Progress®
Kemp® LoadMaster®

Deployment Guide VMware Horizon Workspace

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 6

Intended Audience 6

Chapter 2: VMware Horizon Workspace Overview 8

Horizon Connector Virtual Appliance (Connector-VA) 8

Horizon Gateway Virtual Appliance (Gateway-VA) 9

Other Horizon Workspace Components 9

Load Balancing VMware Horizon Gateway-VAs 11

Load Balancing VMware Horizon Connector-VAs 12

Chapter 3: Example Environment Setup 15

Chapter 4: Prerequisites 16

Configure Gateway-VA NGINX Components 16

Horizon Workspace 1.5 X-Forwarded-For Configuration 17

Horizon Workspace 1.0 X-Forwarded-For Configuration 17

Create a Content Matching Rule 18

DNS 19

SSL Certificate Import on the LoadMaster 19

Update Connector iDP Hostname 20

Chapter 5: Template 21

Chapter 6: Virtual Service Configuration 22

Gateway-VAs (External Virtual Service) 22

Gateway-VAs (Internal Virtual Service) 24

Connector-VAs 24

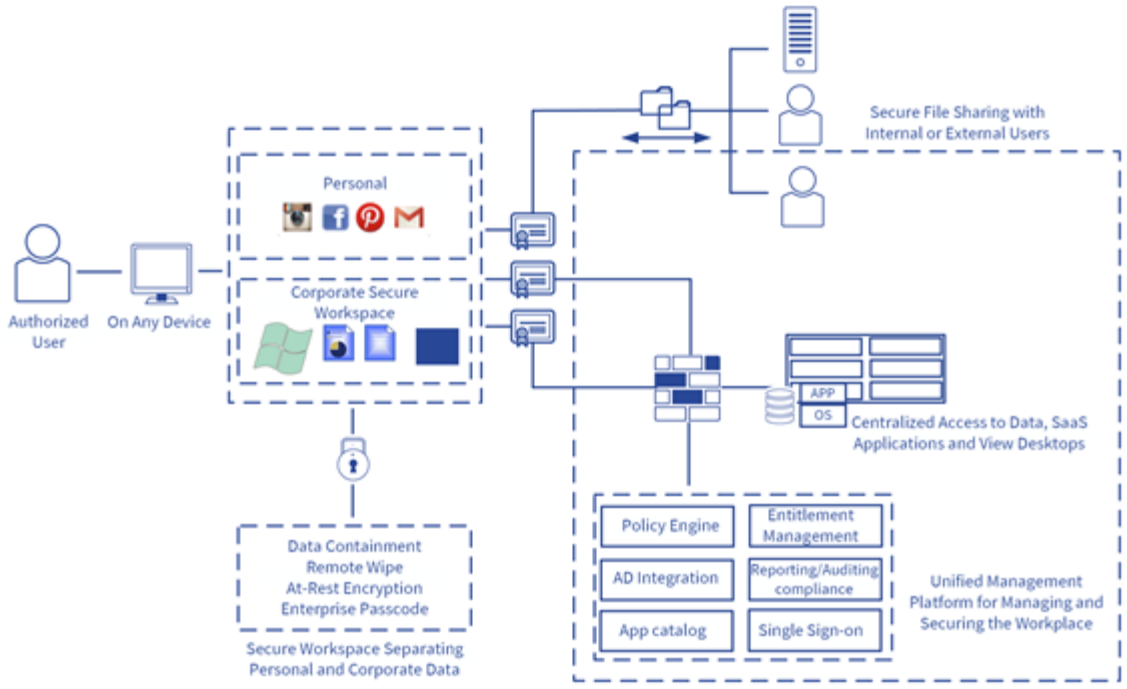
Chapter 7: References 27

1

Introduction

VMware Horizon Workspace provides a single workspace for easy and secure access to applications, files and desktops on virtually any device. It is delivered as a SUSE Linux-based vApp (an Open Virtual Appliance (.OVA) file) consisting of multiple Virtual Appliances (VA) that are deployed through VMware vCenter in a VMware infrastructure. The various deployed Virtual Appliances are used by the Workspace solution to provide:

- A centralized workspace for application and data access
- Cloud-Identity management
- Compliance requirements support
- Data and file synchronization
- Data leak prevention through separation of corporate and personal data
- Secure file sharing both internally and externally for collaboration enablement
- Simplified administrative management of resource entitlement and policy control



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 the LoadMaster to provide High Availability (HA) for a VMware Horizon Workspace 1.5 environment. This document is not exclusively restricted to this version of VMware Horizon Workspace 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. As the intent of this document is 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, Windows and Linux Operating systems, VMware and the Horizon suite, DNS, Active Directory and general computer and network terminology. It is further assumed that the VMware

Horizon Workspace environment, DNS and Active Directory have all been set up and that the LoadMaster is installed. We recommend reviewing the LoadMaster documentation and VMware Horizon Workspace 1.5 documentation.

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

2

VMware Horizon Workspace Overview

This section provides:

- A description of the VMware Horizon Workspace Virtual Appliances that require high availability provided by an Application Delivery Controller (ADC), that is, the LoadMaster
- A description of some other Workspace components
- A reference diagram of the VMware Horizon Workspace architecture

Related Links

- Horizon Connector Virtual Appliance (Connector-VA)
- Horizon Gateway Virtual Appliance (Gateway-VA)
- Other Horizon Workspace Components
- Load Balancing VMware Horizon Gateway-VAs
- Load Balancing VMware Horizon Connector-VAs

Horizon Connector Virtual Appliance (Connector-VA)

The Horizon Connector provides capabilities for local user authentication and Active Directory binding and synchronization services. Additional services provided by the Connector-VA are ThinApp catalog loading and View pool synchronization.

Note: To provide high availability and improved scalability, multiple Connector virtual appliances should be deployed behind an internal load balancer/reverse proxy.

Horizon Gateway Virtual Appliance (Gateway-VA)

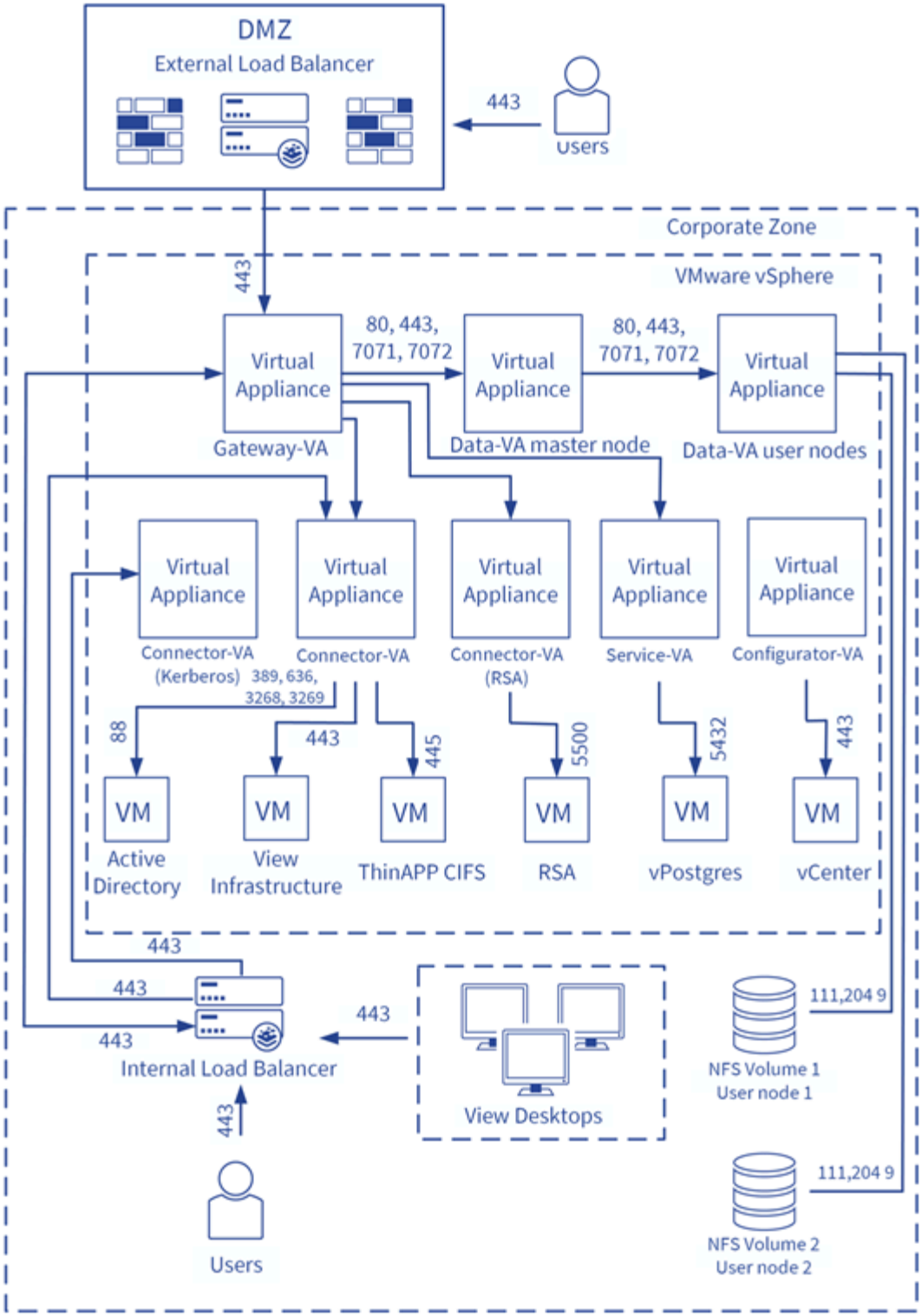
The Horizon Gateway serves as the single namespace for all Horizon Workspace interaction and enables a user-facing domain for access to Horizon Workspace. It serves as the central aggregation point for all client connections, routes client traffic to the correct destination and proxies all requests. Horizon Workspace requires one Gateway-VA for every two data virtual appliances or one Gateway-VA for every 2,000 users.

Note: To provide high availability and improved scalability, multiple Gateway virtual appliances should be deployed behind a load balancer/reverse proxy. It is not supported to place Gateway virtual appliances in the DMZ.

Other Horizon Workspace Components

Other virtual appliances included in the Horizon Workspace vApp are:

- **Horizon Configurator (Configurator-VA)** – An administrative console and web user interface for central SSL management as well as network, Gateway, vCenter and SMTP configuration of the virtual appliances in the Horizon vApp.
- **Horizon Manager (Service-VA)** – A web-based administrative interface allowing configuration of the application catalog, user entitlement management and systems reporting.
- **VMware Horizon Data (Data-VA)** – Serves as a datastore for user files, controls file sharing policies, provides file preview services and acts as the Horizon Workspace web interface for end-users.



Note: Internal and external Gateway load balancing can be handled either by two separate load balancers or a single load balancer with connections to both the DMZ and internal trusted local area network segments.

Note: Connector load balancing is handled by the internal load balancer.

Load Balancing VMware Horizon Gateway-VAs

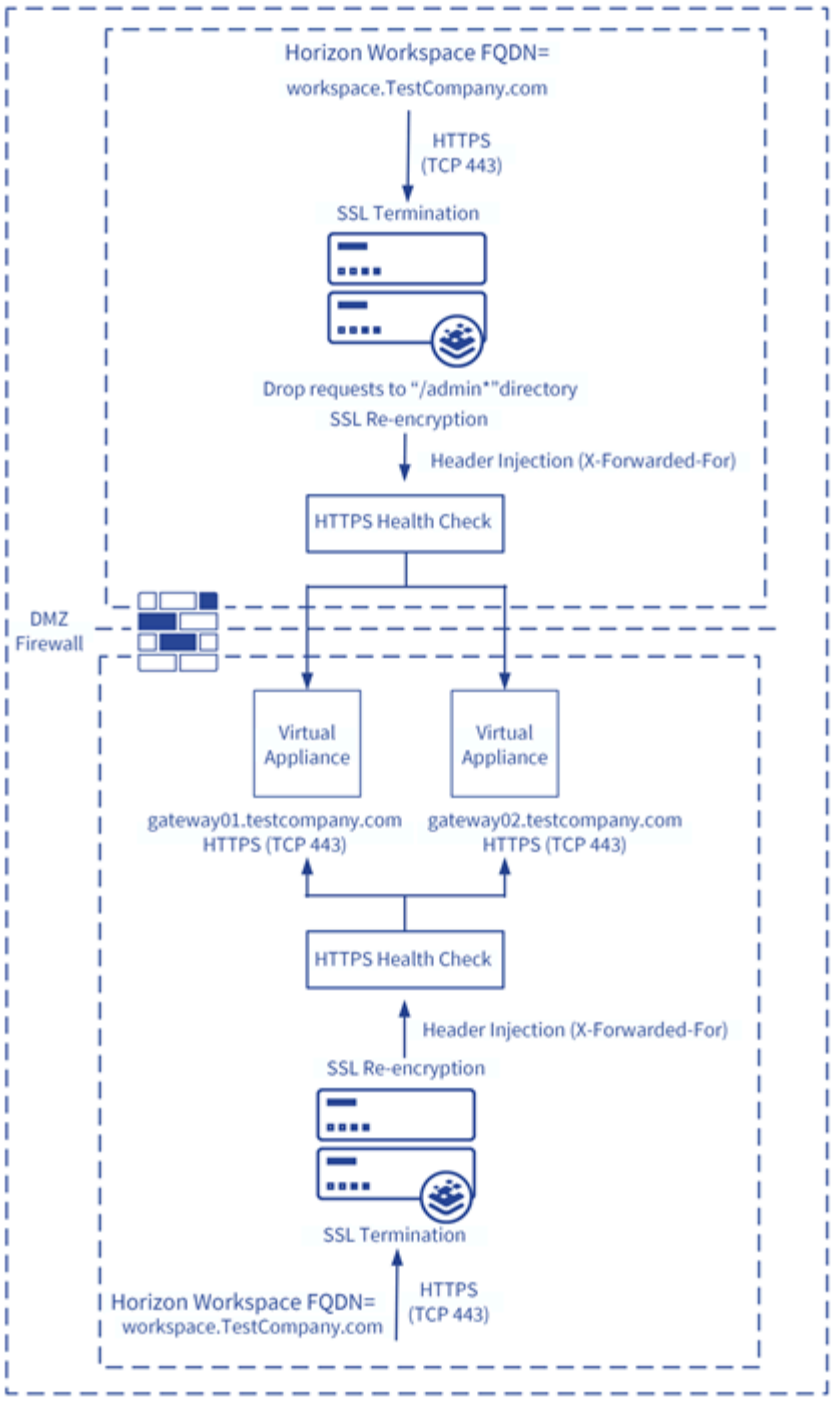
The steps and diagram below depict a LoadMaster deployment with a VMware Horizon Workspace environment:

1. The client establishes an SSL connection to the LoadMaster Virtual Service for the VMware Horizon Workspace URL and the LoadMaster performs SSL decryption.

   Note: If desired, the LoadMaster can be configured to deny external access to the administrative section of Horizon Workspace for added security.

2. The X-Forwarded-For header with the requestor's client IP address is inserted.
3. The LoadMaster re-encrypts the connection and continues communication with Gateway Virtual Appliance(s).
4. The client request is load balanced to the most appropriate Gateway Virtual Appliance based on health check and persistence validation.

Note: Traffic initiated by internal clients behaves in the same manner aside from restricting access to the administrative virtual directory.



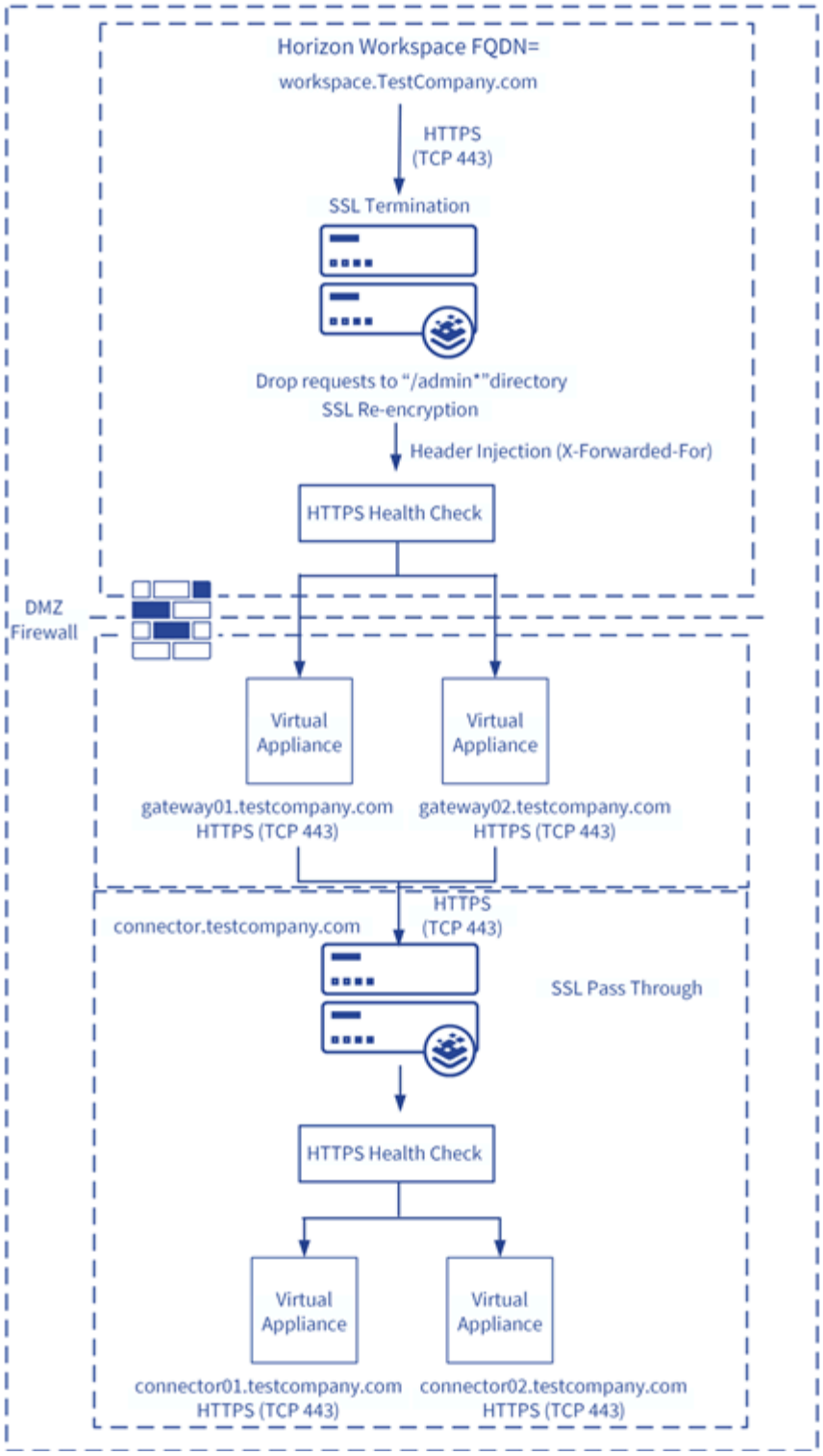
Load Balancing VMware Horizon Connector-VAs

The steps and diagram below depict a LoadMaster deployment with a VMware Horizon Workspace environment:

1. After client traffic is passed through the LoadMaster to the appropriate Gateway-VA as detailed in the

Load Balancing VMware Horizon Gateway-VAs section, the Gateway looks at the X-Forwarded-For header to determine which Connectors to use for authentication.

2. The client request is then redirected to the appropriate Connector iDP URL. The LoadMaster hosting the Connector Virtual Service sends the response to the best suited Connector-VA.
3. The Connector sends an HTTPS redirect to the client so that the client now connects directly to its FQDN.
4. Using Kerberos, the Connector authenticates the client request against Active Directory.


Horizon Workspace FQDN=
workspace.TestCompany.com
HTTPS
(TCP 443)
SSL Termination
Drop requests to "/admin*"directory
SSL Re-encryption
Header Injection (X-Forwarded-For)
HTTPS Health Check
DMZ
Firewall
Virtual
Appliance
Virtual
Appliance
gateway01.testcompany.com
HTTPS (TCP 443)
gateway02.testcompany.com
HTTPS (TCP 443)
connector.testcompany.com
HTTPS
(TCP 443)
SSL Pass Through
HTTPS Health Check
Virtual
Appliance
Virtual
Appliance
connector01.testcompany.com
HTTPS (TCP 443)
connector02.testcompany.com
HTTPS (TCP 443)

3

Example Environment Setup

TestCompany has deployed VMware Horizon Workspace 1.5 in their environment to provide centralized workspace access from a variety of devices by their workforce. The infrastructure is accessed by clients both internally and externally. Among other supporting components, the deployment contains the following:

- Two VMware Horizon Gateway-VAs
- Two VMware Horizon Connector-VAs
- One LoadMaster HA cluster deployed in the DMZ
- One LoadMaster HA Ccuster deployed in the trusted corporate LAN

In the deployment architecture defined herein, the LoadMaster handles internal and external HTTPS connectivity to the Gateway-VAs as well as connectivity for the Connector-VAs. The LoadMaster provides the following for Workspace deployments:

- Scheduling and health check algorithms which ensure that requests are sent to the best target
- L7 content matching capabilities which minimize attack vectors for added security
- Header injection functionality which ensures that client IPs are detected by Gateway-VAs
- SSL overlay functions ensure L7 processing and an end-to-end secure traffic stream

4

Prerequisites

Prerequisites

Minimally, the following prerequisites should be complete:

- Implemented Active Directory, DNS and other core requirements for Horizon Workspace
- Installed VMware ESXi servers, vCenter server, and Workspace virtual appliances
- Configured Certificate Authority (CA)-signed SSL certificates for the Workspace infrastructure
- Installed LoadMaster(s) with interfaces on the same network(s) as the virtual appliances
- Established administrative access to the LoadMaster Web User Interface (WUI)

Related Links

- Configure Gateway-VA NGINX Components
- Create a Content Matching Rule
- DNS
- SSL Certificate Import on the LoadMaster
- Update Connector iDP Hostname

Configure Gateway-VA NGINX Components

Refer to the following sections for details on configuring the Gateway-VA NGINX components.

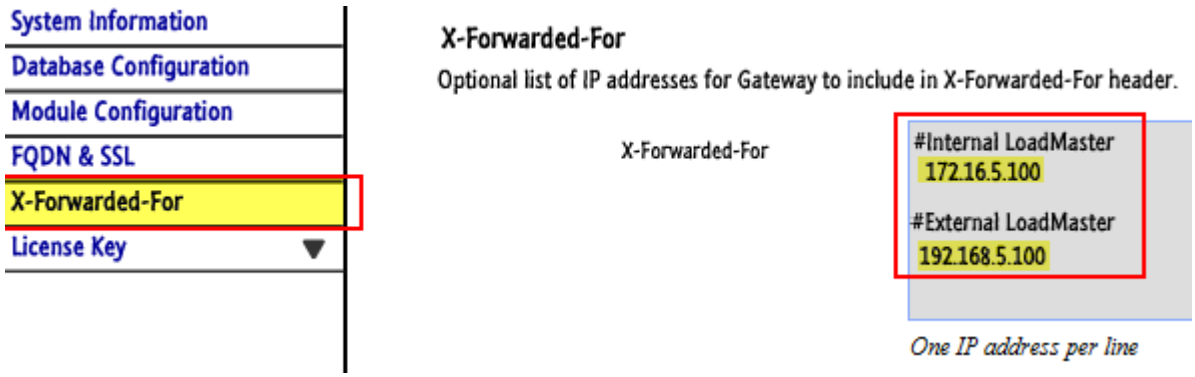
Related Links

- Horizon Workspace 1.5 X-Forwarded-For Configuration
- Horizon Workspace 1.0 X-Forwarded-For Configuration

Horizon Workspace 1.5 X-Forwarded-For Configuration

To allow LoadMaster to request web services that are deployed behind the Gateway-VAs in Horizon Workspace 1.5, the following change must be made:

1. Navigate to the Configurator-VA URL and log in.



2. In the menu on the left, click **X-Forwarded-For**.
3. Enter the load balancer IP address(es) with descriptive comments (one per line).
4. Click **Save** and reboot all Gateway-VAs if changes do not take effect within a few minutes.

Note: This X-Forwarded-For modification also sets the real_ip_header value in **/opt/vmware/nginx/conf/nginx.conf**.

Horizon Workspace 1.0 X-Forwarded-For Configuration

To allow LoadMaster to request web services that are deployed behind the Gateway-VAs in Horizon Workspace 1.0, the following change must be made:

1. SSH into each gateway-VA with the sshuser and su to root.
2. Edit **/opt/vmware/nginx/conf/nginx.conf** using VI, or another screen editor.
3. Find the section of the file that reads similar to the following:

   Note: real_ip_headerX-Forwarded-For; real_ip_recursive off;include gen/real_ip.conf;

   ---

4. Below the line that reads **include gen/real_ip.conf;** add a line - **set_real_ip_from <LoadMaster IP Address>** as shown in the example below:

   Note: real_ip_headerX-Forwarded-For; real_ip_recursive off;include gen/real_ip.conf; set_real_ip_from 172.16.5.100

   ---

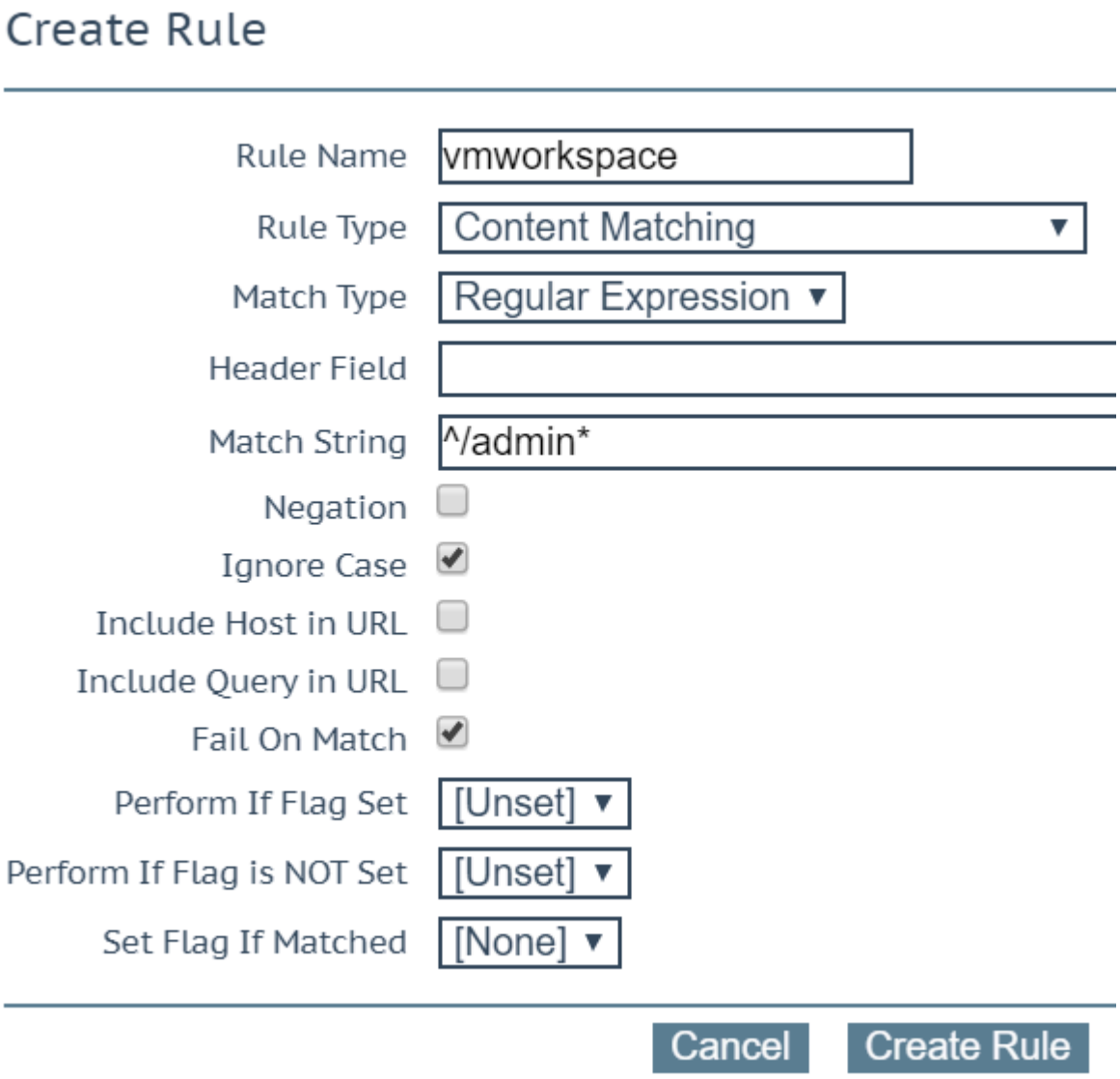
5. Commit the changes that have just been made and restart the nginx service:

1. If using VI to edit the file, type **ZZ** or **:wq!**.
2. To restart the nginx service type **service nginx restart**.

Create a Content Matching Rule

Follow the steps below to create a content matching rule on the LoadMaster that is used later to block external access to the administrative portion of the Workspace environment:

1. Log in to the LoadMaster WUI.
2. In the menu on the left select **Rules & Checking** and select **Content Rules**.
3. Click the **Create New…** button.



4. Enter the **Rule Name**, for example **vmworkspace**.

5. Ensure the **Rule Type** is set to **Content Matching**.
6. Ensure the **Match Type** is set to **Regular Expression**.
7. Enter **^/admin*** as the pattern in the **Match String** text box.
8. Tick the **Ignore Case** check box.
9. Tick the **Fail on Match** check box.
10. Click the **Create Rule** button.

DNS

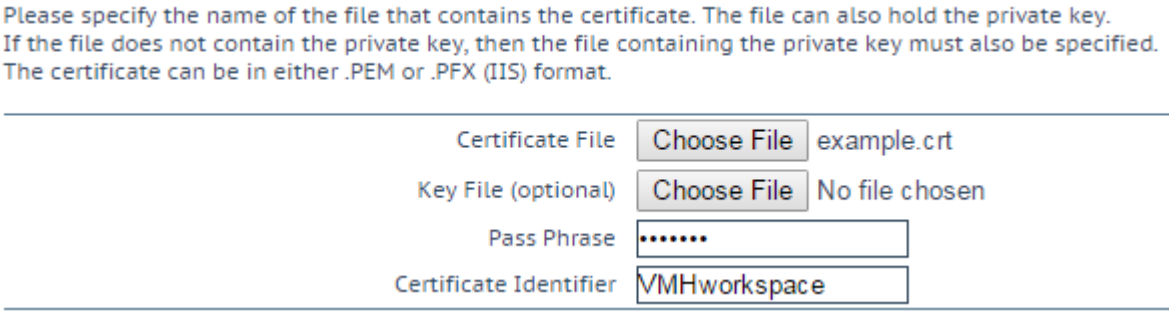
Access to the DNS system(s) used in the network environment must be available to configure name resolution (A and PTR records) for the Horizon Workspace Gateway and Connector namespaces to point to the Virtual Service IP address(es) that is configured on the LoadMaster.

Note: The FQDN configured for the Horizon Workspace environment cannot be changed after installation. In the event that the namespace requires changing post-installation, the Horizon Workspace vApp must be re-deployed. The same namespace should be used for both internal and external access.

SSL Certificate Import on the LoadMaster

Follow the steps below to import the relevant Horizon Workspace certificate on the LoadMaster:

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



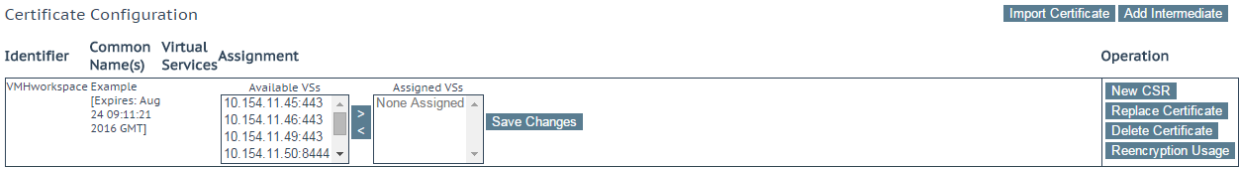
3. Click **Choose File** in the **Certificate File** field.
4. Browse to and select the certificate in use in the Horizon Workspace infrastructure.

Note: This must be a .PFX or .PEM file containing private keys for the certificate used on the Horizon Workspace servers.

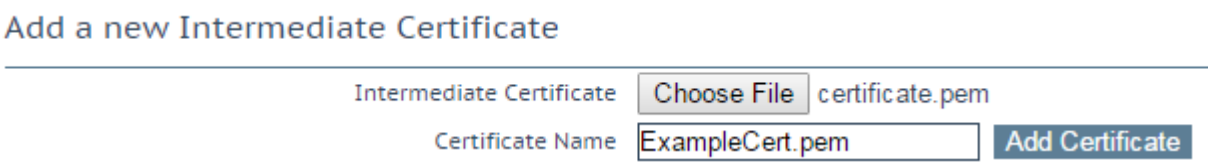
---

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. Click **OK**.



10. If additional intermediate certificate(s) are required to complete the certificate chain, click **Add Intermediate**.



11. Click **Choose File** in the **Intermediate Certificate** field.
12. Browse to and select the appropriate intermediate certificate.
13. Enter a recognizable name in the **Desired File Name** text box.
14. Click **Add Certificate**.

Update Connector iDP Hostname

To change the iDP hostname on the Connector-VAs, take the following steps:

1. Log in to the web admin console of each Connector-VA.
2. Navigate to **Identity Provider**.
3. Change the iDP hostname to the FQDN corresponding to the IP address that is used for the Virtual Service that is created in the Connector-VAs section for load balancing the Connector-VAs and click **Save**.

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

This section outlines instructions on adding and configuring the required Workspace Virtual Services to the LoadMaster.

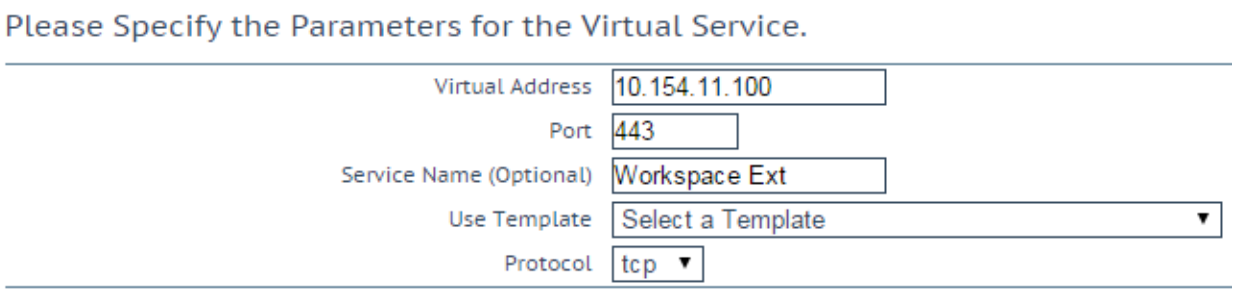
Related Links

- Gateway-VAs (External Virtual Service)
- Gateway-VAs (Internal Virtual Service)
- Connector-VAs

Gateway-VAs (External Virtual Service)

To add an External Virtual Service for the Gateway-VAs, follow the steps below:

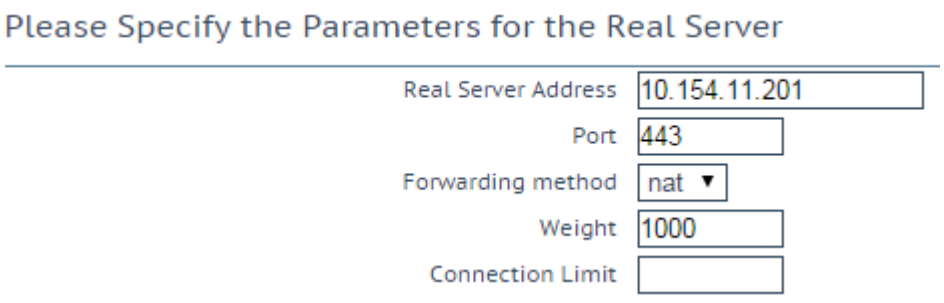
1. In the main menu of the LoadMaster WUI, select **Virtual Services** and **Add New**.



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 **Workspace Ext**.
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	Click **OK**.
	Reencrypt	Enabled	
	Certificates	Select the relevant certificate.	Click **>** to assign the certificate. Click **Set Certificates**.
Standard Options	Persistence Mode	Super HTTP	
	Persistence Timeout	30 Minutes	Do not set the persistence timeout to less than 30 minutes. A lower value may result in a 502 error ('The service is currently unavailable') for clients attempting to connect.
	Scheduling Method	least connection	
Real Servers	Real Server Check Method	HTTPS Protocol	
	URL	/	Click **Set URL**.
	HTTP Method	GET	

7. Click **Add New**.



8. Enter a Gateway-VA address in the **Real Server Address** field.
9. Ensure that **443** is entered 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** of each Gateway-VA and clicking **Add This Real Server** until all servers in the pool are added. When finished, click the **Back** button.
13. Expand the **Advanced Properties** section.
14. Select the **Enable** button in the **Content Switching** section.
15. Select **X-Forwarded-For** from the **Add HTTP Headers** drop down menu.
16. Click the **Add HTTP Redirector** button.
17. Expand the **Real Servers** section.



18. Click **None** in the **Rules** column for the first listed Real Server.



19. Select the content matching rule created in the Create a Content Matching Rule section.
20. Click **Add**.
21. Click the **Back** button.
22. Repeat for each **Real Server** to add the content matching rule to all pool members.
23. In the main menu of the LoadMaster WUI, click **View/Modify Services**.
24. 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.

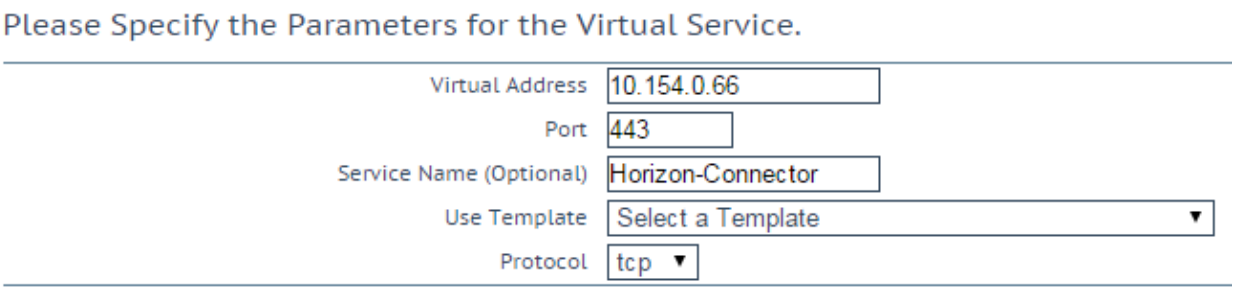
Gateway-VAs (Internal Virtual Service)

To add an Internal Virtual Service for the Gateway-VAs, either on the same LoadMaster or another cluster, repeat Steps 1 to 29 of the Gateway-VAs (External Virtual Service) section, but give the Virtual Service a different name.

Connector-VAs

To add a Virtual Service for the Connector-VAs, follow the steps below:

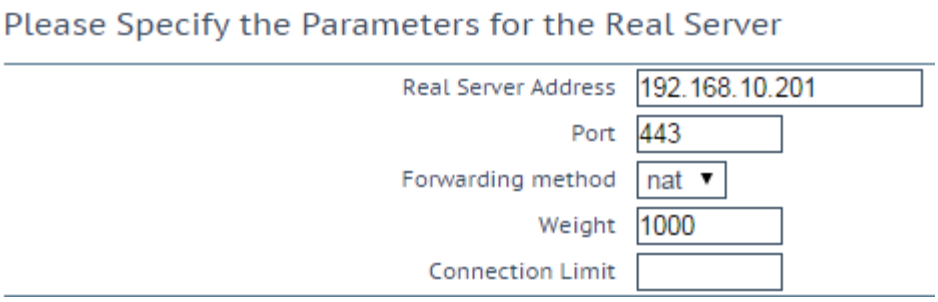
1. In the main menu of the LoadMaster WUI, select **Virtual Services** and **Add New**.



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 **Horizon-Connector**.
5. Click **Add this Virtual Service**.
6. Configure the settings as shown in the following table:

Section	Option	Value	Comment
Standard Options	Force L4	Disabled	Disable this, unless your deployment scheme dictates otherwise.
	Transparency	Disabled	Disable this, unless your deployment scheme dictates otherwise.
	Persistence Mode	Source IP Address	
	Persistence Timeout	30 Minutes	Do not set the persistence timeout to less than 30 minutes. A lower value may result in a 502 error ('The service is currently unavailable') for clients attempting to connect.
	Scheduling Method	least connection	
Real Servers	Real Server Check Method	HTTPS Protocol	
	URL	/	Click **Set URL**.
	HTTP Method	GET	

7. Click **Add New**.



8. Enter a Connector-VA address in the **Real Server Address** text box.
9. Enter **443** 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** of each Connector-VA 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.

7

References

Product documentation can be found at https://docs.progress.com/.

Virtual Services and Templates, Feature Description

WUI, Configuration Guide