Progress®
Kemp® LoadMaster®

Deployment Guide Dell Wyse vWorkspace

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 4

Document Purpose 4

Intended Audience 5

Chapter 2: Load Balancing vWorkspace 6

vWorkspace Roles 11

Load Balancing Web Access Services 11

Load Balancing Secure Access Services 11

Chapter 3: General Configuration 12

Enable Subnet Originating Requests Globally 12

SSL Certificates 13

Chapter 4: Configure Virtual Services for vWorkspace 15

Secure Access Prerequisites 15

Virtual Services – Secure Access 18

Web Access Prerequisites 19

Virtual Services – Web Access 21

Chapter 5: Testing 23

1

Introduction

Introduction

Dell Wyse vWorkspace provides desktop and application virtualization to organizations. Workspace virtualization helps to group and deliver a list of applications or desktops together as a single complete virtual workspace. vWorkspace delivers secure, full-featured virtual workspaces from a centralized infrastructure, that consists of virtual and physical computers, and provisions new users quickly.

Related Links

- Document Purpose
- Intended Audience

Document Purpose

Document Purpose

This deployment guide provides instructions on how to configure the LoadMaster to load balance the various roles in the Dell Wyse vWorkspace environment.

Intended Audience

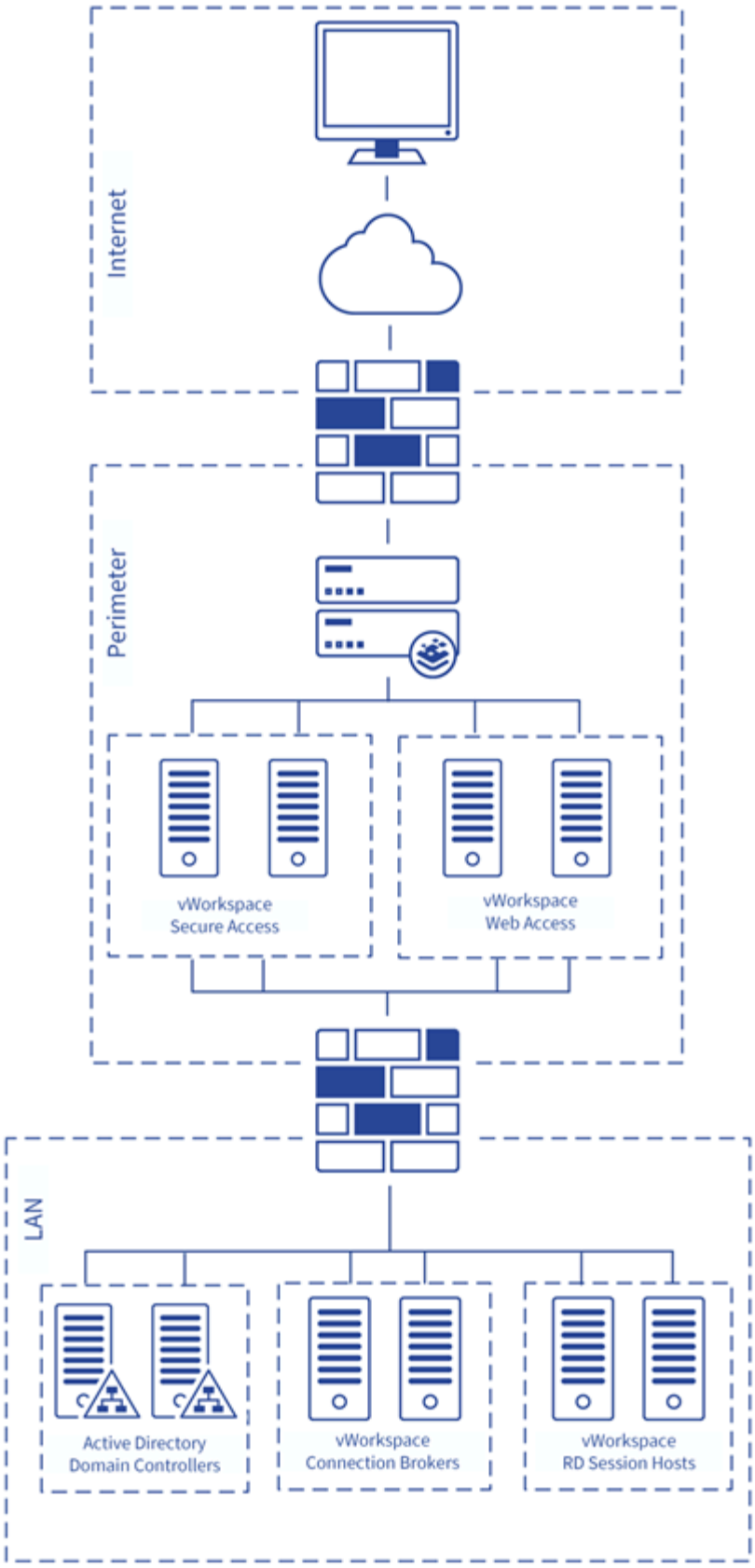
Intended Audience

This document is intended to be read by anyone who is interested in finding out how to configure the LoadMaster to load balance Dell Wyse vWorkspace.

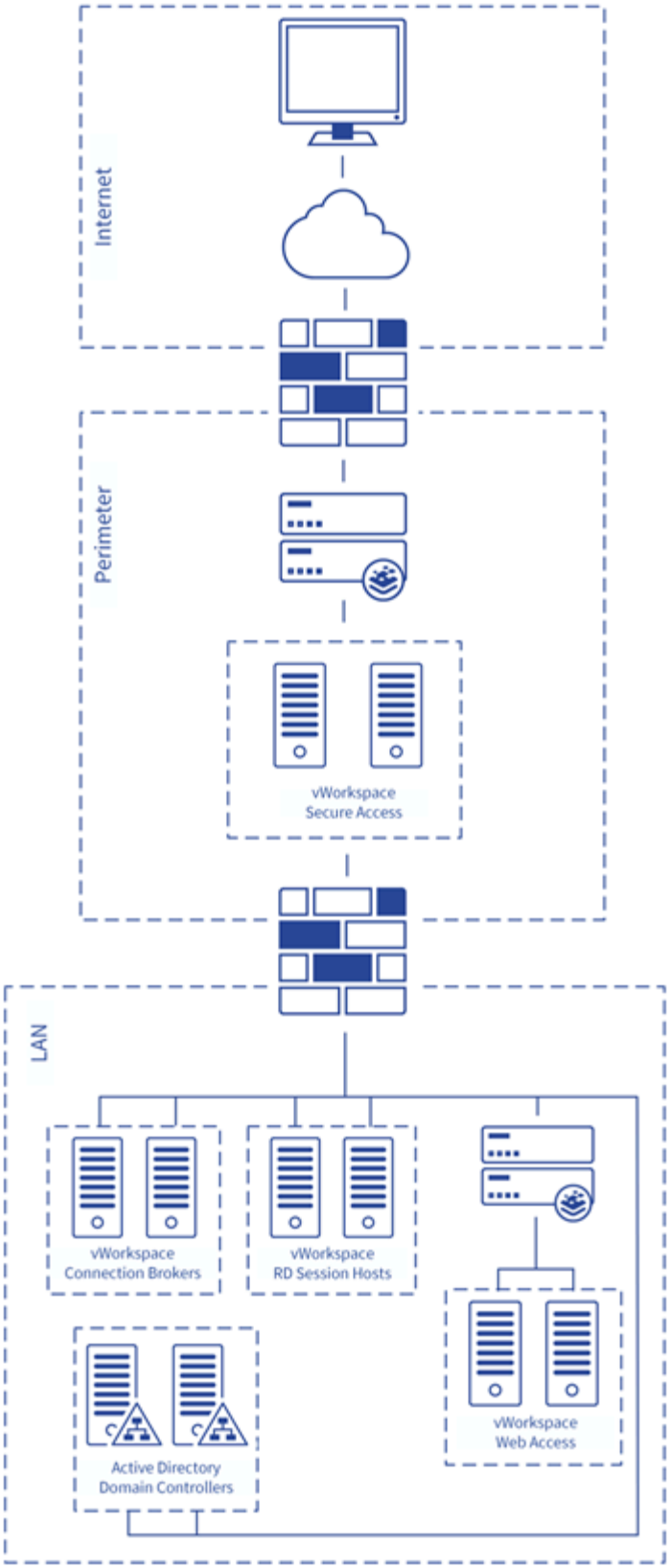
2

Load Balancing vWorkspace

Load Balancing vWorkspace


Internet
Perimeter
vWorkspace
Secure Access
vWorkspace
Web Access
LAN
Active Directory
Domain Controllers
vWorkspace
Connection Brokers
vWorkspace
RD Session Hosts

The figure above shows a scenario where the LoadMaster can be used to load balance vWorkspace services. In this configuration, both Secure Access Services and Web Access are deployed in the DMZ. If your configuration differs from this configuration and there are issues deploying the LoadMaster, please contact the local Progress Kemp Support Team for assistance: http://kemptechnologies.com/load-balancing-support/kemp-support



The figure above shows a different scenario where the LoadMaster can be used to load balance vWorkspace

services. In this configuration the Secure Access Services are deployed in the DMZ and the Web Access is deployed in the corporate network. If your configuration differs from this configuration and there are issues deploying the LoadMaster, please contact the local Progress Kemp Support Team for assistance: http://kemptechnologies.com/load-balancing-support/kemp-support

Related Links

- vWorkspace Roles

vWorkspace Roles

vWorkspace Roles

Wyse vWorkspace consists of various roles. The LoadMaster can be configured to load balance some of these roles. The sections below discuss the various scenarios in which the LoadMaster can be used load balance vWorkspace.

Related Links

- Load Balancing Web Access Services
- Load Balancing Secure Access Services

Load Balancing Web Access Services

Load Balancing Web Access Services

Web Access is a web application that acts as a web-based portal to a vWorkspace farm. It provides users with a list of available applications and desktops using their web browser.

The Web Access role also authenticates users with multiple vWorkspace farms within the same Active Directory domain.

Load Balancing Secure Access Services

Load Balancing Secure Access Services

vWorkspace Secure Access Service is an SSL gateway that simplifies the deployment of applications over the Internet. The Secure Access Service allows access to published applications through the vWorkspace Web Access client and starts these applications over SSL connections.

The Secure Access Service provides a proxy connection to vWorkspace components such as RDP Sessions, the Web Access client and connection brokers.

3

General Configuration

General Configuration

Refer to the following sections for general configuration information about the **Subnet Originating Requests** option and SSL certificates.

Related Links

- Enable Subnet Originating Requests Globally
- SSL Certificates

Enable Subnet Originating Requests Globally

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 Real Server sees traffic originating from 10.20.20.21 (LoadMaster eth1 address) and responds correctly in most scenarios.

With **Subnet Originating Requests** disabled, the Real Server sees traffic originating from 10.0.0.15 (LoadMaster Virtual Service address on **eth0**) and responds to **eth0** which could cause asymmetric routing.

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 User Interface (UI), go to **System Configuration > Miscellaneous Options > Network Options**.
2. Select the **Subnet Originating Requests** check box.

SSL Certificates

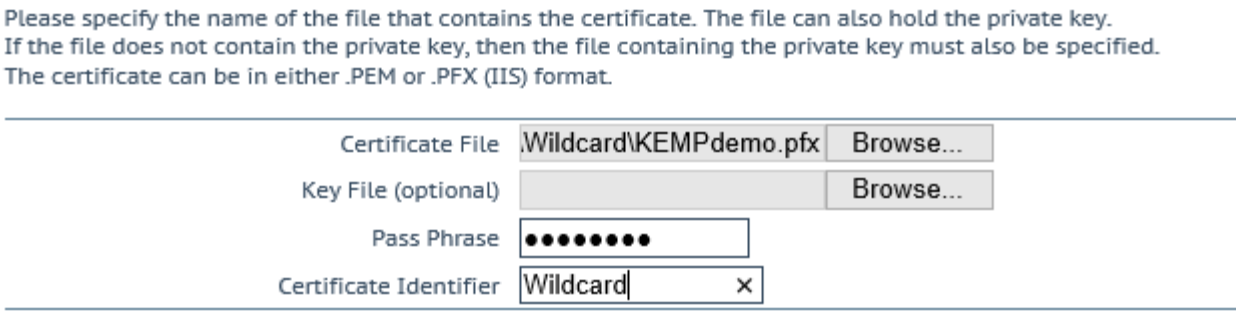
SSL Certificates

An SSL certificate is required to be installed on the LoadMaster to support load-balanced components such as the Secure Access Service.

The certificate needs to match the hostname which is used to connect to the load-balanced services of the LoadMaster and can be a single wildcard, for example *.domain.com, or multiple regular certificates, for example secure.domain.com.

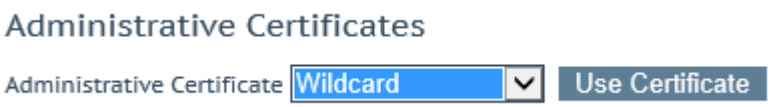
To install an SSL certificate on the LoadMaster, follow the steps below in the LoadMaster Web User Interface (WUI):

1. In the main menu, select **Certificates & Security > SSL Certificates**.
2. Click **Import Certificate**.



1. Click **Choose File** or **Browse**.
2. Browse to and select the certificate.
3. Enter a **Pass Phrase** if needed.
4. Enter a name (preferably the DNS name of the service) in the **Certificate Identifier** field.
5. Click **Save**.
6. Click **OK**.

This certificate will be assigned to some of the Virtual Services in later steps.



It is also possible to use this certificate for administrative purposes (browsing the LoadMaster WUI). To do this, on the **Manage Certificates** screen, select the certificate in the **Administrative Certificate** drop-down list and click **Use Certificate**.

4

Configure Virtual Services for vWorkspace

Configure Virtual Services for vWorkspace

Refer to the following sections for details on prerequisites and Virtual Services for vWorkspace.

Related Links

- Secure Access Prerequisites
- Virtual Services – Secure Access
- Web Access Prerequisites
- Virtual Services – Web Access

Secure Access Prerequisites

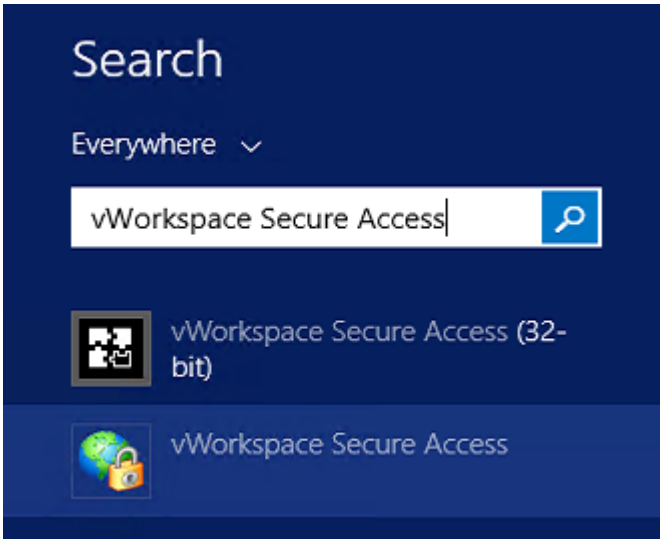
Secure Access Prerequisites

As described in the SSL Certificates section, implementing load balancing for vWorkspace Secure Access Services requires connectivity over HTTPS protocol (port 443).

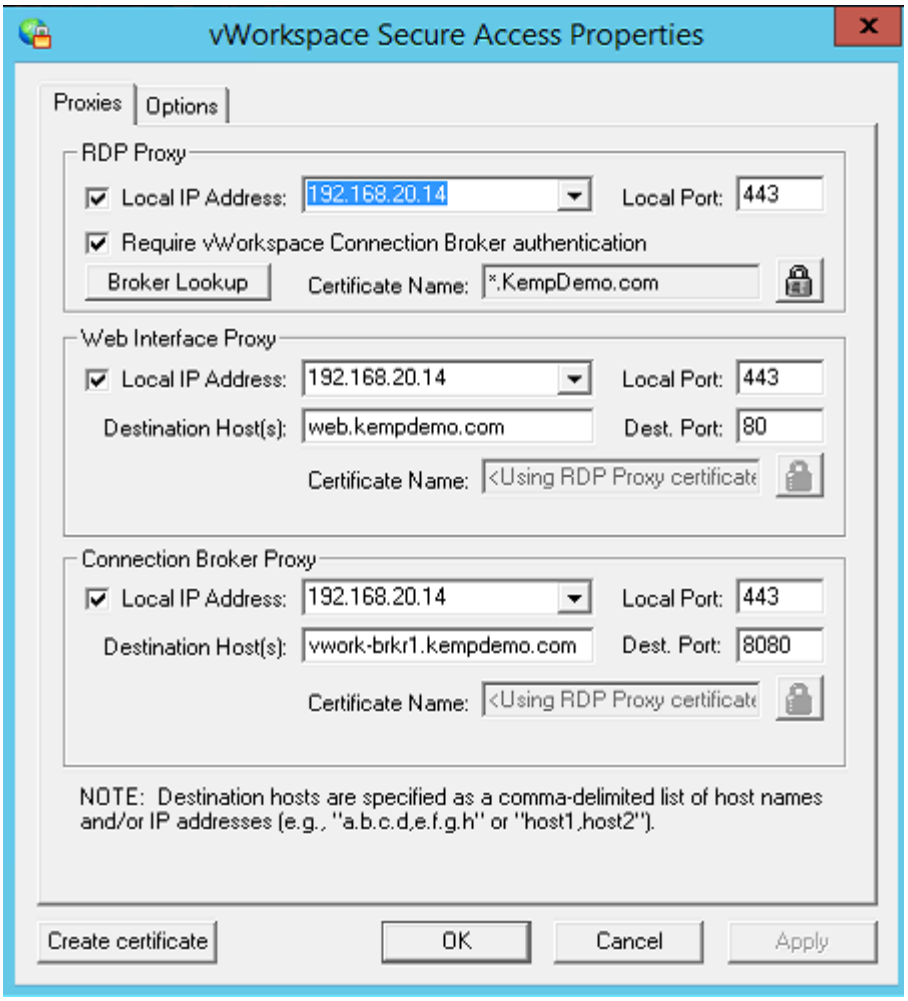
Note: This document will cover an example of the settings required for vWorkspace. The vWorkspace administrator should follow the Deployment Guide provided by Dell to complete the configuration based on their unique topology.

Before adding Virtual Services to the LoadMaster, ensure to have the DNS names and IP addresses available for all Secure Access Service roles in your deployment. The DNS Names used must be included in the Certificate that was installed in the SSL Certificates section.

1. Install the Certificate that will be used to encrypt the traffic on each of the Secure Access Servers.



2. On each of the vWorkspace Secure Access Servers, launch the Secure Access configuration utility from the Windows Server 2012 Start Menu.



3. Under the properties of the Secure Access Service, configure the following settings:
   1. In the **RDP Proxy** section:
      1. Select the **Local IP Address**.
      2. Enter **443** as the **Local Port**.
      3. Select the SSL certificate to be used to encrypt traffic.
   2. In the Web Interface Proxy section:
      1. Select the **Local IP Address**.
      2. Enter **443** as the **Local Port**.
      3. Enter **80** as the **Dest. Port**.
      4. Enter the **Destination Host URL** for the Web Access Server.

      Note: This will point to the LoadMaster Virtual Service for the Web Access Role.

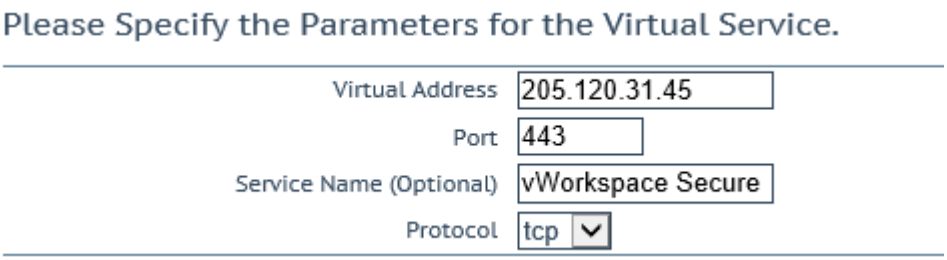
   3. In the Connection Broker Proxy section:
      1. Select the **Local IP Address**.
      2. Enter **443** as the **Local Port**.
      3. Enter **8080** as the **Dest. Port**.
      4. Enter the **Destination Host(s)** for the internal Connection Broker(s).
4. Click **OK.**

Virtual Services – Secure Access

Virtual Services – Secure Access

Configure the LoadMaster settings by following the steps below in the LoadMaster WUI:

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



2. Enter the relevant IP address in the **Virtual Address** text box.
3. Enter **443** as the **Port**.
4. Enter a recognizable **Service Name**, such as **vWorkspace Secure Access Service**.
5. Click **Add this Virtual Service**.
6. Enter the details shown in the following table:

Section	Option	Value	Comments
Standard Options	Persistence Mode	Source IP Address	
	Timeout	6 minutes	
	Scheduling Method	least connection	
SSL Properties	SSL Acceleration	Enabled	
	Reencrypt	Enabled	
	Assigned Certificates	Selected	Select the certificate in the **Available Certificates** box. Click the right arrow to move the certificate to the **Assigned**

Section	Option	Value	Comments
			Certificates box then click **Set Certificates**
Real Servers	Real Server Check Method	HTTPS Protocol	
	Checked Port	443	Click **Set Check PortNew**.

7. Select **Reencrypt**.

Note: The LoadMaster will use this information to check if the Secure Access servers are reachable.

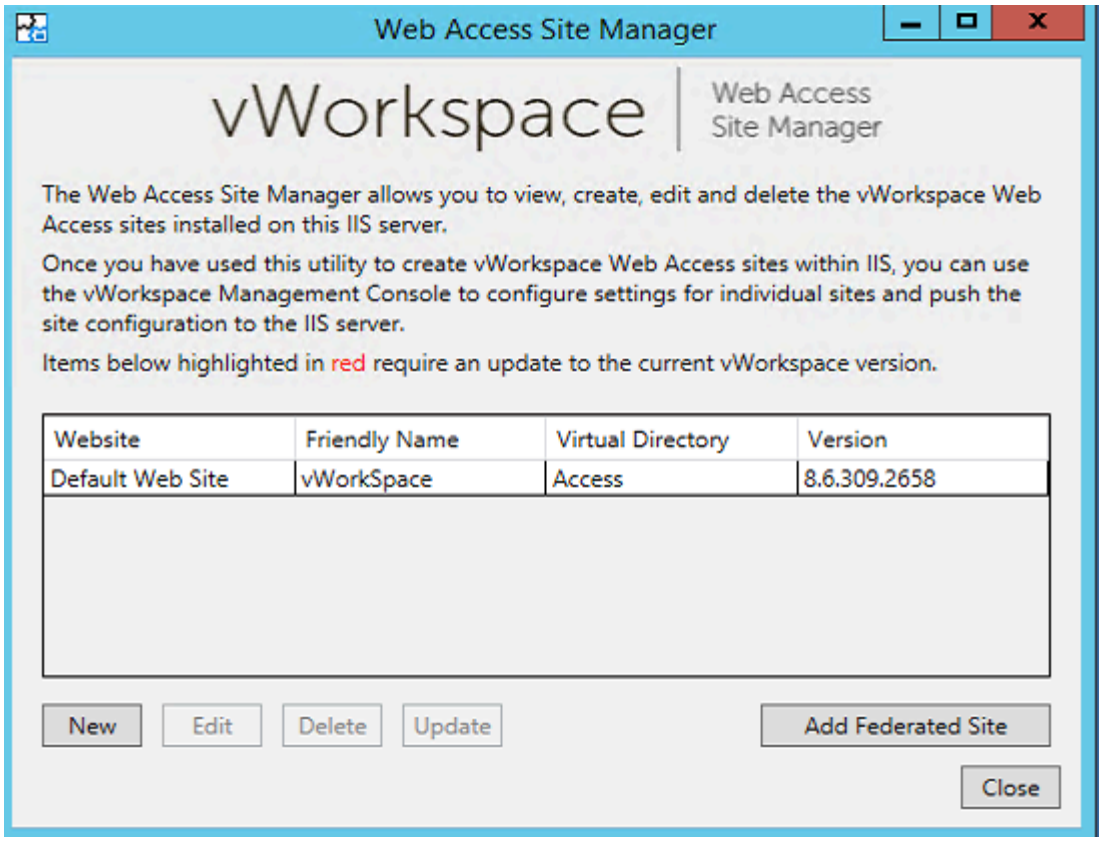
8. Add the Real Servers.
   1. Click **Add New** to add the Secure Access servers as Real Servers.
   2. Enter the **Real Server Address**.
   3. Enter **443** as the **Port**.
   4. Click **Add This Real Server**.
   5. Repeat the three steps above until all Real Servers have been added.

Web Access Prerequisites

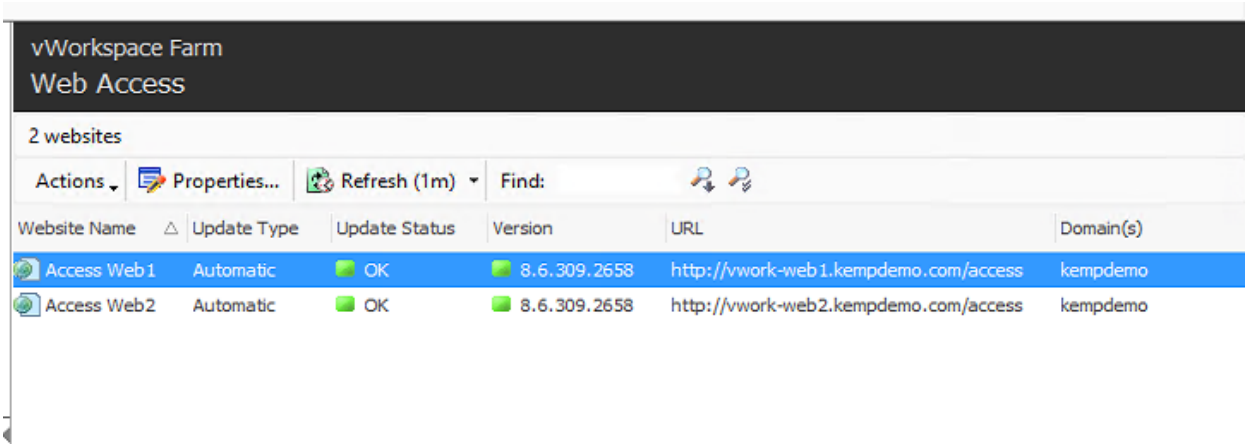
Web Access Prerequisites

Before configuring the LoadMaster, ensure to have the DNS names and IP addresses available for all Web Access roles in your deployment.

Note: This document will cover an example of the settings required for vWorkspace. The vWorkspace administrator should follow the Deployment Guide provided by Dell to complete the configuration based on their unique topology.



1. Configure the website on each of the Web Access Servers using the Web Access Site Manager.



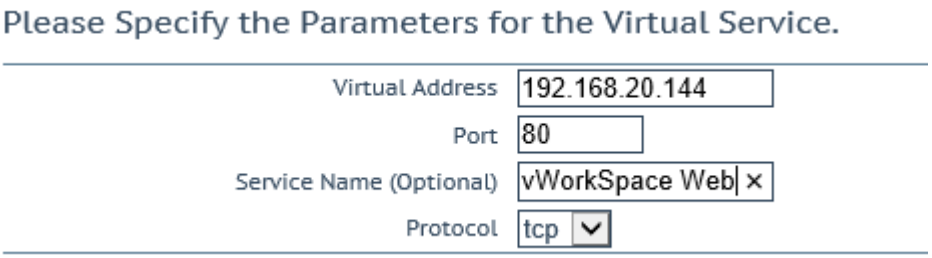
2. Within the vWorkspace Management Console, select Web Access in the left-hand navigation, and add the website for each of the Web Access servers.

Virtual Services – Web Access

Virtual Services – Web Access

Configure the LoadMaster settings by following the steps below in the LoadMaster WUI:

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



2. Enter the relevant IP address in the **Virtual Address** text box.
3. Enter **80** as the **Port**.
4. Enter a recognizable **Service Name**, such as vWorkspace Web Access.
5. Click **Add this Virtual Service**.
6. Enter the details shown in the following table:

Note: The LoadMaster will use this information to check if the Web Access servers are reachable.

Section	Option	Value	Comments
Standard Options	Persistence Mode	Source IP Address	
	Timeout	6 minutes	
	Scheduling Method	least connection	
Real Servers	Real Server Check Method	HTTP Protocol	
	Checked Port	80	Click **Set Check Port**.

7. Add the Real Servers.
   1. Click **Add New** to add the Secure Access servers as Real Servers.

2. Enter the **Real Server Address**.
3. Enter **80** as the **Port**.
4. Click **Add This Real Server**.
5. Repeat the three steps above until all Real Servers have been added.

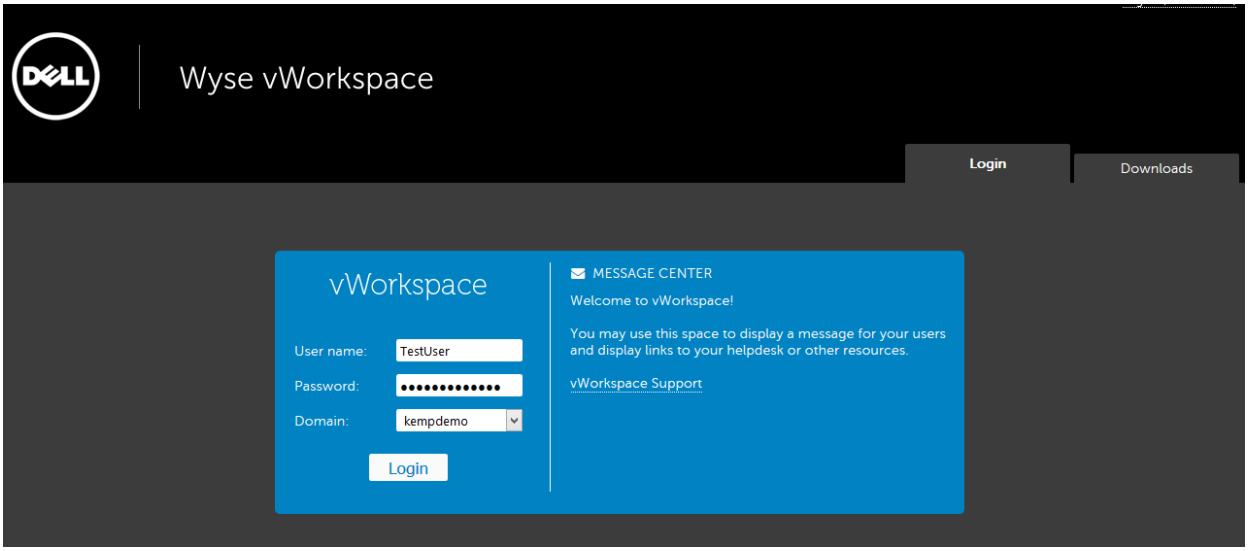
5

Testing

Testing

After following the implementation steps in the previous section, follow the steps below to test the load-balanced vWorkspace environment:

1. Open a web browser that is able to reach the load-balanced IP.
2. Browse to the configured DNS name for the load-balanced service, for example **https://Secure.kempdemo.com/access**. A web page should be presented with the vWorkspace login page. This indicates that the LoadMaster has redirected the session to a Real Server.



3. Enter a username and password with permissions to access the vWorkspace environment.
4. In the LoadMaster WUI, go to **Statistics > Real Time Statistics**.
5. Click the **Real Servers** button.

Note: This overview shows the active sessions, sessions over the last hour, in addition to how many requests each Real Server handled.

Global | Real Servers | Virtual Services

Name	RS-IP	Status	Total Conns	Last 60 Sec
1⇒	192.168.20.12	Up	0	0
2⇒	192.168.20.13	Up	0	0
3⇒	192.168.20.14	Up	3	3
4⇒	192.168.20.15	Up	0	0
4		System Total Conns	3	3

6. Open another web browser on a different client and perform the first three steps above.

Global | Real Servers | Virtual Services

Name	RS-IP	Status	Total Conns	Last 60 Sec
1⇒	192.168.20.12	Up	0	0
2⇒	192.168.20.13	Up	0	0
3⇒	192.168.20.14	Up	3	3
4⇒	192.168.20.15	Up	4	4
4		System Total Conns	7	7

7. Refresh the LoadMaster statistics page. Notice that, based on the load balancing method we chose, load is spread over both Secure Access Servers (192.168.20.14 and 192.168.20.15).