Copyright Notices

Copyright © 2002-2016 KEMP Technologies, Inc. All rights reserved. KEMP Technologies and the KEMP Technologies logo are registered trademarks of KEMP Technologies, Inc.

KEMP Technologies, Inc. reserves all ownership rights for the LoadMaster product line including software and documentation. The use of the LoadMaster Exchange appliance is subject to the license agreement. Information in this guide may be modified at any time without prior notice.

Microsoft Windows is a registered trademark of Microsoft Corporation in the United States and other countries. All other trademarks and service marks are the property of their respective owners.

Limitations: This document and all of its contents are provided as-is. KEMP Technologies has made efforts to ensure that the information presented herein are correct, but makes no warranty, express or implied, about the accuracy of this information. If any material errors or inaccuracies should occur in this document, KEMP Technologies will, if feasible, furnish appropriate correctional notices which Users will accept as the sole and exclusive remedy at law or in equity. Users of the information in this document acknowledge that KEMP Technologies cannot be held liable for any loss, injury or damage of any kind, present or prospective, including without limitation any direct, special, incidental or consequential damages (including without limitation lost profits and loss of damage to goodwill) whether suffered by recipient or third party or from any action or inaction whether or not negligent, in the compiling or in delivering or communicating or publishing this document.

Any Internet Protocol (IP) addresses, phone numbers or other data that may resemble actual contact information used in this document are not intended to be actual addresses, phone numbers or contact information. Any examples, command display output, network topology diagrams, and other figures included in this document are shown for illustrative purposes only. Any use of actual addressing or contact information in illustrative content is unintentional and coincidental.

Portions of this software are; copyright (c) 2004-2006 Frank Denis. All rights reserved; copyright (c) 2002 Michael Shalayeff. All rights reserved; copyright (c) 2003 Ryan McBride. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE ABOVE COPYRIGHT HOLDERS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE ABOVE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The views and conclusions contained in the software and documentation are those of the authors and should not be interpreted as representing official policies, either expressed or implied, of the above copyright holders.

Portions of the LoadMaster software are copyright (C) 1989, 1991 Free Software Foundation, Inc. -51 Franklin Street, Fifth Floor, Boston, MA 02110-1301, USA- and KEMP Technologies Inc. is in full compliance of the GNU license requirements, Version 2, June 1991. Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.
Portions of this software are Copyright (C) 1988, Regents of the University of California. All rights reserved. Redistribution and use in source and binary forms are permitted provided that the above copyright notice and this paragraph are duplicated in all such forms and that any documentation, advertising materials, and other materials related to such distribution and use acknowledge that the software was developed by the University of California, Berkeley. The name of the University may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

Portions of this software are Copyright (C) 1998, Massachusetts Institute of Technology

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Portions of this software are Copyright (C) 1995-2004, Jean-loup Gailly and Mark Adler

This software is provided 'as-is', without any express or implied warranty. In no event will the authors be held liable for any damages arising from the use of this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:

1. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.

2. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.

3. This notice may not be removed or altered from any source distribution.

Portions of this software are Copyright (C) 2003, Internet Systems Consortium

Permission to use, copy, modify, and/or distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND THE AUTHOR DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Used, under license, U.S. Patent Nos. 6,473,802, 6,374,300, 8,392,563, 8,103,770, 7,831,712, 7,606,912, 7,346,695, 7,287,084 and 6,970,933
# Table of Contents

1. **Introduction** ................................................................. 5  
   1.1 Document Purpose ....................................................... 5  
   1.2 Intended Audience ...................................................... 5  
   1.3 About the Author .......................................................... 5  
   1.4 Assumptions ............................................................... 6  
2. **Load Balancing DirectAccess** ........................................... 7  
   2.1 Example Environment Setup .......................................... 8  
   2.2 Prerequisites ............................................................. 9  
3. **Virtual Service Configuration** .......................................... 10  
   3.1 Enable Subnet Originating Requests Globally ..................... 10  
   3.2 Configure DirectAccess for Load Balancing ...................... 11  
   3.3 Configure the Servers Virtual Services ............................ 11  
      3.3.1 Configure a DirectAccess Server Virtual Service ............ 11  
      3.3.2 Configure an Additional Virtual Service for the DirectAccess Server ........................................ 12  
      3.3.3 Configure a Network Location Server (NLS) Virtual Service .............................................. 14  
      3.3.4 Configure an NLS (Offloaded) Virtual Service .............. 16  
   3.4 Configure DirectAccess to use a Load-Balanced NLS ............. 18  
   3.5 Configure Geographic Load Balancing for NLS ................... 19  
4. **Multisite Configuration and Load Balancing** ....................... 22  
   4.1 Configure DirectAccess for Multisite ............................... 22  
   4.2 Add an Additional DirectAccess Entry Point ....................... 23  
   4.3 Configure a DirectAccess Entry Point for Load Balancing .......... 24  
   4.4 Configure Geographic Load Balancing for Multisite ................. 25  

References .................................................................................... 27  

Document History ......................................................................... 28
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.

1.1 Document Purpose

This document provides guidance for configuring KEMP 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 KEMP Support team: http://kemptechnologies.com/load-balancing-support/KEMP-support/.

1.2 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.

1.3 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.
1.4 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 KEMP 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.
2 Load Balancing DirectAccess

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

- **DirectAccess Server**: The DirectAccess server is the gateway between the corporate network and remote DirectAccess clients. DirectAccess clients are configured via 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 KEMP LoadMaster.

- **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 KEMP LoadMaster.

- **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 KEMP LoadMaster GEO feature to provide more intelligent site selection for Windows 8.x clients.

- **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 KEMP 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.

Users should note that, KEMP supports “Split DNS” We do not, currently, support “Force Tunneling”
2.1 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:

- DirectAccess Servers – 2 per site
- NLS servers – 2 per site
- KEMP 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

### 2.2 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 KEMP 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 example `da-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

3.1 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 LoadMaster will route traffic so that the Real Server will see traffic arriving from the LoadMaster interface that is in that network/subnet.

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 or not 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 WUI, go to System Configuration > Miscellaneous Options > Network Options.

2. Tick the Subnet Originating Requests check box.
3.2 Configure DirectAccess for Load Balancing

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:

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.

3.3 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

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

3.3.1 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.

![Figure 3-2: Virtual Service Parameters]
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. If the DirectAccess server has a single Network Interface Card (NIC) or does not use the LoadMaster as its default gateway, deselect Transparency.
8. Select Source IP Address as the Persistence Mode.
9. Select 30 minutes as the Timeout value.
10. Select Round Robin as the Scheduling Method.
11. Expand the Real Servers section.

12. Ensure the Real Server Check Parameters is set to TCP Connection Only.
13. 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.
14. 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.

3.3.2 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.

   ![Figure 3-5: Virtual Service Parameters](image)

   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. Expand the **Standard Options** section.

   ![Figure 3-6: Standard Options](image)

   6. Remove the tick from the **Transparency** check box.

   ![Figure 3-7: Real Servers Section](image)
7. Expand the **Real Servers** section.
8. Click **Add New**.

![Figure 3-8: Real Server Parameters](image)

9. In the **Real Server Address** text box, enter the address of the internal network interface of the first DirectAccess server.
10. Click **Add This Real Server**.
11. Repeat the two steps above for all additional DirectAccess servers.
12. 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.

### 3.3.3 Configure a Network Location Server (NLS) Virtual Service

This Virtual Service should only be configured if offloading is **NOT** required. If offloading is required, please refer to Section 3.3.4.

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**.

![Figure 3-9: Virtual Service Parameters](image)

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. Expand the **Standard Options** section.
7. Ensure the **Transparency** check box is selected.
8. Set **Round Robin** as the **Scheduling Method**.
9. Expand the **Real Servers** section.

10. Click **Add New**.

11. Enter the address in the **Real Server Address** text box.
12. Click **Add This Real Server**.
13. Repeat the two steps above for all additional NLS servers.
14. 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.
3.3.4 Configure an NLS (Offloaded) Virtual Service

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 Section 3.3.3.

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. Expand the Basic Properties section.

7. Enter a Service Name and click Set Nickname.
8. Ensure the Service Type is set to HTTP/HTTPS.
9. Select the Activate or Deactivate Service check-box.
10. Expand the Standard Options section.

11. Ensure the Transparency check box is selected.
12. For Persistence Options the Mode should be None.
13. From the Scheduling Method drop down menu, select Round Robin.
14. Expand the SSL Properties section.

![Figure 3-16: SSL Properties](image)

15. For SSL Acceleration, select the Enabled check box.
16. For Supported Protocols, select the three TLS check boxes.
17. No Client Certificates are required.
18. Expand the Advanced Properties section.

![Figure 3-17: Advance Properties](image)

19. Ensure Content Switching is disabled.
20. Select Legacy Operation (X-ClientSide) from the Add HTTP Headers drop-down menu.
22. Enter an Error Message and click the Set Message button.
23. Ensure https://%h% is set as the Redirection URL and click the Add HTTP Redirector button.
3.4 Configure DirectAccess to use a Load-Balanced NLS

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.

### 3.5 Configure Geographic Load Balancing for NLS

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.
   - **Figure 3-19: New FQDN**
3. Enter the New Fully Qualified Domain Name to be used for NLS and click Add FQDN.
4. Click OK.
   - **Figure 3-20: Section of the Modify FQDN screen**
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:
   a) Select Tcp Connect as the Checker.
   b) Enter the IPv4 address of the NLS Virtual Service in the Addr text box.
   c) Enter port 443.
d) Click **Set Addr**.

9. In the main menu, select **IP Range Selection Criteria**.

![Add a new custom location](image)

**Figure 3-21: Add a new custom location**

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**.

![Add a new IP Address](image)

**Figure 3-22: Add a new IP address**

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

![IP Address Ranges configured](image)

**Figure 3-23: Modify the IP range**

12. Click **Modify**.

![Select the custom location](image)

**Figure 3-24: Select the custom location**

13. Then, select the custom location from the drop-down list.

14. In the main menu, click **Manage FQDNs**.

![Figure 3-25: Modify](image)

15. Click **Modify**.
16. For the first IP address click **Show Locations**.

![Figure 3-26: Show Locations](image)

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

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 via 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.

4.1 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**.

### 4.2 Add an Additional DirectAccess Entry Point

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. 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. 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**.

### 4.3 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.
4.4 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.

   ![Add a FQDN](image)
   
   **Figure 4-2: New FQDN**

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

   ![Modify FQDN](image)
   
   **Figure 4-3: Modify FQDN**

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

   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:
   a) Select Tcp Connect in the Checker column.
   b) Enter the global load balancing IPv4 address of each DirectAccess entry point in the Addr text box.
   c) Enter port 443.
   d) 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.
DirectAccess

References

Further information can be found in the links below:

GEO, Feature Description
http://kemptechnologies.com/loadmaster-documentation/

DirectAccess in Windows Server

Planning for Multi-site DirectAccess

DirectAccess Unsupported Configurations

DirectAccess Troubleshooting Guide

Richard Hicks’ DirectAccess Blog
http://directaccess.richardhicks.com/
## Document History

<table>
<thead>
<tr>
<th>Date</th>
<th>Change</th>
<th>Reason for Change</th>
<th>Version</th>
<th>Resp.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jan 2015</td>
<td>Initial draft</td>
<td>First draft of document</td>
<td>1.0</td>
<td>RH</td>
</tr>
<tr>
<td>Aug 2015</td>
<td>Minor changes</td>
<td>Enhancements made</td>
<td>1.1</td>
<td>RH</td>
</tr>
<tr>
<td>Sep 2015</td>
<td>Release updates</td>
<td>Updates for 7.1-30</td>
<td>3.0</td>
<td>LB</td>
</tr>
<tr>
<td>Nov 2015</td>
<td>Template updates</td>
<td>Enhancements made</td>
<td>4.0</td>
<td>KG</td>
</tr>
<tr>
<td>Feb 2016</td>
<td>Minor changes</td>
<td>Enhancements made</td>
<td>5.0</td>
<td>LB</td>
</tr>
<tr>
<td>Feb 2016</td>
<td>Minor changes</td>
<td>Enhancements made</td>
<td>6.0</td>
<td>LB</td>
</tr>
<tr>
<td>Mar 2016</td>
<td>Release updates</td>
<td>Updates for 7.1-34</td>
<td>7.0</td>
<td>LB</td>
</tr>
<tr>
<td>July 2016</td>
<td>Release updates</td>
<td>Updates for 7.1.35</td>
<td>8.0</td>
<td>LB</td>
</tr>
<tr>
<td>Aug 2016</td>
<td>Minor changes</td>
<td>Enhancements made</td>
<td>9.0</td>
<td>DD</td>
</tr>
</tbody>
</table>