Microsoft Exchange 2013 Deployment Guide

VERSION: 9.0
UPDATED: JULY 2016
Copyright Notices

Copyright © 2002-2016 KEMP Technologies, Inc. All rights reserved. KEMP Technologies and the KEMP Technologies logo are registered trademarks of KEMP Technologies, Inc.

KEMP Technologies, Inc. reserves all ownership rights for the LoadMaster product line including software and documentation. The use of the LoadMaster Exchange appliance is subject to the license agreement. Information in this guide may be modified at any time without prior notice.

Microsoft Windows is a registered trademark of Microsoft Corporation in the United States and other countries. All other trademarks and service marks are the property of their respective owners.

Limitations: This document and all of its contents are provided as-is. KEMP Technologies has made efforts to ensure that the information presented herein are correct, but makes no warranty, express or implied, about the accuracy of this information. If any material errors or inaccuracies should occur in this document, KEMP Technologies will, if feasible, furnish appropriate correctional notices which Users will accept as the sole and exclusive remedy at law or in equity. Users of the information in this document acknowledge that KEMP Technologies cannot be held liable for any loss, injury or damage of any kind, present or prospective, including without limitation any direct, special, incidental or consequential damages (including without limitation lost profits and loss of damage to goodwill) whether suffered by recipient or third party or from any action or inaction whether or not negligent, in the compiling or in delivering or communicating or publishing this document.

Any Internet Protocol (IP) addresses, phone numbers or other data that may resemble actual contact information used in this document are not intended to be actual addresses, phone numbers or contact information. Any examples, command display output, network topology diagrams, and other figures included in this document are shown for illustrative purposes only. Any use of actual addressing or contact information in illustrative content is unintentional and coincidental.

Portions of this software are; copyright (c) 2004-2006 Frank Denis. All rights reserved; copyright (c) 2002 Michael Shalayeff. All rights reserved; copyright (c) 2003 Ryan McBride. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE ABOVE COPYRIGHT HOLDERS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE ABOVE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The views and conclusions contained in the software and documentation are those of the authors and should not be interpreted as representing official policies, either expressed or implied, of the above copyright holders..

Portions of the LoadMaster software are copyright (C) 1989, 1991 Free Software Foundation, Inc. -51 Franklin Street, Fifth Floor, Boston, MA 02110-1301, USA- and KEMP Technologies Inc. is in full compliance of the GNU license requirements, Version 2, June 1991. Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.
Portions of this software are Copyright (C) 1988, Regents of the University of California. All rights reserved.
Redistribution and use in source and binary forms are permitted provided that the above copyright notice and this paragraph are duplicated in all such forms and that any documentation, advertising materials, and other materials related to such distribution and use acknowledge that the software was developed by the University of California, Berkeley. The name of the University may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED ``AS IS'' AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

Portions of this software are Copyright (C) 1998, Massachusetts Institute of Technology

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Portions of this software are Copyright (C) 1995-2004, Jean-loup Gailly and Mark Adler

This software is provided 'as-is', without any express or implied warranty. In no event will the authors be held liable for any damages arising from the use of this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:

1. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.

2. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.

3. This notice may not be removed or altered from any source distribution.

Portions of this software are Copyright (C) 2003, Internet Systems Consortium

Permission to use, copy, modify, and/or distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND THE AUTHOR DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Used, under license, U.S. Patent Nos. 6,473,802, 6,374,300, 8,392,563, 8,103,770, 7,831,712, 7,606,912, 7,346,695, 7,287,084 and 6,970,933
Table of Contents

1  Introduction .................................................................................................................. 5

1.1  About This Manual ................................................................................................. 5

1.2  Prerequisites ........................................................................................................... 5

2  Exchange 2013 Overview ........................................................................................... 6

2.1  Differences Between Exchange 2010 and Exchange 2013 .................................... 6

2.2  Understanding Server Load Balancing .................................................................... 7

3  Virtual Service Templates ........................................................................................... 9

4  Configuring Virtual Services for Exchange 2013 ...................................................... 10

4.1  HTTPS Virtual Service ............................................................................................ 10

4.1.1  HTTPS using SubVSs ......................................................................................... 13

4.1.2  HTTPS Offloading Using SubVSs ..................................................................... 18

4.1.3  HTTPS Offloading Using ESP and SubVSs ....................................................... 22

4.2  IMAP Virtual Service .............................................................................................. 25

4.2.1  IMAP STARTTLS Virtual Service .................................................................... 27

4.2.2  IMAPS Virtual Service ...................................................................................... 28

4.2.3  IMAPS Offloaded Virtual Service .................................................................... 30

4.3  POP Virtual Service ............................................................................................... 31

4.3.1  POP with STARTTLS Virtual Service ............................................................. 33

4.3.2  POPS Virtual Service ....................................................................................... 34

4.3.3  POPS Offloaded Virtual Service .................................................................... 35

4.4  SMTP Virtual Service ............................................................................................. 37

4.4.1  SMTPS Virtual Service ....................................................................................... 39

4.4.2  SMTPS Offloaded Virtual Service .................................................................... 40

4.4.3  SMTP with STARTTLS Virtual Service ......................................................... 42

4.4.4  SMTP with ESP Virtual Service ........................................................................ 43

References ....................................................................................................................... 45

Document History .......................................................................................................... 46
1 Introduction

The KEMP LoadMaster combines versatility with ease-of-use to speed deployment of the complete portfolio of advanced messaging applications and protocols used by Exchange 2013, including Outlook Web App (OWA), Outlook Anywhere (OA), Exchange ActiveSync (EAS), Simple Mail Transfer Protocol (SMTP), Post Office Protocol version 3 (POP3) and Internet Message Access Protocol version 4 (IMAP4). With built-in SSL acceleration and/or overlay, the LoadMaster offloads a key source of CPU drain to improve the capacity of Client Access Servers (CASs). Layer 7 health checking at the LoadMaster ensures that if one of the CASs becomes inaccessible, the load balancer will take that server offline, while automatically re-routing and reconnecting users to other functioning servers.

The entire KEMP LoadMaster product family, including the Virtual LoadMaster (VLM) supports Microsoft Exchange 2013.

1.1 About This Manual

This manual addresses how to deploy and configure a LoadMaster appliance with Microsoft Exchange 2013.

KEMP’s LoadMaster family of products is available in various models to support networks of different throughput requirements. Information in this manual applies to all LoadMaster models.

1.2 Prerequisites

It is assumed that the reader is a network administrator or a person otherwise familiar with networking and general computer terminology. It is further assumed that the Exchange 2013 environment has been set up and the KEMP LoadMaster has been installed.

LoadMaster documentation is available at http://www.kemptechnologies.com/documentation.

At a minimum, you should have:

- Installed the Microsoft Servers, Active Directories and followed other Microsoft requirements
- Installed the LoadMaster on the same network as the servers.
- Established access to the LoadMaster Web User Interface (WUI)
2 Exchange 2013 Overview

Microsoft Exchange Server is a mail server, calendaring software and contact manager. It is a server program that runs on Windows Server and is part of the Microsoft Servers line of products. The improvements made in Exchange 2013 have made it easier to load balance Exchange-related traffic.

Exchange 2013 includes the following solutions for switchover and failover redundancy:

- **High availability:** Exchange 2013 uses Database Availability Groups (DAGs) to keep multiple copies of your mailboxes on different servers synchronized. That way, if a mailbox database fails on one server, users can connect to a synchronized copy of the database on another server.

- **Site resilience:** You can deploy two Active Directory sites in separate geographic locations, keep the mailbox data synchronized between the two, and have one of the sites take on the entire load if the other fails.

- **Online mailbox moves:** During an online mailbox move, email accounts are still accessible. Users are only locked out for a brief period of time at the end of the process, when the final synchronization occurs. Online mailbox moves can be performed across forests or in the same forest.

- **Shadow redundancy:** Shadow redundancy protects the availability and recoverability of messages while they are in transit. With shadow redundancy, the deletion of a message from the transport databases is delayed until the transport server verifies that all the next hops for that message have completed. If any of the next hops fail before reporting successful delivery, the message is resubmitted for delivery to the hop that did not complete.

2.1 Differences Between Exchange 2010 and Exchange 2013

One of the biggest changes in Exchange 2013 is that the number of server roles has reduced to just two. In older versions of Exchange there were a number of server roles for Hub Transport, Unified Messaging, Mailbox and Client Access. In Exchange 2013 there are just two server roles:

- The **Mailbox Server** which includes all of the functions to route mail, render web content and receive voicemail
- The **CAS** which authenticates clients and routes requests to the correct mailbox server

The CAS now acts as a reverse proxy. The CAS no longer renders OWA when a user accesses it. The CAS determines which mailbox database their mailbox is located on and provides the request to the back-end mailbox server that hosts the database. The mailbox server then renders the OWA content, not the CAS.

Clients no longer interact with Exchange using RPC, it is all done over HTTPS. Outlook Anywhere is the protocol that Outlook clients use to access their mailbox.
Exchange 2013 Service Pack 1 introduces new connectivity option MAPI/HTTP which is disabled by default. It must be manually enabled by administrator and is only available as a connectivity option to clients running Office 2013 Service Pack 1 or later. Older clients continue using RPC/HTTP.

Outlook 2003 is not supported with Exchange 2013.

Unlike previous versions of Exchange, Exchange 2013 no longer requires session affinity at the load balancing layer. For more information, refer to the related article in The Exchange Team Blog: Load Balancing in Exchange 2013.

2.2 Understanding Server Load Balancing

Server load balancing is a way to manage which servers receive traffic. Server load balancing provides failover redundancy to ensure users continue to receive service in case of failure. It also enables your deployment to handle more traffic than one server can process while offering a single host name for clients.

Server load balancing serves two primary purposes. It reduces the impact of a single CAS failure within one Active Directory site. In addition, server load balancing ensures that the load on the CAS and Transport servers is optimally distributed.

Two key changes in Exchange 2013 make load balancing a lot simpler:

- HTTPS-only access from clients means that there is only one protocol to consider. The HTTP failure states are well known and clients typically respond in a similar way.
- As OWA is rendered on the same server that is hosting the user’s mailbox database; if a client hits a different CAS there is no performance degradation as the session rendering for that user is already up and running.

Forms-based authentication has also been improved. The authentication cookie is provided to the user after logon and it is encrypted using the CAS’s SSL certificate. This allows a logged in user to resume their session on a different CAS without having to re-authenticate (if servers share the same SSL certificate).
Figure 2-1: Load Balancing Exchange 2013
3 Virtual Service Templates

KEMP have developed templates containing our recommended settings for Exchange 2013. These templates can be installed on the LoadMaster and can be used when creating each of the Virtual Services. Using a template automatically populates the settings in the Virtual Services. This is quicker and easier than manually configuring each Virtual Service. If needed, you can make changes to any of the Virtual Service settings after using the templates.

Released templates can be downloaded from the KEMP documentation page: http://www.kemptechnologies.com/documentation/.

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

For steps on how to manually add and configure the Virtual Services, refer to the sections below.

The Microsoft Exchange 2013 templates currently available are grouped in three downloadable files as follows:

- **Exchange2013Core**
  
  This file contains templates for non-SSL offloaded HTTPS, SSL offloaded HTTPS and SMTP Virtual Services. This is the primary set of services needed to balance Exchange 2013.

- **Exchange2013ESP**
  
  This set contains individual templates for a HTTPS service with SSL offloading and an SMTP service, both with ESP enabled. These services are only necessary if you want to use ESP functionality.

- **Exchange2013Additional**
  
  This set contains templates for IMAP, POP and SMTP services, including variants for STARTTLS and SSL secured services.

If you create another Virtual Service using the same template, ensure to change the **Service Name** to a unique name.

When using SNMP monitoring of ESP-enabled Virtual Services that were created using a template, ensure to monitor each SubVS directly rather than relying on the master service. This is because the Authentication Proxy sub-service will always be marked as up and, as a consequence, so will the master service.
4 Configuring Virtual Services for Exchange 2013

The sections below give instructions on how to configure the various Virtual Services related to Microsoft Exchange. The settings in this document are recommended by KEMP. They may not be applicable to your specific configuration. For further information and help, please contact our Support team.

If using Exchange 2013 (not SP1), ensure to enable SSL re-encryption. Also, if using Exchange 2013 (not SP1), MAPI is not used and can be removed.

4.1 HTTPS Virtual Service

Follow the instructions below to set up a HTTPS Virtual Service:

1. Select the Add New option within the Virtual Services section of the main menu tree.

![Figure 4-1: Virtual Service parameters](image)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual Address</td>
<td>10.11.0.194</td>
</tr>
<tr>
<td>Port</td>
<td>443</td>
</tr>
<tr>
<td>Service Name (Optional)</td>
<td>Exchange 2013 HTTPS</td>
</tr>
<tr>
<td>Use Template</td>
<td>Select a Template</td>
</tr>
<tr>
<td>Protocol</td>
<td>tcp</td>
</tr>
</tbody>
</table>

2. Enter the IP address of the Virtual Service in the Virtual Address field.
3. Enter 443 in the Port field.
4. Type a name, for example Exchange 2013 HTTPS in the Service Name field.
5. Select tcp in the Protocol drop-down list.
6. Click the Add this Virtual Service button to add the Virtual Service.

![Figure 4-2: Basic Properties](image)

7. Within the Basic Properties section of the Virtual Services options page, select the following options:
   a) Select HTTP/HTTPS in the Service Type drop-down list
8. Within the **Standard Options** section of the Virtual Services options page, select the following options:
   a) Ensure the **Force L7** checkbox is selected.
   b) Remove the tick from the **Transparency** checkbox.
   c) Ensure that **none** is selected in the **Persistence Options** drop-down list.
   d) Ensure that **round robin** is selected in the **Scheduling Method** drop-down list.
   e) Enter **1800** in the **Idle Connection Timeout** field and click **Set Idle Timeout** button.

   *When L7 is referred to in KEMP documentation it is in relation to the actual TCP connection. When Microsoft refer to L7 for Exchange it is in relation to SSL decryption and re-encryption. This is different and what KEMP recommends is not necessarily L7 configuration unless SSL acceleration is enabled.*

9. Within the **SSL Properties** section, ensure that the **SSL Acceleration** check box is not selected.

10. Within the **Advanced Options** section, select the following options:
   a) Ensure that **https://%h%** is the value of the **Redirection URL** in the **Add a Port 80 Redirector VS** section.
   b) Click **Add HTTP Redirector**.

   *This creates a new redirect Virtual Service on port 80 with the same IP address.*
11. Within the **ESP Options** section, ensure that the **Enable ESP** checkbox is not selected.

![Figure 4-5: ESP Options](image)

12. Within the **Real Servers** section of the Virtual Services options page, select the following options:
   a) Ensure that **HTTPS Protocol** has been selected as the health-checking option.
   b) Enter **443** in the **Checked Port** field and click on the **Set Check Port** button.
   c) Enter **/owa/healthcheck.htm** in the **URL** field and click on the **Set URL** button.
   d) Ensure the **Use HTTP/1.1** checkbox is deselected.
   e) Select **GET** from the **HTTP Method** drop-down list.

To add content rules to the VS, follow the steps in Section 4.1.1.3.

Minor changes now need to be made to the redirect Virtual Service that was added:

1. Click **View/Modify Services** in the main menu.
2. Click **Modify** on the **Redirect** Virtual Service with the blank name which has the same IP address as the Virtual Service that was just created.

![Figure 4-7: Basic Properties](image)

3. Enter a recognizable **Service Name**, for example **Exchange 2013 HTTP Redirect** and click **Set Nickname**.
4. In **Standard Options**, set the **Persistence Mode** to **None**.
4.1.1 HTTPS using SubVSs

Follow the instructions below to set up a HTTPS Virtual Service with SubVSs.

4.1.1.1 Create the Parent Virtual Service

Follow the instructions below to set up the parent HTTPS Virtual Service:

1. Select the Add New option within the Virtual Services section of the main menu tree.

![Virtual Service Parameters](image)

![Standard Options](image)

2. Enter the IP address of the Virtual Service in the Virtual Address field.
3. Enter 443 in the Port field.
4. Type a name, for example Exchange 2013 HTTPS in the Service Name field.
5. Select tcp in the Protocol drop-down list.
6. Click the Add this Virtual Service button to add the Virtual Service.
7. Within the Basic Properties section of the Virtual Services options page, select the following options:
   a) Select HTTP/HTTPS in the Service Type drop-down list.
   b) Ensure the Force L7 checkbox is selected.
   c) Remove the tick from the Transparency checkbox.
   d) Ensure that none is selected in the Persistence Options drop-down list.
   e) Ensure that round robin is selected in the Scheduling Method drop-down list.
8. Within the Standard Options section of the Virtual Services options page, set the fields as outlined below:
   a) Ensure the Force L7 checkbox is selected.
   b) Remove the tick from the Transparency checkbox.
   c) Ensure that none is selected in the Persistence Options drop-down list.
   d) Ensure that round robin is selected in the Scheduling Method drop-down list.
e) Enter **1800** in the **Idle Connection Timeout** field and click the **Set Idle Timeout** button.

![Figure 4-10: SSL Properties](image)

9. Within the **SSL Properties** section, select the **Enabled** check box.
10. Click **OK**.
11. Select the **Reencrypt** check box.

![Figure 4-11: Advanced Properties](image)

12. Within the **Advanced Properties** section, select the following options:
   a) Ensure that **https://%h%** is the value of the Redirection URL in the **Add a Port 80 Redirector VS** section. Click **Add HTTP Redirector**.
This creates a redirect Virtual Service on port 80 with the same IP address.

![ESP Options](image)

Figure 4-12: ESP Options

13. Within the ESP Options section, ensure that the Enable ESP check box is not selected.

### 4.1.1.2 Create the SubVSs

Follow the instructions below to set up the SubVSs:

1. In the Real Servers section of the Virtual Services options page, click the Add SubVS button.
2. A message stating that the SubVS has been created appears, click OK.

The Real Servers section should now be renamed to SubVSs.

The following steps deal with creating a SubVS for an Exchange service such as owa.

3. In the SubVSs section of the SubVS options page, click the Modify button next to the SubVS and select the following options:

![Basic Properties](image)

Figure 4-13: Basic Properties

- a) In the SubVS Name field enter a relevant name such as owa
- b) In the SubVS Type field select the HTTP/HTTPS option

![ESP Options](image)

Figure 4-14: ESP Options

4. Within the ESP Options section, ensure that the Enable ESP check box is not selected.
5. In the **Real Servers** section of the SubVS options page select the following options:
   a) Enter `/owa/healthcheck.htm` in the **URL** field and click the **Set URL** button.
   b) Ensure the **Use HTTP/1.1** checkbox is deselected
   c) Ensure that the **GET** option is selected from the **HTTP Method** drop-down list.

6. When finished editing the SubVS, click **Back**. Now you can add other SubVSs to this Virtual Service as needed.

7. Configure each SubVS using the settings in the table below.

<table>
<thead>
<tr>
<th>SubVS Name</th>
<th>Healthcheck URL</th>
<th>Allowed Virtual Directories</th>
</tr>
</thead>
<tbody>
<tr>
<td>OWA (as in steps above)</td>
<td>/owa/healthcheck.htm</td>
<td>/owa*</td>
</tr>
<tr>
<td>Autodiscover</td>
<td>/autodiscover/healthcheck.htm</td>
<td>/autodiscover*</td>
</tr>
<tr>
<td>ECP</td>
<td>/ecp/healthcheck.htm</td>
<td>/ecp*</td>
</tr>
<tr>
<td>EWS</td>
<td>/ews/healthcheck.htm</td>
<td>/ews*</td>
</tr>
<tr>
<td>ActiveSync</td>
<td>/microsoft-server-activesync/healthcheck.htm</td>
<td>/microsoft-server-activesync*</td>
</tr>
<tr>
<td>OAB</td>
<td>/oab/healthcheck.htm</td>
<td>/oab*</td>
</tr>
<tr>
<td>Powershell</td>
<td>/powershell/healthcheck.htm</td>
<td>/powershell*</td>
</tr>
<tr>
<td>RPC</td>
<td>/rpc/healthcheck.htm</td>
<td>/rpc*</td>
</tr>
<tr>
<td>MAPI</td>
<td>/mapi/healthcheck.htm</td>
<td>/mapi*</td>
</tr>
<tr>
<td>Authentication Proxy</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Figure 4-16: Health check URLs**

If you are using Kerberos Constrained Delegation (KCD) please ensure you add a Real Server to the Authentication Proxy SubVS. For further information on KCD, refer to the **KCD, Feature Description**

### Create Content Rules

Content Rules need to be created for the Virtual Services to function correctly.

To create a Modify URL rule for **owa** please complete the following steps:

1. Select the **Rules & Checking > Content Rules** menu option
2. Click the **Create New** button
3. Enter a relevant name, for example `Redirect_Root` in the `Rule Name` field
4. Select the `Modify URL` option in the `Rule Type` drop-down
5. Enter `/^\$/` in the `Match String` field
6. Enter `/owa` in the `Modified URL` field
7. Click the `Create Rule` button

To create a Content Matching rule for `owa` please complete the following steps:


2. Click the `Create New` button.
3. Enter a relevant name, for example **OWA** in the **Rule Name** field.
4. Select the **Content Matching** option is selected in the **Rule Type** drop-down list.
5. Ensure the **Regular Expression** option is selected in the **Match Type** drop-down list.
6. Enter `/\^\/owa.*/` in the **Match String** field.
7. Select the **Ignore Case** checkbox.
8. Click the **Create Rule** button.

Create additional Content Matching rules following steps 1 to 8 above but using the values as described in the table below.

<table>
<thead>
<tr>
<th>Rule Name</th>
<th>Match String</th>
<th>Ignore Case</th>
</tr>
</thead>
<tbody>
<tr>
<td>ActiveSync</td>
<td><code>/\^\/microsoft-server-activesync.*/</code></td>
<td>yes</td>
</tr>
<tr>
<td>Autodiscover</td>
<td><code>/\^\/autodiscover.*/</code></td>
<td>yes</td>
</tr>
<tr>
<td>ECP</td>
<td><code>/\^\/ecp.*/</code></td>
<td>yes</td>
</tr>
<tr>
<td>EWS</td>
<td><code>/\^\/ews.*/</code></td>
<td>yes</td>
</tr>
<tr>
<td>OAB</td>
<td><code>/\^\/oab.*/</code></td>
<td>yes</td>
</tr>
<tr>
<td>PowerShell</td>
<td><code>/\^\/powershell.*/</code></td>
<td>yes</td>
</tr>
<tr>
<td>RPC</td>
<td><code>/\^\/rpc.*/</code></td>
<td>yes</td>
</tr>
<tr>
<td>Root</td>
<td><code>/\^\/$/</code></td>
<td>No</td>
</tr>
<tr>
<td>MAPI</td>
<td><code>/\^\/mapi.*/</code></td>
<td>yes</td>
</tr>
<tr>
<td>Authentication Proxy</td>
<td><code>/\^\/lm_auth_proxy*$/</code></td>
<td>yes</td>
</tr>
</tbody>
</table>

**Table 4-1: Content Rules**

### 4.1.2 HTTPS Offloading Using SubVSs

To set up HTTPS Offloading Using SubVSs, follow the steps below:

1. Select the **Add New** option within the **Virtual Services** section of the main menu tree.

![Figure 4-20: Virtual Service Parameters](image)
2. Enter a valid IP address in the **Virtual Address** text box.
3. Enter **443** as the **Port**.
4. Enter a recognizable **Service Name**, for example **Exchange 2013 HTTPS Offloaded**.
5. Click **Add this Virtual Service**.

Figure 4-21: SSL Properties

6. In the **SSL Properties** section, select the **Enabled** check box.
7. If desired, select the **Reencrypt** check box.

Figure 4-22: Standard Options

8. In the **Standard Options** section, enter **1800** in the **Idle Connection Timeout** text box and click **Set Idle Timeout**.
In the Advanced Properties section, complete the steps below:

a) Click Show Header Rules.
b) Select the Modify URL: Redirect_Root rule and click Add.

c) Click Back.
d) Select X-Forwarded-For in the Add HTTP Headers drop-down list.
e) Click the Add HTTP Redirector button.

If the Redirect Root content rule does not exist yet, refer to Section 4.1.1.3 to create it.

9. In the Advanced Properties section, complete the steps below:

a) Click Show Header Rules.
b) Select the Modify URL: Redirect_Root rule and click Add.

c) Click Back.
d) Select X-Forwarded-For in the Add HTTP Headers drop-down list.
e) Click the Add HTTP Redirector button.

10. In the Real Servers section, click the Add SubVS button.
11. A message stating that the SubVS has been created appears, click OK.

The Real Servers section should now be renamed to SubVSs.

The following steps deal with creating a SubVS for an Exchange service such as owa.

12. In the SubVSs section of the SubVS options page, click the Modify button next to the SubVS and select the following options:

Figure 4-24: Basic Properties
a) In the **SubVS Name** field enter a relevant name such as **owa**
b) In the **SubVS Type** field select the **HTTP/HTTPS** option

![ESP Options](image1)

**Figure 4-25: ESP Options**

13. Within the **ESP Options** section, ensure that the **Enable ESP** check box is not selected.

![Real Servers](image2)

**Figure 4-26: Real Servers**

14. In the **Real Servers** section of the SubVS options page select the following options:
   a) Enter `/owa/healthcheck.htm` in the **URL** field and click the **Set URL** button.
   b) Ensure the **Use HTTP/1.1** checkbox is deselected.
   c) Ensure that the **GET** option is selected from the **HTTP Method** drop-down list.

15. When finished editing the SubVS, click **Back**. Now you can add other SubVSs to this Virtual Service as needed.

16. Configure each SubVS using the settings in the table below.

<table>
<thead>
<tr>
<th>SubVS Name</th>
<th>Healthcheck URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>OWA (as in steps above)</td>
<td><code>/owa/healthcheck.htm</code></td>
</tr>
<tr>
<td>Autodiscover</td>
<td><code>/autodiscover/healthcheck.htm</code></td>
</tr>
<tr>
<td>ECP</td>
<td><code>/ecp/healthcheck.htm</code></td>
</tr>
<tr>
<td>EWS</td>
<td><code>/ews/healthcheck.htm</code></td>
</tr>
<tr>
<td>ActiveSync</td>
<td><code>/microsoft-server-activesync/healthcheck.htm</code></td>
</tr>
<tr>
<td>OAB</td>
<td><code>/oab/healthcheck.htm</code></td>
</tr>
<tr>
<td>Powershell</td>
<td><code>/powershell/healthcheck.htm</code></td>
</tr>
<tr>
<td>RPC</td>
<td><code>/rpc/healthcheck.htm</code></td>
</tr>
<tr>
<td>MAPI</td>
<td><code>/mapi/healthcheck.htm</code></td>
</tr>
</tbody>
</table>

**Table 2: SubVS Healthcheck URLs**
4.1.3 HTTPS Offloading Using ESP and SubVSs

To set up HTTPS Offloading Using ESP, follow the steps below:

1. Select the Add New option within the Virtual Services section of the main menu tree.

   ![Virtual Service parameters](image)

   **Figure 4-27: Virtual Service parameters**

2. Enter a valid IP address in the Virtual Address text box.
3. Enter 443 as the Port.
4. Enter a Service Name, for example Exchange 2013 HTTPS Offloading with ESP.
5. Click Add this Virtual Service.

   ![SSL Properties](image)

   **Figure 4-28: SSL Properties**

6. In the SSL Properties section, select Enabled.
7. If desired, select Reencrypt.
8. In the **Standard Options** section, enter **1800** in the **Idle Connection Timeout** text box and click **Set Idle Timeout**.

9. In the **Advanced Properties** section, complete the steps below:
   a) Click **Show Header Rules**.
   b) Select the **Modify URL: Redirect_Root** rule and click **Add**.

   **If the Redirect Root content rule does not exist yet, refer to Section 4.1.1.3 to create it.**

   c) Click **Back**.
   d) Select **X-Forwarded-For** in the **Add HTTP Headers** drop-down list.
   e) Click the **Add HTTP Redirector** button.

10. Now you need to add the SubVSs. To do this, expand the **Real Servers** section and click **Add SubVS**. Then click the **Modify** button to configure it.

    **Details for each of the SubVSs that need to be created are below.**
11. For each of the SubVSs created, ensure that in the ESP section, the Enable ESP checkbox is selected, and select the following options:
   a) Select the User Access, Security and Connection check boxes in ESP Logging.
   b) Select the relevant SSO Domain.
   c) Enter all of the allowed virtual hosts into the Allowed Virtual Hosts text box, for example mail.example.com, and click the Set Allowed Virtual Hosts button.
   d) Configure each SubVS using the settings in the table below.

<table>
<thead>
<tr>
<th>SubVS Name</th>
<th>Allowed Virtual Directories</th>
<th>Pre-Authorization Excluded Directories</th>
<th>Client Auth. mode</th>
<th>Server Auth. mode</th>
<th>SSO Image Set</th>
<th>SSO Greeting Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>Autodiscover</td>
<td>/autodiscover</td>
<td>None</td>
<td>None</td>
<td>None</td>
<td>n/a</td>
<td></td>
</tr>
<tr>
<td>ECP</td>
<td>/ecp*</td>
<td>Form Based</td>
<td>Basic Auth.</td>
<td>Exchange</td>
<td></td>
<td>Please enter your Exchange credentials.</td>
</tr>
<tr>
<td>EWS</td>
<td>/ews*</td>
<td>None</td>
<td>None</td>
<td>None</td>
<td>n/a</td>
<td></td>
</tr>
<tr>
<td>ActiveSync</td>
<td>/microsoft-server-activesync*</td>
<td>Basic Auth.</td>
<td>Basic Auth.</td>
<td>n/a</td>
<td></td>
<td></td>
</tr>
<tr>
<td>OAB</td>
<td>/oab*</td>
<td>None</td>
<td>None</td>
<td>None</td>
<td>n/a</td>
<td></td>
</tr>
<tr>
<td>Powershell</td>
<td>/powershell*</td>
<td>None</td>
<td>None</td>
<td>None</td>
<td>n/a</td>
<td></td>
</tr>
<tr>
<td>RPC</td>
<td>/rpc*</td>
<td>None</td>
<td>None</td>
<td>None</td>
<td>n/a</td>
<td></td>
</tr>
<tr>
<td>OWA</td>
<td>/owa/<a href="mailto:guid@smtpdomain">guid@smtpdomain</a>*1</td>
<td>Form Based</td>
<td>Basic Authentication</td>
<td>Exchange</td>
<td>Please enter your Exchange credentials.</td>
<td></td>
</tr>
<tr>
<td>MAPI</td>
<td>/mapi*</td>
<td>None</td>
<td>None</td>
<td>None</td>
<td>n/a</td>
<td></td>
</tr>
<tr>
<td>Authentication Proxy</td>
<td>*/</td>
<td>Form Based</td>
<td>Basic Authentication</td>
<td>Exchange</td>
<td>Please enter your Exchange credentials.</td>
<td></td>
</tr>
</tbody>
</table>

If you are using Kerberos Constrained Delegation (KCD) please ensure you add a Real Server to the Authentication Proxy SubVS. For further information on KCD, refer to the KCD, Feature Description

1 GUID is unique to each Exchange deployment. To find the correct GUID, run the following command on the Exchange Server:
The Logoff String must be set to `/owa/logoff.owa` in the OWA SubVS. In a customized environment, if the OWA logoff string has been changed, the modified logoff string must be entered in the Logoff String text box.

The SSO Greeting Message field accepts HTML code, so the users can insert their own or an image can be entered if desired. The grave accent character (``) is not supported. If this character is entered in the SSO Greeting Message, the character will not display in the output, for example `a` becomes `abc`.

For each of the SubVSs created, set the following options in the Real Servers section:

a) Enter 443 in the Checked Port text box and click Set Check Port.

b) Ensure the Use HTTP/1.1 check box is deselected.

c) Select GET as the HTTP Method.

d) Enter the relevant health check URL. Refer to Table 4-16 in Section 4.1.1.2 for the health check URLs.

13. After the SubVSs have been created, in the parent Virtual Service; enable Content Switching by clicking the Enable button in the Advanced Properties section.

### 4.2 IMAP Virtual Service

Follow the instructions below to set up an IMAP Virtual Service:

1. Select the Add New option within the Virtual Services section of the main menu tree.
2. Enter the IP address of the Virtual Service in the **Virtual Address** field.
3. Enter **143** in the **Port** field.
4. Type a name, for example **Exchange 2013 IMAP** in the **Service Name** field.
5. Select **tcp** in the **Protocol** drop-down list.
6. Click the **Add this Virtual Service** button to add the Virtual Service.

7. Within the **Basic Properties** section of the Virtual Services options page, select the following options:
   a) Select **Generic** in the **Service Type** drop-down list/

8. Within the **Standard Options** section of the Virtual Services options page, select the following options:
   a) Ensure the **Force L7** checkbox is selected.
   b) Remove the tick from the **Transparency** check box.
   c) Ensure that **IMAP4** is selected in **Server Initiating Protocols** drop-down list.
   d) Ensure that **none** is selected in the **Persistence Options** drop-down list.
e) Ensure that **round robin** is selected in the **Scheduling Method** drop-down list.

f) Enter **3600** in the **Idle Connection Timeout** text box and click **Set Idle Timeout**.

![Figure 4-35: SSL Properties](image)

9. Within the **SSL Properties** section, ensure that the **SSL Acceleration** checkbox is not selected.

![Figure 4-36: Advanced Properties](image)

10. Do not change any of the options within the **Advanced Options** section.

![Figure 4-37: Real Servers section](image)

11. Within the **Real Servers** section of the Virtual Services options page, select the following options:

a) Ensure that **Mailbox (IMAP) Protocol** has been selected as the health-checking option.

b) Enter **143** in the **Checked Port** field and click on the **Set Check Port** button.

### 4.2.1 IMAP STARTTLS Virtual Service

To configure the IMAP STARTTLS VS, follow the steps below:

1. Select the **Add New** option within the **Virtual Services** section of the main menu tree.

![Figure 4-38: Virtual Service Parameters](image)

2. Enter a **Virtual Address**.

3. Enter **143** as the **Port**.
4. Enter a recognizable **Service Name**, for example **Exchange 2013 IMAP with STARTTLS**.

![Basic Properties](image1)

**Figure 4-39: Basic Properties**

5. Within the **Basic Properties** section of the Virtual Services options page, select the following options:
   a) Select **STARTTLS protocols** in the **Service Type** drop-down list

![Standard Options](image2)

**Figure 4-40: Standard Options**

6. Within the **Standard Options** section of the Virtual Services options page, select the following options:
   a) Remove the tick from the **Transparency** check box.
   b) Ensure that **IMAP** is selected in the **STARTTLS mode** drop-down list.
   c) Enter **3600** in the **Idle Connection Timeout** field and click **Set Idle Timeout**.

![Real Servers](image3)

**Figure 4-41: Real Servers section**

7. In the **Real Servers** section, enter **143** in the **Checked Port** text box and click the **Set Check Port** button.

### 4.2.2 IMAPS Virtual Service

To configure the IMAPS VS, follow the steps below:

1. Select the **Add New** option within the **Virtual Services** section of the main menu tree.
2. Enter the IP address in the **Virtual Address** text box.
3. Enter **993** in the **Port** field.
4. Enter a recognizable **Service Name**, for example **Exchange 2013 IMAPS**.
5. Click **Add this Virtual Service**.

6. Within the **Standard Options** section of the Virtual Services options page:
   a) Remove the tick from the **Transparency** check box.
   b) Select **IMAP4** in the **Server Initiating Protocols** drop-down list.
   c) Enter **3600** in the **Idle Connection Timeout** field and click **Set Idle Timeout**.

7. Within the **Real Servers** section of the Virtual Services options page, select the following options:
   a) Ensure that **TCP Connection Only** has been selected as the health-checking option.
   b) Enter **993** in the **Checked Port** field and click on the **Set Check Port** button.
4.2.3 IMAPS Offloaded Virtual Service

To configure the IMAPS Offloaded, follow the steps below:

1. Select the **Add New** option within the **Virtual Services** section of the main menu tree.

```
Please Specify the Parameters for the Virtual Service.

Virtual Address: 10.11.0.196
Port: 993
Service Name (Optional): Exchange 2013 IMAPS
Use Template: Select a Template
Protocol: tcp

Figure 4-45: Virtual Service parameters
```

2. Enter the IP address of the Virtual Service in the **Virtual Address** field.
3. Enter **993** in the **Port** field.
4. Enter a recognizable **Service Name**, for example **Exchange 2013 IMAPS Offloaded**.

```
SSL Properties

SSL Acceleration: Enabled
Supported Protocols: TLSv1.3, TLSv1.2, SSLv3
Require SNI hostname: No

Available Certificates: None Available
Assigned Certificate: None Assigned

Manage Certificates

Cipher Set: Default
Assigned Ciphers: ECDHE-RSA-AES256-GCM-SHA384, ECDHE-ECDSA-AES256-GCM-SHA384

Ciphers

Client certificates: No Client Certificates required

Figure 4-46: SSL Properties
```

5. In the **SSL Properties** section, select the **SSL Acceleration - Enabled** check box.
6. Click **OK**.
7. Within the **Standard Options** section of the Virtual Services options page, set the following options:
   a) Remove the tick from the **Transparency** check box.
   b) Select **IMAP4** in the **Server Initiating Protocols** drop-down list.
   c) Enter **3600** in the **Idle Connection Timeout** field and click on the **Set Idle Timeout** button.

8. In the **Real Servers** section of the Virtual Services options page, select the following options:
   a) Ensure that **Mailbox (IMAP) Protocol** has been selected as the health-checking option.
   b) Enter **143** in the **Checked Port** text box and click **Set Check Port**.

### 4.3 POP Virtual Service

Follow the instructions below to set up a POP Virtual Service:

1. Select the **Add New** option within the **Virtual Services** section of the main menu tree.

   ![Virtual Service Parameters](image)

   **Figure 4-48: Virtual Service Parameters**

2. Enter the IP address of the Virtual Service in the **Virtual Address** field.
3. Enter **110** in the **Port** field.
4. Type a name, for example **Exchange 2013 POP** in the **Service Name** field.
5. Select **tcp** in the **Protocol** drop-down list.
6. Click the **Add this Virtual Service** button to add the Virtual Service.
Within the **Basic Properties** section of the Virtual Services options page, select the following options:

a) Select **Generic** in the **Service Type** drop-down list

Within the **Standard Options** section of the Virtual Services options page, select the following options:

a) Ensure the **Force L7** checkbox is selected.

b) Remove the tick from the **Transparency** check box.

c) Ensure that **POP3** is selected in **Server Initiating Protocols** drop-down list.

d) Ensure that **none** is selected in the **Persistence Options** drop-down list.

e) Ensure that **round robin** is selected in the **Scheduling Method** drop-down list.

f) Enter **3600** in the **Idle Connection Timeout** field and click **Set Idle Timeout**.

Within the **SSL Properties** section, ensure that the **SSL Acceleration** checkbox is not selected.

Do not change any of the options within the **Advanced Options** section.
11. Within the Real Servers section of the Virtual Services options page, select the following options:
   a) Ensure that Mailbox (POP3) Protocol has been selected as the health-checking option.
   b) Enter 110 in the Checked Port field and click on the Set Check Port button.

4.3.1 POP with STARTTLS Virtual Service

To configure a POP Virtual Service with STARTTLS, follow the steps below:

1. Select the Add New option within the Virtual Services section of the main menu tree.

2. Enter a valid IP address in the Virtual Address text box.
3. Enter 110 as the Port.
4. Enter a recognizable Service Name, for example Exchange 2013 POP with STARTTLS.
5. Click Add this Virtual Service.

6. Within the Basic Properties section of the Virtual Services options page, select the following options:
   a) Select STARTTLS protocols in the Service Type drop-down list.
7. Within the **Standard Options** section of the Virtual Services options page, select the following options:
   a) Remove the tick from the **Transparency** check box.
   b) Enter *3600* in the **Idle Connection Timeout** text box and click **Set Idle Timeout**.

8. In the **Real Servers** section, enter *110* in the **Checked Port** text box and click the **Set Check Port** button.

### 4.3.2 POPS Virtual Service

To configure a POPS VS, follow the steps below:

1. Select the **Add New** option within the **Virtual Services** section of the main menu tree.

2. Enter a valid IP address in the **Virtual Address** text box.
3. Enter *995* in the **Port** field.
4. Enter a recognizable **Service Name**, for example *Exchange 2013 POPS*. 
5. In the **Standard Options** section:
   a) Remove the tick from the **Transparency** check box.
   b) Select **POP3** in the **Server Initiating Protocols** drop-down list.
   c) Enter **3600** in the **Idle Connection Timeout** text box and click **Set Idle Timeout**.

6. Within the **Real Servers** section of the Virtual Services options page, enter **995** in the **Checked Port** field and click on the **Set Check Port** button.

### 4.3.3 POPS Offloaded Virtual Service

To configure a POPS Offloaded Virtual Service, follow the steps below:

1. Select the **Add New** option within the **Virtual Services** section of the main menu tree.

2. Enter a valid IP address in the **Virtual Address** text box.

3. Enter **995** in the **Port** field.

4. Enter a recognizable **Service Name**, for example **Exchange 2013 POPS Offloaded**.

5. Click **Add this Virtual Service**.
6. Within the **SSL Properties** section, select the **SSL Acceleration - Enabled** checkbox.

7. Click **OK**.

8. Within the **Standard Options** section of the Virtual Services options page:
   a) Remove the tick from the **Transparency** checkbox.
   b) Select **POP3** in the **Server Initiating Protocols** drop-down list.
   c) Enter **3600** in the **Idle Connection Timeout** text box and click **Set Idle Timeout**.
9. Within the **Real Servers** section:
   a) Set the **Real Server Check Parameters** drop-down list to **Mailbox (POP3) Protocol**.
   b) Enter **110** in the **Checked Port** text box and click **Set Check Port**.

4.4 **SMTP Virtual Service**

Follow the instructions below to set up an SMTP Virtual Service:

1. Select the **Add New** option within the **Virtual Services** section of the main menu tree.

![Figure 4-64: Virtual Service parameters](image)

2. Enter the IP address of the Virtual Service in the **Virtual Address** field.
3. Enter **25** in the **Port** field.
4. Type a name, for example **Exchange 2013 SMTP** in the **Service Name** field.
5. Select **tcp** in the **Protocol** drop-down list.
6. Click the **Add this Virtual Service** button to add the Virtual Service.

![Figure 4-65: Basic Properties](image)

7. Within the **Basic Properties** section of the Virtual Services options page, select the following options:
   a) Select **Generic** in the **Service Type** drop-down list
Within the **Standard Options** section of the Virtual Services options page, select the following options:

a) Ensure the **Force L7** checkbox is selected.
b) Remove the tick from the **Transparency** checkbox.
c) Ensure that **SMTP** is selected in **Server Initiating Protocols** drop-down list.
d) Select **Source IP Address** as the **Persistence Mode**.
e) Set the **Timeout** value to **1 Hour**.
f) Ensure that **round robin** is selected in the **Scheduling Method** drop-down list.
g) Enter **120** in the **Idle Connection Timeout** text box and click **Set Idle Timeout**.

Within the **SSL Properties** section, ensure that the **SSL Acceleration** check box is not selected.

Do not change any of the options within the **Advanced Options** section.

Within the **ESP Options** section, ensure that the **Enable ESP** checkbox is not selected.
12. Within the Real Servers section of the Virtual Services options page, select the following options:
   a) Ensure that Mailbox (SMTP) Protocol has been selected as the health-checking option.
   b) Enter 25 in the Checked Port field and click on the Set Check Port button.

4.4.1 SMTPS Virtual Service

To configure an SMTPS Virtual Service, follow the steps below:

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

   Please Specify the Parameters for the Virtual Service.

   - Virtual Address: Enter a valid IP address.
   - Port: Enter 587 as the Port.
   - Service Name (Optional): Enter a recognizable Service Name, for example Exchange 2013 SMTPS.
   - Protocol: Enter the Protocol as TCP.

2. Enter a valid IP address in the Virtual Address text box.
3. Enter 587 as the Port.
4. Enter a recognizable Service Name, for example Exchange 2013 SMTPS.
5. Click Add this Virtual Service.

   Figure 4-71: Virtual Service Parameters

   Standard Options

   - Force L7
   - Transparency
   - Subnet Originating Requests
   - Extra Ports
   - Server: Initiating Protocols
   - Persistence Options
     - Mode: Source IP Address
     - Timeout: 1 Hour
   - Scheduling Method: Round Robin
   - Idle Connection Timeout
   - Use Address for Server NAT
   - Quality of Service

   Figure 4-72: Standard Options
6. Within the **Standard Options** section, set the fields as follows:
   a) Remove the tick from the **Transparency** check box.
   b) Select **SMTP** from the **Server Initiating Protocols** drop-down list.
   c) Set the **Persistence Mode** to **Source IP Address**.
   d) Set the **Timeout** value to **1 Hour**.
   e) Enter **120** in the **Idle Connection Timeout** text box and click **Set Idle Timeout**.

![Figure 4-73: Real Servers section](image)

7. In the **Real Servers** section, enter **587** and click **Set Check Port**.

### 4.4.2 SMTPS Offloaded Virtual Service

To configure a SMTPS Offloaded Virtual Service, follow the steps below:

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

![Figure 4-74: Virtual Service Parameters](image)

2. Enter a valid IP address in the **Virtual Address** text box.
3. Enter **587** in the **Port** field.
4. Enter a recognizable **Service Name**, for example **Exchange 2013 SMTPS Offloaded**.
5. Click **Add this Virtual Service**.
6. Expand the **SSL Properties** section.
7. Select Enabled.
8. Click OK.

9. Within the **Standard Options** section of the Virtual Services options page, select the following options:
   a) Remove the tick from the **Transparency** check box.
   b) Select **SMTP** in the **Server Initiating Protocols** drop-down list.
   c) Select **Source IP Address** as the **Persistence Mode**.
   d) Select 1 Hour as the **Timeout** value.
   e) Enter 120 in the **Idle Connection Timeout** field and click **Set Idle Timeout**.

10. Within the **Real Servers** section of the Virtual Services options page:
   a) Select **Mail (SMTP) Protocol** as the health-checking option.
   b) Enter 25 in the **Checked Port** text box and click **Set Check Port**.
4.4.3  SMTP with STARTTLS Virtual Service

To configure a SMTP Virtual Service with STARTTLS, follow the steps below:

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

2. Enter a valid IP address in the Virtual Address text box.
3. Enter 25 as the Port.
4. Enter a recognizable Service Name, for example Exchange 2013 SMTP with STARTTLS.
5. Click Add this Virtual Service.

6. Within the Basic Properties section of the Virtual Services options page:
   a) Select STARTTLS protocols in the Service Type drop-down list.

7. Within the Standard Options section of the Virtual Services options page:
   a) Remove the tick from the Transparency check box.
b) Ensure that **SMTP (STARTTLS if requested)** is selected in the **STARTTLS mode** drop-down list.

c) Set the **Persistence Mode** to **Source IP Address**.

d) Set the **Timeout** value to **1 Hour**.

e) Enter **120** in the **Idle Connection Timeout** text box and click **Set Idle Timeout**.

---

8. In the **Real Servers** section:

a) Enter **25** in the **Checked Port** text box and click **Set Check Port**.

---

### 4.4.4 SMTP with ESP Virtual Service

To configure a **SMTP VS with ESP**, follow the steps below:

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

---

2. Enter a valid IP address in the **Virtual Address** text box.

3. Enter **25** as the **Port**.

4. Enter a recognizable **Service Name**, for example **Exchange 2013 SMTP with ESP**.

5. Click **Add this Virtual Service**.

---

6. Within the **ESP Options** section, select the following options:

   a) Ensure that the **Enable ESP** checkbox is selected.

   b) Ensure that the **Connection Logging** checkbox is selected.

   c) Enter the all the permitted domains that are allowed to be received by this service and click the **Set Permitted Domains** button.
7. Within the **Standard Options** section, set the fields as follows:
   a) Remove the tick from the **Transparency** check box.
   b) Ensure that **SMTP** is selected in the **Server Initiating Protocols** drop-down list.
   c) Set the **Persistence Mode** to **Source IP Address**.
   d) Set the **Timeout** value to **1 Hour**.
   e) Enter **120** in the **Idle Connection Timeout** text box and click **Set Idle Timeout**.

8. Within the **Real Servers** section, set the fields as follows:
   a) Enter **25** in the **Checked Port** text box and click **Set Check Port**.
References

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

- Web User Interface (WUI), Configuration Guide
- Virtual Services and Templates, Feature Description
- ESP, Feature Description
- Microsoft Exchange 2010, Deployment Guide
- Exchange Team Blog post on Load Balancing in Exchange 2013
- KCD, Feature Description
- View or configure Outlook Web App virtual directories
## Document History

<table>
<thead>
<tr>
<th>Date</th>
<th>Change</th>
<th>Reason for Change</th>
<th>Ver.</th>
<th>Resp.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dec 2015</td>
<td>Release updates</td>
<td>Updates for 7.1-32 release</td>
<td>5.0</td>
<td>LB</td>
</tr>
<tr>
<td>Jan 2016</td>
<td>Minor change</td>
<td>Updated Copyright Notices</td>
<td>6.0</td>
<td>LB</td>
</tr>
<tr>
<td>Feb 2016</td>
<td>Minor change</td>
<td>Defect resolved</td>
<td>7.0</td>
<td>KG</td>
</tr>
<tr>
<td>Mar 2016</td>
<td>Minor change</td>
<td>Enhancement made</td>
<td>8.0</td>
<td>LB</td>
</tr>
<tr>
<td>July 2016</td>
<td>Minor change</td>
<td>Enhancement made</td>
<td>9.0</td>
<td>LB</td>
</tr>
</tbody>
</table>