Progress®
Kemp® LoadMaster®

Deployment Guide Windows Server 2012 R2 DirectAccess

Generated on: 12 January 2026

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

About the Author 6

Chapter 2: Load Balancing DirectAccess 7

Example Environment Setup 8

Prerequisites 9

Chapter 3: Virtual Service Configuration 10

Enable Subnet Originating Requests Globally 10

Configure DirectAccess for Load Balancing 11

Configure the Servers Virtual Services 11

Configure a DirectAccess Server Virtual Service 12

Configure an Additional Virtual Service for the DirectAccess Server 13

Configure a Network Location Server (NLS) Virtual Service 14

Configure an NLS (Offloaded) Virtual Service 15

Configure DirectAccess to use a Load-Balanced NLS 17

Configure Geographic Load Balancing for NLS 18

Chapter 4: Multisite Configuration and Load Balancing 21

Configure DirectAccess for Multisite 21

Add an Additional DirectAccess Entry Point 22

Configure a DirectAccess Entry Point for Load Balancing 23

Configure Geographic Load Balancing for Multisite 23

Chapter 5: References 25

1

Introduction

DirectAccess is a remote access technology included with the Unified Remote Access role in Windows Server 2012 R2. DirectAccess is a unique solution designed to provide secure, seamless, transparent and always-on remote corporate network access for Windows 7 Enterprise/Ultimate or Windows 8.x Enterprise and later domain-joined clients. DirectAccess is based on common Windows platform technologies such as Active Directory Domain Services (AD DS), Active Directory Certificate Services (AD CS), IPsec, and IPv6. IPv6 transition and translation protocols ensure interoperability with networks and services that are IPv4 only.

Document Purpose

This document provides guidance for configuring LoadMaster products and DirectAccess to eliminate single points of failure and to provide fault tolerance and high availability for a Windows Server 2012 R2 DirectAccess deployment. This document refers to a representative DirectAccess deployment which is described in detail later. This document does not address all possible deployment scenarios for a DirectAccess solution. For questions regarding unique configurations, contact the Progress Kemp Support team: http://kemptechnologies.com/load-balancing-support/Kemp-support/.

Intended Audience

This document is designed for the Windows network engineer tasked with eliminating single points of failure and providing fault tolerance and high availability for an existing DirectAccess deployment. The engineer should have a strong understanding of Windows infrastructure (AD architecture and administration, DNS, and Public Key Infrastructure (PKI)) and should already be familiar with the basics of DirectAccess. They should have a detailed working knowledge of IPv4 networking. Knowledge and experience with IPv6 networking is not required, but strongly recommended.

Assumptions

This document assumes that DirectAccess has been configured and deployed in a single server, single site configuration and is currently in working order. It also assumes that the DirectAccess servers will have two network adapters, with the internal network interface on the LAN and the external network interface in a perimeter (DMZ) network with the LoadMaster connected directly to the public Internet. In addition, the features and configuration in this document require the use of PKI for the issuance and management of digital certificates required for DirectAccess functionality.

Contents

- About the Author

About the Author

Richard Hicks is a network and security expert specializing in Microsoft Technologies. He is an MCP, MCSE, MCSA, MCITP Enterprise Administrator, and Microsoft Most Valuable Professional (MVP) for Enterprise Security. Richard has designed and implemented Microsoft edge security and remote access solutions for some of the largest companies in the world. Richard is an independent consultant focused on helping organizations large and small implement DirectAccess and client-based VPN remote access solutions on the Microsoft platform. You can learn more about Richard by visiting www.richardhicks.com.

2

Load Balancing DirectAccess

An enterprise DirectAccess deployment presents many opportunities to deploy LoadMaster products to eliminate single points of failure and to provide fault tolerance and high availability. The LoadMaster can be deployed to provide load balancing for the following DirectAccess infrastructure components:

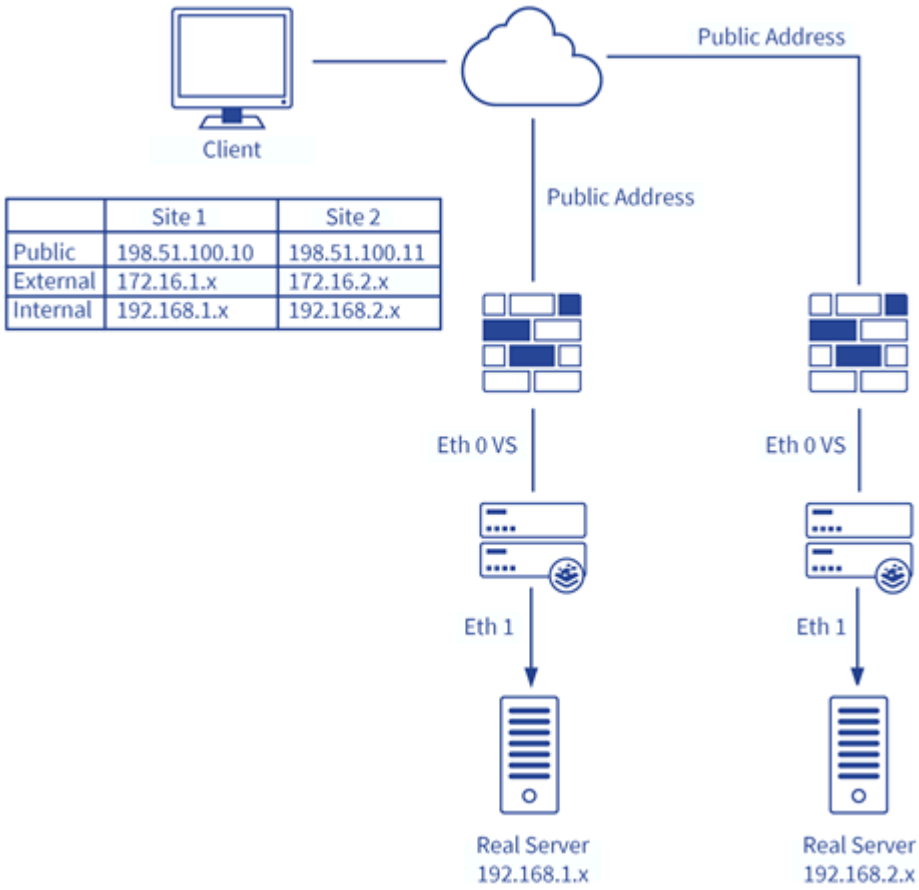
1. **DirectAccess Server:** The DirectAccess server is the gateway between the corporate network and remote DirectAccess clients. DirectAccess clients are configured using group policy to establish DirectAccess sessions with the gateway. The DirectAccess server itself is a single point of failure and should be configured in a highly available cluster using the LoadMaster.
2. **Network Location Server:** The Network Location Server (NLS) is used by DirectAccess clients to determine if they are inside or outside of the corporate network. When a DirectAccess client first establishes network connectivity, a probe is sent to the NLS. If the NLS does not respond, the client attempts to establish DirectAccess connectivity. If the NLS is offline for any reason (planned or unplanned) DirectAccess clients on the internal network may lose connectivity to corporate resources until the NLS is back online. To prevent service disruption, the NLS should be made highly available using the LoadMaster.
3. **Global Load Balancing for DirectAccess:** DirectAccess supports multisite deployments, where multiple DirectAccess entry points can be configured in different geographic locations to provide redundancy. Windows 8.x and later clients can automatically select the best entry point to use and can also fail over to another site if their existing location becomes unavailable. The site selection logic used by the client is quite simplistic, however. Organizations will benefit greatly from the use of the LoadMaster GEO feature to provide more intelligent site selection for Windows 8.x clients.
4. **Global Load Balancing for NLS:** DirectAccess uses a single Fully Qualified Domain Name (FQDN) for NLS. A minimum of two NLSs configured for load balancing is essential to ensure the highest levels of availability. In some cases, network location servers will be located in different geographies, and it might be desirable to have DirectAccess clients connect to the NLS closest to them. The LoadMaster GEO feature can be used to provide intelligent traffic routing for internal DirectAccess clients accessing the NLS, ensuring that clients always connect to a local NLS.

Note: Users should note that, Progress Kemp supports “Split DNS”. We do not, currently, support “Force Tunneling”.

Contents

- Example Environment Setup
- Prerequisites

Example Environment Setup



In this documentation example, Windows Server 2012 R2 DirectAccess has been deployed in a single server, single site deployment. The DirectAccess servers are configured with two network interfaces; the internal network interface resides on the internal LAN and the external network interfaces resides in the external perimeter network or DMZ. DirectAccess is configured for certificate authentication and supports both Windows 7 and Windows 8.x clients. The NLS are deployed on dedicated systems. Infrastructure is in place to facilitate load balancing DirectAccess servers in site A, as well as to deploy DirectAccess in a multisite configuration with load balanced DirectAccess servers in site B. An additional LoadMaster is located in site A to provide internal geographic load balancing for NLS. Although not specifically documented here, the LoadMasters themselves are single points of failure and should be configured in a redundant manner to ensure the highest levels of availability. In all, the deployment includes the following:

1. DirectAccess Servers – 2 per site

2. NLS servers – 2 per site
3. LoadMasters – 2 edge-facing (1 per site) and 1 internal

The external DNS name space used in this environment is **example.net**. The Internal DNS name space is **lab.example.net**.

The following use cases will be included in this documentation:

- Load balancing of DirectAccess servers
- Load balancing of NLS
- Geographic load balancing of DirectAccess entry points
- Geographic load balancing of NLS

Prerequisites

A number of prerequisites must be in place before proceeding with this documentation. In addition to the assumptions outlined earlier in this document, it is assumed that the LoadMaster has been configured and that network connectivity to all networks has been verified. In addition, the following prerequisites must be in place before continuing:

- A unique internal hostname for the load balanced NLS, for example nls.corp.example.com
- A unique external hostname for each entry point that resolves to the external IPv4 address assigned to the DirectAccess Virtual Service on the LoadMaster, for exampleda-west.example.com, da-east.example.com
- DirectAccess must be configured to use certificate authentication
- The NLS cannot be collocated on the DirectAccess server. It must reside on a separate system
- Intra-Site Automatic Tunnel Addressing Protocol (ISATAP) for outbound DirectAccess client management is not supported when using external load balancers and must be disabled prior to implementing the LoadMaster

3

Virtual Service Configuration

Refer to the following sections for details on configuring the LoadMaster using the recommended settings for DirectAccess.

Contents

- Enable Subnet Originating Requests Globally
- Configure DirectAccess for Load Balancing
- Configure the Servers Virtual Services
- Configure DirectAccess to use a Load-Balanced NLS
- Configure Geographic Load Balancing for NLS

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.

Configure DirectAccess for Load Balancing

Note: Ensure that the second DirectAccess server is configured prior to executing this step. The server should be joined to the domain, have valid IPv4 addresses assigned for all network interfaces, all required certificates should be installed and the DirectAccess role should be installed.

To configure DirectAccess for load balancing, follow the steps below:

1. In the Windows Server 2012 R2 Remote Access Management console, click **Enable Load Balancing** under **Load Balanced Cluster** in the **Tasks** pane.
2. Select the option to **Use an external load balancer**.
3. Provide a new IPv4 address to be assigned to the internal network interface of the DirectAccess server.
4. Provide a new IPv4 address to be assigned to the external network interface of the DirectAccess server.
5. Review the configuration and click **Commit**.
6. Click **Add or Remove Servers** under **Load Balanced Cluster** in the **Tasks** pane.
7. Click **Add Server** and enter the hostname of the second DirectAccess server. Confirm the network and certificate configuration, click **Next**, and then click **Add**, **Close**, and then **Commit**.

Configure the Servers Virtual Services

Three Virtual Services should be configured in a DirectAccess environment:

- A DirectAccess Server Virtual Service
- A Web Probe Server Virtual Service
- A Network Location Server (NLS) Virtual Service

Note: The NLS Virtual Service can be configured with or without SSL offloading.

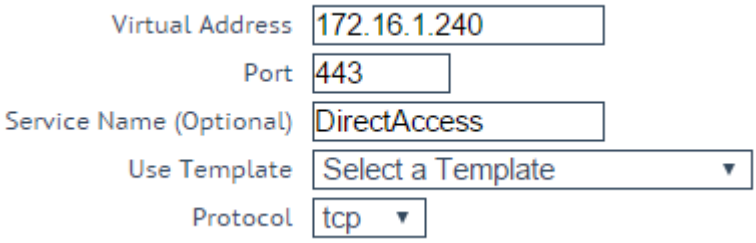
Contents

- Configure a DirectAccess Server Virtual Service
- Configure an Additional Virtual Service for the DirectAccess Server
- Configure a Network Location Server (NLS) Virtual Service
- Configure an NLS (Offloaded) Virtual Service

Configure a DirectAccess Server Virtual Service

To configure a DirectAccess Server Virtual Service manually, follow the steps below in the LoadMaster Web User Interface (WUI):

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



2. Enter an IPv4 address in the **Virtual Address** text box.
3. Change the **Port** to **443**.
4. Provide a **Service Name** (optional).
5. Click **Add this Virtual Service**.
6. Expand the **Standard Options** section.
7. Configure the settings as recommended in the following table:

Section	Option	Value	Comment
Standard Options	Force L7	Enabled	
	Transparency	Enabled	If the DirectAccess server has a single Network Interface Card (NIC) or does not use the LoadMaster as its default

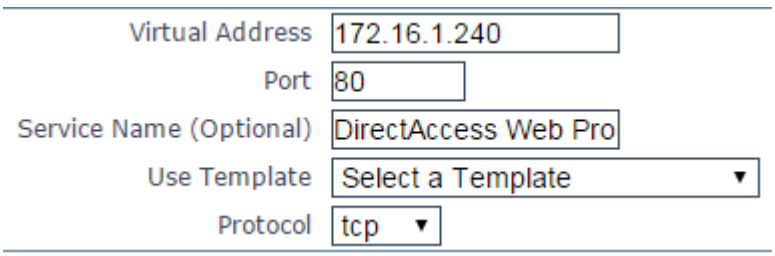
Section	Option	Value	Comment
			gateway, deselect **Transparency**.
	Persistence Mode	Source IP Address	
	Timeout	30 minutes	
	Scheduling Method	Round Robin	
	Quality of Service	Normal-Service	
Real Servers	Real Server Check Parameters	TCP Connection Only	Click **Add New**, enter the **Real Server Address** of the external network interface of the first DirectAccess server, and then click **Add This Real Server**. Repeat this step for all additional DirectAccess servers.

8. In the main menu, go to **Statistics > Real Time Statistics** and then click **Virtual Services**. Verify that the Virtual Service is up and that all Real Servers are online and available.

Configure an Additional Virtual Service for the DirectAccess Server

If DirectAccess is configured to use the default settings for the Network Connectivity Assistant, it will be necessary to configure an additional Virtual Service on the LoadMaster for this resource. To do this, follow the steps below in the LoadMaster WUI:

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



2. In the **Virtual Address** text box, enter the IPv4 address that was originally assigned to the internal network interface of the first DirectAccess server when load balancing was initially configured.

   Note: This is the same IPv4 address that the hostname **directaccess-webprobehost** resolves to in internal DNS.

3. Provide a **Service Name** (optional).
4. Click **Add this Virtual Service** when finished.
5. Configure the settings as recommended in the following table:

Section	Option	Value	Comment
Standard Options	Force L7	Enabled	
	Transparency	Disabled	
	Scheduling Method	round robin	
Real Servers			Click **Add New**. In the **Real Server Address** text box, enter the address of the internal network interface of the first DirectAccess server. Click **Add This Real Server**. Repeat the two steps above for all additional DirectAccess servers.

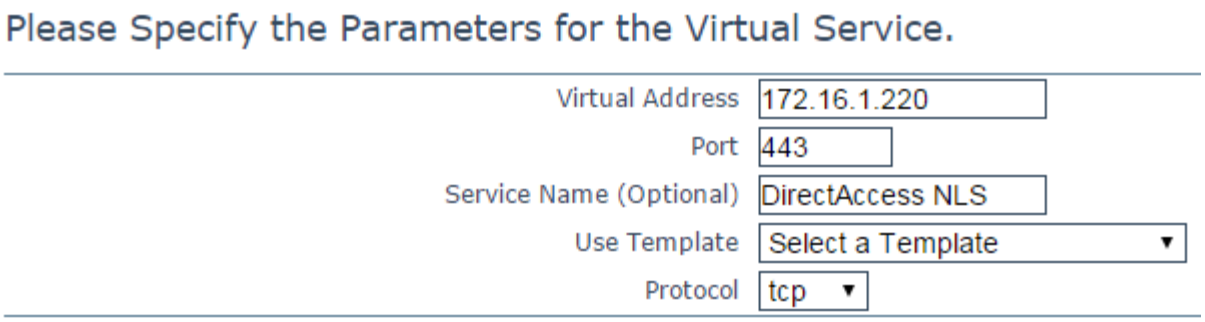
6. In the main menu, click **Statistics** and then click **Virtual Services**. Verify that the Virtual Service is up and that all Real Servers are online and available.

Configure a Network Location Server (NLS) Virtual Service

Note: This Virtual Service should only be configured if offloading is NOT required. If offloading is required, please refer to the Configure an NLS (Offloaded) Virtual Service section.

To configure an NLS Virtual Service, follow the steps below in the LoadMaster WUI:

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



2. Enter a unique IPv4 address in the **Virtual Address** text box.
3. Enter **443** as the **Port**.
4. Provide a **Service Name** (optional).
5. Click **Add this Virtual Service** when finished.
6. Configure the settings as recommended in the following table:

Section	Option	Value	Comment
Standard Options	Force L7	Enabled	
	Transparency	Enabled	
	Scheduling Method	round robin	
Real Servers			Click **Add New**. In the **Real Server Address** text box, enter the address in the Real Server text box. Click **Add This Real Server**. Repeat the two steps above for all additional NLS servers.

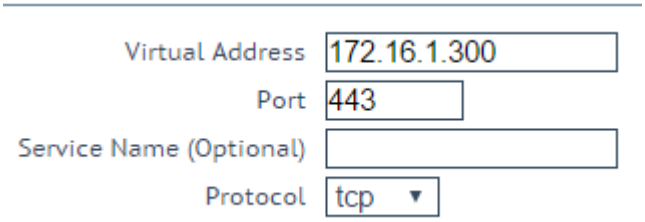
7. In the main menu, click **Statistics** and click **Virtual Services**. Verify that the Virtual Service is up and that all Real Servers are online and available.

Configure an NLS (Offloaded) Virtual Service

Note: This Virtual Service should only be configured if offloading is required. It cannot be configured if an NLS (without offloading) has previously been added. If an NLS (without offloading) is required, please refer to the Configure a Network Location Server (NLS) Virtual Service section.

To configure an NLS (Offloaded) Virtual Service, use the following steps in the LoadMaster WUI:

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



2. Enter a unique IPv4 address in the **Virtual Address** text box.
3. Enter **443** as the **Port**.
4. Provide a **Service Name** (optional).
5. Click **Add this Virtual Service** when finished.
6. Configure the settings as recommended in the following table:

Section	Option	Value	Comment
Basic Properties	Service Name	Direct Access NLS Offloaded	Click **Set Nickname**
	Service Type	HTTP/HTTPS	
	Activate or Deactivate Service	Selected	
Standard Options	Transparency	Selected	
	Persistence Options	None	
	Scheduling Method	round robin	
SSL Properties	SSL Acceleration	Enabled	
	Supported Protocols	TLS1.0; TLS1.1; TLS1.2; TLS1.3	While this workload may not support TLS1.3 yet, Progress Kemp recommend enabling it for future proofing.

Section	Option	Value	Comment
Advanced Properties	Content Switching	Disabled	
	Add HTTP Headers	Legacy Operation (X-ClientSide)	
	Error Code	200 OK	
	Error Message	Select Message	Click the **Set Message** button.
	Redirection URL	https://%h%s	Click **Add HTTP Redirector** button.
Real Servers			.

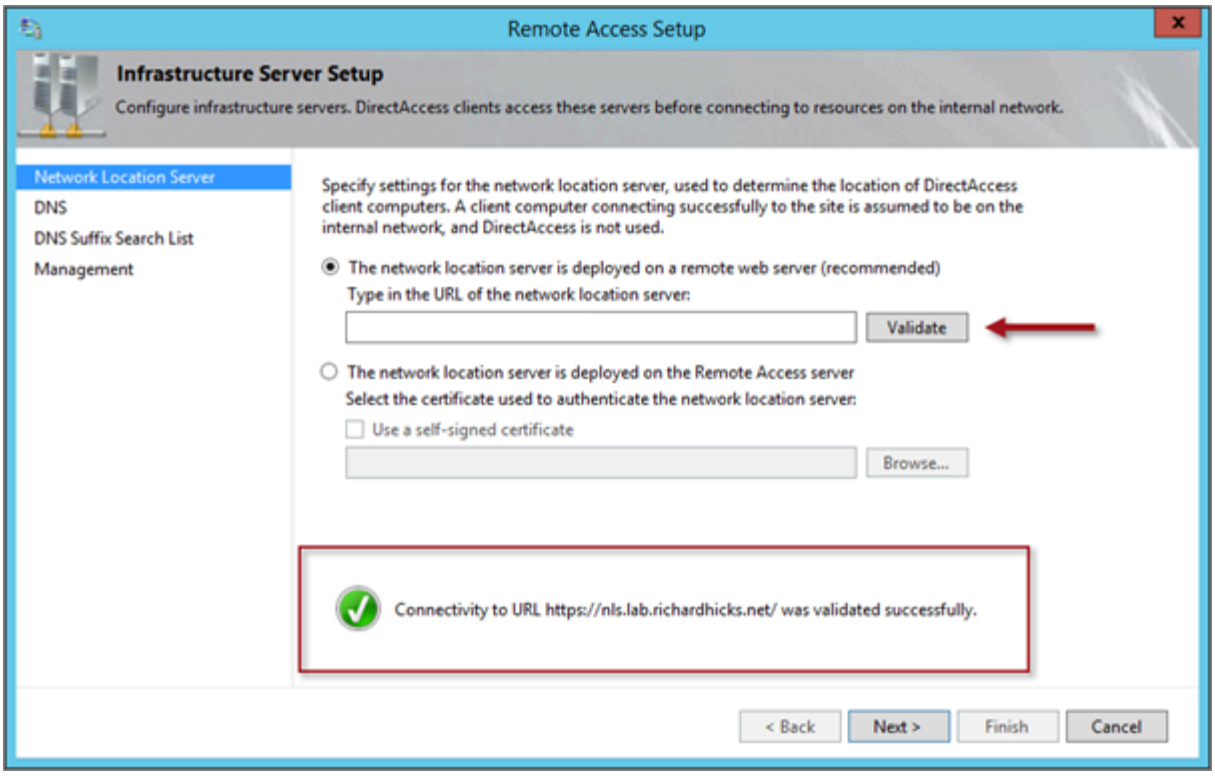
Note: No Real Server is needed for an NLS (Offloading) as a **Port 80 Redirector VS** has been added.

Configure DirectAccess to use a Load-Balanced NLS

Note: Clients on the internal network will lose connectivity to the domain if the NLS is unavailable. If enabling load balancing for NLS for an existing DirectAccess deployment, it is recommended that the NLS be reachable by clients and have a valid SSL certificate available during the transition. As the NLS hostname will be changing when this happens, a hostname mismatch will occur on the original NLS during the cutover, causing clients to fail the NLS check. This issue can be addressed by assigning a multi-SAN certificate to the NLS that includes both the original NLS name and the new load-balanced name prior to implementing this change.

To configure DirectAccess to use a load-balanced NLS, follow the steps below:

1. In the internal DNS, create a DNS record with a hostname that resolves to the virtual IP address configured for the NLS Virtual Service.
2. In the Remote Access Management console, click **DirectAccess and VPN** under the **Configuration** node in the navigation tree.
3. In the **Step 3 Infrastructure Servers** box, click **Edit**.



4. Enter the new NLS URL and click **Validate**.
5. Ensure that connectivity to the URL is validated successfully before proceeding.
6. Save and apply the configuration.

Configure Geographic Load Balancing for NLS

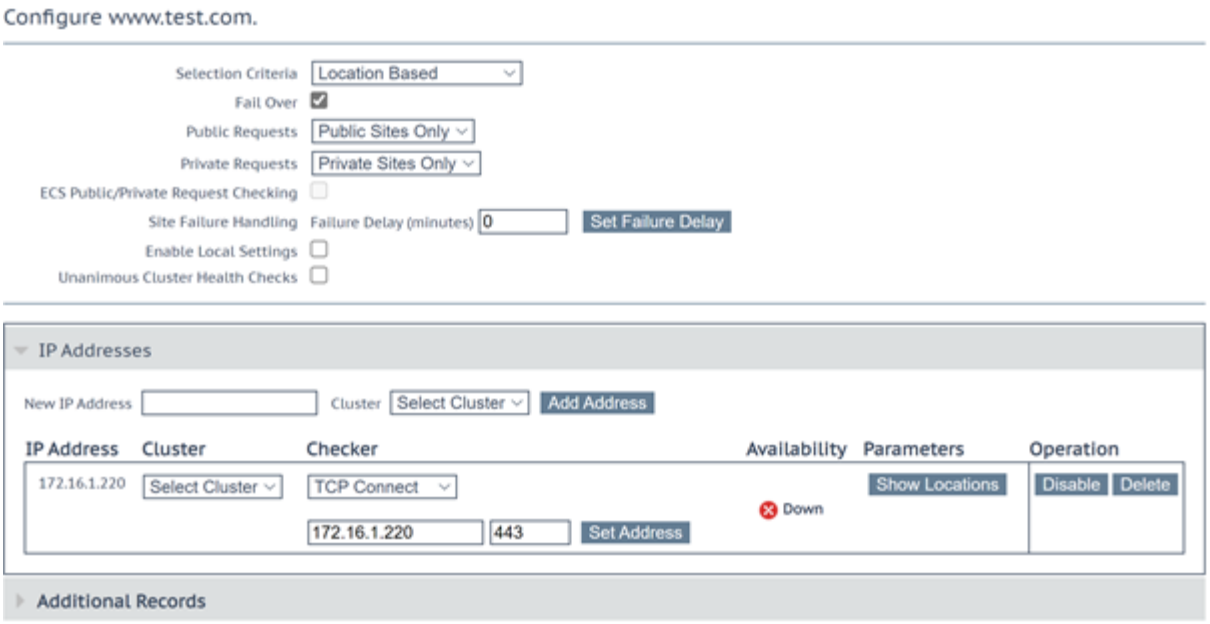
Note: Since the LoadMasters which were configured previously in this document are configured as edge facing, with eth0 connected to the public Internet and the NLS traffic as internal only, a dedicated LoadMaster for NLS geographic load balancing is used for full segregation. It is also possible to use a single LoadMaster for both edge facing traffic and internal GSLB traffic by assigning an internal-only interface for internal GSLB traffic through modification of the **Use for GEO Responses and Requests** option which is available on each interface.

To configure geographic load balancing for NLS, follow the steps below in the LoadMaster WUI:

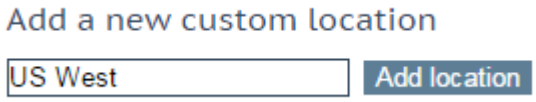
1. In the main menu, expand **Global Balancing** and click **Manage FQDNs**.
2. Click **Add FQDN**.



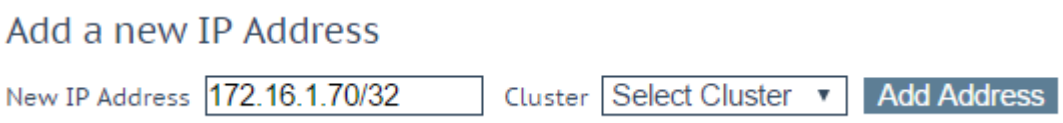
3. Enter the **New FQDN** to be used for NLS and click **Add FQDN**.
4. Click **OK**.



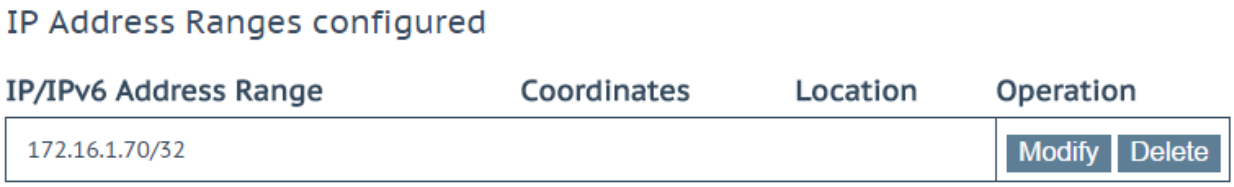
5. For **Selection Criteria** choose **Location Based**.
6. Tick the **Fail Over** check box.
7. Enter the IP addresses assigned to the NLS Virtual Services in each site, clicking **Add Address** after entering each one.
8. For each IP address:
   1. Select **Tcp Connect** as the **Checker**.
   2. Enter the IPv4 address of the NLS Virtual Service in the **Addr** text box.
   3. Enter port **443**.
   4. Click **Set Addr**.
9. In the main menu, select **IP Range Selection Criteria**.



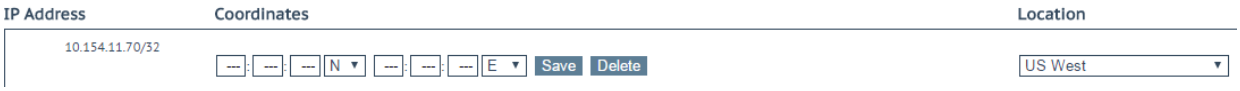
10. In the **Add a new custom location** text box, enter a name for the custom location, for example **US West** and click **Add Location**.



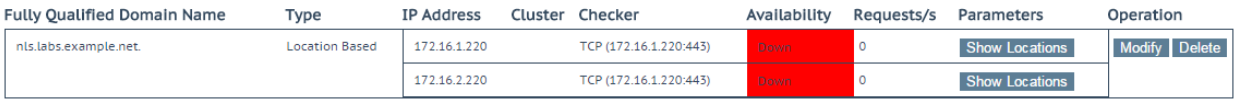
11. In the **Add a new IP address** text box, enter the IPv4 subnet where each NLS resides and click **Add Address**.



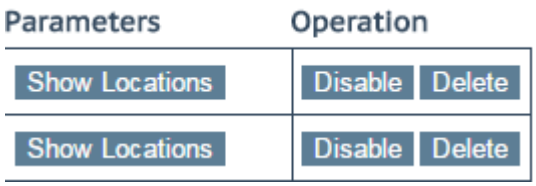
12. Click **Modify**.



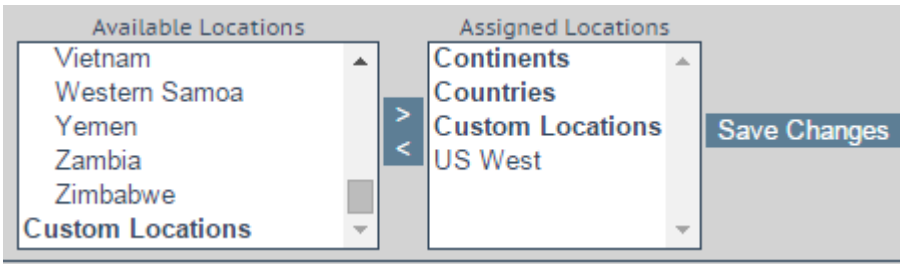
13. Then, select the custom location from the drop-down list.
14. In the main menu, click **Manage FQDNs**.



15. Click **Modify**.



16. For the first IP address click **Show Locations**.



17. From the **Available Locations** list, select the custom location which was created previously and click **>** to add it to the **Assigned Locations** list
18. Click **Save Changes**.
19. Repeat these steps for the second IP address, this time creating and choosing a different custom location.
20. Refer to the GEO, Feature Description document for guidance on configuring DNS delegation for the NLS FQDN.

4

Multisite Configuration and Load Balancing

Note: Enabling multisite DirectAccess alters the configuration in a way that will instantly and permanently disconnect any DirectAccess connections for existing remote clients. This occurs because when DirectAccess multisite is enabled, the IPv6 addresses of the Dynamic Tunnel Endpoints (DTEs) change immediately. However, the connection security rules for DirectAccess clients can only be updated using group policy, and with the loss of corporate network connectivity over DirectAccess the client is unable to obtain this new information. To resolve this issue, the DirectAccess client will have to connect to the LAN and update group policy to obtain the new settings. Optionally, a remote network connection using client-based VPN can be established and group policy can be updated over the VPN connection. When the VPN connection is closed, the client will once again establish a DirectAccess connection to the corporate network.

Contents

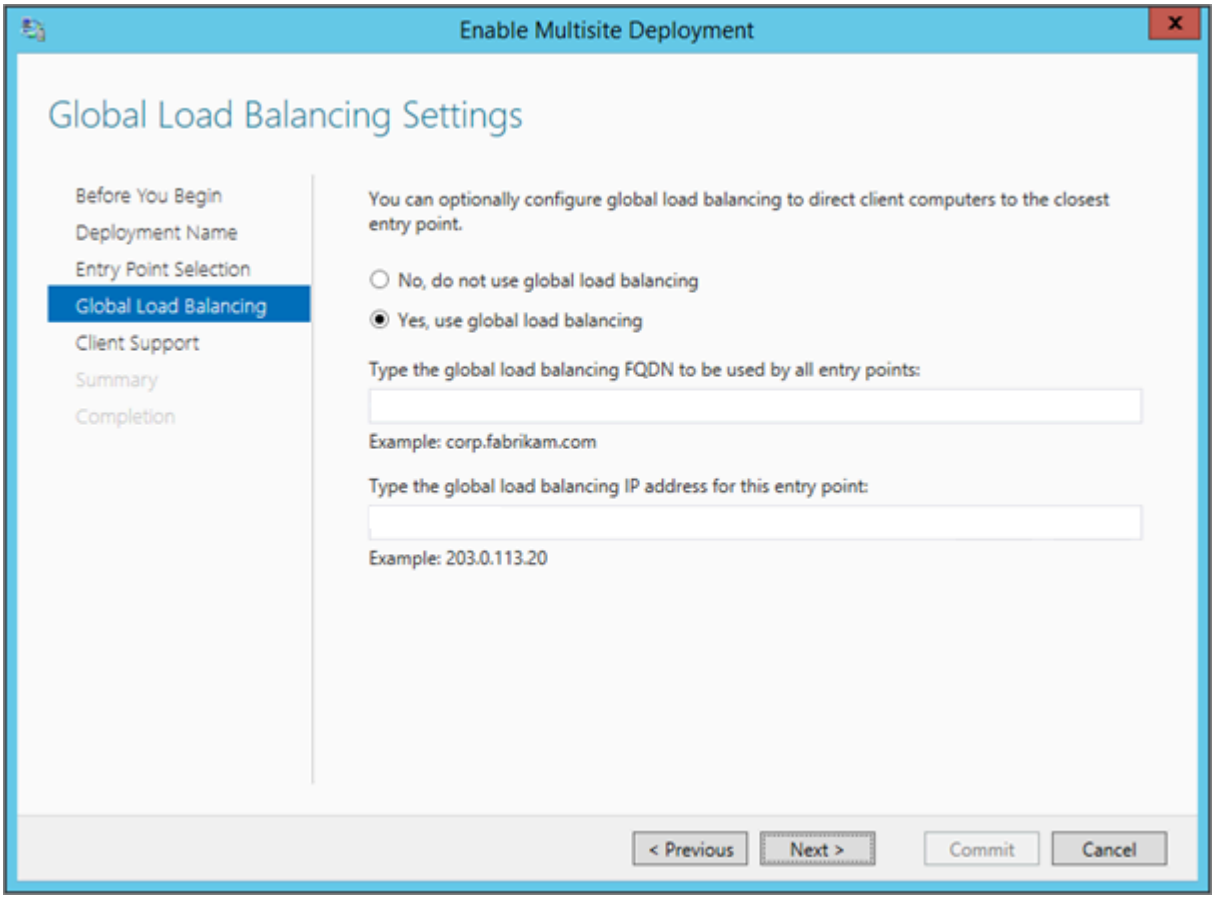
- Configure DirectAccess for Multisite
- Add an Additional DirectAccess Entry Point
- Configure a DirectAccess Entry Point for Load Balancing
- Configure Geographic Load Balancing for Multisite

Configure DirectAccess for Multisite

To configure DirectAccess for multisite, follow the steps below:

1. In the Remote Access Management console, highlight **DirectAccess and VPN** under the **Configuration** node in the navigation tree.
2. Click **Enable Multisite** under **Multisite Deployment** in the **Tasks** pane.

3. Provide a **Multisite deployment name** and **First entry point name**.
4. Choose an entry point selection method.



5. Select **Yes, use global load balancing**.
6. Enter the global load balancing FQDN to be used by all entry points.
7. Enter the global load balancing IPv4 address for this entry point. This is the public IPv4 address assigned to the DirectAccess Virtual Service on the LoadMaster. Global Server Load Balancing (GSLB) on the LoadMaster will be configured later.
8. If Windows 7 client support is required, choose the option to **Allow client computers running Windows 7 to access this entry point**, click **Add,** and then choose a security group.
9. Validate Group Policy Objects (GPOs).
10. Review the changes and click **Commit**.

Add an Additional DirectAccess Entry Point

Note: Be sure that the DirectAccess servers for the new entry point are configured prior to executing this step. The servers should be joined to the domain, have proper IPv4 addresses assigned for all network interfaces, all required certificates should be installed and the DirectAccess role should be installed.

To add an additional DirectAccess entry point, follow the steps below:

1. In the Remote Access Management console, click **Add an Entry Point** under **Multisite Deployment** in the **Tasks** pane.
2. Enter the name of the server that will be the first server in the new entry point and provide a unique name for this entry point.
3. Enter the global load balancing IPv4 address for this entry point.

   Note: This is the public IPv4 address assigned to the DirectAccess Virtual Service on the LoadMaster for this entry point.

4. Select the network topology that corresponds to your deployment.
5. Enter the public hostname for the entry point.

   Note: This hostname should resolve to the public IPv4 address assigned to the DirectAccess Virtual Service on the LoadMaster for this entry point.

6. Confirm the network and certificate settings.
7. If Windows 7 client support is required, choose the option to **Allow client computers running Windows 7 to access this entry point**, click **Add,** and then choose a security group.
8. Validate Group Policy Objects (GPOs).
9. Review the changes and click **Commit**.

Configure a DirectAccess Entry Point for Load Balancing

To configure a DirectAccess Entry Point for load balancing, follow the steps below:

1. In the Remote Access Management console, highlight **DirectAccess and VPN** under the **Configuration** node in the navigation tree.
2. Click **Enable Load Balancing** under **Load Balanced Cluster** in the **Tasks** pane.
3. Select the option to **Use an external load balancer**.
4. Provide a new IPv4 address to be assigned to the external network interface of the DirectAccess server.
5. Provide a new IPv4 address to be assigned to the internal network interface of the DirectAccess server.
6. Review the configuration and click **Commit**.
7. Click **Add or Remove Servers** under **Load Balanced Cluster** in the **Tasks** pane.
8. Click **Add Server** and enter the hostname of the second DirectAccess server for this entry point.
9. Confirm the network and certificate configuration.
10. Confirm the server settings and click **Add**, **Close**, and **Commit**.
11. Follow the steps outlined previously in this document for configuring Virtual Services for the DirectAccess server, web probe host, and NLS for this site.

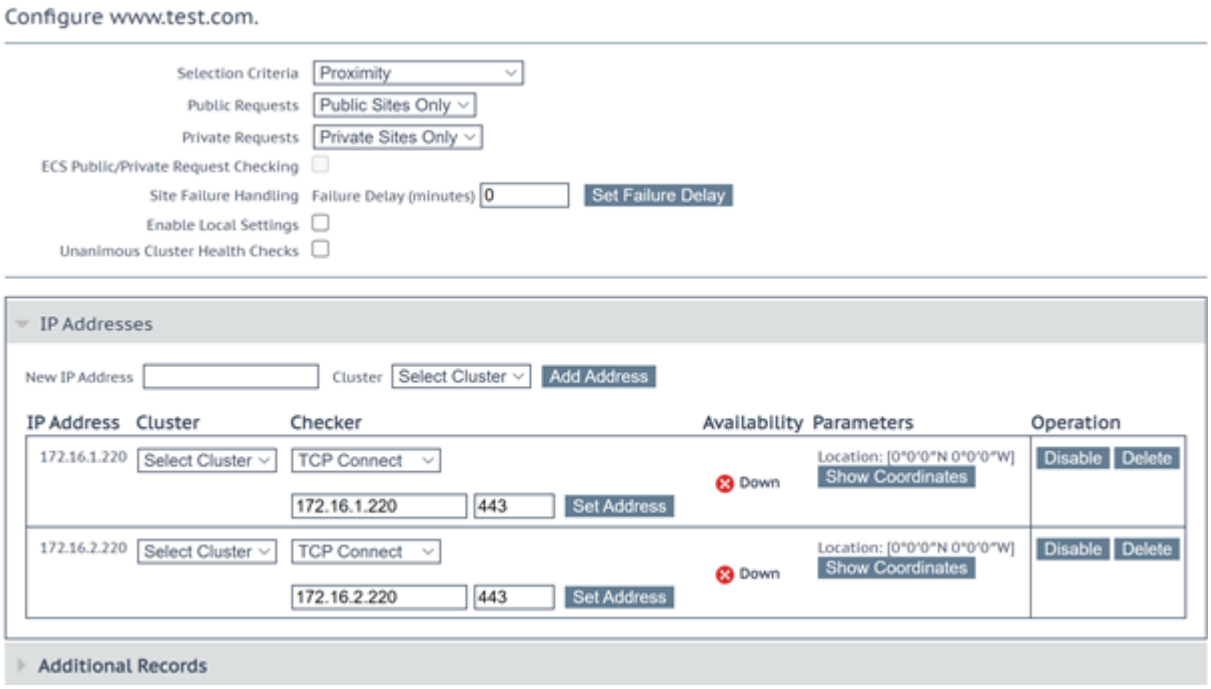
Configure Geographic Load Balancing for Multisite

To configure geographic load balancing for multisite, follow the steps below in the LoadMaster WUI:

1. In the main menu, expand **Global Balancing** and click **Manage FQDNs**.
2. Click **Add FQDN**.



3. Enter the DirectAccess global load balancing FQDN and click **Add FQDN**.
4. Click **OK**.



5. Choose an appropriate **Selection Criteria** that meets your requirements.

Note: If DirectAccess entry points are widely dispersed, for example if there is one entry point in Los Angeles and another in New York, **Proximity** or **Location Based** are ideal choices. If **Location Based** is chosen, select the option to enable **Fail Over**.

---

6. Enter the GSLB IPv4 address for each DirectAccess entry point and click **Add Address** after entering each IP address.
7. For each IP address:
   1. Select **Tcp Connect** in the **Checker** column.
   2. Enter the global load balancing IPv4 address of each DirectAccess entry point in the **Addr** text box.
   3. Enter port **443**.
   4. Click **Set Addr**.
8. If the **Selection Criteria** is set to **Location Based**, click **Show Locations** and assign a continent or country where the entry point resides.

Refer to the GEO, Feature Description document for guidance on configuring DNS delegation for the DirectAccess global load balancing FQDN.

5

References

Further information can be found in the links below:

GEO, Feature Description

DirectAccess in Windows Server

Planning for Multi-site DirectAccess

DirectAccess Unsupported Configurations

DirectAccess Troubleshooting Guide

Richard Hicks' DirectAccess Blog