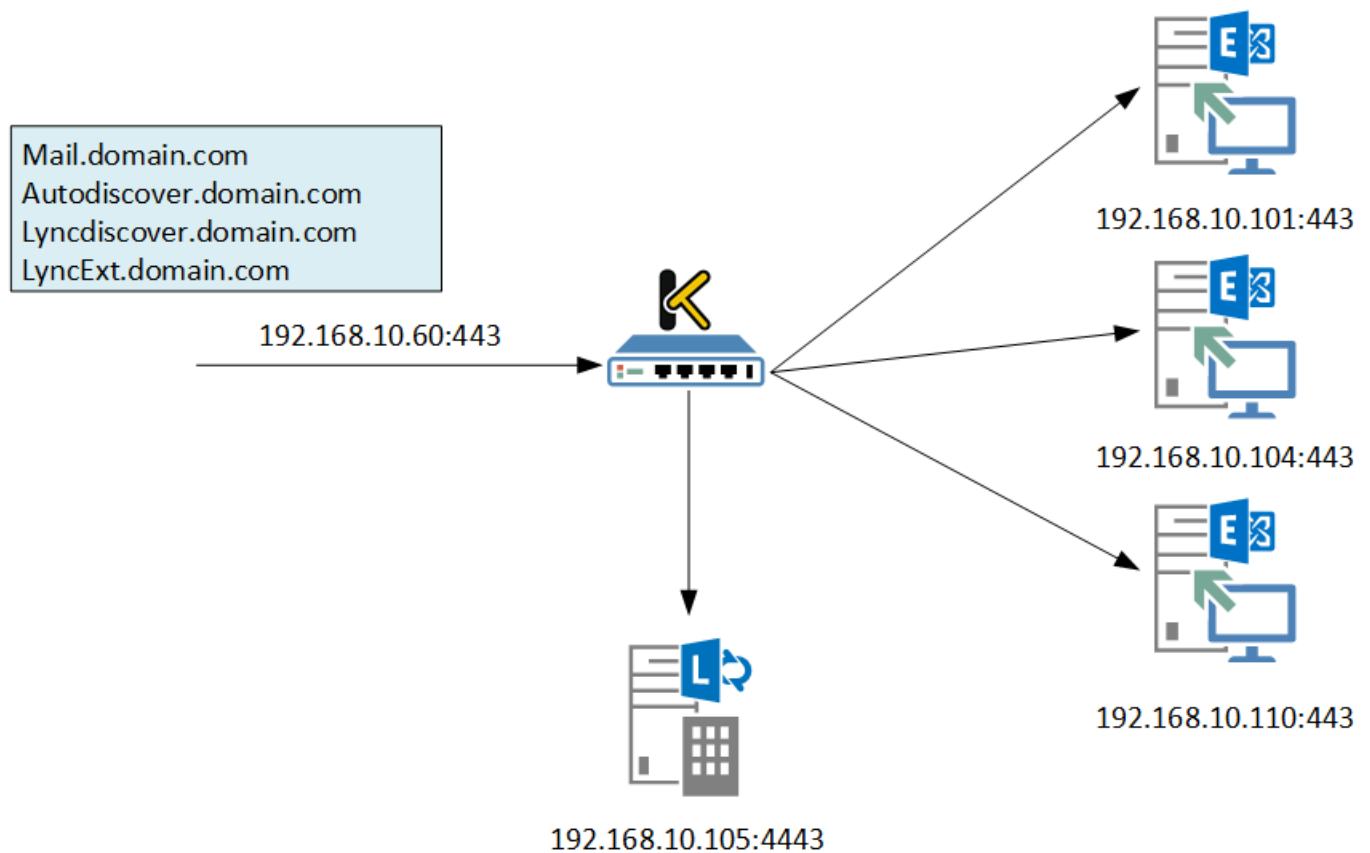
Using this information dramatically increases the flexibility and maximizes the utilization of an Exchange server by preventing a single workload failure to cause an entire server to be taken out of the pool of available servers.

4 Configuring Content Rules

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

4.1 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.

4.1.1 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

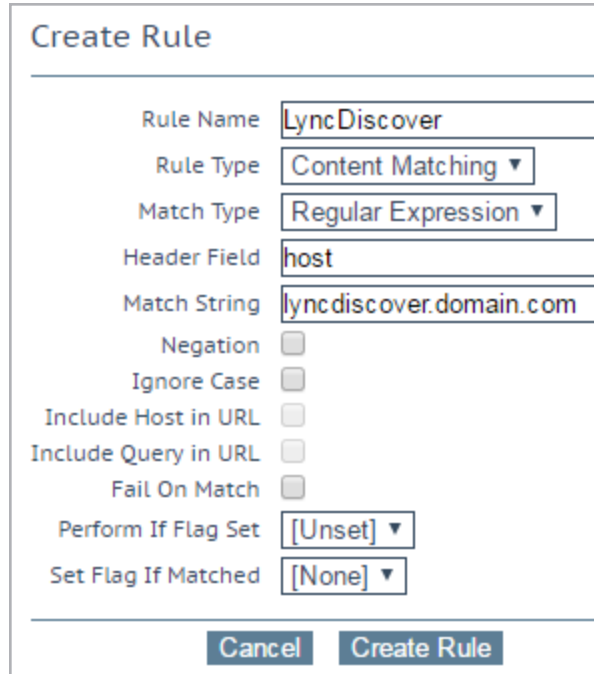
Lyncdiscover.domain.com

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.

4.1.2 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**.

4 Configuring Content Rules

2. Select **SSL Certificates**.
3. Click **Import Certificate**.

| | | |
|------------------------|--|-----------------|
| Certificate File | <input type="button" value="Choose File"/> | Certificate.pfx |
| Key File (optional) | <input type="button" value="Choose File"/> | No file chosen |
| Pass Phrase | <input type="password" value="....."/> | |
| Certificate Identifier | <input type="text" value="CertName"/> | |

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

4.1.3 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**.

| | |
|--|--|
| Please Specify the Parameters for the Virtual Service. | |
| Virtual Address | <input type="text" value="192.168.10.60"/> |
| Port | <input type="text" value="443"/> |
| Service Name (Optional) | <input type="text" value="Exchange-Lync"/> |
| Use Template | <input type="text" value="Select a Template"/> |
| Protocol | <input type="text" value="tcp"/> |

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**.

| Standard Options | |
|---------------------------------------|---|
| Force L4 | <input type="checkbox"/> |
| Transparency | <input checked="" type="checkbox"/> |
| Extra Ports | <input type="text"/> Set Extra Ports |
| Persistence Options | Mode: <input type="text" value="None"/> |
| Scheduling Method | <input type="text" value="round robin"/> |
| Idle Connection Timeout (Default 660) | <input type="text"/> Set Idle Timeout |
| Quality of Service | <input type="text" value="Normal-Service"/> |

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

| SSL Properties | |
|----------------------------------|--|
| SSL Acceleration | Enabled: <input checked="" type="checkbox"/> Reencrypt: <input checked="" type="checkbox"/> |
| Supported Protocols | <input type="checkbox"/> SSLv3 <input checked="" type="checkbox"/> TLS1.0 <input checked="" type="checkbox"/> TLS1.1 <input checked="" type="checkbox"/> TLS1.2 |
| Require SNI hostname | <input type="checkbox"/> |
| Certificates | <p>Self Signed Certificate in use.</p> <div> <div>Available Certificates</div> <div><input type="text" value="None Available"/></div> </div> <div> <div>Assigned Certificates</div> <div><input type="text" value="None Assigned"/></div> </div> <div>Set Certificates</div> <div>Manage Certificates</div> |
| Ciphers | <div>Cipher Set <input type="text" value="Default"/> Modify Cipher Set</div> <div>Assigned Ciphers</div> <div> <input type="text" value="ECDHE-RSA-AES256-SHA384"/> <input type="text" value="ECDHE-ECDSA-AES256-SHA384"/> <input type="text" value="DHE-RSA-AES256-SHA256"/> <input type="text" value="DHE-DSS-AES256-SHA256"/> <input type="text" value="DH-RSA-AES256-SHA256"/> <input type="text" value="DH-DSS-AES256-SHA256"/> </div> |
| Client Certificates | <input type="text" value="No Client Certificates required"/> |
| Reencryption Client Certificate | None required |
| Reencryption SNI Hostname | <input type="text"/> Set SNI Hostname |
| Strict Transport Security Header | <input type="text" value="Don't add the Strict Transport Security Header"/> |

8. Expand the **SSL Properties** section.

9. Select **Enabled**.

10. Click **OK** if a warning appears.

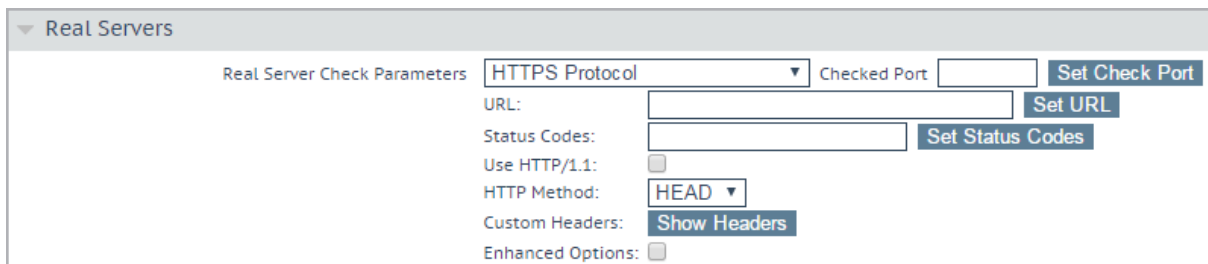
4 Configuring Content Rules

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**.

4.1.4 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.

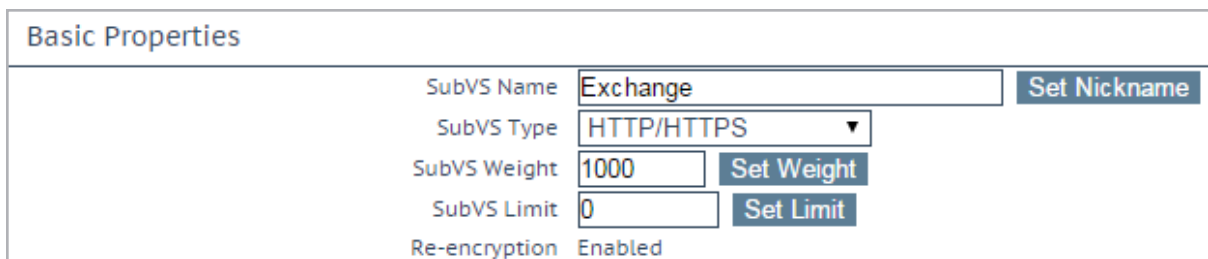


2. Click **Add SubVS**.
3. Click **OK** on the confirmation message.

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

| SubVSs Add New ... | | | | | |
|---------------------------------|------|--------|-------|---------|--|
| Id | Name | Weight | Limit | Status | Rules Operation |
| 7 | | 1000 | 0 | Enabled | <div>None</div> <div>Disable</div> <div>Modify</div> <div>Delete</div> |

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



4 Configuring Content Rules

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

| | |
|---------------------------------------|--|
| ▼ Standard Options | |
| Transparency | Disabled |
| Subnet Originating Requests | Enabled |
| Persistence Options | Mode: <input type="text" value="None"/> |
| Scheduling Method | <input type="text" value="round robin"/> |
| Idle Connection Timeout (Default 660) | <input type="text"/> <input type="button" value="Set Idle Timeout"/> |
| Quality of Service | <input type="text" value="Normal-Service"/> |

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

There is no persistence required for Exchange 2013.

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

| | |
|------------------------------|--|
| ▼ Real Servers | |
| Real Server Check Parameters | <input type="text" value="HTTPS Protocol"/> <input type="text" value="443"/> <input type="button" value="Set Check Port"/> |
| URL: | <input type="text" value="/owa"/> <input type="button" value="Set URL"/> |
| Status Codes: | <input type="text"/> <input type="button" value="Set Status Codes"/> |
| Use HTTP/1.1: | <input type="checkbox"/> |
| HTTP Method: | <input type="text" value="GET"/> |
| Reply 200 Pattern: | <input type="text"/> <input type="button" value="Set Pattern"/> |
| Custom Headers: | <input type="button" value="Show Headers"/> |
| Enhanced Options: | <input type="checkbox"/> |

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**.

4 Configuring Content Rules

Please Specify the Parameters for the Real Server

| | |
|------------------------|---|
| Allow Remote Addresses | <input type="checkbox"/> |
| Real Server Address | <input type="text" value="10.11.0.15"/> |
| Port | <input type="text" value="443"/> |
| Forwarding method | <input type="text" value="nat"/> |
| Weight | <input type="text" value="1000"/> |
| Connection Limit | <input type="text" value="0"/> |

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

11. Enter the relevant **Port**.

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.

▼ Advanced Properties

| | |
|------------------------------------|--|
| Content Switching | Enabled |
| HTTP Selection Rules | Show Selection Rules |
| HTTP Header Modifications | Show Header Rules |
| Enable Caching | <input type="checkbox"/> |
| Enable Compression | <input type="checkbox"/> |
| Detect Malicious Requests | <input type="checkbox"/> |
| Add Header to Request | <input type="text"/> : <input type="text"/> Set Header |
| "Sorry" Server | <input type="text"/> Port <input type="text"/> Set Server Address |
| Not Available Redirection Handling | Error Code: <input type="text"/> Set Redirect URL |
| Add a Port 80 Redirector VS | Redirect URL: <input type="text"/> Add HTTP Redirector |
| Default Gateway | Redirection URL: <input type="text" value="https://%h%s"/> Set Default Gateway |
| Service Specific Access Control | Access Control |

16. Click **Enable**.

| Rules | Operation |
|----------------------|---|
| None | Disable Modify Delete |

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



A dialog box titled "Add Rule". It contains a label "Rule:" followed by a dropdown menu showing "default" and a blue "Add" button.

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.

4.2 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)

4.2.1 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 | <code>/^\\owa.*</code> | <code>/owa/healthcheck.htm</code> |
| EAC/ECP | <code>/^\\ecp.*</code> | <code>/ecp/healthcheck.htm</code> |
| EWS | <code>/^\\ews.*</code> | <code>/ews/healthcheck.htm</code> |
| OA | <code>/^\\rpc.*</code> | <code>/rpc/healthcheck.htm</code> |
| MAPI | <code>/^\\mapi.*</code> | <code>/mapi/healthcheck.htm</code> |
| OAB | <code>/^\\oab.*</code> | <code>/oab/healthcheck.htm</code> |
| EAS | <code>/^\\Microsoft-server-activesync.*</code> | <code>/Microsoft-server-activesync/healthcheck.htm</code> |
| AutoD | <code>/^\\autodiscover.*</code> | <code>/autodiscover/healthcheck.htm</code> |

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 Configuring Content Rules

Create Rule

Rule Name

ECP

Rule Type

Content Matching ▼

Match Type

Regular Expression ▼

Header Field

Match String

/^\/ecp.*\/

Negation

☐

Ignore Case

☒

Include Host in URL

☐

Include Query in URL

☐

Fail On Match

☐

Perform If Flag Set

[Unset] ▼

Set Flag If Matched

[None] ▼

Cancel

Create Rule

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.

4.2.2 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**.

4.2.3 Step 3: Create and Configure a Virtual Service

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

4 Configuring Content Rules

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

Please Specify the Parameters for the Virtual Service.

| | |
|-------------------------|---------------------|
| Virtual Address | 192.168.10.60 |
| Port | 443 |
| Service Name (Optional) | Exchange |
| Use Template | Select a Template ▼ |
| Protocol | tcp ▼ |

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.

▼ Standard Options

| | |
|---------------------------------------|--|
| Force L4 | <input type="checkbox"/> |
| Transparency | <input checked="" type="checkbox"/> |
| Extra Ports | <input type="text"/> <input type="button" value="Set Extra Ports"/> |
| Persistence Options Mode: | None ▼ |
| Scheduling Method | round robin ▼ |
| Idle Connection Timeout (Default 660) | <input type="text"/> <input type="button" value="Set Idle Timeout"/> |
| Quality of Service | Normal-Service ▼ |

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

4 Configuring Content Rules

| SSL Properties | |
|----------------------------------|--|
| SSL Acceleration | Enabled: <input checked="" type="checkbox"/> Reencrypt: <input checked="" type="checkbox"/> |
| Supported Protocols | <input type="checkbox"/> SSLv3 <input checked="" type="checkbox"/> TLS1.0 <input checked="" type="checkbox"/> TLS1.1 <input checked="" type="checkbox"/> TLS1.2 |
| Require SNI hostname | <input type="checkbox"/> |
| Certificates | <p>Self Signed Certificate in use.</p> <div> <div>Available Certificates</div> <div>None Available</div> </div> <div> <div>Assigned Certificates</div> <div>None Assigned</div> </div> <div>Set Certificates</div> <div>Manage Certificates</div> |
| Ciphers | <p>Cipher Set: Default Modify Cipher Set</p> <p>Assigned Ciphers</p> <div> ECDHE-RSA-AES256-SHA384 ECDHE-ECDSA-AES256-SHA384 DHE-RSA-AES256-SHA256 DHE-DSS-AES256-SHA256 DH-RSA-AES256-SHA256 DH-DSS-AES256-SHA256 </div> |
| Client Certificates | No Client Certificates required |
| Reencryption Client Certificate | None required |
| Reencryption SNI Hostname | <input type="text"/> Set SNI Hostname |
| Strict Transport Security Header | Don't add the Strict Transport Security Header |

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**.

4.2.4 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.

| |
|---|
| <div>Add New ...</div> <div>Add SubVS ...</div> |
|---|

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

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.

| Basic Properties | |
|------------------|-----------------------------|
| SubVS Name | OWA <div>Set Nickname</div> |
| SubVS Type | HTTP/HTTPS ▼ |
| SubVS Weight | 1000 <div>Set Weight</div> |
| SubVS Limit | 0 <div>Set Limit</div> |
| Re-encryption | Enabled |

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

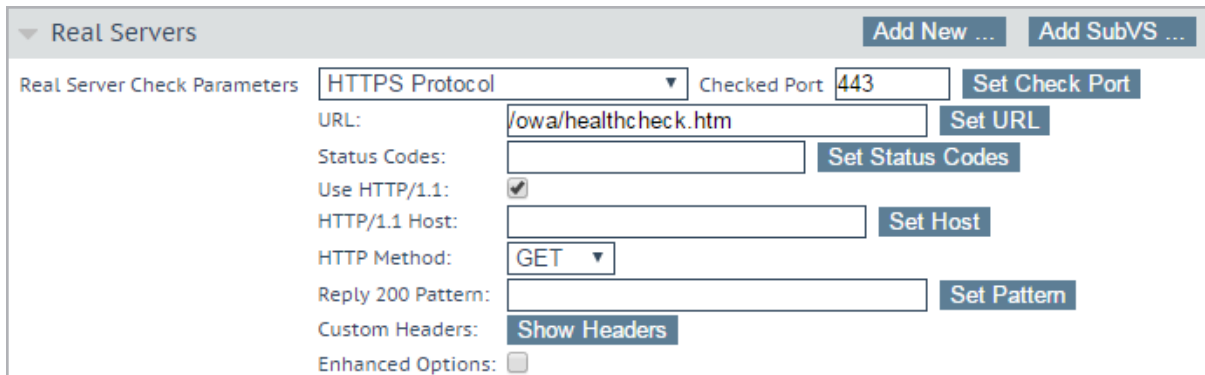
| ▼ Standard Options | |
|---------------------------------------|---|
| Transparency | Disabled |
| Subnet Originating Requests | Enabled |
| Persistence Options | Mode: None ▼ |
| Scheduling Method | round robin ▼ |
| Idle Connection Timeout (Default 660) | <div></div> <div>Set Idle Timeout</div> |
| Quality of Service | Normal-Service ▼ |

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

There is no persistence required for Exchange 2013.

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

4 Configuring Content Rules



The screenshot shows the 'Real Servers' configuration window. The 'Real Server Check Parameters' section is expanded, showing the following settings:

- Protocol: HTTPS Protocol
- Checked Port: 443
- URL: /owa/healthcheck.htm
- Status Codes: (empty)
- Use HTTP/1.1: ☒
- HTTP/1.1 Host: (empty)
- HTTP Method: GET
- Reply 200 Pattern: (empty)
- Custom Headers: Show Headers
- Enhanced Options: ☐

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:

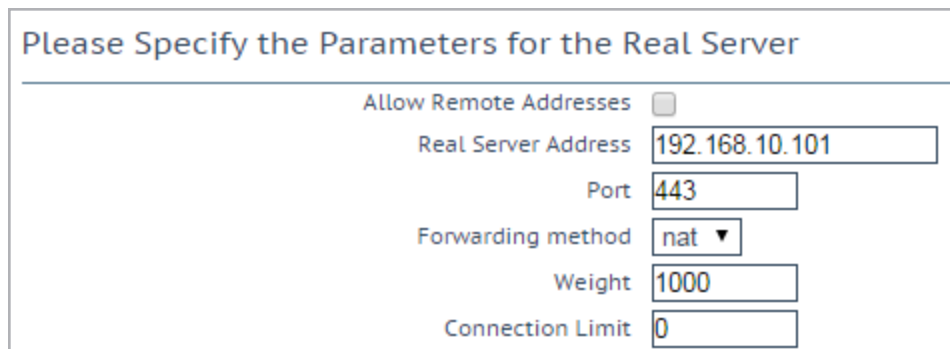
Checked Port: 443

URL: /owa/healthcheck.htm

Use HTTP/1.1: Enabled

HTTP Method: GET

9. Click **Add New**.



The screenshot shows the 'Please Specify the Parameters for the Real Server' dialog box. The parameters are as follows:

- Allow Remote Addresses: ☐
- Real Server Address: 192.168.10.101
- Port: 443
- Forwarding method: nat
- Weight: 1000
- Connection Limit: 0

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

11. Enter the relevant **Port**.

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

12. Click **Add This Real Server**.

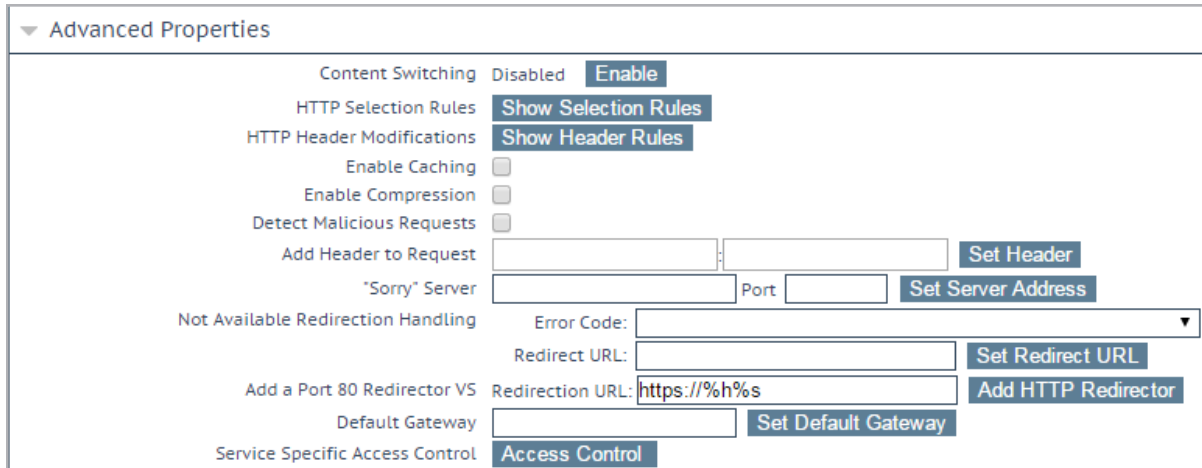
13. Repeat steps 12 to 14 above for each Real Server that needs to be added to this SubVS.

4 Configuring Content Rules

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.



The screenshot shows the 'Advanced Properties' section of a configuration interface. It contains several settings and buttons:

- Content Switching:** Disabled (with an 'Enable' button).
- HTTP Selection Rules:** (with a 'Show Selection Rules' button).
- HTTP Header Modifications:** (with a 'Show Header Rules' button).
- Enable Caching:** (checkbox).
- Enable Compression:** (checkbox).
- Detect Malicious Requests:** (checkbox).
- Add Header to Request:** (text input field with a 'Set Header' button).
- *Sorry* Server:** (text input field with a 'Set Server Address' button).
- Not Available Redirection Handling:** (dropdown menu with 'Error Code:' label).
- Redirect URL:** (text input field with a 'Set Redirect URL' button).
- Add a Port 80 Redirector VS:** (text input field with a 'Add HTTP Redirector' button).
- Redirection URL:** (text input field containing 'https://%h%s').
- Default Gateway:** (text input field with a 'Set Default Gateway' button).
- Service Specific Access Control:** (button labeled 'Access Control').

17. Click **Enable**.



The screenshot shows the 'Rules Operation' section. It contains a table with two columns: 'Rules' and 'Operation'. The 'Rules' column has a 'None' button highlighted with a red border. The 'Operation' column has three buttons: 'Disable', 'Modify', and 'Delete'.

18. Click **None**.



The screenshot shows the 'Add Rule' dialog box. It contains a 'Rule:' label, a dropdown menu with 'default' selected, and an 'Add' button.

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

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

4 Configuring Content Rules

| ▼ SubVSs | | | | | | Add New ... | | |
|----------|-----|--------|-------|---------|-----------------|-------------|--------|--------|
| | | | | | | | | |
| Id Name | | Weight | Limit | Status | Rules Operation | | | |
| 1 | OWA | 1000 | 0 | Enabled | 1 | Disable | Modify | Delete |
| 2 | ECP | 1000 | 0 | Enabled | 1 | Disable | Modify | Delete |
| 3 | RPC | 1000 | 0 | Enabled | 1 | Disable | Modify | Delete |
| 4 | EWS | 1000 | 0 | Enabled | 1 | Disable | Modify | Delete |
| 5 | EAS | 1000 | 0 | Enabled | 1 | Disable | Modify | Delete |
| 6 | OAB | 1000 | 0 | Enabled | 1 | Disable | Modify | Delete |

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.

References

Unless otherwise specified, the following documents can be found at <http://kemptechnologies.com/documentation>.

SSL Accelerated Services, Feature Description

Content Rules, Feature Description

Web User Interface (WUI), Configuration Guide

Last Updated Date

This document was last updated on 27 July 2023.