



VMware Horizon View 7

Deployment Guide

UPDATED: 27 July 2023

Copyright Notices

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

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

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

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

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

Table of Contents

1 Introduction	6
1.1 Document Purpose	7
1.2 Intended Audience	7
1.3 About this Document	7
2 Template	8
3 Architecture	9
4 Horizon Protocols	11
4.1 Primary Horizon Protocol	11
4.2 Secondary Horizon Protocols	11
5 Configure the LoadMaster	13
5.1 Enable Subnet Originating Requests Globally	13
5.2 Enable Check Persist Globally	14
6 Unified Access Gateway Session Affinity Options	16
6.1 Method 1 - Source IP Affinity	16
6.1.1 Create the VMware Unified Access Gateway Source IP Affinity Virtual Services	17
6.1.1.1 Create a UAGLB TCP HTTPS Affinity Virtual Service	17
6.1.1.2 Create a UAGLB TCP Blast Affinity Virtual Service	18
6.1.1.3 Create a UAGLB UDP Blast Affinity Virtual Service	20
6.1.1.4 Create a UAGLB TCP PCoIP Affinity Virtual Service	21
6.1.1.5 Create a UAGLB UDP PCoIP Affinity Virtual Service	22
6.2 Method 2 - Multiple Port Number Groups	23

6.2.1 Create the VMware Unified Access Gateway Multiple Port Number Groups Virtual Services	25
6.2.1.1 Create a UAGLB – HTTPS Multiple Ports Virtual Service	25
6.2.1.2 Create a UAG01 TCP - Blast Multiple Ports Virtual Service	27
6.2.1.3 Create a UAG01 – UDP - Blast Multiple Ports Virtual Service	28
6.2.1.4 Create a UAG01 – TCP - PCoIP Multiple Ports Virtual Service	29
6.2.1.5 Create a UAG01 – UDP - PCoIP Multiple Ports Virtual Service	30
6.2.1.6 Create a UAG02 - TCP - Blast Multiple Ports Virtual Service	32
6.2.1.7 Create a UAG02 – UDP - Blast Multiple Ports Virtual Service	33
6.2.1.8 Create a UAG02 – TCP - PCoIP Multiple Ports Virtual Service	34
6.2.1.9 Create a UAG02 - UDP - PCoIP Multiple Ports Virtual Service	35
6.3 Method 3 - Multiple VIPs	37
6.3.1 Create the Multiple VIPs Virtual Services	38
6.3.1.1 Create an HTTPS-UAGLB Multiple VIPs Virtual Service	38
6.3.1.2 Create a UAG01 TCP Blast-UDP Multiple VIPs Virtual Service	40
6.3.1.3 Create a UAG01 – UDP Blast Multiple VIPs Virtual Service	41
6.3.1.4 Create a UAG01 - TCP - PCoIP Multiple VIPs Virtual Service	42
6.3.1.5 Create a UAG01 - UDP - PCoIP Multiple VIPs Virtual Service	43
6.3.1.6 Create a UAG - TCP - Blast Multiple VIPs Virtual Service	44
6.3.1.7 Create a UAG02 – UDP - Blast Multiple VIPs Virtual Service	45
6.3.1.8 Create a UAG02 – TCP - PCoIP Multiple VIPs Virtual Service	46
6.3.1.9 Create a UAG02 – UDP- PCoIP Multiple VIPs Virtual Service	47
7 Connection Server	49

7.1 Create the Connection Server Virtual Services	49
8 App Volume Manager	52
8.1 Create App Volume Manager Virtual Services	52
9 Identity Manager	55
9.1 Create Identity Manager Virtual Services	55
Last Updated Date	58

1 Introduction

VMware Horizon View is a virtual desktop infrastructure (VDI) solution that simplifies administration and delivery of personalized virtual desktops. It consists of several components and delivers a secure optimized virtual desktop infrastructure.

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 Unified Access Gateway appliance. This article also covers health monitoring and SSL offload/SSL bridging for load balancers.

Unified Access Gateway (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. Unified Access Gateway 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

Connection Servers are the core component of VMware Horizon View. This role defines virtual desktop pools, applications and permissions.

App Volume Manager is a console for managing configuration, creation of AppStacks and assignment of AppStacks and writable volumes.

Identity Manager is a portal where users gain access to different types of applications including Software as a Service (SaaS) based, enterprise identity management to sync and extend Active Directory, and single sign on.

The Kemp LoadMaster is used to load balance the VMware Unified Access Gateway, Connection Servers, Identity Manager, and App Volume Manager. 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 Introduction

This document provides guidance and recommended settings on how to load balance Horizon View 7 with a Kemp LoadMaster. 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>.

1.1 Document Purpose

This document provides the recommended LoadMaster settings used when load balancing the VMware Horizon View and Horizon Air Hybrid-Mode use cases using the Unified Access Gateway. 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 Horizon workload.

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 Template

Kemp has developed a template containing our recommended settings for this workload. You can install this template to help create Virtual Services (VSs) because it automatically populates the settings. You can use the template to easily create the required VSs with the recommended settings. You can remove templates after use and this will not affect deployed services. If needed, you can make changes to any of the VS settings after using the template.

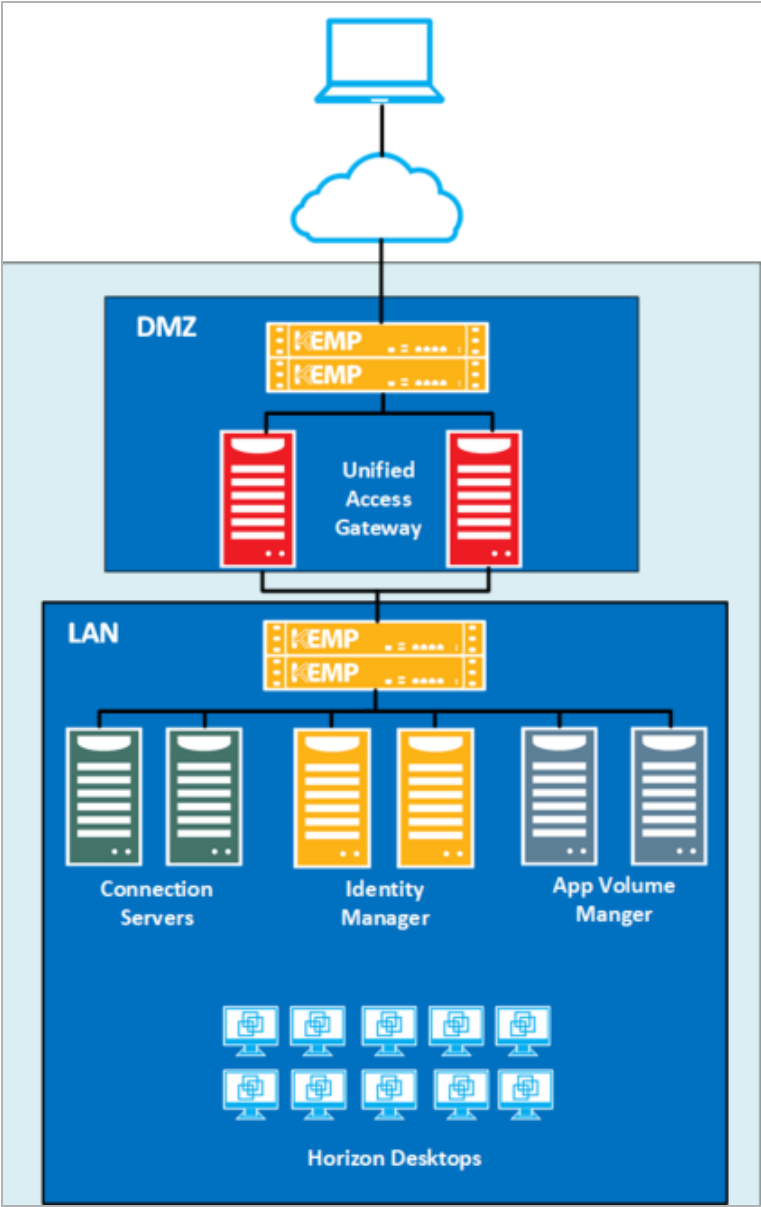
Download released templates from the following page: [LoadMaster Templates](#).

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

3 Architecture

Unified Access Gateway is typically deployed in a DMZ. For high availability and scalability requirements in a production deployment, several Unified Access Gateway 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.

3 Architecture



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 the **Architecture** section, the load balancer routes this connection to one of the Unified Access Gateway 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 Unified Access Gateway appliances.

4.2 Secondary Horizon Protocols

After the Horizon Client has established a secure communication to one of the Unified Access Gateway 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 8443 and UDP 8443).
- PCoIP display protocol (TCP 4172 and UDP 4172).

These secondary Horizon protocols must be routed to the same Unified Access Gateway appliance to which the primary Horizon protocol is routed. This is so that Unified Access Gateway can authorize the secondary protocols based on the authenticated user session. An important security capability of Unified Access Gateway 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 Unified Access Gateway 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 Unified Access Gateway 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.

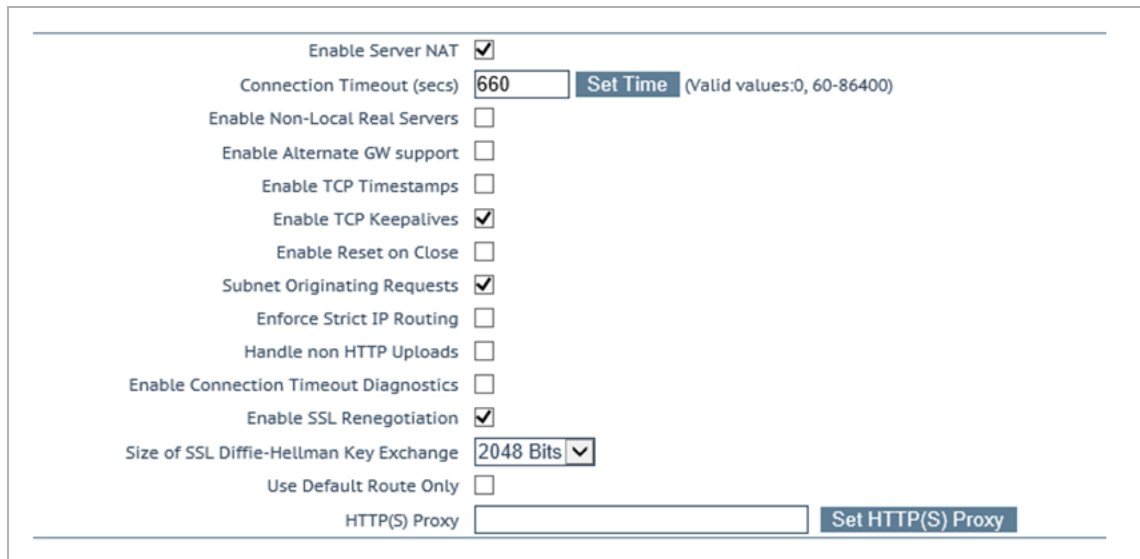
When **Subnet Originating Requests** is enabled, the LoadMaster routes traffic so that the Real Server sees traffic arriving from the LoadMaster interface that is in that network/subnet.

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 choose whether 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 Web User Interface (WUI), go to **System Configuration > Miscellaneous Options > Network Options**.

5 Configure the LoadMaster



The screenshot shows a configuration window with the following settings:

- Enable Server NAT: ☒
- Connection Timeout (secs): 660 [Set Time (Valid values:0, 60-86400)]
- Enable Non-Local Real Servers: ☐
- Enable Alternate GW support: ☐
- Enable TCP Timestamps: ☐
- Enable TCP Keepalives: ☒
- Enable Reset on Close: ☐
- Subnet Originating Requests: ☒
- Enforce Strict IP Routing: ☐
- Handle non HTTP Uploads: ☐
- Enable Connection Timeout Diagnostics: ☐
- Enable SSL Renegotiation: ☒
- Size of SSL Diffie-Hellman Key Exchange: 2048 Bits [v]
- Use Default Route Only: ☐
- HTTP(S) Proxy: [] [Set HTTP(S) Proxy]

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**.

5 Configure the LoadMaster

Enable Server NAT	<input checked="" type="checkbox"/>
Connection Timeout (secs)	<input type="text" value="660"/> Set Time (Valid values:0, 60-86400)
Enable Non-Local Real Servers	<input type="checkbox"/>
Enable Alternate GW support	<input type="checkbox"/>
Enable TCP Timestamps	<input type="checkbox"/>
Enable TCP Keepalives	<input checked="" type="checkbox"/>
Enable Reset on Close	<input type="checkbox"/>
Subnet Originating Requests	<input checked="" type="checkbox"/>
Enforce Strict IP Routing	<input type="checkbox"/>
Handle non HTTP Uploads	<input type="checkbox"/>
Enable Connection Timeout Diagnostics	<input type="checkbox"/>
Legacy TCP Timewait handling	<input type="checkbox"/>
Enable SSL Renegotiation	<input checked="" type="checkbox"/>
Force Real Server Certificate Checking	<input type="checkbox"/>
Size of SSL Diffie-Hellman Key Exchange	<input type="text" value="2048 Bits"/>
Log SSL errors	<input type="text" value="Fatal errors only"/>
Use Default Route Only	<input type="checkbox"/>
HTTP(S) Proxy	<input type="text"/> Set HTTP(S) Proxy

2. Click the **Always Check Persist** drop-down arrow and select **Yes – Accept Changes**.

6 Unified Access Gateway 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 Unified Access Gateway 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.

Unified Access Gateway Configuration for External URLs for this configuration is shown in the following table.

In our example, the Fully Qualified Domain Name (FQDN) `https://uag.myco.com` resolves to `10.1.160.35`.

Unified Access Gateway Appliance	Configuration Item	Value
UAG01	tunnelExternalURL	https://uag.myco.com:443
UAG01	blastExternalURL	https://uag.myco.com:443
UAG01	pcoipExternalURL	10.1.160.35:4172

Unified Access Gateway Appliance	Configuration Item	Value
UAG02	tunnelExternalURL	https://uag.myco.com:443
UAG02	blastExternalURL	https://uag.myco.com:443
UAG02	pcoipExternalURL	10.1.160.35:4172

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.

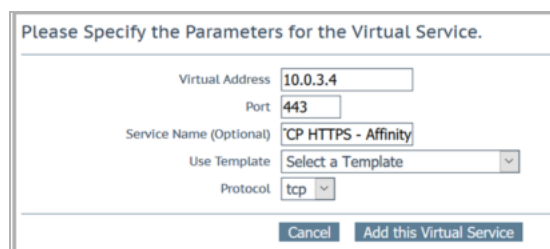
6.1.1 Create the VMware Unified Access Gateway Source IP Affinity Virtual Services

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

6.1.1.1 Create a UAGLB TCP HTTPS Affinity Virtual Service

The following are the steps involved and the recommended settings to configure the UAGLB TCP HTTPS Affinity 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 **443** as the **Port**.
4. Enter a recognizable **Service Name**, such as **UAGLB TCP HTTPS - Affinity**.
5. Click **Add this Virtual Service**.
6. Configure the settings as recommended in the following table:

6 Unified Access Gateway Session Affinity Options

Section	Option	Value	Comment
Standard Options	Persistence Mode	Source IP Address	
	Timeout	1 Hour	
	Scheduling Method	least connection	
Advanced Properties	Add a Port 80 Redirector VS	https://%h%s	Click the Add HTTP Redirector button. This automatically creates a redirect on port 80.
Real Servers	Real Server Check Method	HTTPS Protocol	
	URL	/favicon.ico	

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 UAGLB TCP-IP Affinity HTTPS HTTP Redirect Virtual Service

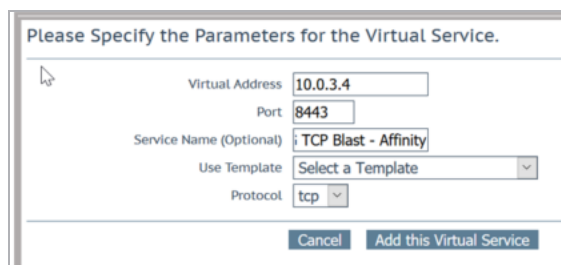
Clicking the **Add HTTP Redirector** button automatically creates a port 80 redirect Virtual Service. This is optional, but the purpose of this Virtual Service is to redirect any clients who have connected using HTTP to the HTTPS Virtual Service.

6.1.1.2 Create a UAGLB TCP Blast Affinity Virtual Service

The following are the steps involved and the recommended settings to configure the UAGLB TCP Blast Affinity Virtual Service:

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

6 Unified Access Gateway Session Affinity Options



2. Type a valid **Virtual Address**.
3. Type **8443** as the **Port**.
4. Enter a recognizable **Service Name**, such as **UAGLB TCP Blast Affinity**.
5. Select **tcp** as the **Protocol**.
6. Click **Add this Virtual Service**.
7. Configure the settings as recommended in the following table:

Section	Option	Value
Basic Properties	Service Type	HTTP-HTTP/2-HTTPS
Standard Options	Persistence Mode	Source IP Address
	Timeout	1 Hour
	Scheduling Method	least connection
Real Servers	Real Server Check Method	TCP Connection Only

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 a UAGLB UDP Blast Affinity Virtual Service

The following are the steps involved and the recommended settings to configure the UAGLB UDP Blast 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

Port

Service Name (Optional)

Use Template

Select a Template ▾

Protocol

udp ▾

Cancel

Add this Virtual Service

2. Type a valid **Virtual Address**.
3. Type **8443** as the **Port**.
4. Enter a recognizable **Service Name**, such as **UAGLB UDP Blast Affinity**.
5. Select **udp** as the **Protocol**.
6. Click **Add this Virtual Service**.
7. Configure the settings as recommended in the following table:

Section	Option	Value
Standard Options	Force L4	Disabled
	Persistence Mode	Source IP Address
	Timeout	1 Hour
	Scheduling Method	least connection

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.

6.1.1.4 Create a UAGLB TCP PCoIP Affinity Virtual Service

The following are the steps involved and the recommended settings to configure the UAGLB TCP PCoIP 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	<input style="width: 80%;" type="text" value="10.0.3.4"/>
Port	<input style="width: 80%;" type="text" value="4172"/>
Service Name (Optional)	<input style="width: 80%;" type="text" value="TCP PCoIP - Affinity"/>
Use Template	<input style="width: 80%;" type="text" value="Select a Template"/>
Protocol	<input style="width: 80%;" type="text" value="tcp"/>

2. Type a valid **Virtual Address**.
3. Type **4172** as the **Port**.
4. Enter a recognizable **Service Name**, such as **UAGLB TCP PCoIP Affinity**.
5. Select **tcp** as the **Protocol**.
6. Click **Add this Virtual Service**.
7. Configure the settings as recommended in the following table:

Section	Option	Value
Basic Properties	Service Type	HTTP-HTTP/2-HTTPS
Standard Options	Persistence Mode	Source IP Address
	Timeout	1 Hour
	Scheduling Method	least connection
Real Servers	Real Server Check Method	TCP Connection Only

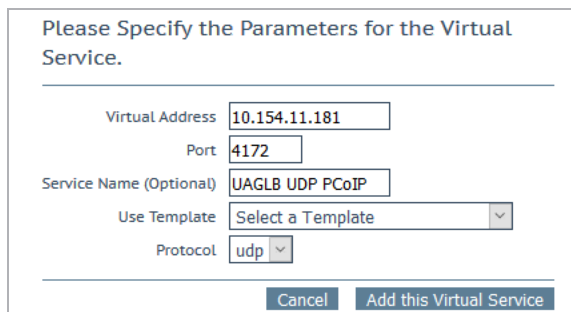
8. Add the Real Servers:

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

6.1.1.5 Create a UAGLB UDP PCoIP Affinity Virtual Service

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

- 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: 10.154.11.181

Port: 4172

Service Name (Optional): UAGLB UDP PCoIP

Use Template: Select a Template

Protocol: udp

Buttons: Cancel, Add this Virtual Service

- Type a valid **Virtual Address**.
- Type **4172** as the **Port**.

4. Enter a recognizable **Service Name**, such as **UAGLB UDP PCoIP Affinity**.
5. Select **udp** as the **Protocol**.
6. Click **Add this Virtual Service**.
7. Configure the settings as recommended in the following table:

Section	Option	Value
Standard Options	Force L4	Disabled
	Persistence Mode	Source IP Address
	Timeout	1 Hour
	Scheduling Method	least connection
Advanced Properties	Port Following	No VIP Selected

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 Unified Access Gateway appliance. The primary Horizon protocol on HTTPS port 443 is load balanced to allocate the session to a specific Unified Access Gateway appliance based on health and least loaded. The secondary connections are then routed to the correct Unified Access Gateway appliance based on the following Load Balancer configuration table.

Virtual IP Address	Primary/Secondary	Protocol	Name	Real Servers
10.1.160.31:443	Primary	TCP	UAGLB - HTTPS	10.1.160.183:443 10.1.160.184:443
10.1.160.31:10143	Secondary	TCP	UAG01 - BLAST-TCP	10.1.160.183:10143
10.1.160.31:10143	Secondary	UDP	UAG01 - BLAST-UDP	10.1.160.183:10143
10.1.160.31:10172	Secondary	TCP	UAG01 - PCOIP	10.1.160.183:10172
10.1.160.31:10172	Secondary	UDP	UAG01 - PCOIP-UDP	10.1.160.183:10172
10.1.160.31:10243	Secondary	TCP	UAG02 - BLAST-TCP	10.1.160.184:10243
10.1.160.31:10243	Secondary	UDP	UAG02 - BLAST-UDP	10.1.160.184:10243
10.1.160.31:10272	Secondary	TCP	UAG02 - PCOIP	10.1.160.184:10272
10.1.160.31:10272	Secondary	UDP	UAG02 - PCOIP-UDP	10.1.160.184:10272

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

BLAST-TCP

- 10143 → UAG01 10143
- 10172 → UAG01 10172
- 10243 → UAG02 10243
- 10272 → UAG02 10272

The same convention is used for multiple Unified Access Gateways

- 10343 → UAG03 10343
- 10372 → UAG03 10372

The Unified Access Gateway Configuration for External URLs is shown below.

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

Unified Access Gateway Appliance	Configuration Item	Value
UAG01	tunnelExternalURL	<code>https://uag.myco.com:443</code>
UAG01	blastExternalURL	<code>https://uag.myco.com:10143</code>

Unified Access Gateway Appliance	Configuration Item	Value
UAG01	pcoipExternalURL	10.1.60.31:10172
UAG02	tunnelExternalURL	https://uag.myco.com:443
UAG02	blastExternalURL	https://uag.myco.com:10243
UAG02	pcoipExternalURL	10.1.60.31:10272

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 Unified Access Gateway appliances themselves are standard.

6.2.1 Create the VMware Unified Access Gateway Multiple Port Number Groups Virtual Services

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

6.2.1.1 Create a UAGLB – HTTPS Multiple Ports Virtual Service

The following are the steps involved and the recommended settings to configure the UAGLB – 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.

Virtual Address

Port

Service Name (Optional)

Use Template

Protocol

6 Unified Access Gateway Session Affinity Options

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

Section	Option	Value	Comment
Advanced Properties	Add a Port 80 Redirector VS		Click the Add HTTP Redirector button. This automatically creates a redirect on port 80.
	Persistence Mode	SSL Session ID	
Standard Options	Timeout	1 Hour	
	Scheduling Method	least connection	
Real Servers	Real Server Check Method	HTTPS Protocol	
	URL	/favicon.ico	

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 a UAGLB – 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 a UAG01 TCP - Blast Multiple Ports Virtual Service

The following are the steps involved and the recommended settings to configure the UAG01 – TCP Blast 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.

Virtual Address

Port

Service Name (Optional)

Use Template

Select a Template ▾

Protocol

tcp ▾

Cancel

Add this Virtual Service

2. Type a valid **Virtual Address**.
3. Type **10143** as the **Port**.
4. Enter a recognizable **Service Name**, such as **UAG01 – TCP – Blast Multiple Ports**.
5. Click **Add this Virtual Service**.
6. Configure the settings as recommended in the following table:

Section	Option	Value
Basic Properties	Service Type	Generic
Standard Options	Persistence Mode	SSL Session ID
	Timeout	1 Hour
	Scheduling Method	least connection

Section	Option	Value
Real Servers	Real Server Check Method	TCP Connection Only

7. Add the Real Servers:

- Expand the **Real Servers** section.
- Click **Add New**.
- Type the address of the relevant Real Server.
- Type **10143** as the **Port** number.
- Complete the other fields as required.
- Click **Add this Real Server** then click **OK** to the pop-up message.

6.2.1.3 Create a UAG01 – UDP - Blast Multiple Ports Virtual Service

The following are the steps involved and the recommended settings to configure the UAG01 - UDP - Blast Multiple Ports Virtual Service:

- 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

Port

Service Name (Optional)

Use Template

Select a Template ▾

Protocol

udp ▾

Cancel

Add this Virtual Service

- Type a valid **Virtual Address**.
- Type **10143** as the **Port**.
- Enter a recognizable **Service Name**, such as **UAG01 – UDP Blast Multiple Ports**.

5. Select **udp** as the **Protocol**.
6. Click **Add this Virtual Service**.
7. Configure the settings as recommended in the following table:

Section	Option	Value
Standard Options	Force L4	Disabled
Real Servers	Real Server Check Method	ICMP Ping

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 **10143** as the **Port**.
 - e) Complete the other fields as required.
 - f) Click **Add this Real Server** then click **OK** to the pop-up message.

6.2.1.4 Create a UAG01 – TCP - PCoIP Multiple Ports Virtual Service

The following are the steps involved and the recommended settings to configure the UAG01 – TCP - PCoIP 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.

Virtual Address

Port

Service Name (Optional)

Use Template

Select a Template ▾

Protocol

tcp ▾

Cancel

Add this Virtual Service

2. Type a valid **Virtual Address**.
3. Type **10172** as the **Port**.
4. Enter a recognizable **Service Name**, such as **UAG01 - TCP-PCoIP Multiple Ports**.
5. Click **Add this Virtual Service**.
6. Configure the settings as recommended in the following table:

Section	Option	Value
Basic Properties	Service Type	Generic
Standard Options	Persistence Mode	SSL Session ID
	Timeout	1 Hour
	Scheduling Method	least connection
Real Servers	Real Server Check Method	TCP Connection Only

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 **10172** as the **Port**.
 - e) Complete the other fields as required.
 - f) Click **Add this Real Server** then click **OK** to the pop-up message.

6.2.1.5 Create a UAG01 – UDP - PCoIP Multiple Ports Virtual Service

The following are the steps involved and the recommended settings to configure the UAG01-UDP-PCoIP 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.

Virtual Address

Port

Service Name (Optional)

Use Template

Select a Template ▾

Protocol

udp ▾

Cancel

Add this Virtual Service

2. Type a valid **Virtual Address**.
3. Type **10172** as the **Port**.
4. Enter a recognizable **Service Name**, such as **UAG01 – UDP-PCoIP** Multiple Port.
5. Select **udp** as the **Protocol**.
6. Click **Add this Virtual Service**.
7. Configure the settings as recommended in the following table:

Section	Option	Value
Standard Options	Force L4	Disabled
Real Servers	Real Server Check Method	ICMP Ping

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 **10172** as the **Port**.
 - e) Complete the other fields as required.
 - f) Click **Add this Real Server** then click **OK** to the pop-up message.

6.2.1.6 Create a UAG02 - TCP - Blast Multiple Ports Virtual Service

The following are the steps involved and the recommended settings to configure the UAG02 - TCP - Blast 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.

Virtual Address

Port

Service Name (Optional)

Use Template

Select a Template ▾

Protocol

tcp ▾

Cancel

Add this Virtual Service

2. Type a valid **Virtual Address**.
3. Type **10243** as the **Port**.
4. Enter a recognizable **Service Name**, such as **UAG02 - TCP - Blast Multiple Port**.
5. Click **Add this Virtual Service**.
6. Configure the settings as recommended in the following table:

Section	Option	Value
Basic Properties	Service Type	Generic
Standard Options	Persistence Mode	SSL Session ID
	Timeout	1 Hour
	Scheduling Method	least connection
Real Servers	Real Server Check Method	TCP Connection Only

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 **10243** as the **Port**.
- e) Complete the other fields as required.
- f) Click **Add this Real Server** then click **OK** to the pop-up message.

6.2.1.7 Create a UAG02 – UDP - Blast Multiple Ports Virtual Service

The following are the steps involved and the recommended settings to configure the UAG02 – Blast Extreme-UDP 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.

Virtual Address	<input style="width: 60%;" type="text" value="10.154.11.181"/>
Port	<input style="width: 60%;" type="text" value="10243"/>
Service Name (Optional)	<input style="width: 60%;" type="text" value="UAG02 - UDP - BLA"/>
Use Template	<input style="width: 60%;" type="text" value="Select a Template"/> ▼
Protocol	<input style="width: 60%;" type="text" value="udp"/> ▼

2. Type a valid **Virtual Address**.
3. Type **10243** as the **Port**.
4. Enter a recognizable **Service Name**, such as **UAG02 - UDP - Blast Multiple Port**.
5. Click **Add this Virtual Service**.
6. Configure the settings as recommended in the following table:

Section	Option	Value
Standard Options	Force L4	Disabled
Real Servers	Real Server Check Method	HTTPS Protocol

7. Add the Real Servers:

- Expand the **Real Servers** section.
- Click **Add New**.
- Type the address of the relevant Real Server.
- Type **10243** as the **Port**.
- Complete the other fields as required.
- Click **Add this Real Server** then click **OK** to the pop-up message.

6.2.1.8 Create a UAG02 – TCP - PCoIP Multiple Ports Virtual Service

The following are the steps involved and the recommended settings to configure the UAG02 - TCP - PCoIP Multiple Ports Virtual Service:

- 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

Port

Service Name (Optional)

Use Template

Select a Template ▾

Protocol

tcp ▾

Cancel

Add this Virtual Service

- Type a valid **Virtual Address**.
- Type **10272** as the **Port**.
- Enter a recognizable **Service Name**, such as **UAG02 - TCP - PCoIP Multiple Port**.

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

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

Section	Option	Value
Basic Properties	Service Type	Generic
Standard Options	Persistence Mode	SSL Session ID
	Timeout	1 Hour
	Scheduling Method	least connection
Real Servers	Real Server Check Method	TCP Connection Only

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 **10272** as the **Port**.
- e) Complete the other fields as required.
- f) Click **Add this Real Server** then click **OK** to the pop-up message.

6.2.1.9 Create a UAG02 - UDP - PCoIP Multiple Ports Virtual Service

The following are the steps involved and the recommended settings to configure the UAG02 - UDP - PCoIP 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.

Virtual Address

Port

Service Name (Optional)

Use Template

Select a Template ▾

Protocol

udp ▾

Cancel

Add this Virtual Service

2. Type a valid **Virtual Address**.
3. Type **10272** as the **Port**.
4. Enter a recognizable **Service Name**, such as **UAG02 - UDP - PCoIP Multiple Ports**.
5. Select **udp** as the **Protocol**.
6. Click **Add this Virtual Service**.
7. Configure the settings as recommended in the following table:

Section	Option	Value
Standard Options	Force L4	Disabled
Real Servers	Real Server Check Method	ICMP Ping

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 **10272** as the **Port**.
 - e) Complete the other fields as required.
 - f) Click **Add this Real Server** then click **OK** to the pop-up message.

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 Unified Access Gateway appliance, it dedicates an individual VIP to each appliance in addition to the primary load balanced VIP. If you have two Unified Access Gateway 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 Unified Access Gateway appliance based on health and least loaded. The secondary connections are then routed to the correct Unified Access Gateway appliance based on the following Load Balancer configuration table.

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

Virtual IP Address	Primary/Secondary	Protocol	Name	Real Servers
10.1.160.32:443	Primary	TCP	UAGLB - HTTPS	10.1.160.186:443
				10.1.160.187:443
10.1.160.33:443	Secondary	TCP	UAG01 - HTTPS BLAST	10.1.160.186:8443
10.1.160.33:443	Secondary	UDP	UAG01 - BLAST-UDP	10.1.160.186:8443
10.1.160.33:4172	Secondary	TCP	UAG01 - PCOIP	10.1.160.186:4172
10.1.160.33:4172	Secondary	UDP	UAG01 - PCOIP-UDP	10.1.160.186:4172
10.1.160.34:443	Secondary	TCP	UAG02 - BLAST	10.1.160.187:8443
10.1.160.34:443	Secondary	UDP	UAG02 - BLAST-UDP	10.1.160.187:8443
10.1.160.34:4172	Secondary	TCP	UAG02 - PCOIP	10.1.160.187:4172
10.1.160.34:4172	Secondary	UDP	UAG02 - PCOIP-UDP	10.1.160.187:4172

In our example, the FQDN `http://uag1.myco.com` resolves to 10.1.160.33 and `https://uag2.myco.com:4172` resolves to 10.1.160.34

Unified Access Gateway Appliance	Configuration Item	Value
UAG01	tunnelExternalURL	https://uag1.myco.com:443
UAG01	blastExternalURL	https://uag1.myco.com:8443
UAG01	pcoipExternalURL	10.20.30.33:4172

Unified Access Gateway Appliance	Configuration Item	Value
UAG02	tunnelExternalURL	https://uag2.myco.com:443
UAG02	blastExternalURL	https://uag2.myco.com:8443
UAG02	pcoipExternalURL	10.20.30.34:4172

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 Unified Access Gateway appliance in addition to the primary load balanced VIP.

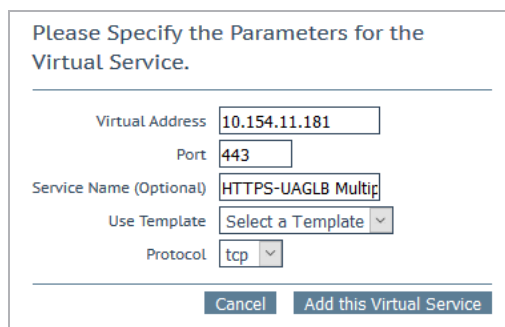
6.3.1 Create the Multiple VIPs Virtual Services

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

6.3.1.1 Create an HTTPS-UAGLB Multiple VIPs Virtual Service

The following are the steps involved and the recommended settings to configure the HTTPS-UAGLB Multiple VIPs 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: 10.154.11.181

Port: 443

Service Name (Optional): HTTPS-UAGLB Multip

Use Template: Select a Template

Protocol: tcp

Buttons: Cancel, Add this Virtual Service

2. Type a valid **Virtual Address**.
3. Type **443** as the **Port**.
4. Enter a recognizable **Service Name**, such as **UAG-HTTPS Multiple VIPs**.
5. Click **Add this Virtual Service**.

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

Section	Option	Value	Comment
Advanced Properties	Add a Port 80 Redirector VS	https://%h%s	Click the Add HTTP Redirector button. This automatically creates a redirect on port 80.
Basic Properties	Service Type	Generic	
Standard Options	Persistence Mode	SSL Session ID	
	Timeout	6 minutes	
	Scheduling Method	least connection	
Real Servers	Real Server Check Method	HTTPS Protocol	
	URL	/favicon.ico	

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.

Create a HTTPS - UAG Multiple Ports HTTPS HTTP Redirect Virtual Service

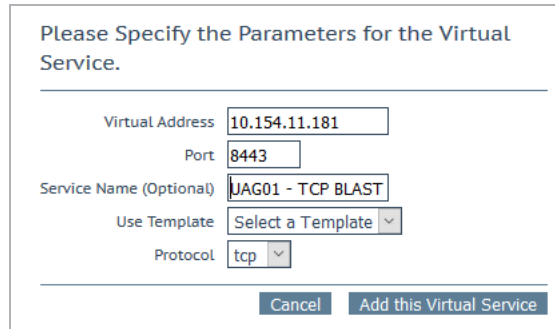
Clicking the **Add HTTP Redirector** button automatically creates a port 80 redirect Virtual Service. This is optional, but the purpose of this Virtual Service is to redirect any clients who have connected using HTTP to the HTTPS Virtual Service.

6 Unified Access Gateway Session Affinity Options

6.3.1.2 Create a UAG01 TCP Blast-UDP Multiple VIPs Virtual Service

The following are the steps involved and the recommended settings to configure the UAG01 - TCP Blast 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 **8443** as the **Port**.
4. Enter a recognizable **Service Name**, such as **UAG01 – TCP Blast Multiple VIP**.
5. Click **Add this Virtual Service**.
6. Configure the settings as recommended in the following table:

Section	Option	Value
Basic Properties	Service Type	Generic
Standard Options	Persistence Mode	SSL Session ID
	Timeout	1 Hour
	Scheduling Method	least connection
Real Servers	Real Server Check Method	TCP Connection Only

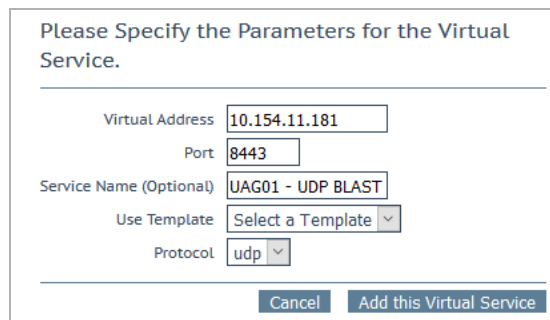
7. Add the Real Servers:
 - a) Expand the **Real Servers** section.
 - b) Click **Add New**.
 - c) Type the address of the relevant Real Server.

- d) Type **8443** as the **Port**.
- e) Complete the other fields as required.
- f) Click **Add this Real Server** then click **OK** to the pop-up message.

6.3.1.3 Create a UAG01 – UDP Blast Multiple VIPs Virtual Service

The following are the steps involved and the recommended settings to configure the UAG01 - UDP Blast Multiple VIPs 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: 10.154.11.181

Port: 8443

Service Name (Optional): UAG01 - UDP BLAST

Use Template: Select a Template

Protocol: udp

Buttons: Cancel, Add this Virtual Service

2. Type a valid **Virtual Address**.
3. Type **8443** as the **Port**.
4. Enter a recognizable **Service Name**, such as **UAG01 - UDP Blast Multiple VIPs**.
5. Click **Add this Virtual Service**.
6. Configure the settings as recommended in the following table:

Section	Option	Value
Standard Options	Force L4	Disabled
Real Servers	Real Server Check Method	ICMP Ping

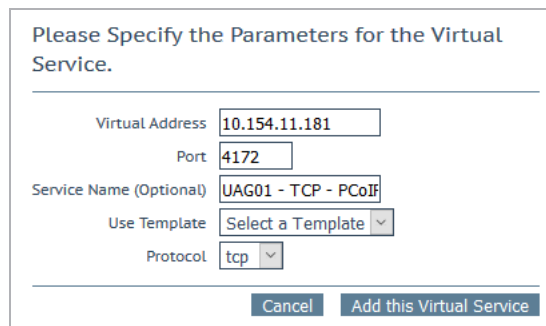
7. Add the Real Servers:
 - a) Expand the **Real Servers** section.
 - b) Click **Add New**.
 - c) Type the address of the relevant Real Server.

- d) Type **8443** as the **Port**.
- e) Complete the other fields as required.
- f) Click **Add this Real Server** then click **OK** to the pop-up message.

6.3.1.4 Create a UAG01 - TCP - PCoIP Multiple VIPs Virtual Service

The following are the steps involved and the recommended settings to configure the UAG01 - TCP - 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 **UAG01 - TCP - PCoIP Multiple VIPs**.
5. Click Add this **Virtual Service**.
6. Configure the settings as recommended in the following table:

Section	Option	Value
Basic Properties	Service Type	Generic
Standard Options	Persistence Mode	SSL Session ID
	Timeout	1 Hour
	Scheduling Method	least connection
Real Servers	Real Server Check Method	TCP Connection Only

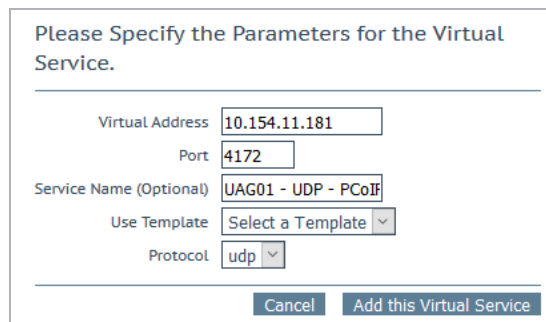
7. Add the Real Servers:

- 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.

6.3.1.5 Create a UAG01 - UDP - PCoIP Multiple VIPs Virtual Service

The following are the steps involved and the recommended settings to configure the UAG01 - UDP - PCoIP Multiple VIPs 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: 10.154.11.181

Port: 4172

Service Name (Optional): UAG01 - UDP - PCoIP

Use Template: Select a Template

Protocol: udp

Buttons: Cancel, Add this Virtual Service

2. Type a valid **Virtual Address**.
3. Type **4172** as the **Port**.
4. Enter a recognizable **Service Name**, such as **AG01 - UDP - PCoIP Multiple VIP**.
5. Select **udp** as the **Protocol**.
6. Click **Add this Virtual Service**.
7. Configure the settings as recommended in the following table:

Section	Option	Value
Standard Options	Force L4	Disabled
Real Servers	Real Server Check Method	ICMP Ping

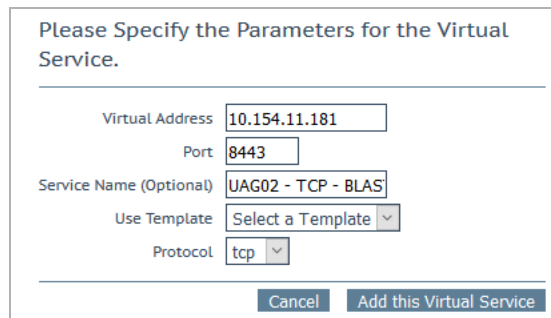
8. Add the Real Servers:

- 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.

6.3.1.6 Create a UAG - TCP - Blast Multiple VIPs Virtual Service

The following are the steps involved and the recommended settings to configure the UAG02 – TCP - Blast Multiple VIPs 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: 10.154.11.181

Port: 8443

Service Name (Optional): UAG02 - TCP - BLAS

Use Template: Select a Template

Protocol: tcp

Buttons: Cancel, Add this Virtual Service

2. Type a valid **Virtual Address**.
3. Type **8443** as the **Port**.
4. Enter a recognizable **Service Name**, such as **UAG02 – TCP - Blast Multiple VIPs**.
5. Select **tcp** as the **Protocol**.
6. Click **Add this Virtual Service**.
7. Configure the settings as recommended in the following table:

Section	Option	Value
Basic Properties	Service Type	Generic

Section	Option	Value
Standard Options	Persistence Mode	SSL Session ID
	Timeout	1 Hour
	Scheduling Method	least connection
Real Servers	Real Server Check Method	TCP Connection Only

8. Add the Real Servers:

- Expand the **Real Servers** section.
- Click **Add New**.
- Type the address of the relevant Real Server.
- Type **8443** as the **Port**.
- Complete the other fields as required.
- Click **Add this Real Server** then click **OK** to the pop-up message.
- Repeat the steps above to add more Real Servers as needed, based on your environment.

6.3.1.7 Create a UAG02 – UDP - Blast Multiple VIPs Virtual Service

The following are the steps involved and the recommended settings to configure the UAG02 - UDP - Blast Multiple VIPs Virtual Service:

- 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

Port

Service Name (Optional)

Use Template

Protocol

- Type a valid **Virtual Address**.
- Type **8443** as the **Port**.

4. Enter a recognizable **Service Name**, such as **UAG02 – UDP – Blast Multiple VIP**.
5. Select **udp** as the **Protocol**.
6. Click **Add this Virtual Service**.
7. Configure the settings as recommended in the following table:

Section	Option	Value
Standard Options	Force L4	Disabled
Real Servers	Real Server Check Method	ICMP Ping

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 **8443** as the **Port**.
 - e) Complete the other fields as required.
 - f) Click **Add this Real Server** then click **OK** to the pop-up message.

6.3.1.8 Create a UAG02 – TCP - PCoIP Multiple VIPs Virtual Service

The following are the steps involved and the recommended settings to configure the UAG02 – TCP - PCoIP Multiple VIPs 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

Port

Service Name (Optional)

Use Template

Protocol

2. Type a valid **Virtual Address**.

3. Type **4172** as the **Port**.
4. Enter a recognizable **Service Name**, such as **UAG02 - TCP - PCoIP Multiple VIP**.
5. Click **Add this Virtual Service**.
6. Configure the settings as recommended in the following table:

Section	Option	Value
Basic Properties	Service Type	Generic
Standard Options	Persistence Mode	SSL Session ID
	Timeout	1 Hour
	Scheduling Method	least connection
Real Servers	Real Server Check Method	TCP Connection Only

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.

6.3.1.9 Create a UAG02 – UDP- PCoIP Multiple VIPs Virtual Service

The following are the steps involved and the recommended settings to configure the **UAG02 – PCoIP-UDP Multiple VIPs Virtual Service**:

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

6 Unified Access Gateway Session Affinity Options

Please Specify the Parameters for the Virtual Service.

Virtual Address

10.154.11.181

Port

4172

Service Name (Optional)

UAG02 - UDP - PCoIP

Use Template

Select a Template

Protocol

udp

Cancel

Add this Virtual Service

2. Type a valid **Virtual Address**.
3. Type **4172** as the **Port**.
4. Enter a recognizable **Service Name**, such as **UAG02 – UDP - PCoIP Multiple VIP**.
5. Select **udp** as the **Protocol**.
6. Click **Add this Virtual Service**.
7. Configure the settings as recommended in the following table:

Section	Option	Value
Standard Options	Force L4	Disabled
Real Servers	Real Server Check Method	ICMP Ping

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.

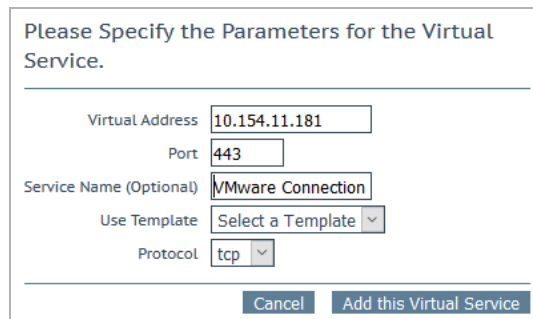
7 Connection Server

The Connection Server is a core component of VMware Horizon View. This role defines virtual desktop pools, applications and permissions. The initial Primary Horizon Protocol is load balanced between Connection Servers in the environment. The Secondary Horizon Protocols are connected by directly bypassing the load balancer.

7.1 Create the Connection Server Virtual Services

The following are the steps involved and the recommended settings to configure the VMware Connection Server 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 **443** as the **Port**.
4. Enter a recognizable Service Name, such as **VMware Connection Server**.
5. Click **Add this Virtual Service**.
6. Configure the settings as recommended in the following table:

Section	Option	Value	Comment
SSL Properties	SSL Acceleration	Enabled	
	Reencrypt	Enabled	
	Supported	TLS1.0;	While this workload may not support TLS1.3 yet,

		TLS1.1;	
	Protocols	TLS1.2;	Kemp recommend enabling it for future proofing.
		TLS1.3	
	Cipher Set	Best Practices	
Standard Options	Persistence Mode	Active Cookie	
	Timeout	1 Hour	
	Cookie Name	JSESSIONID	
	Scheduling Method	least connection	
Advanced Properties	Add a Port 80 Redirector VS	https://%h%s	Click the Set Redirect button. This automatically creates a redirect on port 80.
Real Servers	URL	/	
	HTTP Method	GET	

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.

Create a HTTPS – Connection Server 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. Kemp also recommends changing the **Persistence Mode** and **Real Server Check Method** to **None**.

8 App Volume Manager

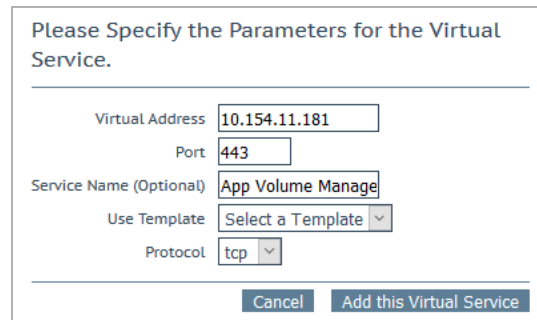
The App Volume Manager is a console for managing configuration, creation of AppStacks, and assignment of AppStacks and writable volumes.

8.1 Create App Volume Manager Virtual Services

The following sections describe the recommended settings for the VMware App Volume Manager Virtual Services.

The following are the steps involved and the recommended settings to configure the VMware App Volume Manager 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 **443** as the **Port**.
4. Enter a recognizable Service Name, such as **VMware App Volume Mgr**
5. Click **Add this Virtual Service**.
6. Configure the settings as recommended in the following table:

Section	Option	Value	Comment
SSL Properties	SSL Acceleration	Enabled	
	Reencrypt	Enabled	
	Supported Protocols	TLS1.0;	While this workload

		TLS1.1; TLS1.2; TLS1.3	may not support TLS1.3 yet, Kemp recommend enabling it for future proofing.
	Cipher Set	Best Practices	
Standard Options	Persistence Mode	Active Cookie	
	Timeout	1 Hour	
	Cookie name	JSESSIONID	
	Scheduling Method	least connection	
Advanced Properties	Add a Port 80 redirector VS	https://%h%s	Click the Add HTTP Redirector button. This automatically creates a redirect on port 80.
Real Servers	URL	/	
	HTTP Method	GET	

7. Add the Real Servers:

- Expand the **Real Servers** section.
- Click **Add New**.
- Type the address of the relevant Real Server.
- Type **443** as the **Port**.
- Complete the other fields as required.
- Click **Add this Real Server** then click **OK** to the pop-up message.
- Repeat the steps above to add more Real Servers as needed, based on your environment.

Create a HTTPS – Connection Server 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. Kemp also recommends changing the **Persistence Mode** and **Real Server Check Method** to **None**.

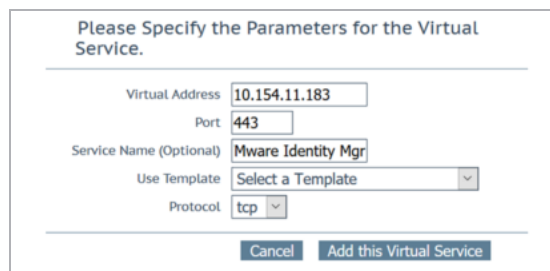
9 Identity Manager

The VMware Identity Manager provides several functions in relation to the Horizon View 7 implementation such as a portal where users gain access to different types of applications including SaaS-based, enterprise identity management to sync and extend Active Directory, and single sign on. There is also a self-service app store that enables users to search and select applications in a simple way.

9.1 Create Identity Manager Virtual Services

The following are the steps involved and the recommended settings to configure the VMware Identity Manager 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 **443** as the **Port**.
4. Enter a recognizable **Service Name**, such as **VMware Identity Mgr**.
5. Click **Add this Virtual Service**.
6. Configure the settings as recommended in the following table:

Section	Option	Value	Comments
SSL Properties	SSL Acceleration	Enabled	
	Reencrypt	Enabled	
	Supported	TLS1.0;	While this workload may not support TLS1.3 yet,

Section	Option	Value	Comments
		TLS1.1;	
	Protocols	TLS1.2; TLS1.3	Kemp recommend enabling it for future proofing.
	Cipher Set	Best Practices	
Standard Options	Persistence Mode	Active Cookie	
	Timeout	1 Hour	
	Cookie name	JSESSIONID	
	Scheduling Method	least connection	
Advanced Properties	Add a Port 80 redirector VS	https://%h%s	Click the Add HTTP Redirector button. This automatically creates a redirect on port 80.
Real Servers	URL	/	
	HTTP Method	GET	

7. Add the Real Servers:

- Expand the **Real Servers** section.
- Click **Add New**.
- Type the address of the relevant Real Server.
- Type **443** as the **Port**.
- Complete the other fields as required.
- Click **Add this Real Server** then click **OK** to the pop-up message.
- Repeat the steps above to add more Real Servers as needed, based on your environment.

Create a HTTPS – Connection Server 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. Kemp also recommends changing the **Persistence Mode** and **Real Server Check Method** to **None**.

Last Updated Date

This document was last updated on 27 July 2023.