Progress®
Kemp® LoadMaster®

Deployment Guide VMware Horizon View 5.2

Generated on: 16 September 2024

Copyright

Visit the following page online to see Progress Software Corporation's current Product Documentation Copyright Notice/Trademark Legend: Product Documentation Copyright Notice & Trademarks | Progress

Table of Contents

Chapter 1: Introduction 5

Document Purpose 5

Intended Audience 6

Chapter 2: Load Balancing VMware Horizon View 7

Horizon View Connection Server 7

Horizon View Security Server 7

Load Balancing VMware Horizon View Connection Servers. 8

Load Balancing VMware Horizon View Security Servers 10

Chapter 3: Example Environment Setup 12

Chapter 4: Prerequisites 13

Allow HTTP Connections 13

Modify Secure Tunnel External URL 14

DNS. 14

SSL Certificate Import on the LoadMaster 15

Chapter 5: Template 16

Chapter 6: Virtual Service Configuration 17

View Connection Servers 17

View Security Servers 19

Chapter 7: References 21

1

Introduction

VMware Horizon View (formerly VMware View) is a virtual desktop infrastructure solution that simplifies desktop management. It delivers personalized virtual desktops from a virtualized platform. This solution provides:

- Reduction of complexity of PC management
- Reduction of cost through virtualization
- Increased PC uptime
- Overall improved user experience
- Simplified desktop security

The Horizon View server roles that require services from an Application Delivery Controller (ADC) for high availability are the Connection Server and the Security Server.

Related Links

- Document Purpose
- Intended Audience

Document Purpose



The Virtual LoadMaster is VMware ready. This document is intended to provide guidance on how to configure LoadMaster products to provide high availability for a VMware Horizon View 5.2 environment. This document is not exclusively explicit to this version of VMware Horizon View nor does it claim explicit support for any or every other version of the application.

This documentation is created using a representative sample environment which is described later in the document. This document contains settings recommended by Progress Kemp. This document does not to cover every possible deployment scenario; it may not address your unique setup, requirements, network layout or needs. In such an event that your infrastructure needs are not illustrated or reflected herein, the Progress Kemp Engineering and Support Teams are available to provide guidance surrounding scenarios otherwise not explicitly defined.

Intended Audience

It is assumed that the reader is a server or network administrator who is familiar with networking, virtualization technologies, VMware, Virtual Desktop Infrastructure (VDI), DNS, Active Directory and general computer and network terminology. It is further assumed that you have set up the VMware Horizon View environment, DNS, Active Directory and have installed the LoadMaster. You should have reviewed the LoadMaster documentation and VMware Horizon View 5.2 documentation.

LoadMaster documentation is available at https://docs.progress.com.

2

Load Balancing VMware Horizon View

Descriptions of the VMware Horizon View server roles requiring high availability provided by an ADC and a descriptive VMware Horizon View diagram are described below.

Related Links

- Horizon View Connection Server
- Horizon View Security Server
- Load Balancing VMware Horizon View Connection Servers
- Load Balancing VMware Horizon View Security Servers

Horizon View Connection Server

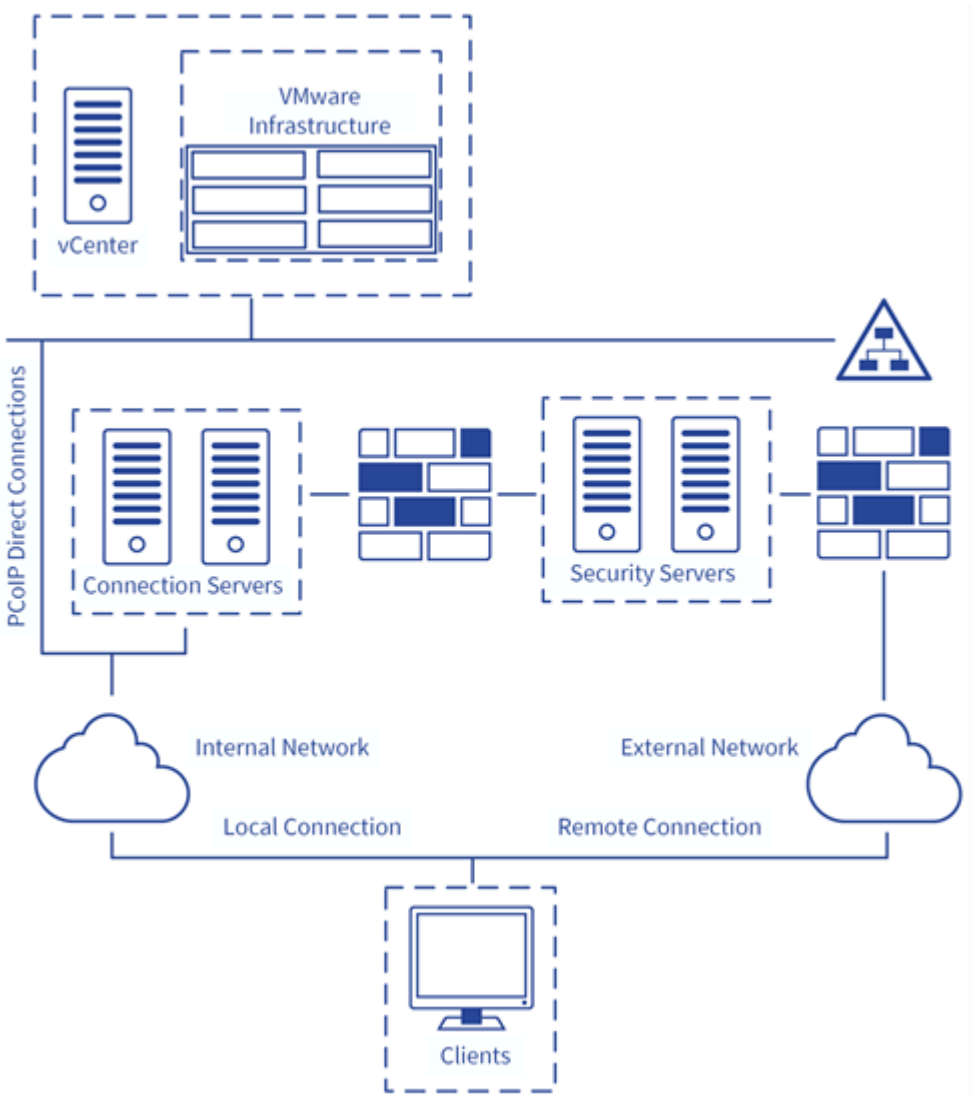
Horizon View Connection Server is the broker for client connections. It authenticates users to Active Directory and directs incoming user desktop requests to the correct endpoint. It also assigns packaged applications to desktops and pools and manages desktop sessions. In the deployment architecture defined herein, the LoadMaster does not handle the load balancing of PC over IP (PCoIP) traffic for connection servers.

Horizon View Security Server

Horizon View Security Server provides an extra layer of security for external Internet users who use a View Connection Server to access the internal network. Typically deployed in the DMZ, it proxies incoming

connections to View Connection Servers on the trusted network. In the deployment architecture defined herein, LoadMaster does not handle the load balancing of PCoIP traffic for security servers.

To provide high availability and improved scalability, ADCs should be deployed to provide high availability and acceleration services for both security and connection servers.



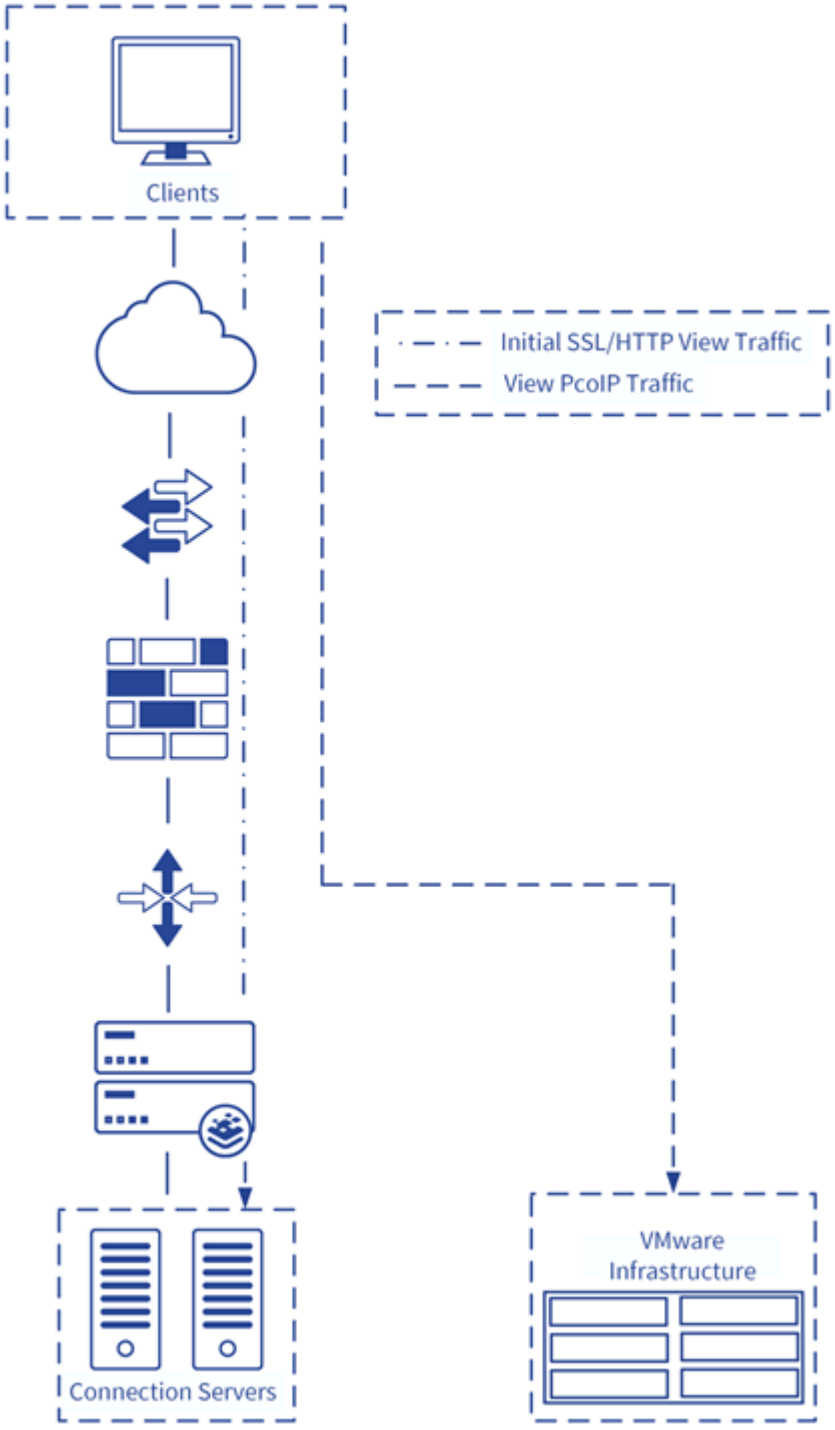
Load Balancing VMware Horizon View Connection Servers

The steps and diagram below depict a LoadMaster deployment with VMware View Connection Servers:

1. The client establishes an SSL connection to the LoadMaster Virtual Service for the VMware View Connection Server pool.
2. LoadMaster performs SSL decryption and load balances the connection to the most appropriate Connection Server.

Note: If desired, the LoadMaster can re-encrypt the connection before sending the traffic to the Connection Server.

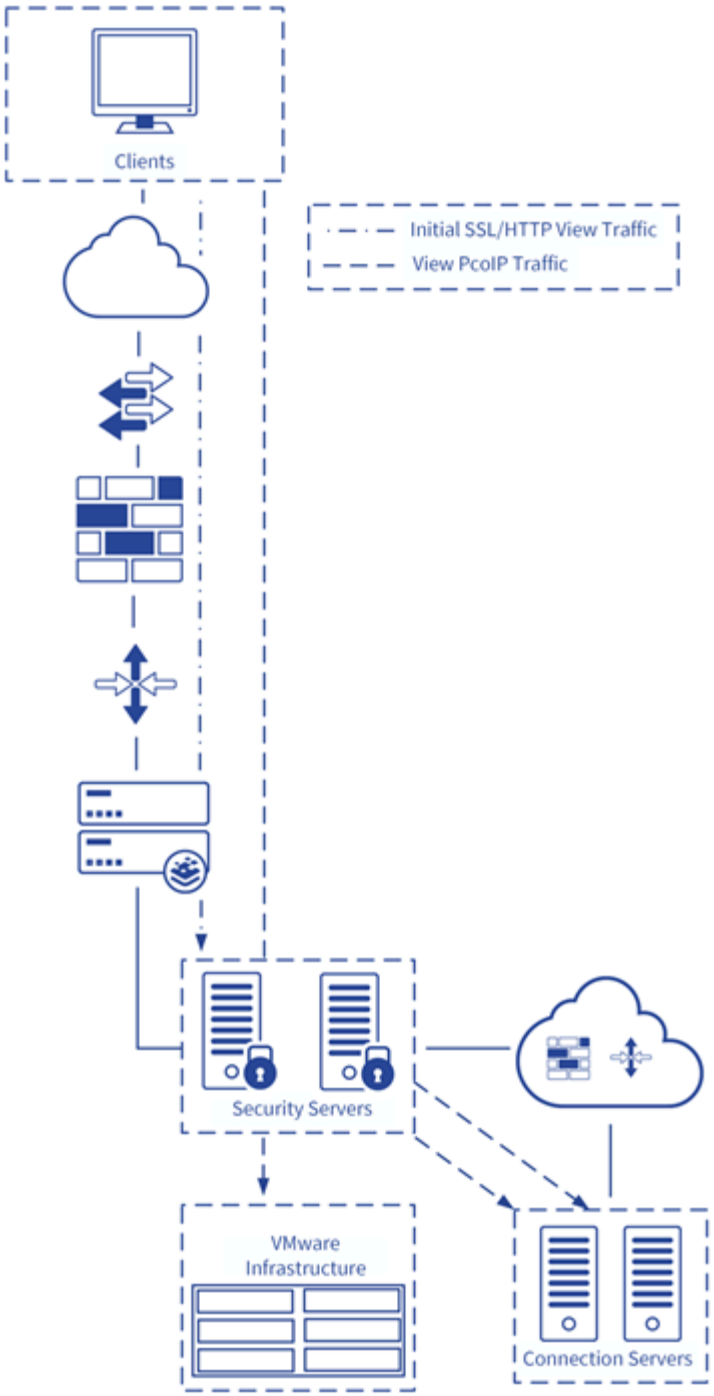
3. Authentication, desktop entitlement and desktop selection all take place. Then, PCoIP connections are established directly to the selected View Desktop, bypassing the LoadMaster.



Load Balancing VMware Horizon View Security Servers

The steps and diagram below depict a LoadMaster deployment with VMware View Security Servers:

1. Client establishes SSL connection to the LoadMaster Virtual Service for the VMware View Security Server pool.
2. The LoadMaster performs SSL decryption and load balances the connection to the most appropriate Security Server. The LoadMaster re-encrypts the connection before sending the traffic to the Security Server.
3. Authentication, desktop entitlement and desktop selection take place. Then, PCoIP connections are established directly to the selected View Security Server, bypassing the LoadMaster.


Clients
Initial SSL/HTTP View Traffic
View PcoIP Traffic
Security Servers
VMware
Infrastructure
Connection Servers

3

Example Environment Setup

TestCompany has deployed VMware Horizon 5.2 in their environment to provide a VDI accessed both by internal and external clients. The deployment contains the following:

- Two VMware Horizon View Connection Servers
- Two VMware Horizon View Security Servers
- Two LoadMaster HA Clusters

In the deployment architecture defined herein, the LoadMaster does not handle the load balancing of PCoIP traffic for Connection or Security servers. For this reason, the following should be noted:

- Connectivity between external clients and the View Security servers is required
- Connectivity between internal clients and the VMware infrastructure is required

The following scenarios are defined:

- Access to the Horizon View environment using Connection Servers which are being load balanced and serviced by a LoadMaster ADC cluster
- Access to Horizon View using Security servers which are being load balanced and serviced by a LoadMaster ADC cluster

4

Prerequisites

Minimally, you should have:

- Implemented Active Directory, DNS and other core requirements for Horizon View
- Installed VMware ESXi servers, vCenter server, View Connection and Security servers
- Configured SSL certificates for authentication of View Connection and Security servers
- Installed the LoadMaster(s) on the same network(s) as the servers to be load balanced
- Established administrative access to the LoadMaster Web User Interface (WUI)

Related Links

- Allow HTTP Connections
- Modify Secure Tunnel External URL
- DNS
- SSL Certificate Import on the LoadMaster

Allow HTTP Connections

To allow SSL-offloaded connections from the LoadMaster to the Connection Servers that are not re-encrypted, the Connection Servers must be configured to accept HTTP connections from intermediate devices. This is accomplished by modifying the locked.properties file on each Connection Server on which HTTP connections are desired. Steps on how to do this are outlined below. The servers will also continue to accept HTTPS connections.

1. Navigate to the locked.properties file in the SSLGateway configuration folder on the Connection Server, for example <install_directory>\VMware\VMware View\Server\sslgateway\conf\locked.properties
2. Add the serverProtocol property. Set it to http using lower case letters
3. The next two steps are optional:
   1. If desired, change the HTTP listening port from 80 to a non-default port by setting the serverPortNonSSL to an alternate port number on which the LoadMaster will communicate with the Connection Server for HTTP connections.
   2. If the Connection Server has multiple network interfaces and you would like to designate a single interface for HTTP connections, set the server Host to the IP address of the desired interface.
4. Save the locked.properties file.
5. Restart the View Connection Server service on the server

Note: SSL offloading is not supported with smart card authentication.

Modify Secure Tunnel External URL

The following changes to the Secure Tunnel External URL parameters are required for the LoadMaster and the VMware Horizon View environment to interoperate correctly:

1. Log in to the View Manager Administrator tool.
2. Expand **View Configuration** and click **Servers**.
3. Select the **Connection Servers** tab.
4. Select each Connection server and click the **Edit** button after which the **Edit View Connection Server Settings** box will open.
5. Navigate to the **General** tab. In the **HTTP(S) Secure Tunnel External URL** text box, enter the LoadMaster Virtual Service IP address or DNS FQDN to be used for the Security Server pool followed by a colon and the appropriate port number.
6. Select the **Use Secure Tunnel Connection to Desktop** check box.
7. Click **OK**.
8. Next, select each Security Server and click the **Edit** button.
9. On the **General** tab in the **HTTP(S) Secure Tunnel External URL** text box, enter the LoadMaster Virtual Service IP address or DNS FQDN to be used for the Security Server pool followed by a colon and the appropriate port number.
10. Click **OK**.

Note: Do not change the IP address configured in the PCoIP External URL field.

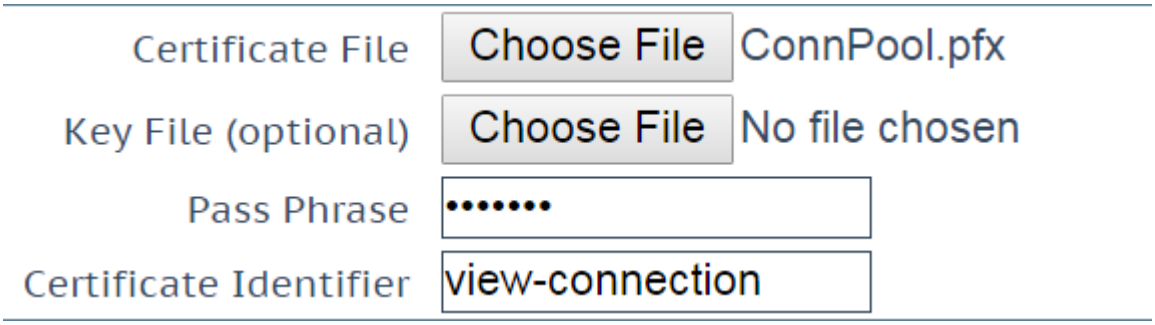
DNS

Access to the DNS system used in the network environment must be available to set up name resolution of your Horizon View namespaces to the Virtual Service IP addresse(s) that will be configured on the LoadMaster.

SSL Certificate Import on the LoadMaster

Follow the steps below to import the relevant View Connection and Security certificates on the LoadMaster:

1. In the main menu of the LoadMaster WUI, go to **Certificates & Security > SSL Certificates**.
2. Click **Import Certificate**.



3. Click **Choose File** in the **Certificate File** field.
4. Browse to and select the signed certificate file which is in use in the Horizon View infrastructure.

Note: This must be a .pfx file containing private keys for the certificate used on the Horizon View servers.

5. If relevant, click **Choose File** in the **Key File (optional)** field to browse to and select the key file.
6. Enter the **Pass Phrase**.
7. Enter a recognizable name in **the Certificate Identifier** text box.
8. Click **Save**.
9. If required, repeat the steps above to add a Security certificate.

5

Template

Progress 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. For some workloads, additional manual steps may be required such as assigning a certificate or applying port following. These steps are covered in the document, if needed.

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.

6

Virtual Service Configuration

The sections below outline instructions on how to add Virtual Services for the View Connection and Security servers.

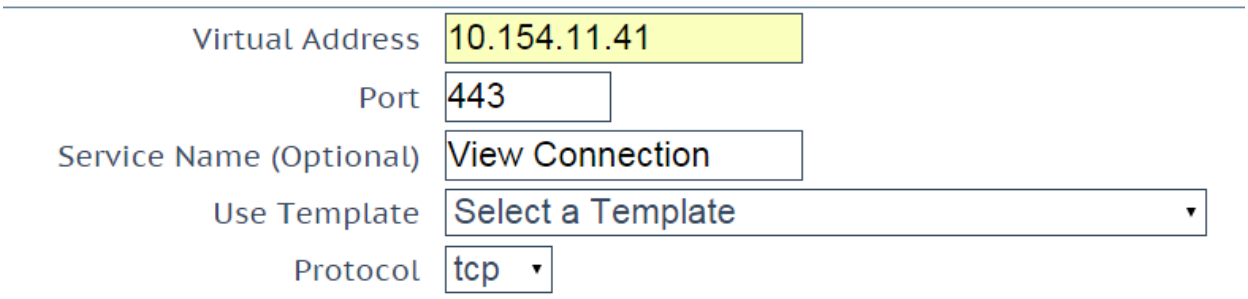
Related Links

- View Connection Servers
- View Security Servers

View Connection Servers

To add a Virtual Service for the View Connection Servers, follow the steps below:

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

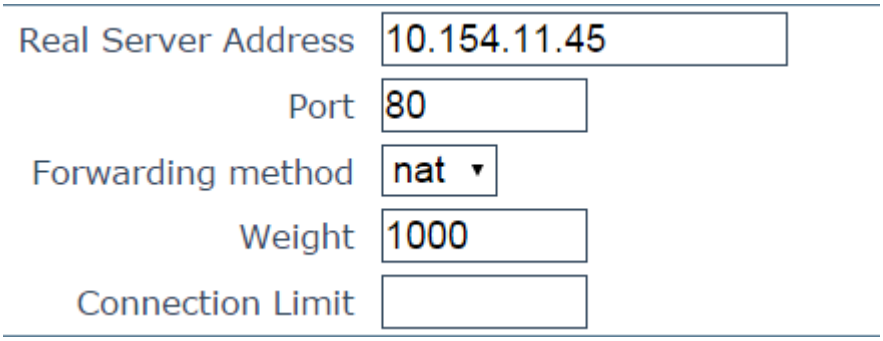


2. Enter a valid IP address in the **Virtual Address** field.

3. Enter **443** as the **Port**.
4. Enter a recognizable **Service Name**, for example **View Connection**.
5. Click **Add this Virtual Service**.
6. Configure the settings as shown in the following table:

Section	Option	Value	Comment
SSL Properties	SSL Acceleration	Enabled	
	Certificates	Select the relevant certificate.	Click **>** to assign the certificate. Click **Set Certificates**.
Standard Options	Transparency	Disabled	
	Persistence Mode	Server Cookie	
	Persistence Timeout	6 Minutes	
	Cookie name	JSESSIONID	Click **Set Cookie**.
	Scheduling Method	least connection	
Real Servers	URL	/	Click **Set URL**.
	HTTP Method	GET	

7. Click **Add New**.



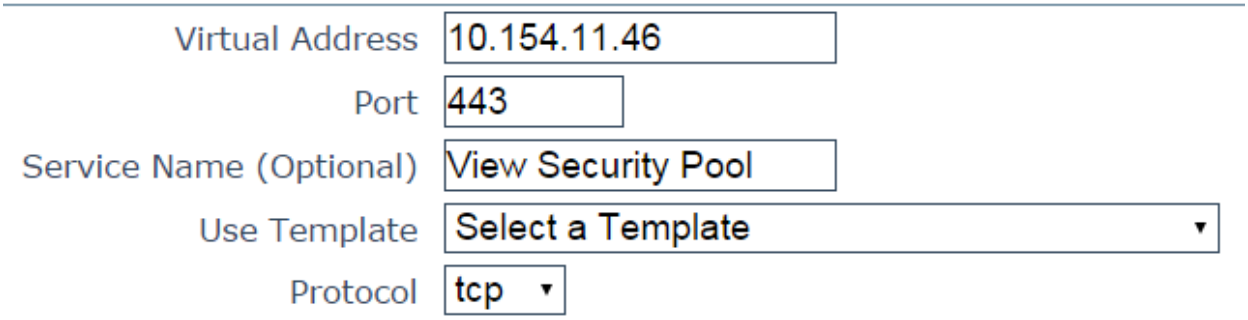
8. Enter the relevant **Real Server Address**.
9. Enter **80** as the **Port**.
10. Click **Add This Real Server**.
11. Click **OK**.
12. Continue to add the remaining Real Servers by entering the **Real Server Address** and clicking **Add This Real Server** until all servers in the pool are added. When finished, click the **Back** button.
13. In the main menu of the LoadMaster WUI, click **View/Modify Services**.
14. Confirm that the newly created service is listed with a status of **Up** and that all of the added member

servers are listed in black, non-bold font.

View Security Servers

To add the Virtual Service for the View Security Servers, follow the steps below:

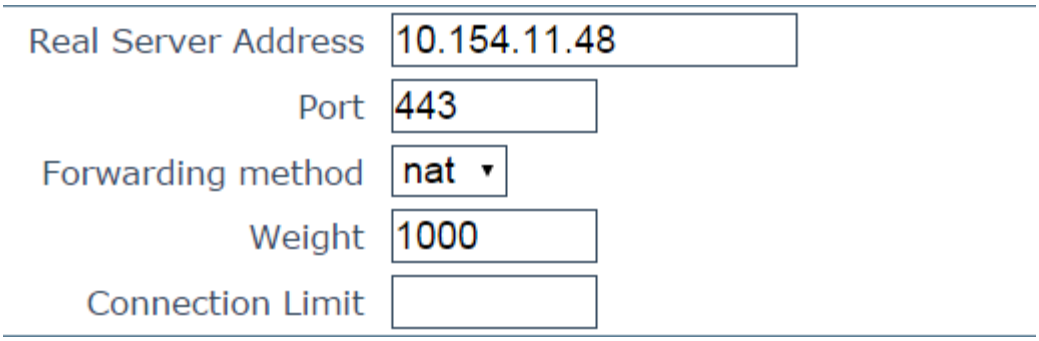
1. In the main menu of the LoadMaster WUI, select **Virtual Services** and **Add New**.



2. Enter a valid IP address in the **Virtual Address** text box.
3. Enter **443** as the **Port**.
4. Enter a recognizable **Service Name**, for example **View Security Pool**.
5. Click **Add this Virtual Service**.
6. Configure the settings as shown in the following table:

Section	Option	Value	Comment
SSL Properties	SSL Acceleration	Enabled	
	Reencrypt	Enabled	
	Certificates	Select the relevant certificate.	Click **>** to assign the certificate. Click **Set Certificates**.
Standard Options	Persistence Mode	Server Cookie	
	Persistence Timeout	6 Minutes	
	Cookie name	JSESSIONID	Click **Set Cookie**.
	Scheduling Method	least connection	
Real Servers	URL	/	Click **Set URL**.
	HTTP Method	GET	

7. Click **Add New**.



8. Enter the relevant **Real Server Address**.
9. Click **Add This Real Server**.
10. Click **OK**.
11. Continue to add Real Servers until every server in the pool has been added. Then, click the **Back** button.
12. In the main menu of the LoadMaster WUI, select **View/Modify Services**.
13. Confirm that the newly created service is listed with a status of **UP**. Ensure that all member servers are listed in black, non-bold font.

7

References

The below links contain further information.

Web User Interface, Configuration Guide

https://docs.progress.com/

Virtual Services and Templates, Feature Description

https://docs.progress.com/