Copyright Notices

Copyright © 2002-2017 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 Document Purpose ................................................................................................................................. 5
   1.2 Intended Audience ................................................................................................................................. 5
   1.3 About this Document ............................................................................................................................. 5
2. **VMware Application Server Template** .................................................................................................. 6
3. **Architecture** ............................................................................................................................................... 7
4. **Horizon Protocols** .................................................................................................................................. 8
   4.1 Primary Horizon Protocol ....................................................................................................................... 8
   4.2 Secondary Horizon Protocols ................................................................................................................ 8
5. **Configure the LoadMaster** ...................................................................................................................... 9
   5.1 Enable Subnet Originating Requests Globally ....................................................................................... 9
   5.2 Enable Check Persist Globally ................................................................................................................ 10
6. **Session Affinity Options** ......................................................................................................................... 11
   6.1 Method 1 - Source IP Affinity ............................................................................................................... 11
      6.1.1 Create the VMware Access Point Source IP Affinity Virtual Services ........................................ 12
   6.2 Method 2 - Multiple Port Number Groups ........................................................................................... 15
      6.2.1 Create the VMware Access Point Multiple Port Number Groups Virtual Services ................... 17
   6.3 Method 3 - Multiple VIPs ..................................................................................................................... 26
      6.3.1 Create the Multiple VIPs Virtual Services ....................................................................................... 27

References ......................................................................................................................................................... 37

Document History ............................................................................................................................................. 38
1 Introduction

Access Point is a Unified Gateway from VMware that comes in virtual appliance format and is designed to protect desktop and application resources to enable remote access from the Internet. Access Point is the default gateway for the following products:

- VMware Horizon View
- VMware Horizon Air (DaaS)
- VMware Horizon Air Hybrid-Mode
- VMware Identity Manager
- Airwatch Tunnel Gateway/Proxy

The KEMP LoadMaster is used to load balance the VMware Access Point workload. The LoadMaster offers advanced Layer 4 and Layer 7 server load balancing, SSL Acceleration and a multitude of other advanced Application Delivery Controller (ADC) features. The LoadMaster intelligently and efficiently distributes user traffic among the application servers so that users get the best experience possible.

1.1 Document Purpose

This document provides the recommended LoadMaster settings used when load balancing the VMware Access Point workload for the Horizon View and Horizon Air Hybrid-Mode use cases. The KEMP Support Team is available to provide solutions for scenarios not explicitly defined. The KEMP support site can be found at: https://support.kemptechnologies.com

1.2 Intended Audience

This document is intended to be read by anyone who is interested in configuring the LoadMaster to optimize VMware Access Point Server.

1.3 About this Document

This document was written with help from Mark Benson and Vish Kalsi of VMware. Some of the content in this document is based on the following VMware document:

https://communities.vmware.com/docs/DOC-32792

In addition, you can find more information at https://www.vmware.com/support/pubs/access-point-pubs.html
2 VMware Application Server Template

KEMP has developed a template containing our recommended settings for VMware. You can install this template on the LoadMaster and use it when creating Virtual Services. Using a template automatically populates the settings in the Virtual Services, which 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 template.

Download released templates from the Templates section on the KEMP documentation page: http://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 each of the Virtual Services, refer to Section 5 of this document.
3 Architecture

Access Point is typically deployed in a DMZ. For high availability and scalability requirements in a production deployment, several Access Point appliances are usually set up behind a load balancer as shown in Figure 3-1. The LoadMaster is deployed in-line as a proxy for all services including PCoIP. Alternative deployment options could have the secondary Horizon protocols bypass the LoadMaster as it is only the initial session establishment (HTTPS) that can be load balanced.

This deployment guide focuses on the load balancing requirements for the Horizon View and Horizon Air Hybrid-Mode use cases. It discusses the distinction between the primary and secondary Horizon protocols and describes the three methods for guaranteeing session affinity. The three methods ensure that all protocol traffic from a Horizon client session goes to the same Access Point appliance. This article also covers health monitoring and SSL offload/SSL bridging for load balancers.
4 Horizon Protocols

When a Horizon Client user connects to a Horizon environment, several different protocols are used. The first connection is always the primary XML-API protocol over HTTPS. Following successful authentication, one or more secondary protocols are also made.

4.1 Primary Horizon Protocol

The user enters a hostname at the Horizon Client and this starts the primary Horizon protocol. This is a control protocol for authentication, authorization and session management. It uses XML-structured messages over HTTPS (HTTP over SSL). This protocol is sometimes known as the Horizon XML-API control protocol. In a load-balanced environment as shown in Section 3, the load balancer routes this connection to one of the Access Point appliances. The load balancer usually selects the appliance based first on availability, and then out of the available appliances will route traffic based on the least number of current sessions. This has the effect of evenly distributing the traffic from different clients across the available set of Access Point appliances.

4.2 Secondary Horizon Protocols

After the Horizon Client has established a secure communication to one of the Access Point appliances, the user authenticates. If this authentication attempt is successful, then one or more secondary connections are made from the Horizon client. These secondary connections can include:

- HTTPS Tunnel used for encapsulating TCP protocols such as RDP, MMR/CDR and the client framework channel (TCP 443).
- Blast Extreme display protocol (TCP 443 and UDP 443).
- PCoIP display protocol (TCP 4172 and UDP 4172).

These secondary Horizon protocols must be routed to the same Access Point appliance to which the primary Horizon protocol is routed. This is so that Access Point can authorize the secondary protocols based on the authenticated user session. An important security capability of Access Point is that it will only forward traffic into the corporate datacenter if the traffic is on behalf of an authenticated user. If the secondary protocols were to be misrouted to a different Access Point appliance to the primary protocol one, they would not be authorized and would therefore be dropped in the DMZ and the connection would fail. Misrouting the secondary protocols is a common problem if the Load Balancer is not configured correctly.
5 Configure the LoadMaster

The deployed VMware Access Point environment determines which of the following setups is used.

5.1 Enable Subnet Originating Requests Globally

It is best practice to enable the Subnet Originating Requests option globally.

In a one-armed setup (where the Virtual Service and Real Servers are on the same network/subnet), Subnet Originating Requests is usually not needed. However, enabling Subnet Originating Requests should not affect the routing in a one-armed setup.

In a two-armed setup where the Virtual Service is on network/subnet A, for example, and the Real Servers are on network B, Subnet Originating Requests should be enabled on LoadMasters with firmware version 7.1-16 and above.

When Subnet Originating Requests is enabled, the LoadMaster routes traffic so that the Real Server sees traffic arriving from the LoadMaster interface that is in that network/subnet.

When Subnet Originating Requests is enabled globally, it is automatically enabled on all Virtual Services. If the Subnet Originating Requests option is disabled globally, you can select whether or not to enable Subnet Originating Requests on a per-Virtual Service basis.

To enable Subnet Originating Requests globally, follow the steps below:

1. In the main menu of the LoadMaster WUI, go to System Configuration > Miscellaneous Options > Network Options.

![Figure 5-1: Subnet Originating Requests](image)

2. Select the Subnet Originating Requests check box.
5.2 Enable Check Persist Globally

It is recommended that you change the **Always Check Persist** option to **Yes – Accept Changes**. Use the following steps:

1. Go to **System Configuration > Miscellaneous Options > L7 Configuration**.

   ![Figure 5-2: Enable Check Persist Globally](image)

2. Click the **Always Check Persist** dropdown arrow and select **Yes – Accept Changes**.
6 Session Affinity Options

There are three main configuration options for session affinity. These are:

- Source IP Affinity
- Multiple Port Number Groups
- Multiple VIPs

6.1 Method 1 - Source IP Affinity

Method 1 is recommended for all environments where source IP address affinity is possible. Where it is not possible, then either method 2 or method 3 should be used.

Method 1 is the simplest configuration for a load balancer because it uses standard port numbers and a single load balanced VIP. It relies on the load balancer to route secondary protocols to the same Access Point appliance as was selected for the primary Horizon protocol. It does this on the basis of repeat connections coming from the same Horizon client IP address. Unfortunately, this method does not work in all situations. For example, with certain Network Service Providers or NAT devices, the source IP address is not available for this affinity configuration. If source IP affinity cannot be used in your environment, then one of the other two methods should be used as they do not rely on source IP affinity.

Access Point Configuration for External URLs for this configuration is shown in the following table. In our example, the Fully Qualified Domain Name (FQDN) http://ap.myco.com resolves to 10.1.160.35.

<table>
<thead>
<tr>
<th>Access Point Appliance</th>
<th>Configuration Item</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>AP01</td>
<td>tunnelExternalURL</td>
<td><a href="https://ap.myco.com:443">https://ap.myco.com:443</a></td>
</tr>
<tr>
<td>AP01</td>
<td>blastExternalURL</td>
<td><a href="https://ap.myco.com:443">https://ap.myco.com:443</a></td>
</tr>
<tr>
<td>AP01</td>
<td>pcoipExternalURL</td>
<td>10.1.160.35:4172</td>
</tr>
<tr>
<td>AP02</td>
<td>tunnelExternalURL</td>
<td><a href="https://ap.myco.com:443">https://ap.myco.com:443</a></td>
</tr>
<tr>
<td>AP02</td>
<td>blastExternalURL</td>
<td><a href="https://ap.myco.com:443">https://ap.myco.com:443</a></td>
</tr>
<tr>
<td>AP02</td>
<td>pcoipExternalURL</td>
<td>10.1.160.35:4172</td>
</tr>
</tbody>
</table>

Table 6-1: Access Point Configuration for External URLs

Advantages of Source IP Affinity

- Uses standard port numbers
- Does not require multiple public virtual IP addresses

Disadvantages of Source IP Affinity

- Relies on source IP address affinity, which is not always possible.
6.1.1 Create the VMware Access Point Source IP Affinity Virtual Services

The following sections describe the recommended settings for the VMware Access Point Source IP Affinity Virtual Services.

6.1.1.1 Create a APLB TCP-IP Affinity Virtual Service

The following are the steps involved and the recommended settings to configure the APLB TCP-IP Affinity HTTP Virtual Service:

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

   ![Figure 6-1: Virtual Service parameters](image)

2. Type a valid Virtual Address.
3. Type 443 as the Port.
4. Enter a recognizable Service Name, such as APLB TCP-IP Affinity.
5. Click Add this Virtual Service.
6. Configure the settings as recommended in the following table:

<table>
<thead>
<tr>
<th>Section</th>
<th>Option</th>
<th>Value</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Standard Options</td>
<td>Extra Ports</td>
<td>4172</td>
<td>Click Set Extra Ports.</td>
</tr>
<tr>
<td></td>
<td>Persistence Mode</td>
<td>Source IP Address</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Timeout</td>
<td>6 minutes</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Scheduling Method</td>
<td>least connection</td>
<td></td>
</tr>
<tr>
<td>Advanced Properties</td>
<td>Add a Port 80 Redirector VS</td>
<td></td>
<td>Click the Add HTTP Redirector button. This automatically creates a redirect on port 80.</td>
</tr>
<tr>
<td>Real Servers</td>
<td>Real Server Check Method</td>
<td>HTTPS Protocol</td>
<td></td>
</tr>
<tr>
<td></td>
<td>URL</td>
<td>/favicon.ico</td>
<td></td>
</tr>
</tbody>
</table>

   Table 6-2: APLB TCP-IP Affinity Recommended Settings

7. Add the Real Servers:
   a) Expand the Real Servers section.
b) Click Add New.
c) Type the address of the relevant Real Server.
d) Complete the other fields as required.
e) Click Add this Real Server then click OK to the pop-up message.
f) Repeat the steps above to add more Real Servers as needed, based on your environment.

Create an APLB TCP-IP Affinity HTTPS HTTP Redirect Virtual Service

Clicking the Add HTTP Redirector button automatically creates a port 80 redirect Virtual Service. This is optional, but the purpose of this Virtual Service is to redirect any clients who have connected using HTTP to the HTTPS Virtual Service.

6.1.1.2 Create an APLB UDP 443 Affinity Virtual Service

The following are the steps involved and the recommended settings to configure the APLB UDP 443 Affinity Virtual Service:

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

   Please Specify the Parameters for the Virtual Service.

   | Virtual Address | 10.1.160.35 |
   | Port | 443 |
   | Service Name (Optional) | APLB UDP 443 - IP Aff |
   | Use Template | Select a Template |
   | Protocol | udp |

   Figure 6-2: Virtual Service parameters

2. Type a valid Virtual Address.
3. Type 443 as the Port.
4. Enter a recognizable Service Name, such as APLB UDP 443 Affinity.
5. Select udp as the Protocol.
6. Click Add this Virtual Service.

7. Configure the settings as recommended in the following table:

<table>
<thead>
<tr>
<th>Section</th>
<th>Option</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Standard Options</td>
<td>Force L4</td>
<td>Disabled</td>
</tr>
<tr>
<td></td>
<td>Persistence Mode</td>
<td>Source IP Address</td>
</tr>
<tr>
<td></td>
<td>Timeout</td>
<td>6 minutes</td>
</tr>
</tbody>
</table>
8. Add the Real Servers:
   a) Expand the Real Servers section.
   b) Click Add New.
   c) Type the address of the relevant Real Server.
   d) Complete the other fields as required.
   e) Click Add this Real Server then click OK to the pop-up message.
   f) Repeat the steps above to add more Real Servers as needed, based on your environment.

### 6.1.1.3 Create an APLB - UDP 4172 - Affinity Virtual Service

The following are the steps involved and the recommended settings to configure the APLB - UDP 4172 - Affinity Virtual Service:

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

   ![Image of Virtual Service parameters]

   **Figure 6-3: Virtual Service parameters**

   2. Type a valid Virtual Address.
   3. Type 4172 as the Port.
   4. Enter a recognizable Service Name, such as APLB - UDP 4172.
   5. Select udp as the Protocol.
   6. Click Add this Virtual Service.
   7. Configure the settings as recommended in the following table:

<table>
<thead>
<tr>
<th>Section</th>
<th>Option</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Advanced</td>
<td>Port Following</td>
<td>tcp/10.1.160.35:443</td>
</tr>
<tr>
<td>Real Servers</td>
<td>Real Server Check Method</td>
<td>ICMP Ping</td>
</tr>
</tbody>
</table>

Table 6-3: APLB UDP 443 Affinity Recommended Settings
8. Add the Real Servers:
   a) Expand the Real Servers section.
   b) Click Add New.
   c) Type the address of the relevant Real Server.
   d) Complete the other fields as required.
   e) Click Add this Real Server then click OK to the pop-up message.
   f) Repeat the steps above to add more Real Servers as needed, based on your environment.

6.2 Method 2 - Multiple Port Number Groups

Multiple port group affinity does not rely on source IP address for affinity. Instead, the load balancer is configured to route the secondary Horizon protocols based on a group of unique port numbers assigned to each Access Point appliance. The primary Horizon protocol on HTTPS port 443 is load balanced to allocate the session to a specific Access Point appliance based on health and least loaded. The secondary connections are then routed to the correct Access Point appliance based on the following Load Balancer configuration table.

<table>
<thead>
<tr>
<th>Virtual IP Address</th>
<th>Primary/Secondary</th>
<th>Protocol</th>
<th>Name</th>
<th>Real Servers</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.1.160.31:443</td>
<td>Primary</td>
<td>TCP</td>
<td>APLB - HTTPS</td>
<td>10.1.160.183:443</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>10.1.160.184:443</td>
</tr>
<tr>
<td>10.1.160.31:10143</td>
<td>Secondary</td>
<td>TCP</td>
<td>AP01 - HTTPS</td>
<td>10.1.160.183:443</td>
</tr>
<tr>
<td>10.1.160.31:10172</td>
<td>Secondary</td>
<td>TCP</td>
<td>AP01 - PCOIP</td>
<td>10.1.160.183:4172</td>
</tr>
<tr>
<td>10.1.160.31:10243</td>
<td>Secondary</td>
<td>TCP</td>
<td>AP02 - HTTPS</td>
<td>10.1.160.184:443</td>
</tr>
</tbody>
</table>
Virtual IP Address | Primary/Secondary | Protocol | Name | Real Servers
--- | --- | --- | --- | ---
10.1.160.31:10243 | Secondary | UDP | AP02 - BLAST-UDP | 10.1.160.184:443
10.1.160.31:10272 | Secondary | TCP | AP02 - PCOIP | 10.1.160.184:4172

Table 6-5: Load Balancer Configuration Table

The same port mapping scheme can be used for additional Access Point appliances 03 > 99. For example, we use the following mapping convention in this document for two access points:

- 10143 → AP01 443
- 10172 → AP01 4172
- 10243 → AP02 443
- 10272 → AP02 4172

The same convention is used for multiple access points:

- 10343 → AP03 443
- 10372 → AP03 4172

The Access Point Configuration for External URLs is shown below.

In our example, the FQDN http://ap.myco.com resolves to 10.1.160.31.

<table>
<thead>
<tr>
<th>Access Point Appliance</th>
<th>Configuration Item</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>AP01</td>
<td>tunnelExternalURL</td>
<td><a href="https://ap.myco.com:10143">https://ap.myco.com:10143</a></td>
</tr>
<tr>
<td>AP01</td>
<td>blastExternalURL</td>
<td><a href="https://ap.myco.com:10143">https://ap.myco.com:10143</a></td>
</tr>
<tr>
<td>AP01</td>
<td>pcoipExternalURL</td>
<td>10.1.60.31:10172</td>
</tr>
<tr>
<td>AP02</td>
<td>tunnelExternalURL</td>
<td><a href="https://ap.myco.com:10243">https://ap.myco.com:10243</a></td>
</tr>
<tr>
<td>AP02</td>
<td>blastExternalURL</td>
<td><a href="https://ap.myco.com:10243">https://ap.myco.com:10243</a></td>
</tr>
<tr>
<td>AP02</td>
<td>pcoipExternalURL</td>
<td>10.1.60.31:10272</td>
</tr>
</tbody>
</table>

Table 6-6: Access Point Configuration for External URLs

Advantages of Multiple Port Number Groups

- Does not rely on source IP affinity
Does not require multiple public virtual IP addresses

Disadvantages of Multiple Port Number Groups

- Uses non-standard port numbers from the Internet although the port numbers on the Access Point appliances themselves are standard.

6.2.1 Create the VMware Access Point Multiple Port Number Groups Virtual Services

The following sections describe the recommended settings for the VMware Access Point Multiple Port Number Groups Virtual Services.

6.2.1.1 Create a APLB – HTTPS – Multiple Ports Virtual Service

The following are the steps involved and the recommended settings to configure the APLB – HTTPS – Multiple Ports Virtual Service:

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

![Figure 6-4: Virtual Service parameters](image)

2. Type a valid Virtual Address.
3. Type 443 as the Port.
4. Enter a recognizable Service Name, such as APLB – HTTPS Multiple Ports.
5. Click Add this Virtual Service.
6. Configure the settings as recommended in the following table:

<table>
<thead>
<tr>
<th>Section</th>
<th>Option</th>
<th>Value</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Advanced Properties</td>
<td>Add a Port 80 Redirector VS</td>
<td></td>
<td>Click the Add HTTP Redirector button. This automatically creates a redirect on port 80.</td>
</tr>
<tr>
<td>Basic Properties</td>
<td>Service Type</td>
<td>Generic</td>
<td></td>
</tr>
<tr>
<td>Standard Options</td>
<td>Persistence Mode</td>
<td>SSL Session ID</td>
<td></td>
</tr>
<tr>
<td>Section</td>
<td>Option</td>
<td>Value</td>
<td>Comment</td>
</tr>
<tr>
<td>------------</td>
<td>----------------------------------</td>
<td>------------------------</td>
<td>--------------------------------</td>
</tr>
<tr>
<td></td>
<td>Timeout</td>
<td>6 minutes</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Scheduling Method</td>
<td>least connection</td>
<td></td>
</tr>
<tr>
<td>Real Servers</td>
<td>Real Server Check Method</td>
<td>HTTPS Protocol</td>
<td></td>
</tr>
<tr>
<td></td>
<td>URL</td>
<td>/favicon.ico</td>
<td></td>
</tr>
</tbody>
</table>

Table 6-7: APLB – HTTPS – Multiple Ports Recommended Settings

7. Add the Real Servers:
   a) Expand the **Real Servers** section.
   b) Click **Add New**.
   c) Type the address of the relevant Real Server.
   d) Type 443 as the port number.
   e) Complete the other fields as required.
   f) Click **Add this Real Server** then click **OK** to the pop-up message.
   g) Repeat the steps above to add more Real Servers as needed, based on your environment.

Create an APLB – HTTPS – Multiple Ports HTTPS HTTP Redirect Virtual Service

Clicking the **Add HTTP Redirector** button automatically creates a port 80 redirect Virtual Service. This is optional, but the purpose of this Virtual Service is to redirect any clients who have connected using HTTP to the HTTPS Virtual Service.

6.2.1.2 Create an AP01 – HTTPS – Multiple Ports Virtual Service

The following are the steps involved and the recommended settings to configure the AP01 – HTTPS – Multiple Ports Virtual Service:

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

   ![Please Specify the Parameters for the Virtual Service](image)

2. Type a valid **Virtual Address**.
3. Type **10143** as the **Port**.
4. Enter a recognizable **Service Name**, such as **AP01 – HTTPS – Multiple Ports**.
5. Click **Add this Virtual Service**.
6. Configure the settings as recommended in the following table:

<table>
<thead>
<tr>
<th>Section</th>
<th>Option</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Basic Properties</td>
<td>Service Type</td>
<td>HTTP/HTTPS</td>
</tr>
<tr>
<td>Standard Options</td>
<td>Force L4</td>
<td>Disabled</td>
</tr>
<tr>
<td>Real Servers</td>
<td>Real Server Check Method</td>
<td>HTTPS Protocol</td>
</tr>
<tr>
<td></td>
<td>Checked Port</td>
<td>443</td>
</tr>
<tr>
<td></td>
<td>URL</td>
<td>/favicon.ico</td>
</tr>
</tbody>
</table>

Table 6-8: AP01 – HTTPS – Multiple Ports Recommended Settings

7. Add the Real Servers:
   a) Expand the Real Servers section.
   b) Click Add New.
   c) Type the address of the relevant Real Server.
   d) Type 443 as the port number.
   e) Complete the other fields as required.
   f) Click Add this Real Server then click OK to the pop-up message.
   g) Repeat the steps above to add more Real Servers as needed, based on your environment.

6.2.1.3 Create an AP01 – BLAST-UDP Multiple Ports Virtual Service

The following are the steps involved and the recommended settings to configure the AP01 – Blast-UDP Multiple Ports Virtual Service:

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

![Figure 6-6: Virtual Service parameters](image)

2. Type a valid Virtual Address.
3. Type 10143 as the Port.
4. Enter a recognizable Service Name, such as AP01 – BLAST-UDP Multiple Ports.
   Select udp as the Protocol.
5. Click Add this Virtual Service.
6. Configure the settings as recommended in the following table:

<table>
<thead>
<tr>
<th>Section</th>
<th>Option</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Standard Options</td>
<td>Force L4</td>
<td>Disabled</td>
</tr>
<tr>
<td>Real Servers</td>
<td>Real Server Check Method</td>
<td>ICMP Ping</td>
</tr>
</tbody>
</table>

Table 6-9: AP01 – BLAST-UDP Multiple Ports Recommended Settings

7. Add the Real Servers:
   a) Expand the Real Servers section.
   b) Click Add New.
   c) Type the address of the relevant Real Server.
   d) Type 443 as the Port.
   e) Complete the other fields as required.
   f) Click Add this Real Server then click OK to the pop-up message.
   g) Repeat the steps above to add more Real Servers as needed, based on your environment.

6.2.1.4 Create an AP01 – PCOIP Multiple Ports Virtual Service

The following are the steps involved and the recommended settings to configure the AP01 – PCOIP Multiple Ports Virtual Service:

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

2. Type a valid Virtual Address.
3. Type 10172 as the Port.
4. Enter a recognizable Service Name, such as AP01 – PCOIP Multiple Ports.
5. Click Add this Virtual Service.
6. Configure the settings as recommended in the following table:

<table>
<thead>
<tr>
<th>Section</th>
<th>Option</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Standard Options</td>
<td>Force L4</td>
<td>Disabled</td>
</tr>
<tr>
<td>Real Servers</td>
<td>Checked Port</td>
<td>4172</td>
</tr>
</tbody>
</table>

Table 6-10: AP01 – PCOIP Multiple Ports Recommended Settings
7. Add the Real Servers:
   a) Expand the Real Servers section.
   b) Click Add New.
   c) Type the address of the relevant Real Server.
   d) Type 4172 as the Port.
   e) Complete the other fields as required.
   f) Click Add this Real Server then click OK to the pop-up message.
   g) Repeat the steps above to add more Real Servers as needed, based on your environment.

6.2.1.5 Create an AP01 – PCOIP-UDP Multiple Ports Virtual Service

The following are the steps involved and the recommended settings to configure the AP01 – PCOIP-UDP Multiple Ports Virtual Service:

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

   ![Virtual Service parameters](image)

   **Figure 6-8: Virtual Service parameters**

2. Type a valid Virtual Address.
3. Type 10172 as the Port.
4. Enter a recognizable Service Name, such as AP01 – PCOIP-UDP.
5. Select udp as the Protocol.
6. Click Add this Virtual Service.
7. Configure the settings as recommended in the following table:

<table>
<thead>
<tr>
<th>Section</th>
<th>Option</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Standard Options</td>
<td>Force L4</td>
<td>Disabled</td>
</tr>
<tr>
<td>Real Servers</td>
<td>Real Server Check Method</td>
<td>ICMP Ping</td>
</tr>
</tbody>
</table>

   **Table 6-11: AP01 – PCOIP-UDP Multiple Ports Recommended Settings**

8. Add the Real Servers:
   a) Expand the Real Servers section.
   b) Click Add New.
   c) Type the address of the relevant Real Server.
d) Type 4172 as the Port.
e) Complete the other fields as required.
f) Click Add this Real Server then click OK to the pop-up message.
g) Repeat the steps above to add more Real Servers as needed, based on your environment.

6.2.1.6 Create an AP02 – HTTPS Multiple Ports Virtual Service

The following are the steps involved and the recommended settings to configure the AP02 – HTTPS Multiple Ports Virtual Service:

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

![Virtual Service parameters](image)

Figure 6-9: Virtual Service parameters

2. Type a valid Virtual Address.
3. Type 10243 as the Port.
4. Enter a recognizable Service Name, such as AP02 – HTTPS.
5. Click Add this Virtual Service.
6. Configure the settings as recommended in the following table:

<table>
<thead>
<tr>
<th>Section</th>
<th>Option</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Basic Properties</td>
<td>Service Type</td>
<td>HTTP/HTTPS</td>
</tr>
<tr>
<td>Standard Options</td>
<td>Force L4</td>
<td>Disabled</td>
</tr>
<tr>
<td>Real Servers</td>
<td>Real Server Check Method</td>
<td>HTTPS Protocol</td>
</tr>
<tr>
<td></td>
<td>Checked Port</td>
<td>443</td>
</tr>
<tr>
<td></td>
<td>URL</td>
<td>/favicon.ico</td>
</tr>
</tbody>
</table>

Table 6-12: AP02 – HTTPS Multiple Ports Recommended Settings

7. Add the Real Servers:
   a) Expand the Real Servers section.
   b) Click Add New.
   c) Type the address of the relevant Real Server.
   d) Type 443 as the Port.
   e) Complete the other fields as required.
f) Click **Add this Real Server** then click **OK** to the pop-up message.

g) Repeat the steps above to add more Real Servers as needed, based on your environment.

### 6.2.1.7 Create an AP02 – BLAST-UDP Multiple Ports Virtual Service

The following are the steps involved and the recommended settings to configure the AP02 – Blast-UDP Multiple Ports Virtual Service:

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

![Image](https://via.placeholder.com/150)

**Figure 6-10: Virtual Service parameters**

2. Type a valid Virtual Address.

3. Type **10243** as the Port.

4. Enter a recognizable Service Name, such as **AP02 – BLAST-UDP**.

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

6. Configure the settings as recommended in the following table:

<table>
<thead>
<tr>
<th>Section</th>
<th>Option</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Standard Options</td>
<td>Force L4</td>
<td>Disabled</td>
</tr>
<tr>
<td>Real Servers</td>
<td>Real Server Check Method</td>
<td>HTTPS Protocol</td>
</tr>
</tbody>
</table>

**Table 6-13: AP02 – BLAST-UDP Multiple Ports Recommended Settings**

7. Add the Real Servers:

   a) Expand the **Real Servers** section.

   b) Click **Add New**.

   c) Type the address of the relevant Real Server.

   d) Type **443** as the Port.

   e) Complete the other fields as required.

   f) Click **Add this Real Server** then click **OK** to the pop-up message.

   g) Repeat the steps above to add more Real Servers as needed, based on your environment.
### 6.2.1.8 Create an AP02 – PCOIP Multiple Ports Virtual Service

The following are the steps involved and the recommended settings to configure the AP02 – PCOIP Multiple Ports Virtual Service:

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

   ![Image of Virtual Service parameters](image)

   **Figure 6-11: Virtual Service parameters**

2. Type a valid Virtual Address.
3. Type 10272 as the Port.
4. Enter a recognizable Service Name, such as AP02 – PCOIP.
5. Click Add this Virtual Service.
6. Configure the settings as recommended in the following table:

<table>
<thead>
<tr>
<th>Section</th>
<th>Option</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Standard Options</td>
<td>Force L4</td>
<td>Disabled</td>
</tr>
<tr>
<td></td>
<td>Scheduling Method</td>
<td>round robin</td>
</tr>
<tr>
<td>Real Servers</td>
<td>Checked Port</td>
<td>4172</td>
</tr>
</tbody>
</table>

   **Table 6-14: AP02 - PCOIP Multiple VIPs Recommended Settings**

7. Add the Real Servers:
   a) Expand the Real Servers section.
   b) Click Add New.
   c) Type the address of the relevant Real Server.
   d) Type 4172 as the Port.
   e) Complete the other fields as required.
   f) Click Add this Real Server then click OK to the pop-up message.
   g) Repeat the steps above to add more Real Servers as needed, based on your environment.
6.2.1.9 Create an AP02 – PCOIP-UDP Multiple Ports Virtual Service

The following are the steps involved and the recommended settings to configure the AP02 – PCOIP-UDP Multiple Ports Virtual Service:

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

![Figure 6-12: Virtual Service parameters](image)

2. Type a valid Virtual Address.
3. Type 10272 as the Port.
4. Enter a recognizable Service Name, such as AP02 – PCOIP-UDP.
5. Click Add this Virtual Service.
6. Configure the settings as recommended in the following table:

<table>
<thead>
<tr>
<th>Section</th>
<th>Option</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Standard Options</td>
<td>Force L4</td>
<td>Disabled</td>
</tr>
<tr>
<td>Real Servers</td>
<td>Real Server Check</td>
<td>ICMP Ping</td>
</tr>
<tr>
<td>Method</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 6-15: AP02 – PCOIP-UDP Multiple VIPs Recommended Settings

7. Add the Real Servers:
   a) Expand the Real Servers section.
   b) Click Add New.
   c) Type the address of the relevant Real Server.
   d) Type 4172 as the Port.
   e) Complete the other fields as required.
   f) Click Add this Real Server then click OK to the pop-up message.
   g) Repeat the steps above to add more Real Servers as needed, based on your environment.
6.3 Method 3 - Multiple VIPs

This method is similar to the multiple port groups method except instead of dedicating a group of port numbers to each Access Point appliance, it dedicates an individual VIP to each appliance in addition to the primary load balanced VIP. If you have two Access Point appliances, then you would set up three VIPs. The primary Horizon protocol on HTTPS port 443 is load balanced to allocate the session to a specific Access Point appliance based on health and least loaded. The secondary connections are then routed to the correct Access Point appliance based on the following Load Balancer configuration table.

Access Point Configurations for External URLs for this configuration are shown in the following table.

<table>
<thead>
<tr>
<th>Virtual IP Address</th>
<th>Primary/Secondary</th>
<th>Protocol</th>
<th>Name</th>
<th>Real Servers</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.1.160.32:443</td>
<td>Primary</td>
<td>TCP</td>
<td>APLB - HTTPS</td>
<td>10.1.160.186:443</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>10.1.160.187:443</td>
</tr>
<tr>
<td>10.1.160.33:4172</td>
<td>Secondary</td>
<td>TCP</td>
<td>AP01 - PCOIP</td>
<td>10.1.160.186:4172</td>
</tr>
</tbody>
</table>

Table 6-16: Load Balancer Configuration Table

In our example, the FQDN http://ap1.myco.com resolves to 10.1.160.33 and https://ap2.myco.com:4172 resolves to 10.1.160.34

<table>
<thead>
<tr>
<th>Access Point Appliance</th>
<th>Configuration Item</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>AP01</td>
<td>tunnelExternalURL</td>
<td><a href="https://ap1.myco.com:443">https://ap1.myco.com:443</a></td>
</tr>
<tr>
<td>AP01</td>
<td>blastExternalURL</td>
<td><a href="https://ap1.myco.com:443">https://ap1.myco.com:443</a></td>
</tr>
<tr>
<td>AP01</td>
<td>pcoipExternalURL</td>
<td>10.20.30.33:4172</td>
</tr>
<tr>
<td>AP02</td>
<td>tunnelExternalURL</td>
<td><a href="https://ap2.myco.com:443">https://ap2.myco.com:443</a></td>
</tr>
<tr>
<td>AP02</td>
<td>blastExternalURL</td>
<td><a href="https://ap2.myco.com:4172">https://ap2.myco.com:4172</a></td>
</tr>
</tbody>
</table>
Table 6-17: Access Point Configuration for External URLs

<table>
<thead>
<tr>
<th>Access Point Appliance</th>
<th>Configuration Item</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>AP02</td>
<td>pcoipExternalURL</td>
<td>10.20.30.34:4172</td>
</tr>
</tbody>
</table>

**Advantages of multiple VIPs**
- Do not rely on source IP affinity
- Uses standard port numbers

**Disadvantages of multiple VIPs**
- Requires an additional public facing VIP for each Access Point appliance in addition to the primary load balanced VIP.

### 6.3.1 Create the Multiple VIPs Virtual Services

The following sections describe the recommended settings for the VMware Access Point Multiple VIPs Virtual Services.

#### 6.3.1.1 Create an HTTPS-APLB Multiple VIPs Virtual Service

The following are the steps involved and the recommended settings to configure the HTTPS-APLB Multiple VIPs Virtual Service:

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

   ![Figure 6-13: Virtual Service parameters](image)

   Please Specify the Parameters for the Virtual Service.

   - **Virtual Address**: 10.1.160.32
   - **Port**: 443
   - **Service Name (Optional)**: HTTPS - APLB - Multi
   - **Use Template**: Select a Template
   - **Protocol**: tcp

2. Type a valid **Virtual Address**.
3. Type **443** as the **Port**.
4. Enter a recognizable **Service Name**, such as **HTTPS – APLB**.
5. Click **Add this Virtual Service**.
6. Configure the settings as recommended in the following table:
### Session Affinity Options

<table>
<thead>
<tr>
<th>Section</th>
<th>Option</th>
<th>Value</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Advanced Properties</td>
<td>Add a Port 80 Redirector VS</td>
<td></td>
<td>Click the Add HTTP Redirector button. This automatically creates a redirect on port 80.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Basic Properties</th>
<th>Service Type</th>
<th>Generic</th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Standard Options</td>
<td>Persistence Mode</td>
<td>SSL Session ID</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Scheduling Method</td>
<td>least connection</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Real Servers</td>
<td>Real Server Check Method</td>
<td>HTTPS Protocol</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>URL</td>
<td>/favicon.ico</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 6-18: HTTPS – APLB Multiple VIPs Recommended Settings

7. Add the Real Servers:
   a) Expand the Real Servers section.
   b) Click Add New.
   c) Type the address of the relevant Real Server.
   d) Complete the other fields as required.
   e) Click Add this Real Server then click OK to the pop-up message.
   f) Repeat the steps above to add more Real Servers as needed, based on your environment.

#### Create a HTTPS - APLB Multiple Ports HTTPS HTTP Redirect Virtual Service

Clicking the Add HTTP Redirector button automatically creates a port 80 redirect Virtual Service. This is optional, but the purpose of this Virtual Service is to redirect any clients who have connected using HTTP to the HTTPS Virtual Service.

6.3.1.2 **Create an AP01 – BLAST-UDP Multiple VIPs Virtual Service**

The following are the steps involved and the recommended settings to configure the AP01 – BLAST-UDP Multiple VIPs Virtual Service:

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

    ![Figure 6-14: Virtual Service parameters](image-url)
2. Type a valid Virtual Address.
3. Type 443 as the Port.
4. Enter a recognizable Service Name, such as AP01 – BLAST-UDP.
5. Select udp as the Protocol.
6. Click Add this Virtual Service.
7. Configure the settings as recommended in the following table:

<table>
<thead>
<tr>
<th>Section</th>
<th>Option</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Standard Options</td>
<td>Force L4</td>
<td>Disabled</td>
</tr>
<tr>
<td>Real Servers</td>
<td>Real Server Check</td>
<td>ICMP Ping</td>
</tr>
</tbody>
</table>

Table 6-19: AP01 – BLAST-UDP Multiple VIPs Recommended Settings

8. Add the Real Servers:
   a) Expand the Real Servers section.
   b) Click Add New.
   c) Type the address of the relevant Real Server.
   d) Complete the other fields as required.
   e) Click Add this Real Server then click OK to the pop-up message.
   f) Repeat the steps above to add more Real Servers as needed, based on your environment.

6.3.1.3 Create an AP01 – HTTPS Multiple VIPs Virtual Service

The following are the steps involved and the recommended settings to configure the AP01 – HTTPS Multiple VIPs Virtual Service:

1. In the main menu of the LoadMaster Web User Interface (WUI), go to Virtual Services > Add New.
6. Configure the settings as recommended in the following table:

<table>
<thead>
<tr>
<th>Section</th>
<th>Option</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Standard Options</td>
<td>Force L4</td>
<td>Disabled</td>
</tr>
<tr>
<td></td>
<td>Scheduling Method</td>
<td>round robin</td>
</tr>
<tr>
<td>Real Servers</td>
<td>Real Server Check Method</td>
<td>HTTPS Protocol</td>
</tr>
<tr>
<td></td>
<td>Checked Port</td>
<td>443</td>
</tr>
<tr>
<td></td>
<td>URL</td>
<td>/favicon.ico</td>
</tr>
</tbody>
</table>

Table 6-20: AP01 - HTTPS Multiple VIPs Recommended Settings

7. Add the Real Servers:
   a) Expand the Real Servers section.
   b) Click Add New.
   c) Type the address of the relevant Real Server.
   d) Complete the other fields as required.
   e) Click Add this Real Server then click OK to the pop-up message.
   f) Repeat the steps above to add more Real Servers as needed, based on your environment.

6.3.1.4 Create an AP01 - PCOIP Multiple VIPs Virtual Service

The following are the steps involved and the recommended settings to configure the AP01 - PCOIP Multiple VIPs Virtual Service:

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

   ![Virtual Service parameters](Figure 6-16: Virtual Service parameters)

2. Type a valid Virtual Address.
3. Type 4172 as the Port.
4. Enter a recognizable Service Name, such as AP01 - PCOIP.
5. Click Add this Virtual Service.
6. Configure the settings as recommended in the following table:
7. Add the Real Servers:
   a) Expand the **Real Servers** section.
   b) Click **Add New**.
   c) Type the address of the relevant Real Server.
   d) Type **4172** as the **Port**.
   e) Complete the other fields as required.
   f) Click **Add this Real Server** then click **OK** to the pop-up message.
   g) Repeat the steps above to add more Real Servers as needed, based on your environment.

### 6.3.1.5 Create an AP01 – PCOIP-UDP Multiple VIPs Virtual Service

The following are the steps involved and the recommended settings to configure the AP01 – PCOIP-UDP Multiple VIPs Virtual Service:

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

   ![Virtual Service parameters](image)

   **Figure 6-17: Virtual Service parameters**

2. Type a valid **Virtual Address**.
3. Type **4172** as the **Port**.
4. Enter a recognizable **Service Name**, such as **AP01 – PCOIP-UDP**.
5. Select **udp** as the **Protocol**.
6. Click **Add this Virtual Service**.
7. Configure the settings as recommended in the following table:

<table>
<thead>
<tr>
<th>Section</th>
<th>Option</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Standard Options</td>
<td>Force L4</td>
<td>Disabled</td>
</tr>
<tr>
<td>Real Servers</td>
<td>Real Server Check Method</td>
<td>ICMP Ping</td>
</tr>
</tbody>
</table>

Table 6-22: AP01 – PCOIP-UDP Multiple VIPs Recommended Settings

8. Add the Real Servers:
   a) Expand the Real Servers section.
   b) Click Add New.
   c) Type the address of the relevant Real Server.
   d) Complete the other fields as required.
   e) Click Add this Real Server then click OK to the pop-up message.
   f) Repeat the steps above to add more Real Servers as needed, based on your environment.

6.3.1.6 Create an AP02 – BLAST-UDP Multiple VIPs Virtual Service

The following are the steps involved and the recommended settings to configure the AP02 – BLAST-UDP Multiple VIPs Virtual Service:

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

   ![Figure 6-18: Virtual Service parameters](image)

2. Type a valid Virtual Address.
3. Type 443 as the Port.
4. Enter a recognizable Service Name, such as AP02 – BLAST-UDP – Multiple IPs.
5. Select udp as the Protocol.
6. Click Add this Virtual Service.
7. Configure the settings as recommended in the following table:

<table>
<thead>
<tr>
<th>Section</th>
<th>Option</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Standard Options</td>
<td>Force L4</td>
<td>Disabled</td>
</tr>
</tbody>
</table>
Section | Option | Value
---|---|---
Real Servers | Real Server Check Method | ICMP Ping

Table 6-23: AP02 – BLAST-UDP Multiple VIPs Recommended Settings

8. Add the Real Servers:
   a) Expand the Real Servers section.
   b) Click Add New.
   c) Type the address of the relevant Real Server.
   d) Complete the other fields as required.
   e) Click Add this Real Server then click OK to the pop-up message.
   f) Repeat the steps above to add more Real Servers as needed, based on your environment.

6.3.1.7 Create an AP02 – HTTPS Multiple VIPs Virtual Service

The following are the steps involved and the recommended settings to configure the AP02 – HTTPS Multiple VIPs Virtual Service:

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

![Image of Virtual Service parameters](image)

2. Type a valid Virtual Address.
3. Type 443 as the Port.
4. Enter a recognizable Service Name, such as AP02 – HTTPS – Multiple IPs.
5. Click Add this Virtual Service.
6. Configure the settings as recommended in the following table:

<table>
<thead>
<tr>
<th>Section</th>
<th>Option</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Standard Options</td>
<td>Force L4</td>
<td>Disabled</td>
</tr>
<tr>
<td>Real Servers</td>
<td>Real Server Check Method</td>
<td>HTTPS Protocol</td>
</tr>
</tbody>
</table>
Add the Real Servers:

a) Expand the Real Servers section.
b) Click Add New.
c) Type the address of the relevant Real Server.
d) Complete the other fields as required.
e) Click Add this Real Server then click OK to the pop-up message.
f) Repeat the steps above to add more Real Servers as needed, based on your environment.

6.3.1.8 Create an AP02 – PCOIP Multiple VIPs Virtual Service

The following are the steps involved and the recommended settings to configure the AP02 – PCOIP Multiple VIPs Virtual Service:

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

2. Type a valid Virtual Address.
3. Type 4172 as the Port.
4. Enter a recognizable Service Name, such as AP02 – PCOIP.
5. Click Add this Virtual Service.
6. Configure the settings as recommended in the following table:

<table>
<thead>
<tr>
<th>Section</th>
<th>Option</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Standard Options</td>
<td>Force L4</td>
<td>Disabled</td>
</tr>
<tr>
<td>Real Servers</td>
<td>Real Server Check Method</td>
<td>TCP Connection Only</td>
</tr>
<tr>
<td></td>
<td>Checked Port</td>
<td>4172</td>
</tr>
</tbody>
</table>

Table 6-25: AP02 - PCOIP Multiple VIPs Recommended Settings
7. Add the Real Servers:
   a) Expand the Real Servers section.
   b) Click Add New.
   c) Type the address of the relevant Real Server.
   d) Complete the other fields as required.
   e) Click Add this Real Server then click OK to the pop-up message.
   f) Repeat the steps above to add more Real Servers as needed, based on your environment.

6.3.1.9 Create an AP02 – PCOIP-UDP Multiple VIPs Virtual Service

The following are the steps involved and the recommended settings to configure the AP02 – PCOIP-UDP Multiple VIPs Virtual Service:

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

![Figure 6-21: Virtual Service parameters](image)

2. Type a valid Virtual Address.
3. Type 4172 as the Port.
4. Enter a recognizable Service Name, such as AP02 – PCOIP-UDP.
5. Click Add this Virtual Service.
6. Configure the settings as recommended in the following table:

<table>
<thead>
<tr>
<th>Section</th>
<th>Option</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Standard Options</td>
<td>Force L4</td>
<td>Disabled</td>
</tr>
<tr>
<td>Real Servers</td>
<td>Real Server Check Method</td>
<td>ICMP Ping</td>
</tr>
</tbody>
</table>

Table 6-26: AP02 – PCOIP-UDP Multiple VIPs Recommended Settings

7. Add the Real Servers:
   a) Expand the Real Servers section.
   b) Click Add New.
   c) Type the address of the relevant Real Server.
   d) Complete the other fields as required.
   e) Click Add this Real Server then click OK to the pop-up message.
f) Repeat the steps above to add more Real Servers as needed, based on your environment.
Unless otherwise specified, the following documents can be found at http://kemptechnologies.com/documentation.

Virtual Services and Templates, Feature Description
## Document History

<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>Oct 2016</td>
<td>First Release</td>
<td>First release of document</td>
<td>1.0</td>
<td>POC</td>
</tr>
<tr>
<td>Jan 2017</td>
<td>Minor change</td>
<td>Updated Copyright Notices</td>
<td>2.0</td>
<td>LB</td>
</tr>
</tbody>
</table>