Load Balancing VMware Horizon View

Deployment Guide

v1.1.0

Copyright © 2014 Loadbalancer.org, Inc.
# Table of Contents

About this Guide........................................................................................................................................ 4  
Appliances Supported............................................................................................................................... 4  
VMware Horizon View Versions Supported............................................................................................... 4  
Loadbalancer.org Software Versions Supported......................................................................................... 4  
VMware Horizon View.................................................................................................................................. 5  
Horizon View Servers to Load Balance...................................................................................................... 5  
Load Balancing VMware View.................................................................................................................... 5  
  Load Balancing & HA Requirements......................................................................................................... 5  
  Persistence (aka Server Affinity)............................................................................................................... 5  
  SSL Offload.............................................................................................................................................. 5  
  Port Requirements.................................................................................................................................... 5  
Deployment Overview.................................................................................................................................... 6  
Clustered Pair Configuration for HA........................................................................................................ 6  
Load Balancer Deployment Methods........................................................................................................ 6  
  View Client Connection Process (2 Phase).............................................................................................. 6  
External Clients............................................................................................................................................. 7  
  Method 1 – Fully load balanced Phase 1 & 2 (Using Source IP Persistence).............................................. 7  
  Method 2 – Load Balanced Phase 1 (Using Source IP Persistence).......................................................... 8  
  Method 3 – Load Balanced Phase 1 (Using Application Cookie Persistence)....................................... 9  
  External Clients - Helping you Choose the most appropriate Method.................................................... 10  
Internal Clients............................................................................................................................................... 11  
  Method 1 – Load Balanced Phase 1 (Using Source IP Persistence)......................................................... 11  
  Method 2 – Load Balanced Phase 1 (Using Application cookie Persistence).......................................... 12  
  Internal Clients - Helping you Choose the most appropriate Method..................................................... 13  
Loadbalancer.org Appliance – the Basics.................................................................................................... 14  
  Network Configuration.............................................................................................................................. 14  
  Accessing the Web User Interface (WUI)................................................................................................. 15  
Configuring for Horizon View External Clients.......................................................................................... 16  
  Method 1 – Fully load balanced Phase 1 & 2 (Using Source IP Persistence)........................................... 16  
  View Server Configuration...................................................................................................................... 16  
  Appliance Configuration............................................................................................................................ 17  
  Port Requirements................................................................................................................................... 17  
  Configure the Virtual Service & Real Servers......................................................................................... 17  
  Configure HTTP to HTTPS Redirect...................................................................................................... 19  
  Method 2 – Load Balanced Phase 1 (Using Source IP Persistence)...................................................... 20  
  View Server Configuration...................................................................................................................... 20  
  Appliance Configuration............................................................................................................................ 21  
  Port Requirements................................................................................................................................... 21  
  Configure Layer 7 Global Settings........................................................................................................... 21  
  Configure the Virtual Service & Real Servers.......................................................................................... 22  
  Configure HTTP to HTTPS Redirect...................................................................................................... 23  
  Finalizing the Configuration..................................................................................................................... 23  
  Method 3 – Load Balanced Phase 1 (Using Application Cookie Persistence)..................................... 24  
  View Server Configuration...................................................................................................................... 24  
  Appliance Configuration............................................................................................................................ 25  
  Port Requirements................................................................................................................................... 25  
  Configure Layer 7 Global Settings........................................................................................................... 26  
  Configure SSL Termination....................................................................................................................... 26  
  Configure the Virtual Service & Real Servers.......................................................................................... 27  
  Configure HTTP to HTTPS Redirect...................................................................................................... 28
Finalizing the Configuration

Configuring for Horizon View Internal Clients

Method 1 – Load Balanced Phase 1 (Using Source IP Persistence)

Connection Server Configuration

Appliance Configuration

Port Requirements

Configure Layer 7 Global Settings

Configure the Virtual Service & Real Servers

Configure HTTP to HTTPS Redirect

Finalizing the Configuration

Method 2 – Load Balanced Phase 1 (Using Application cookie Persistence)

Connection Server Configuration

Appliance Configuration

Port Requirements

Configure Layer 7 Global Settings

Configure SSL Termination

Configure the Virtual Service & Real Servers

Configure HTTP to HTTPS Redirect

Finalizing the Configuration

Testing & Verification

Using System Overview

Layer 4 Status Report

Layer 7 Statistics Report

Appliance Logs

Technical Support

Conclusion

Appendix

1 – Configuring an HTTP to HTTPS redirect

2 – Clustered Pair Configuration – Adding a Slave Unit

3 – Company Contact Information
About this Guide
This guide details the configuration of Loadbalancer.org appliances for deployment with VMware Horizon View. It includes details of ports/services that must be load balanced, topology considerations for the various VMware Horizon View servers and also steps on how to configure the appliances.

For an introduction on setting up the appliance as well as more technical information, please also refer to our quick-start guides and full administration manuals which are available at the following links:


Appliances Supported
All our products can be used with Horizon View. The complete list of models is shown below:

- Enterprise R16
- Enterprise
- Enterprise MAX
- Enterprise 10G
- Enterprise R320
- Enterprise VA
- Enterprise VA R16

For a full specification comparison of these models please refer to: http://www.loadbalancer.org/matrix.php

VMware Horizon View Versions Supported
- v5.2 and later

Loadbalancer.org Software Versions Supported
- v7.5.2 and later

N.B. this guide includes configuration steps for v7.6 & later. For older versions of the appliance please contact loadbalancer.org sales or support.
VMware Horizon View

VMware® Horizon View™ (formerly VMware View) is a virtual desktop infrastructure solution that simplifies desktop management and provides users with access when needed, whatever their location.

Horizon View Servers to Load Balance

<table>
<thead>
<tr>
<th>Server</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connection Server</td>
<td>View Connection Server acts as a broker for client connections. It authenticates users through Windows Active Directory and directs the request to the appropriate virtual machine, physical or blade PC, or Windows Terminal Services server.</td>
</tr>
<tr>
<td>Security Server</td>
<td>A security server is a special instance of View Connection Server that runs a subset of View Connection Server functions. A security server is used to provide an additional layer of security between the Internet and the internal network. A security server resides within a DMZ and acts as a proxy host for connections inside the trusted network. Each security server is paired with an instance of View Connection Server and forwards all traffic to that instance.</td>
</tr>
</tbody>
</table>

Load Balancing VMware View

Load Balancing & HA Requirements

For high availability and scalability, VMware recommend that multiple Connection Servers and multiple Security Serves are deployed in a load balanced cluster.

Persistence (aka Server Affinity)

It's important that client requests are directed at the same View server for the duration of their session. This can be achieved using either source IP persistence or application cookie (JSESSIONID) persistence.

SSL Offload

The load balancer can be configured to terminate SSL if required. However, this is only recommended when JSESSIONID application cookie persistence is used.

Port Requirements

The following table shows the ports that are load balanced.

_N.B. The exact ports to be load balanced depends on how the View Security/Connection Servers are load balanced. This is covered in later sections in this guide._
### Deployment Overview

A Virtual Services (VIP) is configured on the load balancer that acts as a connection point for clients. Clients then connect to the VIP on the load balancer rather than connecting directly to a one of the View Servers. These connections are then load balanced across the back-end servers (i.e. the View Servers) to distribute the load according to the load balancing algorithm selected.

The load balancer can be deployed as a single unit, although Loadbalancer.org strongly recommends a clustered pair for resilience & high availability.

### Clustered Pair Configuration for HA

In this guide a single unit is deployed first, adding a secondary slave unit is covered in section 1 of the Appendix.

### Load Balancer Deployment Methods

The load balancer can be configured in various ways to support internal and external clients as detailed in the following sections.

#### View Client Connection Process (2 Phase)

View clients connect in 2 phases, these are:

* **Phase 1:** initial connection establishment, authentication, entitlement etc.
* **Phase 2:** tunnel connection

<table>
<thead>
<tr>
<th>Port</th>
<th>Protocol</th>
<th>Uses</th>
</tr>
</thead>
<tbody>
<tr>
<td>443</td>
<td>TCP</td>
<td>HTTPS</td>
</tr>
<tr>
<td>4172</td>
<td>TCP</td>
<td>PCoIP</td>
</tr>
<tr>
<td>4172</td>
<td>UDP</td>
<td>PCoIP</td>
</tr>
<tr>
<td>32111</td>
<td>TCP</td>
<td>USB Redirection</td>
</tr>
</tbody>
</table>
External Clients

External clients connect to the Security Servers located in the DMZ. Each Security Server must be paired with a corresponding Connection Server. The PCoIP gateway on each Security Server must be enabled and correctly configured to ensure that clients can successfully connect.

Method 1 – Fully load balanced Phase 1 & 2 (Using Source IP Persistence)

In this scenario **ALL** client traffic passes via the load balancer. This option has the advantage that only one public IP address is required. Source IP address persistence is used which may result in an unbalanced distribution of connections for external clients due to inline NAT/proxy devices. This can happen because under these circumstances multiple clients can appear to come from the same IP address and therefore the load balancer will forward all these connections to the same Security Server rather than distributing them equally between the servers.

Notes:

- The VIP is configured in Layer 4 NAT mode
- The VIP is used to load balance both phase 1 and phase 2 of the connection process and must listen on TCP ports 443, 4172 & 32111 and UDP port 4172
- The Security Servers must be configured to gateway the connections. Clients then connect to the desktops via the load balancer and the Security Servers
- Source IP address persistence may result in non balanced connections due to inline NAT/proxy devices for external clients
- The VIP and Security Servers must be in different subnets and the default gateway on each Security Server must be an IP address on the load balancer. For a clustered pair this should be a floating IP address to allow failover to the slave device
- See pages 16-19 for appliance and server configuration steps
Method 2 – Load Balanced Phase 1 (Using Source IP Persistence)

In this scenario, only Phase 1 is handled by the load balancer. A single VIP in layer 7 SNAT mode is used and is configured to use source IP address persistence to ensure that clients connect to the same Security Server for the duration of the Phase. Once Phase 1 negotiation is complete, Phase 2 connections are direct from the client to the Security Servers. For this to work, each Security Server must be externally accessible from the Internet.

Notes:

- The VIP is configured in Layer 7 SNAT mode
- The VIP is used to load balance phase 1 of the connection process and must listen on TCP port 443
- The Security Servers must be configured to gateway the connections. Clients then connect to the desktops via the Security Servers bypassing the load balancer
- The Security Servers must be accessible externally for Phase 2 connections
- Source IP address persistence may result in non balanced connections due to inline NAT/proxy devices for external clients
- See pages 20-23 for appliance and server configuration steps
Method 3 – Load Balanced Phase 1 (Using Application Cookie Persistence)

In this scenario, only Phase 1 is handled by the load balancer. A single VIP in layer 7 SNAT mode is used and is configured to use application cookie (JSESSIONID) persistence to ensure that clients connect to the same Security Server for the duration of the Phase. Once Phase 1 negotiation is complete, Phase 2 connections are direct from the client to the Security Servers. For this to work, each Security Server must also be externally accessible from the Internet.

Notes:

- The VIP is configured in Layer 7 SNAT mode
- The VIP is used to load balance phase 1 of the connection process and must listen on TCP port 443
- SSL is terminated on the Load Balancer to enable the JSESSIONID cookie to be read
- The Security Servers must be configured to gateway the connections. Clients then connect to the desktops via the Security Servers bypassing the load balancer
- The Security Servers must be accessible externally for Phase 2 connections
- A locked.properties file must be created on each Security Server and configured to permit HTTP connections from the load balancer
- See pages 24-29 for appliance and server configuration steps
Do external clients have unique IP addresses?

Do you want to use a single public IP address?

Use Option 1

Use Option 2

Use Option 3
Internal Clients

Internal clients connect directly to the Connection Servers located on the LAN. The gateway must be disabled so that clients can connect directly to the desktops rather than passing via the load balancer or gateway.

**Method 1 – Load Balanced Phase 1 (Using Source IP Persistence)**

**Notes:**

- The VIP is configured in Layer 7 SNAT mode
- A single VIP is used to load balance phase 1 of the connection process and must listen on TCP port 443
- The security servers must NOT be configured to gateway the connections. Clients are then able to connect directly to the desktops
- Source IP address persistence may result in non balanced connections due to inline NAT/proxy devices for external clients
- See pages 30-33 for appliance and server configuration steps
Method 2 – Load Balanced Phase 1 (Using Application cookie Persistence)

Notes:

• The VIP is configured in Layer 7 SNAT mode

• A single VIP is used to load balance phase 1 of the connection process and must listen on TCP port 443

• SSL is terminated on the load balancer

  N.B. SSL offload is not supported for smart-card authentication

• The security servers must NOT be configured to gateway the connections. Clients are then able to connect directly to the desktops

• Persistence is based on the JSESSIONID cookie that is inserted by the Connection Servers

• A locked.properties file must be created on each Connection Server and configured to permit HTTP connections from the load balancer

• See pages 34-38 for appliance and server configuration steps
Internal Clients - Helping you Choose the most appropriate Method

START

Do internal clients have unique IP address?

YES → Use Option 1

NO → Use Option 2
Network Configuration
The IP address, default gateway and DNS settings can be configured in several ways as detailed below.

Configure the IP address, Default Gateway & DNS Settings

Using the Network Setup Wizard at the console:
After boot, follow the console instructions to configure the IP address, gateway and DNS settings.

Using the WUI:
Using a browser, connect to the WUI on the default IP address/port: http://192.168.2.21:9080
to set the IP address use: Local Configuration > Network Interface Configuration
to set the default gateway use: Local Configuration > Routing
to configure DNS settings use: Local Configuration > Hostname & DNS

Using Linux commands:
At the console, set the initial IP address using the following command:
ip addr add <IP address>/mask dev eth0
e.g. ip addr add 192.168.2.10/24 dev eth0

At the console, set the initial default gateway using the following command:
route add default gw <IP address> <interface>
e.g. route add default gw 192.168.2.254 eth0

At the console, set the DNS server using the following command:
echo nameserver <IP address> >> /etc/resolv.conf
  e.g. echo nameserver 192.168.64.1 >> /etc/resolv.conf

N.B. If this method is used, you must also configure these settings using the WUI, otherwise settings will be lost after a reboot
Accessing the Web User Interface (WUI)

The WUI can be accessed from a browser at:  

http://192.168.2.21:9080/lbadmin

* Note the port number → 9080

(replace 192.168.2.21 with the IP address of your load balancer if its been changed from the default)

**Username**: loadbalancer  
**Password**: loadbalancer

Once you have entered the logon credentials the Loadbalancer.org Web User Interface will be displayed as shown below.

The screen shot below shows the v7.6 WUI once logged in:
Configuring for Horizon View External Clients

External clients connect to View Security Servers. This section covers the various methods for load balancing Security Servers.

**NOTE:** It's highly recommended that you have a working VMware Horizon View environment first before implementing the load balancer.

Method 1 – Fully load balanced Phase 1 & 2 (Using Source IP Persistence)

This method uses a Firewall Mark configuration which enables a single VIP to support both TCP and UDP.

**View Server Configuration**

The following sections illustrate how the Connection/Security Servers must be configured for external clients.

**Paired Connection Server Settings**

For each Connection Server leave the servers own IP address / DNS FQDN and ensure all check boxes are enabled:

![Edit View Connection Server Settings](image-url)

- **HTTP(S) Secure Tunnel**
  - Use Secure Tunnel connection to desktop
  - External URL: `https://192.168.120.101:443` Example: `https://myserver.com:443`

- **PCoIP Secure Gateway**
  - Use PCoIP Secure Gateway for PCoIP connections to desktop
  - PCoIP External URL: `192.168.120.101:4172` Example: `10.0.0.1:4172`

- **Blast Secure Gateway**
  - Use Blast Secure Gateway for HTML access to desktop
  - Blast External URL: `https://192.168.120.101:8443` Example: `https://myserver.com:8443`
Paired Security Server Settings

For each Security Server set the IP addresses / DNS FQDN’s to be the external address of the VIP, e.g.:

```
N.B. In this example 10.100.120.10 is used, in production publicly accessible IP addresses would be required. In this example the external firewall would NAT 10.100.120.10 to the VIP address 192.168.110.10.
```

Appliance Configuration

Port Requirements

The following table shows the ports that must be load balanced.

<table>
<thead>
<tr>
<th>Port</th>
<th>Protocol</th>
<th>Uses</th>
</tr>
</thead>
<tbody>
<tr>
<td>443</td>
<td>TCP</td>
<td>HTTPS</td>
</tr>
<tr>
<td>4172</td>
<td>TCP</td>
<td>PCoIP</td>
</tr>
<tr>
<td>4172</td>
<td>UDP</td>
<td>PCoIP</td>
</tr>
<tr>
<td>32111</td>
<td>TCP</td>
<td>USB Redirection</td>
</tr>
</tbody>
</table>

Configure the Virtual Service & Real Servers

a) Setting up the Virtual Service

- Using the WUI, go to Cluster Configuration > Layer 4 – Virtual Service and click [Add a New Virtual Service]
- Enter the following details:
- Enter an appropriate label for the VIP, e.g. **ViewExternal**
- Set the **Virtual Service IP address** field to the required Mark value, e.g. **1**
- The **Virtual Service Ports** Field is not required in this case and is disabled
- **Set Protocol** to **Firewall Marks**
- **Set Forwarding Method** to **NAT**
- Click **Update**
- Now click **[Modify]** next to the newly created VIP
- **Set Check Type** to **Negotiate**
- **Set Check Port** to **443**
- **Set Protocol** to **HTTPS**
- **Set Response expected** to **Vmware**
- Click **Update**

**b) Setting up the Real Servers**

- Using the WUI, go to **Cluster Configuration > Layer 4 -- Real Servers** and click **[Add a new Real Server]** next to the newly created VIP
- Enter the following details:
Enter an appropriate label for the RIP, e.g. Security1

Change the Real Server IP Address field to the required IP address, e.g. 192.168.120.100

Leave the Real Server Port field blank

Click Update

Repeat the above steps to add your other Security Server(s)

c) Configure the Firewall Rules (required for Firewall Marks)

Using the WUI, go to Maintenance > Firewall Script

Scroll down to the “Manual Firewall Marks” section and configure the following rules:

```
VIP1="192.168.100.10"
iptables -t mangle -A PREROUTING -p tcp -d $VIP1 --dport 443 -j MARK --set-mark 1
iptables -t mangle -A PREROUTING -p tcp -d $VIP1 --dport 4172 -j MARK --set-mark 1
iptables -t mangle -A PREROUTING -p udp -d $VIP1 --dport 4172 -j MARK --set-mark 1
iptables -t mangle -A PREROUTING -p tcp -d $VIP1 --dport 32111 -j MARK --set-mark 1
```

N.B. set 'VIP1' to the required IP address

Click Update

d) Add the Floating IP address

Using the WUI, go to Cluster Configuration > Floating IP’s

Enter the IP address for the VIP, e.g. 192.168.100.10

Click Add Floating IP

Configure HTTP to HTTPS Redirect

If required, the load balancer can be configured to automatically redirect users who attempt to connect to http://<URL to access VIEW> to https://<URL to access VIEW>. For details on configuring this, please refer to section 1 in the Appendix.
Method 2 – Load Balanced Phase 1 (Using Source IP Persistence)

**View Server Configuration**

The following sections illustrate how the Connection/Security Servers must be configured for external clients.

**Paired Connection Server Settings**

For each Connection Server leave the servers own IP address / DNS FQDN and ensure all check boxes are enabled:

![Edit View Connection Server Settings](image)

**Paired Security Server Settings**

For each Security Server set the IP addresses / DNS FQDN's to be the external address for that Security Server, e.g.: 
N.B. In this example 10.100.100.100 used, in production publicly accessible IP addresses would be required. In this example the external firewall would NAT 10.100.100.100 to the Security Servers address 192.168.100.100

Appliance Configuration

Port Requirements
The following table shows the ports that must be load balanced.

<table>
<thead>
<tr>
<th>Port</th>
<th>Protocol</th>
<th>Uses</th>
</tr>
</thead>
<tbody>
<tr>
<td>443</td>
<td>TCP</td>
<td>HTTPS</td>
</tr>
</tbody>
</table>

Configure Layer 7 Global Settings
To ensure that client connections remain open during periods of inactivity, the Client Timeout and Server Timeout values must be changed from their default values of 43 seconds and 45 seconds respectively to 10 minutes. To do this follow the steps below:

- Go to Cluster Configuration > Layer 7 – Advanced Configuration
Configure the Virtual Service & Real Servers

a) Setting up the Virtual Service

- Using the WUI, go to Cluster Configuration > Layer 7 – Virtual Service and click [Add a New Virtual Service]
- Enter the following details:
  - Enter an appropriate label for the VIP, e.g. ViewExternal
  - Set the Virtual Service IP address field to the required IP address, e.g. 192.168.100.10
  - Set the Virtual Service Ports field to 443
  - Ensure Layer 7 Protocol is set to TCP Mode
  - Click Update
b) Setting up the Real Servers

- Using the WUI, go to Cluster Configuration > Layer 7 – Real Servers and click [Add a new Real Server] next to the newly created VIP

- Enter the following details:

<table>
<thead>
<tr>
<th>Label</th>
<th>Security1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Real Server IP Address</td>
<td>192.168.100.100</td>
</tr>
<tr>
<td>Real Server Port</td>
<td>443</td>
</tr>
<tr>
<td>Weight</td>
<td>100</td>
</tr>
</tbody>
</table>

- Enter an appropriate label for the RIP, e.g. Security1
- Change the Real Server IP Address field to the required IP address, e.g. 192.168.100.100
- Change the Real Server Port field to 443
- Click Update
- Repeat the above steps to add your other Security Server(s)

Configure HTTP to HTTPS Redirect

If required, the load balancer can be configured to automatically redirect users who attempt to connect to http://<URL to access VIEW> to https://<URL to access VIEW>. For details on configuring this, please refer to section 1 in the Appendix.

Finalizing the Configuration

To apply the new settings, HAProxy must be restarted as follows:

- Go to Maintenance > Restart Services and click Restart HAProxy
Method 3 – Load Balanced Phase 1 (Using Application Cookie Persistence)

View Server Configuration
The following sections illustrate how the Connection/Security Servers must be configured for external clients.

Paired Connection Server Settings
For each Connection Server leave the servers own IP address / DNS FQDN and ensure all check boxes are enabled:

Paired Security Server Settings
For each Security Server set the IP addresses / DNS FQDN's to be the external address for that Security Server, e.g.:
N.B. In this example 10.100.100.100 used, in production publicly accessible IP addresses would be required. In this example the external firewall would NAT 10.100.100.100 to the Security Servers address 192.168.100.100.

Allowing HTTP connections
Since SSL is terminated on the load balancer, there will be an HTTP connection from the load balancer to the Security Servers. To enable this, follow these steps for each Security Server:

- Navigate to the folder C:\Program Files\Vmware\Vmware View\Server\sslgateway\conf
- Create a text file called locked.properties with the following contents:

```
ServerProtocol=http
```

Appliance Configuration

Port Requirements
The following table shows the ports that must be load balanced.

<table>
<thead>
<tr>
<th>Port</th>
<th>Protocol</th>
<th>Uses</th>
</tr>
</thead>
<tbody>
<tr>
<td>443</td>
<td>TCP</td>
<td>HTTPS</td>
</tr>
</tbody>
</table>
Configure Layer 7 Global Settings

To ensure that client connections remain open during periods of inactivity, the Client Timeout and Server Timeout values must be changed from their default values of 43 seconds and 45 seconds respectively to 10 minutes. To do this follow the steps below:

• Go to Cluster Configuration > Layer 7 – Advanced Configuration

  | Lock HAProxy Configuration |  
  | Logging |  
  | Log Only Errors |  
  | Redispatch |  
  | Connection Timeout | 4000 ms |  
  | Client Timeout | 600000 ms |  
  | Real Server Timeout | 500000 ms |  

  • Change Client Timeout to 600000 as shown above (i.e. 10 minutes)
  • Change Real Server Timeout to 600000 as shown above (i.e. 10 minutes)
  • Click the Update button to save the settings

Configure SSL Termination

• Using the WUI, go to Cluster Configuration > SSL Termination and click [Add a New Virtual Service]

• Enter the following details:

  | Label | ViewExternalSSL |  
  | Virtual Service IP address | 192.168.100.10 |  
  | Virtual Service Port | 443 |  
  | Backend Virtual Service IP Address | 192.168.100.10 |  
  | Backend Virtual Service Port | 80 |
• Enter an appropriate label for the VIP, e.g. ViewExternalSSL
• Set the Virtual Service IP address field to the required IP address, e.g. 192.168.100.10
• Set the Virtual Service Ports field to 443
• Set the Backend Virtual Service IP Address field to same IP address, e.g. 192.168.100.10
• Set the Backend Virtual Service Port field to 80
• Leave other fields at their default values
• Click Update

Configure the Virtual Service & Real Servers

a) Setting up the Virtual Service

• Using the WUI, go to Cluster Configuration > Layer 7 – Virtual Service and click [Add a New Virtual Service]

• Enter the following details:

<table>
<thead>
<tr>
<th>Label</th>
<th>ViewExternal</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual Service IP Address</td>
<td>192.168.100.10</td>
</tr>
<tr>
<td>Ports</td>
<td>80</td>
</tr>
<tr>
<td>Layer 7 Protocol</td>
<td>HTTP Mode</td>
</tr>
</tbody>
</table>

• Enter an appropriate label for the VIP, e.g. ViewExternal
• Set the Virtual Service IP address field to the required IP address, e.g. 192.168.100.10
• Set the Virtual Service Ports field to 80
• Ensure Layer 7 Protocol is set to HTTP Mode
• Click Update
• Now click [Modify] next to the newly created VIP
• Set Persistence Mode to Application Cookie
• Set Application Cookie Name to JSESSIONID
• Set Application Cookie Length to 32
• Set Application Cookie Hold Time to 1800000
• Click Update
b) Setting up the Real Servers

- Using the WUI, go to Cluster Configuration > Layer 7 – Real Servers and click [Add a new Real Server] next to the newly created VIP
- Enter the following details:

<table>
<thead>
<tr>
<th>Field</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Label</td>
<td>Security1</td>
</tr>
<tr>
<td>Real Server IP Address</td>
<td>192.168.100.100</td>
</tr>
<tr>
<td>Real Server Port</td>
<td>80</td>
</tr>
<tr>
<td>Weight</td>
<td>100</td>
</tr>
</tbody>
</table>

  - Click Update
  - Repeat the above steps to add your other Security Server(s)

Upload The SSL Certificate

1) Export the SSL Certificate from a View Server – note the following points when exporting the certificate from Windows:

- Make sure that the private key is included
- Tick the option ‘Include all certificates in the certification path if possible’

2) Import the SSL Certificate to the Load Balancer – follow the steps listed below:

- Using the WUI goto: Cluster Configuration > SSL Termination, click [Certificate] next to the SSL VIP created earlier
- Using the browse option, navigate to and select the .pfx file created in the previous step
- Click Upload PEM/PFX file
- Now restart Stunnel

Configure HTTP to HTTPS Redirect

If required, the load balancer can be configured to automatically redirect users who attempt to connect to http://<URL to access VIEW> to https://<URL to access VIEW>. For details on configuring this, please refer to section 1 in the Appendix.
Finalizing the Configuration

To apply the new settings, HAProxy must be restarted as follows:

- Go to Maintenance > Restart Services and click Restart HAProxy
Configuring for Horizon View Internal Clients

Internal clients connect to View Connection Servers. This section covers the various methods for load balancing Connection Servers.

NOTE: It's highly recommended that you have a working VMware Horizon View environment first before implementing the load balancer.

Method 1 – Load Balanced Phase 1 (Using Source IP Persistence)

Connection Server Configuration

For each Connection Server leave the servers own IP address / DNS FQDN and un-check the 'Use PCoIP Secure Gateway for PCoIP connections to desktop' checkbox as shown below:
Appliance Configuration

Port Requirements
The following table shows the ports that must be load balanced.

<table>
<thead>
<tr>
<th>Port</th>
<th>Protocol</th>
<th>Uses</th>
</tr>
</thead>
<tbody>
<tr>
<td>443</td>
<td>TCP</td>
<td>HTTPS</td>
</tr>
</tbody>
</table>

Configure Layer 7 Global Settings
To ensure that client connections remain open during periods of inactivity, the Client Timeout and Server Timeout values must be changed from their default values of 43 seconds and 45 seconds respectively to 10 minutes. To do this follow the steps below:

- Go to Cluster Configuration > Layer 7 – Advanced Configuration

  - Lock HAProxy Configuration
  - Logging
    - Log Only Errors
  - Redispatch
  - Connection Timeout: 4000 ms
  - Client Timeout: 600000 ms
  - Real Server Timeout: 600000 ms

- Change Client Timeout to 600000 as shown above (i.e. 10 minutes)
- Change Real Server Timeout to 600000 as shown above (i.e. 10 minutes)
- Click the Update button to save the settings

Configure the Virtual Service & Real Servers

a) Setting up the Virtual Service

- Using the WUI, go to Cluster Configuration > Layer 7 – Virtual Service and click [Add a New Virtual Service]

- Enter the following details:
b) Setting up the Real Servers

- Using the WUI, go to Cluster Configuration > Layer 7 – Real Servers and click [Add a new Real Server] next to the newly created VIP
- Enter the following details:
  
<table>
<thead>
<tr>
<th>Label</th>
<th>Connection1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Real Server IP Address</td>
<td>192.168.100.101</td>
</tr>
<tr>
<td>Real Server Port</td>
<td>443</td>
</tr>
<tr>
<td>Weight</td>
<td>100</td>
</tr>
</tbody>
</table>

- Enter an appropriate label for the RIP, e.g. Connection1
- Change the Real Server IP Address field to the required IP address, e.g. 192.168.100.101
- Change the Real Server Port field to 443
- Click Update
- Repeat the above steps to add your other Connection Server(s)
Configure HTTP to HTTPS Redirect

If required, the load balancer can be configured to automatically redirect users who attempt to connect to http://<URL to access VIEW> to https://<URL to access VIEW>. For details on configuring this, please refer to section 1 in the Appendix.

Finalizing the Configuration

To apply the new settings, HAProxy must be restarted as follows:

- Go to Maintenance > Restart Services and click Restart HAProxy
**Method 2 – Load Balanced Phase 1 (Using Application cookie Persistence)**

**Connection Server Configuration**

For each Connection Server leave the server's own IP address / DNS FQDN and uncheck all checkboxes as shown below:

![Connection Server Configuration](image)

**Allowing HTTP connections**

Since SSL is terminated on the load balancer, there will be an HTTP connection from the load balancer to the Connection Servers. To enable this, follow these steps for each Connection Server:

- Navigate to the folder `C:\Program Files\Vmware\Vmware View\Server\sslgateway\conf`
- Create a text file called `locked.properties` with the following contents:

```
ServerProtocol=http
```
Appliance Configuration

Port Requirements
The following table shows the ports that must be load balanced.

<table>
<thead>
<tr>
<th>Port</th>
<th>Protocol</th>
<th>Uses</th>
</tr>
</thead>
<tbody>
<tr>
<td>443</td>
<td>TCP</td>
<td>HTTPS</td>
</tr>
</tbody>
</table>

Configure Layer 7 Global Settings
To ensure that client connections remain open during periods of inactivity, the Client Timeout and Server Timeout values must be changed from their default values of 43 seconds and 45 seconds respectively to 10 minutes. To do this follow the steps below:

- Go to Cluster Configuration > Layer 7 – Advanced Configuration

Configure SSL Termination

- Using the WUI, go to Cluster Configuration > SSL Termination and click [Add a New Virtual Service]
- Enter the following details:
Configure the Virtual Service & Real Servers

a) Setting up the Virtual Service

- Using the WUI, go to Cluster Configuration > Layer 7 – Virtual Service and click [Add a New Virtual Service]
- Enter the following details:
  - Enter an appropriate label for the VIP, e.g. ViewInternal
  - Set the Virtual Service IP address field to the required IP address, e.g. 192.168.100.10
  - Set the Virtual Service Ports field to 443
  - Set the Backend Virtual Service IP Address field to same IP address, e.g. 192.168.100.10
  - Set the Backend Virtual Service Port field to 80
  - Leave other fields at their default values
  - Click Update

- Now click [Modify] next to the newly created VIP
- Set Persistence Mode to Application Cookie
• Set Application Cookie Name to **JSESSIONID**
• Set Application Cookie Length to **32**
• Set Application Cookie Hold Time to **1800000**
• Click **Update**

**b) Setting up the Real Servers**

• Using the WUI, go to **Cluster Configuration > Layer 7 – Real Servers** and click **[Add a new Real Server]** next to the newly created VIP

• Enter the following details:

<table>
<thead>
<tr>
<th>Label</th>
<th>Connection1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Real Server IP Address</td>
<td>192.168.100.101</td>
</tr>
<tr>
<td>Real Server Port</td>
<td>80</td>
</tr>
<tr>
<td>Weight</td>
<td>100</td>
</tr>
</tbody>
</table>

• Enter an appropriate label for the RIP, e.g. **Connection1**
• Change the **Real Server IP Address** field to the required IP address, e.g. **192.168.100.101**
• Change the **Real Server Port** field to **80**
• Click **Update**
• Repeat the above steps to add your other Connection Server(s)

**Upload The SSL Certificate**

**1) Export the SSL Certificate from a View Server** – note the following points when exporting the certificate from Windows:

• Make sure that the private key is included
• Tick the option ‘**Include all certificates in the certification path if possible**’

**2) Import the SSL Certificate to the Load Balancer** – follow the steps listed below:

• Using the WUI goto: **Cluster Configuration > SSL Termination**, click **[Certificate]** next to the SSL VIP created earlier
• Using the browse option, navigate to and select the .pfx file created in the previous step
• Click **Upload PEM/PFX file**
• Now restart Stunnel
Configure HTTP to HTTPS Redirect

If required, the load balancer can be configured to automatically redirect users who attempt to connect to http://<URL to access VIEW> to https://<URL to access VIEW>. For details on configuring this, please refer to section 1 in the Appendix.

Finalizing the Configuration

To apply the new settings, HAProxy must be restarted as follows:

- Go to Maintenance > Restart Services and click Restart HAProxy
Testing & Verification

Using System Overview
The System Overview is accessed using the WUI. It shows a graphical view of all VIPs & RIPs (i.e. the View Servers) and shows the state/health of each server as well as the state of the each cluster as a whole. The example below shows that both Connection Servers are healthy and available to accept connections.

<table>
<thead>
<tr>
<th>Virtual Service</th>
<th>IP</th>
<th>Ports</th>
<th>Protocol</th>
<th>Method</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>View Internal</td>
<td>192.168.100.10</td>
<td>443</td>
<td>OTHER TCP</td>
<td>Layer 7</td>
<td>Proxy</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Real Server</th>
<th>IP</th>
<th>Ports</th>
<th>Weight</th>
<th>Method</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connection1</td>
<td>192.168.100.101</td>
<td>443</td>
<td>1</td>
<td>Drain</td>
<td>Halt</td>
</tr>
<tr>
<td>Connection2</td>
<td>192.168.100.102</td>
<td>443</td>
<td>1</td>
<td>Drain</td>
<td>Halt</td>
</tr>
</tbody>
</table>

Key: Cluster healthy  Cluster needs attention  Cluster is down  Real Server taken offline

The example below shows that the server 'Connection1' has been put in halt mode, in this situation all connections will be sent to Connection2. Connection1 can be put back online by clicking the 'Online' link.

<table>
<thead>
<tr>
<th>Virtual Service</th>
<th>IP</th>
<th>Ports</th>
<th>Protocol</th>
<th>Method</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>View Internal</td>
<td>192.168.100.10</td>
<td>443</td>
<td>OTHER TCP</td>
<td>Layer 7</td>
<td>Proxy</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Real Server</th>
<th>IP</th>
<th>Ports</th>
<th>Weight</th>
<th>Method</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connection1</td>
<td>192.168.110.101</td>
<td>443</td>
<td>0</td>
<td>Online</td>
<td></td>
</tr>
<tr>
<td>Connection2</td>
<td>192.168.100.102</td>
<td>443</td>
<td>1</td>
<td>Drain</td>
<td>Halt</td>
</tr>
</tbody>
</table>

Key: ...
Layer 4 Status Report

The Layer 4 Status report gives a summary of layer 4 configuration and running stats as shown below. This can be accessed in the WUI using the option: Reports > Layer 4 Status.

Layer 4 Status

Virtual Service Real Server Forwarding Method Weight Active Connections Inactive Connections

ViewExternal

port /hwm

| Connection1 | Masq | 1 | 0 | 0 |
| Connection2 | Masq | 1 | 0 | 0 |

Layer 7 Statistics Report

The Layer 7 Statistics report gives a summary of all layer 7 configuration and running stats as shown below. This can be accessed in the WUI using the option: Reports > Layer 7 Status.

Layer 7 Statistics

HAPProxy

Statistics Report for pid 2611

> General process information

Appliance Logs

Logs are available for both layer 4 and layer 7 services and can be very useful when trying to diagnose issues. Layer 4 logs are active by default and can be accessed using the WUI option: Logs > Layer 4. Layer 7 logging is not enabled by default (because it is extremely verbose) and can be enabled using the WUI option: Cluster Configuration > Layer 7 – Advanced Configuration, and then viewed using the option: Logs > Layer 7.
Technical Support
For more details or assistance with your deployment please don’t hesitate to contact the support team at the following email address: support@loadbalancer.org

Conclusion
Loadbalancer.org appliances provide a very cost effective solution for highly available load balanced VMware Horizon View environments.
Appendix

1 – Configuring an HTTP to HTTPS redirect

An additional layer 7 VIP is required that listens on HTTP port 80 on the same IP address. The VIP is then configured to redirect connections to HTTPS port 443.

e.g. http://view.robtest.com should be redirected to https://view.robtest.com

The steps:

1) Create another Layer 7 VIP with the following settings:

   • Label: HTTP-redirect
   • Virtual Service IP Address: <same as the VIP that’s listening on port 443>
   • Virtual Service Ports: 80
   • Layer 7 Protocol: HTTP Mode
   • Persistence Mode: None
   • Force to HTTPS: Yes

N.B. This VIP will show in red in the System overview since no real servers are defined

2) Apply the new settings— to apply the new settings, HAProxy must be restarted:

   • Using the WUI, go to: Maintenance > Restart Services and click Restart HAProxy

2 – Clustered Pair Configuration – Adding a Slave Unit

If you initially configured just the master unit and now need to add a slave, please refer the section ‘Adding a slave unit after the master has been configured’ in the administration manual which is available at the following link: http://www.loadbalancer.org/pdf/loadbalanceradministrationv7.pdf.

Please don't hesitate to contact our support team if you need further assistance: support@loadbalancer.org
## 3 – Company Contact Information

<table>
<thead>
<tr>
<th>Region</th>
<th>Address</th>
<th>Telephone Numbers</th>
<th>Email Addresses</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Website</strong></td>
<td>URL: <a href="http://www.loadbalancer.org">www.loadbalancer.org</a></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>North America (US)</strong></td>
<td>Loadbalancer.org, Inc. 270 Presidential Drive Wilmington, DE 19807 USA</td>
<td>Tel: +1 866.229.8562 (24x7) Fax: +1 302.213.0122 Email (sales): <a href="mailto:sales@loadbalancer.org">sales@loadbalancer.org</a> Email (support): <a href="mailto:support@loadbalancer.org">support@loadbalancer.org</a></td>
<td></td>
</tr>
<tr>
<td><strong>North America (Canada)</strong></td>
<td>Loadbalancer.org Ltd. 300-422 Richards Street Vancouver, BC V6B 2Z4 Canada</td>
<td>Tel: +1 604.629.7575 Fax: +1 302.213.0122 Email (sales): <a href="mailto:sales@loadbalancer.org">sales@loadbalancer.org</a> Email (support): <a href="mailto:support@loadbalancer.org">support@loadbalancer.org</a></td>
<td></td>
</tr>
<tr>
<td><strong>Europe (UK)</strong></td>
<td>Loadbalancer.org Ltd. Portsmouth Technopole Kingston Crescent Portsmouth PO2 8FA England, UK</td>
<td>Tel: +44(0)870 4438779 (24x7) Fax: +44(0)870 4327672 Email (sales): <a href="mailto:sales@loadbalancer.org">sales@loadbalancer.org</a> Email (support): <a href="mailto:support@loadbalancer.org">support@loadbalancer.org</a></td>
<td></td>
</tr>
<tr>
<td><strong>Europe (Germany)</strong></td>
<td>Loadbalancer.org GmbH Alt Pempelfort 2 40211 Düsseldorf Germany</td>
<td>Tel: +49 (0)30 920 383 6494 Fax: +49 (0)30 920 383 6495 Email (sales): <a href="mailto:vertrieb@loadbalancer.org">vertrieb@loadbalancer.org</a> Email (support): <a href="mailto:support@loadbalancer.org">support@loadbalancer.org</a></td>
<td></td>
</tr>
</tbody>
</table>