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 trademarks 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.
Table of Contents

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

1.1 Document Purpose .................................................................................................... 5

1.2 Intended Audience ................................................................................................... 5

1.3 Prerequisites ............................................................................................................. 6

2  SharePoint Templates .................................................................................................. 7

3  Configure the LoadMaster for SharePoint ..................................................................... 8

3.1 Two-Armed Configurations ....................................................................................... 8

3.2 Configure SharePoint 2010 Virtual Services .............................................................. 9

3.2.1 Configuring the User Portal Site Virtual Services for SharePoint 2010 .............. 9

3.2.2 Configuring the Central Administration Site Virtual Services for SharePoint 2010 .... 16

3.3 Configure SharePoint 2013 Virtual Services ............................................................. 24

3.3.1 Configuring the User Portal Site Virtual Services for SharePoint 2013 .......... 24

3.3.2 Configure the Central Administration Site Virtual Services for SharePoint 2013 .... 31

3.3.3 Configure a SharePoint 2013 HTTP and WAF Virtual Service ......................... 38

3.3.4 Configure a SharePoint 2013 HTTPS Re-encrypted and WAF Virtual Service .......... 40

3.4 Enabling the Edge Security Pack (ESP) with SharePoint ......................................... 43

References ....................................................................................................................... 44

Document History .......................................................................................................... 45
1 Introduction

Microsoft SharePoint is a web platform which provides many capabilities such as:

- Document management
- Version control
- File sharing
- Collaboration
- Social networking
- Enterprise search
- Business intelligence
- Workflow automation
- Website creation

A SharePoint Server Farm can include application servers and Web Front End (WFE) servers. The WFE server is used to handle requests from clients. If the WFE server is receiving a lot of requests it may be necessary to build multiple WFE servers and distribute the load amongst them. To provide resiliency and high performance, these WFEs should be load balanced.

The Office Web Apps (OWA) servers can also be managed and/or load balanced by using the LoadMaster. The SharePoint template and steps in this document provide options for both.

1.1 Document Purpose

The purpose of this document is to provide guidance on how to configure the KEMP LoadMaster for Microsoft SharePoint.

1.2 Intended Audience

This document is intended for use by anyone who is interested in learning about deploying a KEMP LoadMaster with SharePoint.
1.3 Prerequisites

It is assumed that if you are offloading SSL, an SSL certificate and key has already been obtained and installed on the LoadMaster. For help with SSL certificates, refer to the SSL Accelerated Services, Feature Description. It is also assumed that a working SharePoint environment has been installed.
2 SharePoint Templates

KEMP have developed a template containing our recommended settings for SharePoint 2010 and SharePoint 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, changes can be made to any of the Virtual Service settings after using the template.

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

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

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 each of the Virtual Services, refer to Section 3.
Configure the LoadMaster for SharePoint

To configure the LoadMaster for SharePoint, Virtual Services need to be set up:

- Some are for the Central Administration website which is used to administer the SharePoint configuration overall. When you install the first server, it is created. However, when you add more servers you have the choice as an administrator to create more instances so that you can make it Highly Available (HA).

- The other Virtual Services are for the User Portal Site. This is for access to MySites and the rest of the SharePoint infrastructure.

The sections below provide step-by-step instructions on how to manually set up 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, changes can be made to any of the Virtual Service settings after using the template. For more information on the SharePoint templates, refer to Section 2.

It may be possible to have a single Virtual Service for both that has extra ports, but you might want different settings on the different Virtual Services, or you might want one Virtual Service to be only accessible internally, for example.

The sections below give instructions on how to set up Virtual Services in both SharePoint 2010 and SharePoint 2013. Refer to the relevant sections for step-by-step instructions on configuring the Virtual Services, depending on your environment. The settings contained in this document are recommended by KEMP. However, your specific configuration may require different settings.

For more information on what each of the fields mean, refer to the Web User Interface (WUI), Configuration Guide.

3.1 Two-Armed Configurations

If you have a two-armed configuration with SSL offloading, you may need to enable subnet originating requests. This can either be done on a per-Virtual Service basis (Subnet Originating Requests field in Standard Options in the Virtual Service modify screen), or on a global basis (System Configuration > Miscellaneous Options > Network Options > Subnet Originating Requests).

It is recommended that the Subnet Originating Requests option is enabled on a per-Virtual Service basis.
3.2 Configure SharePoint 2010 Virtual Services

Refer to the sections below for instructions on how to set up the Virtual Services for SharePoint 2010. These Virtual Services are not all required – please configure the relevant Virtual Services, based on your environment.

3.2.1 Configuring the User Portal Site Virtual Services for SharePoint 2010

The sections below outline the steps on creating the User Portal Site Virtual Services for SharePoint 2010. Refer to the relevant sections below depending on your environment.

3.2.1.1 Configure a SharePoint 2010 HTTP Virtual Service

Follow the steps below to configure a SharePoint 2010 HTTP Virtual Service:

1. In the main menu of the LoadMaster Web User Interface (WUI), go to Virtual Services > Add New.

2. Enter a valid IP address in the Virtual Address text box.
3. Enter a recognizable Service Name, for example SharePoint 2010 HTTP.
4. Click Add this Virtual Service.
5. Expand the Standard Options section.

6. Remove the tick from the Transparency check box.
7. Set the Persistence Mode to Source IP Address.
8. Set the Timeout to 1 Hour.
3.2.1.2 Configure a SharePoint 2010 HTTPS Virtual Service

Follow the steps below to configure a SharePoint 2010 HTTPS Virtual Service:

1. In the main menu of the LoadMaster Web User Interface (WUI), go to Virtual Services > Add New.

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 SharePoint 2010 HTTPS.

5. Click Add this Virtual Service.
6. Remove the tick from the Transparency check box.
7. Set the Persistence Mode to Source IP Address.
8. Set the Timeout to 1 Hour.
9. Enter 900 in the Idle Connection Timeout text box and click Set Idle Timeout.
10. Expand the Advanced Properties section.

11. Click Add HTTP Redirector.

   It is optional to add a HTTP redirector Virtual Service. Whether you require one or not depends on your environment.

12. Expand the Real Servers section.

13. Enter a forward slash (/) in the URL text box and click Set URL.
14. Add any Real Servers as needed by clicking the Add New button and filling out the details.
3.2.1.3 Configure a SharePoint 2010 HTTPS Offloaded Virtual Service

Follow the steps below to configure a SharePoint 2010 HTTPS offloaded Virtual Service:

1. In the main menu of the LoadMaster Web User Interface (WUI), go to Virtual Services > Add New.

![Figure 3-8: Virtual Service parameters](image)

2. Enter a valid IP address in the Virtual Address text box.
3. Enter 443 in the Port text box.
4. Enter a recognizable Service Name, for example SharePoint 2010 HTTPS Offloaded.
5. Click Add this Virtual Service.
6. Expand the SSL Properties section.

![Figure 3-9: SSL Properties](image)

7. Select the Enabled check box.
8. Click OK to the pop-up message.
9. Expand the Standard Options section.
10. Remove the tick from the **Transparency** check box.
11. Select **Source IP Address** as the **Persistence Mode**.
12. Select **1 Hour** as the **Timeout**.
13. Enter **900** in the **Idle Connection Timeout** text box and click **Set Idle Timeout**.
14. Expand the **Advanced Properties** section.

15. Click the **Add HTTP Redirector** button.

   **It is optional to add a HTTP redirector Virtual Service. Whether you require one or not depends on your environment.**

16. Expand the **Real Server** section.
17. Enter a forward slash (/) in the URL text box and click Set URL.
18. Add any Real Servers as needed by clicking the Add New button and filling out the details.

3.2.1.4 Configure a SharePoint 2010 HTTPS Re-encrypt Virtual Service

Follow the steps below to configure a SharePoint 2010 HTTPS re-encrypt Virtual Service:

1. In the main menu of the LoadMaster Web User Interface (WUI), go to Virtual Services > Add New.

   ![Figure 3-13: Virtual Service parameters](image)

2. Enter a valid IP address in the Virtual Address text box.
3. Enter 443 in the Port text box.
4. Enter a recognizable Service Name, for example SharePoint 2010 HTTPS Re-encrypt.
5. Click Add this Virtual Service.
6. Expand the SSL Properties section.
Configure the LoadMaster for SharePoint

7. Tick the **Enabled** check box.
8. Click **OK** to the pop-up message.
9. Tick the **Reencrypt** check box.
10. Expand the **Standard Options** section.

11. Select **Source IP Address** as the **Persistence Mode**.
12. Select **1 Hour** as the **Timeout**.
13. Enter **900** in the **Idle Connection Timeout** text box and click **Set Idle Timeout**.
14. Expand the **Advanced Properties** section.
15. Click the **Add HTTP Redirector** button.
16. Expand the **Real Servers** section.

17. Enter a forward slash (/) in the **URL** text box and click **Set URL**.
18. Add any Real Servers as needed by clicking the **Add New** button and filling out the details.

### 3.2.2 Configuring the Central Administration Site Virtual Services for SharePoint 2010

The sections below outline the steps on creating the Central Administration Site Virtual Services for SharePoint 2010. Refer to the relevant sections below depending on your environment.

#### 3.2.2.1 Configure a SharePoint 2010 HTTP Central Administration Site Virtual Service

Follow the steps below to configure a SharePoint 2010 HTTP Central Administration Site Virtual Service:

1. In the main menu of the LoadMaster Web User Interface (WUI), go to **Virtual Services > Add New**.
2. Enter a valid IP address in the **Virtual Address** text box.
3. Enter **8000** in the **Port** text box.
4. Enter a recognizable **Service Name**, for example **SharePoint 2010 HTTP Central Administration Site**.
5. Click **Add this Virtual Service**.

![Virtual Service parameters](image)

**Figure 3-18: Virtual Service parameters**

6. Change the **Service Type** to **HTTP/HTTPS**.
7. Expand the **Standard Options** section.

![Basic Properties](image)

**Figure 3-19: Basic Properties**

![Standard Options](image)

**Figure 3-20: Standard Options**

8. Remove the tick from the **Transparency** check box.
9. Select **Source IP Address** as the **Persistence Mode**.
10. Select **1 Hour** as the **Timeout**.
11. Enter **900** in the **Idle Connection Timeout** text box and click **Set Idle Timeout**.
12. Expand the **Real Servers** section.
13. Select **HTTP Protocol** from the drop-down list.
14. Enter a forward slash (/) and click **Set URL**.
15. Add any Real Servers as needed by clicking the **Add New** button and filling out the details.

### 3.2.2.2 Configure a SharePoint 2010 HTTPS Central Administration Site Virtual Service

Follow the steps below to configure a SharePoint 2010 HTTPS Central Administration Site Virtual Service:

1. In the main menu of the LoadMaster Web User Interface (WUI), go to **Virtual Services > Add New**.

![Real Servers](image)

**Figure 3-21: Real Servers**

2. Enter a valid IP address in the **Virtual Address** text box.
3. Enter **8444** in the **Port** text box.
4. Enter a recognizable **Service Name**, for example **SharePoint 2010 HTTPS Central Administration**.
5. Click **Add this Virtual Service**.

![Virtual Service parameters](image)

**Figure 3-22: Virtual Service parameters**

6. Select **HTTP/HTTPS** as the **Service Type**.
7. Expand the **Standard Options** section.
8. Remove the tick from the Transparency check box.
9. Select Source IP Address as the Persistence Mode.
10. Select 1 Hour as the Timeout.
11. Enter 900 in the Idle Connection Timeout text box and click Set Idle Timeout.
12. Expand the Real Servers section.

13. Select HTTPS Protocol from the drop-down list.
14. Enter a forward slash (/) in the URL text box and click Set URL.
15. Add any Real Servers as needed by clicking the Add New button and filling out the details.

### 3.2.2.3 Configure a SharePoint 2010 HTTPS Offloaded Central Administration Site Virtual Service

Follow the steps below to configure a SharePoint 2010 HTTPS Offloaded Central Administration Site Virtual Service:

1. In the main menu of the LoadMaster Web User Interface (WUI), go to Virtual Services > Add New.
Configure the LoadMaster for SharePoint

Please Specify the Parameters for the Virtual Service.

<table>
<thead>
<tr>
<th>Virtual Address</th>
<th>10.154.11.43</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port</td>
<td>8444</td>
</tr>
<tr>
<td>Service Name</td>
<td>SharePoint 2010 HTTPS</td>
</tr>
<tr>
<td>Use Template</td>
<td>Select a Template</td>
</tr>
<tr>
<td>Protocol</td>
<td>tcp</td>
</tr>
</tbody>
</table>

Figure 3-26: Virtual Service parameters

2. Enter a valid IP address in the Virtual Address text box.
3. Enter 8444 as the Port.
4. Enter a recognizable Service Name, such as **SharePoint 2010 HTTPS Central Administration Site Offloaded**.
5. Click Add this Virtual Service.

![Basic Properties](image)

Figure 3-27: Basic Properties

6. Select **HTTP/HTTPS** as the Service Type.
7. Expand the SSL Properties section.

![SSL Properties](image)

Figure 3-28: SSL Properties

8. Select the Enabled check box.
9. Click OK to the pop-up message.
10. Expand the **Standard Options** section.

11. Remove the tick from the **Transparency** check box.
12. Select **Source IP Address** as the **Persistence Mode**.
13. Select **1 Hour** as the **Timeout**.
14. Enter **900** in the **Idle Connection Timeout** text box and click **Set Idle Timeout**.
15. Expand the **Real Servers** section.

16. Select **HTTP Protocol** from the first drop-down list.
17. Enter a forward slash (/) in the **URL** text box and click **Set URL**.
18. Add any Real Servers as needed by clicking the **Add New** button and filling out the details.

### 3.2.2.4 Configure a SharePoint 2010 HTTPS Re-encrypted Central Administration Site Virtual Service

Follow the steps below to configure a SharePoint 2010 HTTPS Re-encrypted Central Administration Site Virtual Service:

1. In the main menu of the LoadMaster Web User Interface (WUI), go to **Virtual Services > Add New**.
2. Enter a valid IP address in the **Virtual Address** text box.
3. Enter **8444** as the **Port**.
4. Enter a recognizable **Service Name**, such as **SharePoint 2010 HTTPS Central Administration Site Re-encrypted**.
5. Click **Add this Virtual Service**.

6. Select **HTTP/HTTPS** as the **Service Type**.
7. Expand the **SSL Properties** section.
8. Select the Enabled check box.
9. Click OK to the pop-up message.
10. Select the Reencrypt check box.
11. Expand the Standard Options section.

![Standard Options](image1)

- Select Source IP Address as the Persistence Mode.
- Select 1 Hour as the Timeout.
- Enter 900 in the Idle Connection Timeout text box and click Set Idle Timeout.
- Expand the Real Servers section.

![Real Servers](image2)

- Select HTTPS Protocol from the drop-down list.
- Enter a forward slash (/) in the URL text box and click Set URL.
- Add any Real Servers as needed by clicking the Add New button and filling out the details.
3.3 Configure SharePoint 2013 Virtual Services

Refer to the sections below for instructions on how to set up the Virtual Services for SharePoint 2013. These Virtual Services are not all required – please configure the relevant Virtual Services, based on your environment.

3.3.1 Configure the User Portal Site Virtual Services for SharePoint 2013

The sections below outline the steps on creating the User Portal Site Virtual Services for SharePoint 2013. Refer to the relevant sections below depending on your environment.

3.3.1.1 Configure a SharePoint 2013 HTTP Virtual Service

Follow the steps below to configure a SharePoint 2013 HTTP Virtual Service:

1. In the main menu of the LoadMaster Web User Interface (WUI), go to Virtual Services > Add New.

2. Enter a valid IP address in the Virtual Address text box.
3. Enter a recognizable Service Name, for example SharePoint 2013 HTTP.
4. Click Add this Virtual Service.
5. Expand the Standard Options section.

6. Remove the tick from the Transparency check box.
7. Enter 900 in the Idle Connection Timeout check box and click Set Idle Timeout.
8. Expand the Real Servers section.

---

**Figure 3-36: Virtual Service parameters**

<table>
<thead>
<tr>
<th>Virtual Address</th>
<th>10.154.11.43</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port</td>
<td>80</td>
</tr>
<tr>
<td>Service Name</td>
<td>SharePoint 2013 HTTP</td>
</tr>
<tr>
<td>Use Template</td>
<td>Select a Template</td>
</tr>
<tr>
<td>Protocol</td>
<td>tcp</td>
</tr>
</tbody>
</table>

**Figure 3-37: Standard Options**

<table>
<thead>
<tr>
<th>Persistence Options</th>
<th>Mode: None</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scheduling Method</td>
<td>round robin</td>
</tr>
<tr>
<td>Idle Connection Timeout</td>
<td>900</td>
</tr>
<tr>
<td>Quality of Service</td>
<td>Normal-Site</td>
</tr>
</tbody>
</table>
9. Enter a forward slash (/) in the URL text box and click Set URL.
10. Add any Real Servers as needed by clicking the Add New button and filling out the details.

### 3.3.1.2 Configure a SharePoint 2013 HTTPS Virtual Service

Follow the steps below to configure a SharePoint 2013 HTTPS Virtual Service:

1. In the main menu of the LoadMaster Web User Interface (WUI), go to Virtual Services > Add New.
2. Enter a valid IP address in the Virtual Address text box.
3. Enter 443 in the Port text box.
4. Enter a recognizable Service Name, for example SharePoint 2013 HTTPS.
5. Click Add this Virtual Service.
6. Expand the Standard Options section.
7. Remove the tick from the Transparency check box.
8. Enter 900 in the Idle Connection Timeout text box and click Set Idle Timeout.
9. Expand the Advanced Properties section.

![Advanced Properties](image)

Figure 3-41: Advanced Properties

10. Click Add HTTP Redirector.

It is optional to add a HTTP redirector Virtual Service. Whether you require one or not depends on your environment.

11. Expand the Real Servers section.

![Real Servers](image)

Figure 3-42: Real Servers section

12. Enter a forward slash (/) in the URL text box and click Set URL.
13. Add any Real Servers as needed by clicking the Add New button and filling out the details.

### 3.3.1.3 Configure a SharePoint 2013 HTTPS Offloaded Virtual Service

Follow the steps below to configure a SharePoint 2013 HTTPS Offloaded Virtual Service:

1. In the main menu of the LoadMaster Web User Interface (WUI), go to Virtual Services > Add New.
2. Enter a valid IP address in the **Virtual Address** text box.
3. Enter **443** in the **Port** text box.
4. Enter a recognizable **Service Name**, for example **SharePoint 2013 HTTPS Offloaded**.
5. Click **Add this Virtual Service**.
6. Expand the **SSL Properties** section.

7. Select the **Enabled** check box.
8. Click **OK** to the pop-up message.
9. Expand the **Standard Options** section.
10. Remove the tick from the **Transparency** check box.
11. Enter **900** in the **Idle Connection Timeout** text box and click **Set Idle Timeout**.
12. Expand the **Advanced Properties** section.

13. Click the **Add HTTP Redirector** button.

   **It is optional to add a HTTP redirector Virtual Service. Whether you require one or not depends on your environment.**

14. Expand the **Real Servers** section.
15. Enter a forward slash (/) in the **URL** text box and click **Set URL**.

16. Add any Real Servers as needed by clicking the **Add New** button and filling out the details.

### 3.3.1.4 Configure a SharePoint 2013 HTTPS Re-encrypt Virtual Service

Follow the steps below to configure a SharePoint 2013 HTTPS re-encrypt Virtual Service:

1. In the main menu of the LoadMaster Web User Interface (WUI), go to **Virtual Services > Add New**.

![Figure 3-48: Virtual Service parameters](image)

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

3. Enter **443** in the **Port** text box.

4. Enter a recognizable **Service Name**, for example **SharePoint 2013 HTTPS Re-encrypt**.

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

6. Expand the **SSL Properties** section.
7. Tick the Enabled check box.
8. Click OK to the pop-up message.
9. Tick the Reencrypt check box.
10. Expand the Standard Options section.

11. Enter 900 in the Idle Connection Timeout and click Set Idle Timeout.
12. Expand the Advanced Properties section.
Configure the LoadMaster for SharePoint

13. Click **Add HTTP Redirector**.
14. Expand the **Real Servers** section.

15. Enter a forward slash (/) in the **URL** text box and click **Set URL**.
16. Add any Real Servers as needed by clicking the **Add New** button and filling out the details.

3.3.2 Configure the Central Administration Site Virtual Services for SharePoint 2013

The sections below outline the steps on creating the Central Administration Site Virtual Services for SharePoint 2013. Refer to the relevant sections below depending on your environment.

3.3.2.1 Configure a SharePoint 2013 HTTP Central Administration Site Virtual Service

Follow the steps below to configure a SharePoint 2013 HTTP Central Administration Site Virtual Service:

1. In the main menu of the LoadMaster Web User Interface (WUI), go to **Virtual Services > Add New**.
2. Enter a valid IP address in the **Virtual Address** text box.
3. Enter **8000** in the **Port** text box.
4. Enter a recognizable **Service Name**, for example **SharePoint 2013 HTTP Central Administration Site**.
5. Click **Add this Virtual Service**.

![Figure 3-53: Virtual Service parameters](image)

6. Select **HTTP/HTTPS** as the **Service Type**.
7. Expand the **Standard Options** section.

![Figure 3-54: Basic Properties](image)

8. Remove the tick from the **Transparency** check box.
9. Enter **900** in the **Idle Connection Timeout** text box and click **Set Idle Timeout**.
10. Expand the **Real Servers** section.

![Figure 3-55: Standard Options](image)
11. Select **HTTP Protocol** from the drop-down list.
12. Enter a forward slash (/) in the **URL** text box and click **Set URL**.
13. Add any Real Servers as needed by clicking the **Add New** button and filling out the details.

### 3.3.2.2 Configure a SharePoint 2013 HTTPS Central Administration Site Virtual Service

Follow the steps below to configure a SharePoint 2013 HTTPS Central Administration Site Virtual Service:

1. In the main menu of the LoadMaster Web User Interface (WUI), go to **Virtual Services > Add New**.

2. Enter a valid IP address in the **Virtual Address** text box.
3. Enter **8444** in the **Port** text box.
4. Enter a recognizable **Service Name**, for example **SharePoint 2013 HTTPS Central Administration Site**.
5. Click **Add this Virtual Service**.

6. Select **HTTP/HTTPS** as the **Service Type**.
7. Expand the **Standard Options** section.

![Standard Options](image)

*Figure 3-59: Standard Options*

8. Remove the tick from the Transparency check box.
9. Enter **900** in the **Idle Connection Timeout** text box and click **Set Idle Timeout**.
10. Expand the **Real Servers** section.

![Real Servers](image)

*Figure 3-60: Real Servers*

11. Select **HTTPS Protocol** from the drop-down list.
12. Enter a forward slash (/) in the **URL** text box and click **Set URL**.
13. Add any Real Servers as needed by clicking the **Add New** button and filling out the details.

### 3.3.2.1 Configure a SharePoint 2013 HTTPS Offloaded Central Administration Site Virtual Service

Follow the steps below to configure a SharePoint 2013 HTTPS Offloaded Central Administration Site Virtual Service:

1. In the main menu of the LoadMaster Web User Interface (WUI), go to **Virtual Services > Add New**.
Configure the LoadMaster for SharePoint

2. Enter a valid IP address in the **Virtual Address** text box.
3. Enter **8444** in the **Port** text box.
4. Enter a recognizable **Service Name**, for example **SharePoint 2013 HTTPS Central Administration Site Offloaded**.
5. Click **Add this Virtual Service**.

6. Select **HTTP/HTTPS** as the **Service Type**.
7. Expand the **SSL Properties** section.

8. Select the **Enabled** check box.
9. Click **OK** to the pop-up message.
10. Expand the **Standard Options** section.

![Figure 3-64: Standard Options](image)

11. Remove the tick from the **Transparency** check box.
12. Enter **900** in the **Idle Connection Timeout** text box and click **Set Idle Timeout**.
13. Expand the **Real Servers** section.

![Figure 3-65: Real Servers](image)

14. Select **HTTP Protocol** from the drop-down list.
15. Enter a forward slash (/) in the **URL** text box and click **Set URL**.
16. Add any Real Servers as needed by clicking the **Add New** button and filling out the details.

### 3.3.2.2 Configure a SharePoint 2013 HTTPS Re-encrypted Central Administration Site Virtual Service

Follow the steps below to configure a SharePoint 2013 HTTPS Re-encrypted Central Administration Site Virtual Service:

1. In the main menu of the LoadMaster Web User Interface (WUI), go to **Virtual Services > Add New**.

![Figure 3-66: Virtual Service Parameters](image)
2. Enter a valid IP address in the **Virtual Address** text box.

3. Enter **8444** in the **Port** text box.

4. Enter a recognizable **Service Name**, for example **SharePoint 2013 HTTPS Central Administration Site Re-encrypted**.

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

6. Select **HTTP/HTTPS** as the **Service Type**.

7. Expand the **SSL Properties** section.

8. Select the **Enabled** check box.

9. Click **OK** to the pop-up message.

10. Select the **Reencrypt** check box.

11. Expand the **Standard Options** section.
Configure the LoadMaster for SharePoint

12. Enter 900 in the **Idle Connection Timeout** text box and click **Set Idle Timeout**.
13. Expand the **Real Servers** section.

14. Select **HTTPS Protocol** from the drop-down list.
15. Enter a forward slash (/) in the **URL** text box and click **Set URL**.
16. Add any Real Servers as needed by clicking the **Add New** button and filling out the details.

### 3.3.3 Configure a SharePoint 2013 HTTPS Virtual Service

Follow the steps below to configure a SharePoint 2013 HTTPS Re-encrypted Central Administration Site Virtual Service:

1. In the main menu of the LoadMaster Web User Interface (WUI), go to **Virtual Services > Add New**.
2. Enter a valid IP address in the **Virtual Address** text box.
3. Enter **80** as the **Port**.
4. Enter a **Service Name** such as **SharePoint 2013 HTTP and WAF**.
5. Click **Add this Virtual Service**.
6. Expand the **Standard Options** section.

![Figure 3-72: Standard Options](image)

7. Remove the tick from the **Transparency** check box.
8. Enter **900** in the **Idle Connection Timeout** text box and click **Set Idle Timeout**.
9. Expand the **WAF Options** section.

![Figure 3-73: WAF Options](image)

10. Tick the **Enabled** text box.
11. In the **Available Rulesets** box, tick the following rule sets:
    - owasp_protocol_violations
    - owasp_protocol_anomalies
    - owasp_bad_robots
    - owasp_generic_attacks
Configure a SharePoint 2013 HTTPS Re-encrypted and WAF Virtual Service

Follow the steps below to configure a SharePoint 2013 HTTPS Re-encrypted Central Administration Site Virtual Service:

1. In the main menu of the LoadMaster Web User Interface (WUI), go to **Virtual Services > Add New**.

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 **SharePoint 2013 HTTPS Re-encrypted and WAF**.

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

- **owasp_common_exceptions**
- **sharepoint_attacks**
  
  All rules should be ticked for each ruleset.

12. Click **Apply**.
13. Expand the **Real Servers** section.

14. Enter / in the **URL** text box and click **Set URL**.
15. Add any Real Servers as needed by clicking the **Add New** button and filling out the details.

![Real Servers section](image-url)

**Figure 3-74: Real Servers section**

![Virtual Service parameters](image-url)

**Figure 3-75: Virtual Service parameters**
6. Expand the **Standard Options** section.

![Figure 3-76: Standard Options](image)

7. Remove the tick from the **Transparency** check box.
8. Enter **900** in the **Idle Connection Timeout** text box and click **Set Idle Timeout**.
9. Expand the **SSL Properties** section.

![Figure 3-77: SSL Properties](image)

10. Tick the **Enabled** check box.
11. Tick the **Reencrypt** check box.
12. Click the **Add HTTP Redirector** button.

It is optional to add a HTTP redirector Virtual Service. Whether you require one or not depends on your environment.

13. Expand the **WAF Options** section.

14. Tick the **Enabled** check box.

15. In the **Available Rule sets** box, tick the following rule sets:
   - `owasp_protocol_violations`
   - `owasp_protocol_anomalies`
   - `owasp_bad_robots`
- `owasp_generic_attacks`
- `owasp_common_exceptions`
- `sharepoint_attacks`
  
  All rules should be ticked for each ruleset.

16. Click **Apply**.
17. Expand the **Real Servers** section.

![Real Servers section](image)

**Figure 3-80: Real Servers section**

18. Enter `/` in the **URL** text box and click **Set URL**.
19. Add any Real Servers as needed by clicking the **Add New** button and filling out the details.

3.4 **Enabling the Edge Security Pack (ESP) with SharePoint**

If desired, you can use ESP with SharePoint. To do this, follow the steps in the ESP, **Feature Description** but ensure to select either **Permanent Cookies Always** or **Permanent Cookies only on Private Computers** for the **Use Session or Permanent Cookies** option.

Selecting a permanent cookie option ensures that Office documents can be opened correctly from SharePoint.
References

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

- ESP, Feature Description
- Web User Interface (WUI), Configuration Guide
- IPsec Tunneling, Feature Description
- Virtual Services and Templates, Feature Description
- SSL Accelerated Services, Feature Description
<table>
<thead>
<tr>
<th>Date</th>
<th>Change</th>
<th>Reason for Change</th>
<th>Version</th>
<th>Resp.</th>
</tr>
</thead>
<tbody>
<tr>
<td>May 2014</td>
<td>Initial draft</td>
<td>First draft of document</td>
<td>1.0</td>
<td>LB</td>
</tr>
<tr>
<td>July 2014</td>
<td>Release updates</td>
<td>Updates for 7.1-18a release</td>
<td>1.1</td>
<td>LB</td>
</tr>
<tr>
<td>Apr 2015</td>
<td>Release updates</td>
<td>Updates for the 7.1-26 release</td>
<td>1.2</td>
<td>LB</td>
</tr>
<tr>
<td>June 2015</td>
<td>Major updates</td>
<td>Updates to reflect new templates</td>
<td>1.3</td>
<td>LB</td>
</tr>
<tr>
<td>July 2015</td>
<td>Major updates</td>
<td>Updates to reflect new templates</td>
<td>3.0</td>
<td>LB</td>
</tr>
<tr>
<td>Sep 2015</td>
<td>Release updates</td>
<td>Updates for the 7.1-30 release</td>
<td>4.0</td>
<td>LB</td>
</tr>
<tr>
<td>Dec 2015</td>
<td>Release updates</td>
<td>Updates for the 7.1-32 release</td>
<td>5.0</td>
<td>LB</td>
</tr>
<tr>
<td>Jan 2016</td>
<td>Minor updates</td>
<td>Updated Copyright Notices</td>
<td>6.0</td>
<td>LB</td>
</tr>
<tr>
<td>Mar 2016</td>
<td>Release updates</td>
<td>Updates for the 7.1-34 release</td>
<td>7.0</td>
<td>LB</td>
</tr>
<tr>
<td>July 2016</td>
<td>Minor updates</td>
<td>Enhancements made</td>
<td>8.0</td>
<td>LB</td>
</tr>
</tbody>
</table>