DEPLOYMENT GUIDE

Load Balancing Microsoft DirectAccess

v1.2.2

Deployment Guide

NOTE: This guide has been archived and is no longer being maintained. While the content is still valid for the particular software versions mentioned, it may refer to outdated software that has now reached end-of-life. For more information please contact support@loadbalancer.org.

loadbalancer.org

Contents

1. About this Guide

This guide details the steps required to configure a load balanced Microsoft DirectAccess environment utilizing Loadbalancer.org appliances. It covers the configuration of the load balancers and also any Microsoft DirectAccess configuration changes that are required to enable load balancing.

For more information about initial appliance deployment, network configuration and using the Web User Interface (WebUI), please also refer to the Administration Manual.

2. Loadbalancer.org Appliances Supported

All our products can be used with DirectAccess. For full specifications of available models please refer to: https://www.loadbalancer.org/products.

Some features may not be supported in all cloud platforms due to platform specific limitations, please check with Loadbalancer.org support for further details.

3. Loadbalancer.org Software Versions Supported

- V8.3.8 and later

4. Microsoft Windows Versions Supported

- Windows 2012 and later

5. Microsoft 2012 DirectAccess

Introduction

DirectAccess is a feature of Windows that allows connectivity to organization network resources without the need for traditional Virtual Private Network (VPN) connections. With DirectAccess, client computers are always connected to your organization – there is no need for remote users to start and stop connections as is required with traditional VPN connections.

From a user's perspective DirectAccess is a completely automatic VPN connection that simplifies accessing corporate LAN services from wherever they are located.

DirectAccess Components

DirectAccess is part of the Remote Access server role. The table below details the key components that must be available for DirectAccess to work.

These are the components that are made highly available using the load balancer:

Component	Purpose
DirectAccess Server	This is the server that clients establish a tunnel with in order to access the corporate network. Client and server settings are configured via Group Policy to

	enable the IPsec tunnels to be established.
Network Location Server	The network location server is used to detect whether computers configured as DirectAccess clients are located in the corporate network. When clients are on the corporate network, DirectAccess is not used to reach internal resources. Instead, clients connect to these resources directly. If the client cannot reach the network location server, the client is considered to be outside the corporate network and a connection is established via the DirectAccess server.
Connectivity Verifier (Web Probe)	This is part of the Network Connectivity Assistant. It is used by clients to verify connectivity to the internal network.

How it Works

DirectAccess clients communicate with the corporate network using Internet Protocol version 6 (IPv6) and IPsec. To enable this to work over the IPv4 based Internet, IPv4 transition technologies (6to4, Teredo, or IP-HTTPS) are used to encapsulate the IPv6 packets in IPv4 packets.

6to4 and Teredo have various pre-requisites that can make deployment more complex. IP-HTTPS is much simpler to deploy and is the only protocol that can be used when the DirectAccess server is deployed behind a NAT firewall.

Network Location Server is used by the client to determine when it's outside the corporate LAN and automatically activates the connection when it is.

DirectAccess uses the Name Resolution Policy Table (NRPT) to identify which hosts should be accessed via the DirectAccess tunnel (i.e. internal servers) and those which should be accessed directly (i.e. Internet based servers). See page 6 for more information on the NRPT.

IPv6 Transition Protocols

Windows 2012 supports the following transition protocols for client to DirectAccess server communication:

Client Transition Protocol	Comments
6to4	- Uses protocol 41 to encapsulate IPv6 packets in IPv4 packets - Does NOT work when the client or the server are behind a NAT device - Both client and server must be assigned public IPv4 addresses
Teredo	- Uses UDP on port 3544 to encapsulate IPv6 packets in IPv4 packets - Supports client behind a NAT device but not server behind NAT - Server must be configured with 2 consecutive public IPv4 addresses
IP-HTTPS *****	- Uses standard port and protocol - Earlier clients/servers caused double encryption (IPsec & SSL/TLS) - Windows 8 and later use null encryption to solve the double encryption

***** *IP-HTTPS is the transition protocol used in this deployment guide*

Note: Additional protocols (NAT64 & DNS64) are used to provide external DirectAccess clients inbound access to IPv4 servers on the corporate LAN. When "mange-out" outbound access from IPv4 servers to DirectAccess clients is needed, ISATAP must be used. These protocols are not covered in this deployment guide.

Note: For Windows 2012 and Windows 8+ clients, IP-HTTPS is now the preferred IPv6 transition technology for DirectAccess as mentioned in this Microsoft blog.

Network Topology Options

DirectAccess supports several topology options including dual/single NIC and supports various connectivity options including directly connected (requires public IP addresses) and behind a NAT device.

Note: When DirectAccess servers are deployed behind a NAT device, the only IPv6 transition protocol that is supported is IP-HTTPS.

Network Location Server (NLS)

NLS is a critical component of DirectAccess and is used by clients to determine if they are inside or outside the corporate LAN. The NLS should only be resolvable/reachable internally, and NOT externally. It is possible to use the DirectAccess server as the location server but this is strongly discouraged by Microsoft. Instead, alternative servers should be selected. These servers require that IIS is installed with HTTPS bindings configured with a certificate that has the FQDN of the network location server. In this guide, this is **directaccess-nls.robstest.com**. Please refer to the following link for more details:

https://technet.microsoft.com/en-us/library/ee649162(v=ws.10).aspx

Client Connectivity Verifier (Web Probe)

The connectivity verifier is used by the Network Connectivity Assistant (NCA) on the DirectAccess clients to check that it can successfully connect to the internal resource. A successful connection indicates that the client is connected. This is not a critical component of DirectAccess, it is only a reporting mechanism and if the the NCA can't connect, DirectAccess functionality is not effected. Typically, the DirectAccess servers are used for this purpose. It's not possible to use Location Servers since by design they are only available when connected to the internal network, and therefore the client would not be able to connect when on the Internet. By default the FQDN for the probe is **directaccess-webprobehost.domain.com**. Note that DNS entries are auto created by the setup wizard.

Windows 7 DirectAccess Connectivity Assistant

Windows 7 clients require the DirectAccess connectivity assistant to be manually installed so they can connect to the web probe DNS address. Windows 8 clients have this installed by default.

It can be downloaded here: https://www.microsoft.com/en-us/download/details.aspx?id=10322

Name Resolution Policy Table (NRPT)

Some technologies (including DirectAccess) require special handling for name queries for specific portions of the DNS namespace. If the DNS name being searched matches specified portions of the namespace, apply the special handling. If the DNS name does not match the specified portions of the namespace, perform a normal DNS query using the interface-configured DNS servers. To address this need, the Name Resolution Policy Table (NRPT) is used.

When a DirectAccess client is on the Internet, the Name Resolution Policy Table (NRPT) causes DNS name queries for internal resources to be sent to internal DNS servers. In some cases this is not desirable, e.g. for the location servers. In these cases a NRPT exception can be added. This tells the DNS client to resolve the name using its normal interface-configured DNS server instead of sending the query to the internal DNS server.

An NRPT exception consists of a fully-qualified DNS name that has no associated DirectAccess DNS Server address (see page 14 for more details).

Certificate Requirements

For this guide, an internal CA was used to generate these certificates, and the same certificate/private key was installed on each DirectAccess/Network Location server. Certificates are required for the following:

1. IP-HTTPS, e.g. **https://directaccess.robstest.com**
2. Network Location Server, e.g. **https://directaccess-nls.robstest.com**

For DirectAccess in Windows Server 2012 and later, the DirectAccess server can act as a Kerberos proxy to perform IPsec authentication without requiring certificates. If the Kerberos protocol is used, it works over SSL, and the Kerberos proxy uses the certificate that is configured for IP-HTTPS for this purpose.

Windows7 clients do not support the Kerberos proxy and require computer certificates for IPSec. In this case, the DirectAccess server and clients are required to obtain a computer certificate. The simplest way to install the certificates is to configure Group Policy-based automatic enrollment for computer certificates. This ensures that all domain members obtain a certificate from the enterprise CA.

For more information on certificate requirements for please refer to the following URL:

https://technet.microsoft.com/en-gb/library/jj134148.aspx#bkmk_1_2_CAs_and_certs

6. Load Balancing DirectAccess

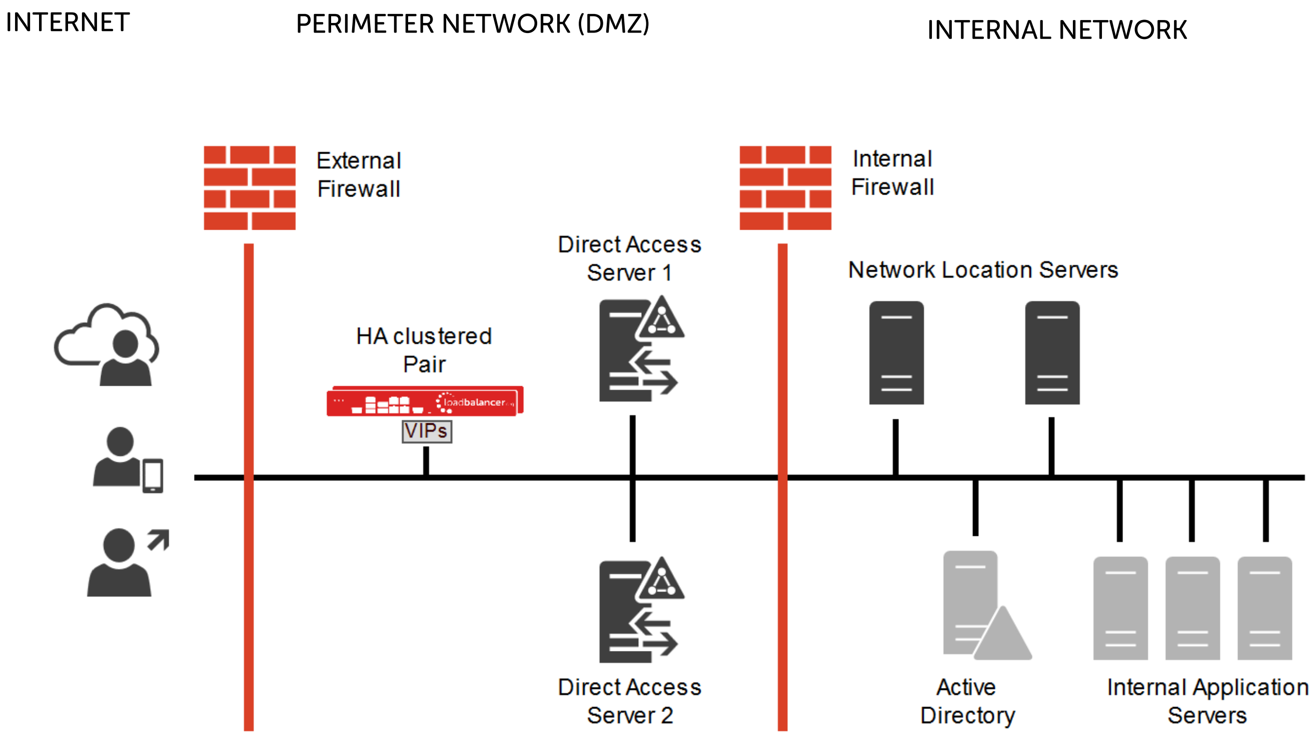
> Note: It's highly recommended that you have a working DirectAccess environment first before implementing the load balancer.

Basic Concepts

To provide resilience and high availability for your DirectAccess infrastructure, multiple DirectAccess servers should be deployed with a load balancer. This helps ensure that users can always connect to the corporate network by constantly checking the health of the DirectAccess servers and only forwarding connections to functional servers.

Load Balancer Deployment

The following diagram shows a typical load balanced DirectAccess deployment.



Notes:

- Load balancers can be deployed as single units or as a clustered pair. Loadbalancer.org recommends deploying a clustered pair for HA and resilience

Load Balancer Deployment Mode

Layer 7 SNAT mode (HAProxy) is recommended for DirectAccess and is used for the configuration presented in this guide. This mode offers good performance and is simple to configure since it requires no configuration changes to the DirectAccess servers.

Layer 4 DR mode, NAT mode and SNAT mode can also be used if preferred. For DR mode you'll need to solve the ARP problem on each DirectAccess server (please see the Administration Manual and search for "DR mode considerations"), for NAT mode the default gateway of the DirectAccess servers must be the load balancer.

Load Balanced Ports & Services

For IP-HTTPS, the following ports/protocols must be load balanced:

Port	Protocol	User
443	TCP/IP-HTTPS	All DirectAccess client to server communication

Persistence (Server Affinity)

Source IP address persistence is used for the DirectAccess servers. This ensures that a particular client will connect to the same DirectAccess server for the duration of the session.

Server Health Checking

To constantly check and verify the health of the DirectAccess servers, the load balancer is configured to perform an HTTPS negotiate check. This check verifies that each server responds with 200 OK.

The heath check for the Network Location Servers and Connectivity Verifier (web probe) servers uses a TCP port connect to verify server health.

Load Balanced DNS Requirements

Internal

The following resources must be resolvable internally:

- The load balanced network location servers, e.g. **directaccess-nls.robstest.com**
- The load balanced web probe server, e.g. **directaccess-webprobehost.robstest.com**

External

The following resources must be resolvable externally:

- The load balanced DirectAccess servers, e.g. **directaccess.robstest.com**
- The load balanced connectivity web probe server, e.g. **directaccess-webprobehost.robstest.com**

> Note: The Network Location Server should NOT be resolvable/reachable from outside the corporate network as mentioned on page 6.

SSL Offloading

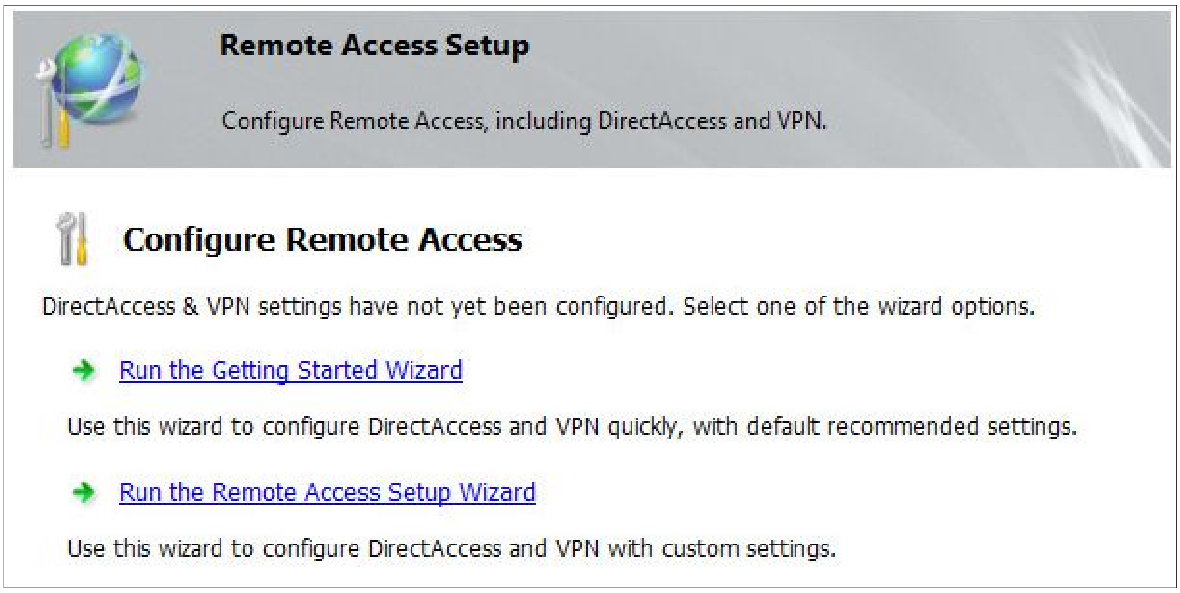
As already mentioned, when IP-HTTPS is used double encryption occurs (IPsec & SSL/TLS). This is mitigated with Win8/Win2012 by using a NULL cipher which solves the performance issue. Windows 7 clients are unable to use the NULL cipher so the double encryption performance issue remains.

It's not possible to enable SSL offload on the load balancer in this case because the load balancer would need to emulate Windows 8 DirectAccess client behavior which is not currently possible.

7. DirectAccess Configuration for Load Balancing

Introduction

DirectAccess is part of the Remote Access role. Once installed, there are 2 wizard options to configure the system:



Remote Access Setup

Configure Remote Access, including DirectAccess and VPN.

Configure Remote Access

DirectAccess & VPN settings have not yet been configured. Select one of the wizard options.

Run the Getting Started Wizard

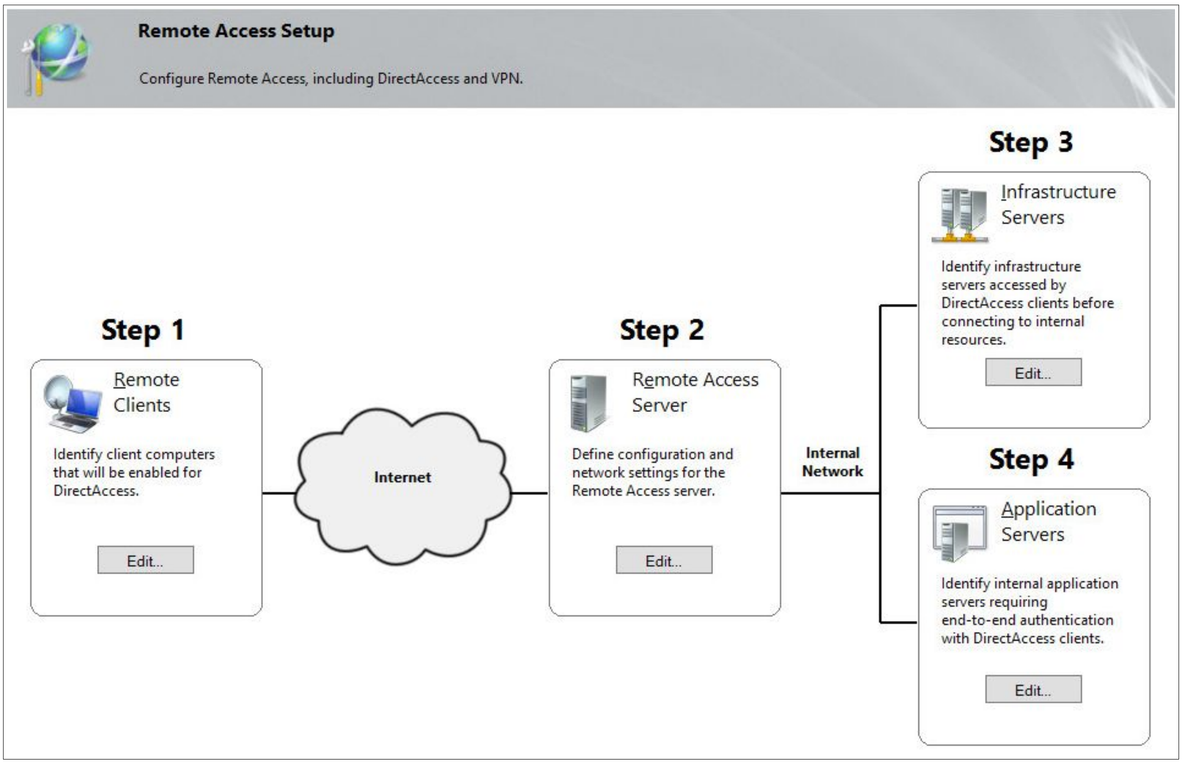
Use this wizard to configure DirectAccess and VPN quickly, with default recommended settings.

Run the Remote Access Setup Wizard

Use this wizard to configure DirectAccess and VPN with custom settings.

The first option (*Getting Started Wizard*) is the simplest as it configures most settings automatically although some of the defaults used are not necessarily desirable – e.g. the DirectAccess servers are set as the Network Location Servers which is not recommended by Microsoft.

The second option (*Remote Access Setup Wizard*) requires each part of the system to be configured manually. Whichever option is used, the resulting configuration can easily be changed using the Remote Access Setup console to edit the configuration.



Remote Access Setup

Configure Remote Access, including DirectAccess and VPN.

Step 1

Remote Clients

Identify client computers that will be enabled for DirectAccess.

Step 2

Remote Access Server

Define configuration and network settings for the Remote Access server.

Step 3

Infrastructure Servers

Identify infrastructure servers accessed by DirectAccess clients before connecting to internal resources.

Step 4

Application Servers

Identify internal application servers requiring end-to-end authentication with DirectAccess clients.

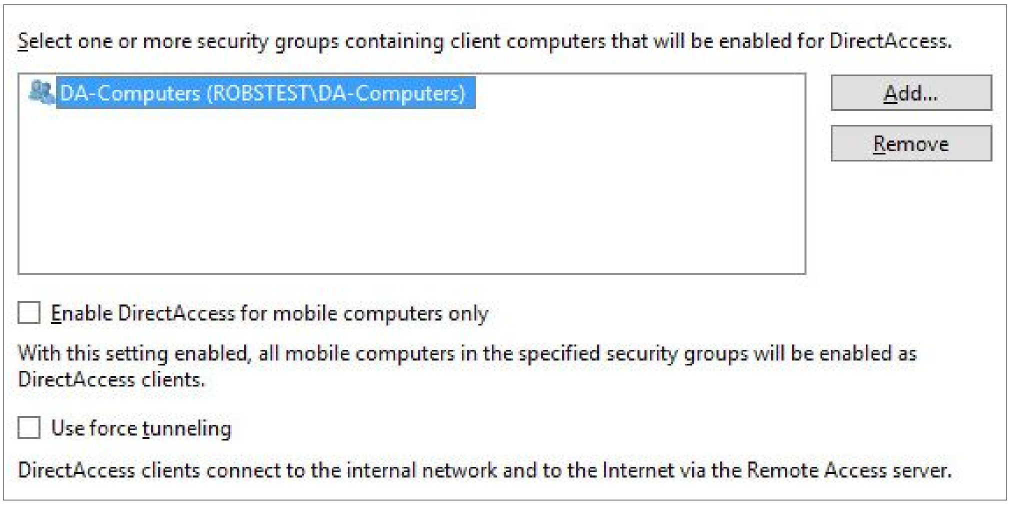
Install & Configure the first DirectAccess & NLS Server

This section lists the key configuration steps that were performed in relation to the test environment used in this guide.

- Using the internal CA, create SSL certs for **directaccess.robstest.com** and **directaccess-nls.robstest.com** and place these in the Personal Certificate Store on the DirectAccess server/Network Location Server (NLS)
- Install IIS on the NLS and ensure that the HTTPS binding is configured to use the **directaccess-nls.robstest.com** certificate
- Add an internal DNS record for **directaccess-nls.robstest.com**
- Install DirectAccess on the first server
- Now run the *Remote Access Setup Wizard*

Remote Access Setup Step 1 – Remote Clients

- Create/select the computer group that will use DirectAccess:



Select one or more security groups containing client computers that will be enabled for DirectAccess.

DA-Computers (ROBSTEST\DA-Computers)

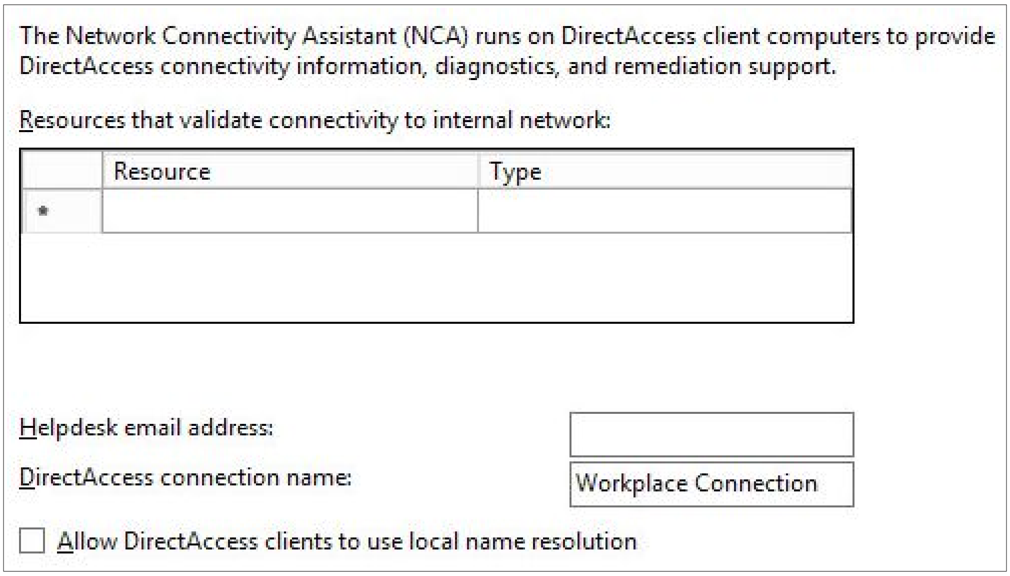
□ Enable DirectAccess for mobile computers only

With this setting enabled, all mobile computers in the specified security groups will be enabled as DirectAccess clients.

□ Use force tunneling

DirectAccess clients connect to the internal network and to the Internet via the Remote Access server.

- The Network Connectivity Assistant settings were left blank as these are auto-populated by the wizard:



The Network Connectivity Assistant (NCA) runs on DirectAccess client computers to provide DirectAccess connectivity information, diagnostics, and remediation support.

Resources that validate connectivity to internal network:

	Resource	Type
*		

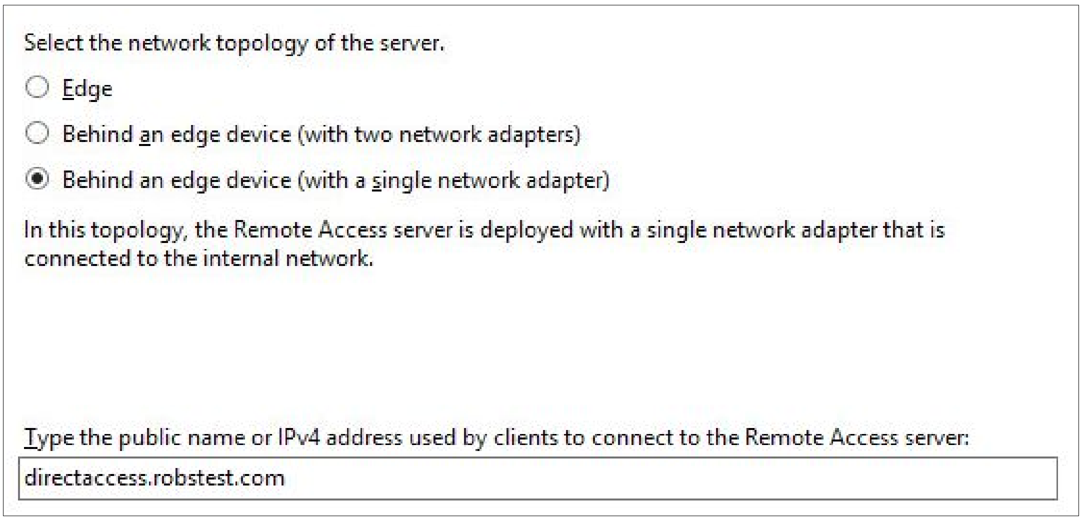
Helpdesk email address:

DirectAccess connection name: Workplace Connection

□ Allow DirectAccess clients to use local name resolution

Remote Access Setup Step 2 – Remote Access Server

- For the RAS server network topology, select *Behind an edge device:*
- Enter the FQDN for DirectAccess:



Select the network topology of the server.

○ Edge

○ Behind an edge device (with two network adapters)

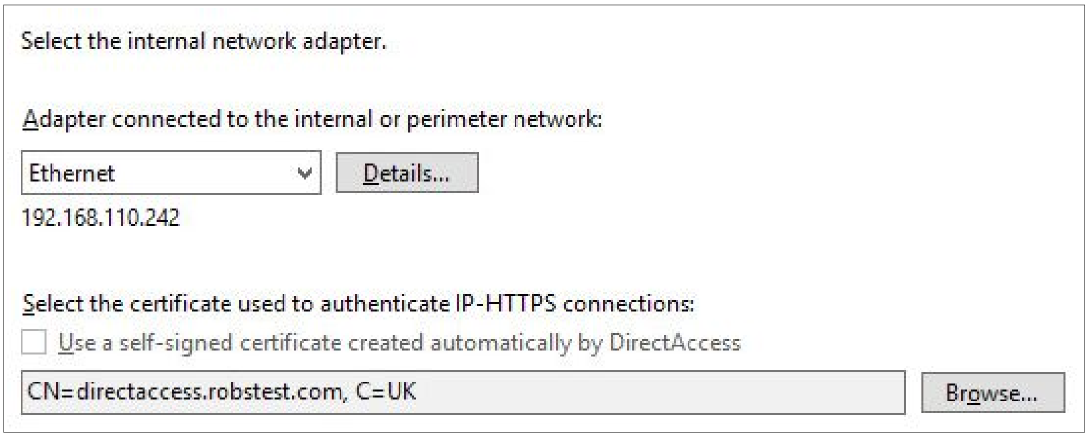
● Behind an edge device (with a single network adapter)

In this topology, the Remote Access server is deployed with a single network adapter that is connected to the internal network.

Type the public name or IPv4 address used by clients to connect to the Remote Access server:

directaccess.robstest.com

- Browse to and select the certificate created earlier:



Select the internal network adapter.

Adapter connected to the internal or perimeter network:

Ethernet

192.168.110.242

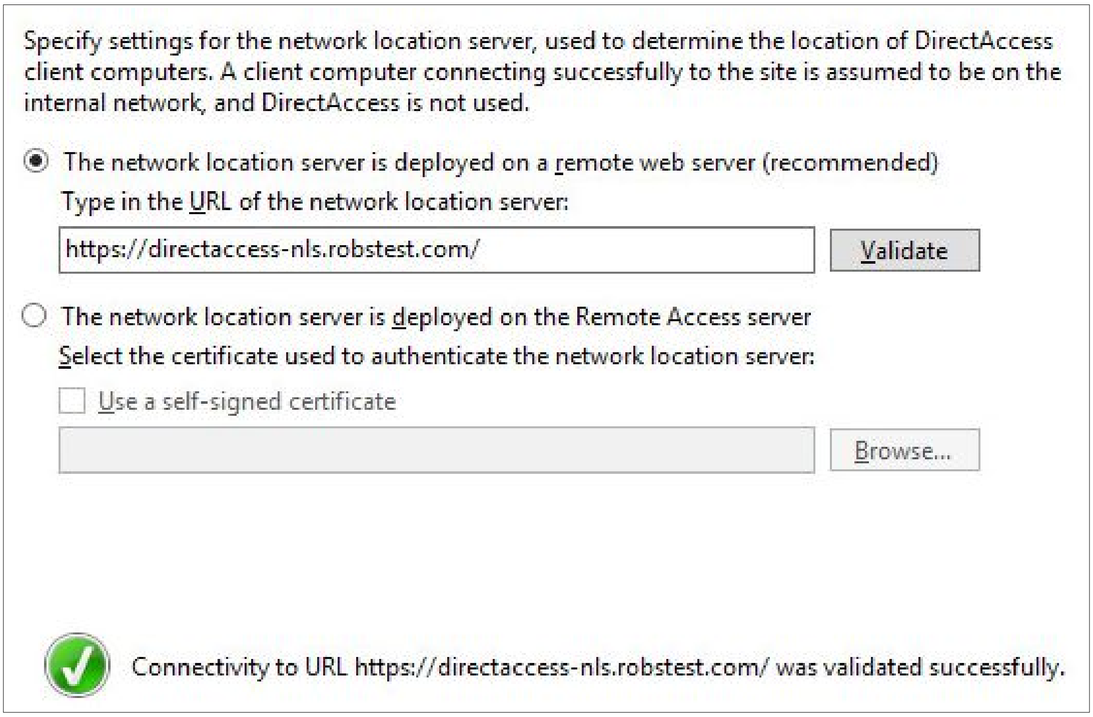
Select the certificate used to authenticate IP-HTTPS connections:

□ Use a self-signed certificate created automatically by DirectAccess

CN=directaccess.robstest.com, C=UK

Remote Access Setup Step 3 – Infrastructure Server Setup

- Specify & validate the Network Location Server:



Specify settings for the network location server, used to determine the location of DirectAccess client computers. A client computer connecting successfully to the site is assumed to be on the internal network, and DirectAccess is not used.

● The network location server is deployed on a remote web server (recommended)

Type in the URL of the network location server:

https://directaccess-nls.robstest.com/

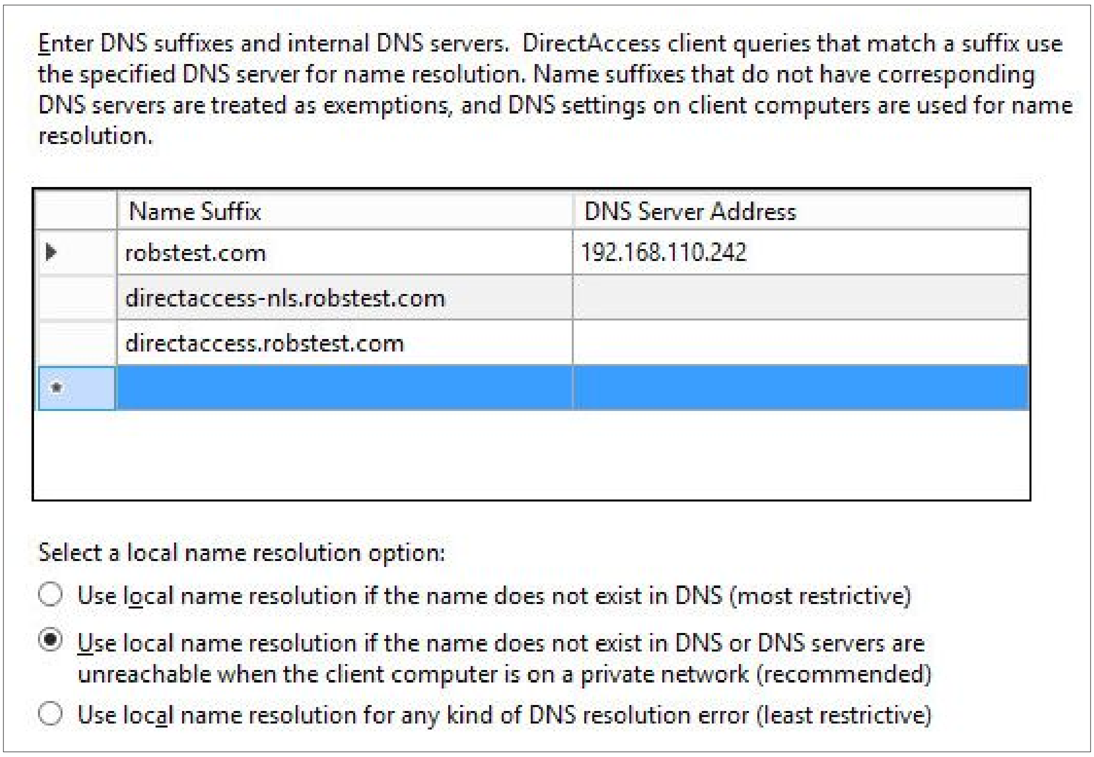
○ The network location server is deployed on the Remote Access server

Select the certificate used to authenticate the network location server:

□ Use a self-signed certificate

Connectivity to URL https://directaccess-nls.robstest.com/ was validated successfully.

- Configure DNS suffixes and servers. The direct access and location servers were both entered as exceptions, i.e. no DNS server address is specified, this causes these names to be resolved using locally defined DNS servers rather than forwarding them to internal DNS servers:



Enter DNS suffixes and internal DNS servers. DirectAccess client queries that match a suffix use the specified DNS server for name resolution. Name suffixes that do not have corresponding DNS servers are treated as exemptions, and DNS settings on client computers are used for name resolution.

Name Suffix	DNS Server Address
robstest.com	192.168.110.242
directaccess-nls.robstest.com	
directaccess.robstest.com	

Select a local name resolution option:

○ Use local name resolution if the name does not exist in DNS (most restrictive)

● Use local name resolution if the name does not exist in DNS or DNS servers are unreachable when the client computer is on a private network (recommended)

○ Use local name resolution for any kind of DNS resolution error (least restrictive)

- Once the wizard is complete, verify that DNS records for the Connectivity Verifiers have been auto-created. These are:

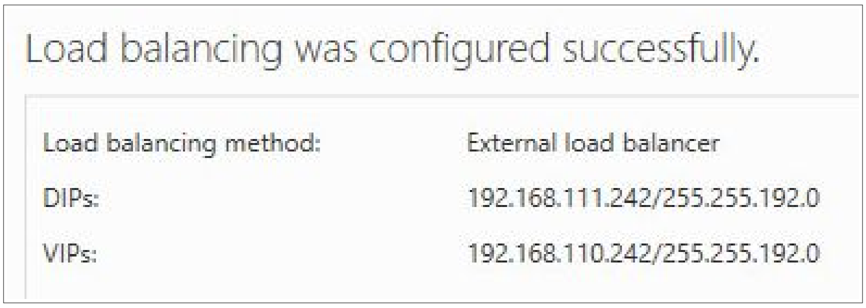
directaccess-copconnectivityhost.robstest.com

and

directaccess-webprobehost.robstest.com

Add Additional DirectAccess Servers & Configure Load Balancing

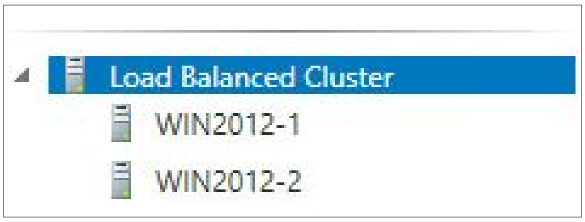
- Install DirectAccess on the second server but don't run the configuration wizard
- Export the SSL certs (and private key) used for **directaccess.robstest.com** and **directaccess-nls.robstest.com** from the existing servers, then import into the Personal Certificate Store on the additional DirectAccess server(s)/NL server(s)
- On the additional NL server(s), install IIS and ensure that the HTTPS binding is configured to use the **directaccess-nls.robstest.com** certificate
- On the first DirectAccess server, enable load balancing, define a new IP address to be used for the interface (the existing IP will be used as the VIP address on the load balancer as explained during configuration)
- Confirm the configuration:



Load balancing was configured successfully.

Load balancing method:	External load balancer
DIPs:	192.168.111.242/255.255.192.0
VIPs:	192.168.110.242/255.255.192.0

- Now add the second DirectAccess server. Once configured, both are listed as part of the load balanced cluster:



Client Configuration

Client configuration settings are deployed via Group Policy. The auto-created GPO is called *DirectAccess Client Settings*. To force a test client to immediately apply these settings, run the following command:

```
gpupdate /force
```

8. Loadbalancer.org Appliance – the Basics

Virtual Appliance Download & Deployment

A fully featured, fully supported 30 day trial is available if you are conducting a PoC (Proof of Concept) deployment. The VA is currently available for VMware, Virtual Box, Hyper-V, KVM and XEN and has been optimized for each Hypervisor. By default, the VA is allocated 1 CPU, 2GB of RAM and has an 8GB virtual disk. The Virtual Appliance can be downloaded here.

> Note: The same download is used for the licensed product, the only difference is that a license key file (supplied by our sales team when the product is purchased) must be applied using the appliance's WebUI.

> Note: Please refer to the Administration Manual and the ReadMe.txt text file included in the VA download for more detailed information on deploying the VA using various Hypervisors.

Initial Network Configuration

The IP address, subnet mask & other network settings are configured using the Network Setup Wizard at the console. After boot up, follow the instructions on the console to start the Wizard.

Accessing the Web User Interface (WebUI)

1. Browse to the following URL: **https://<chosen-IP-address>:9443/lbadmin/**

   ** Note the port number → **9443***

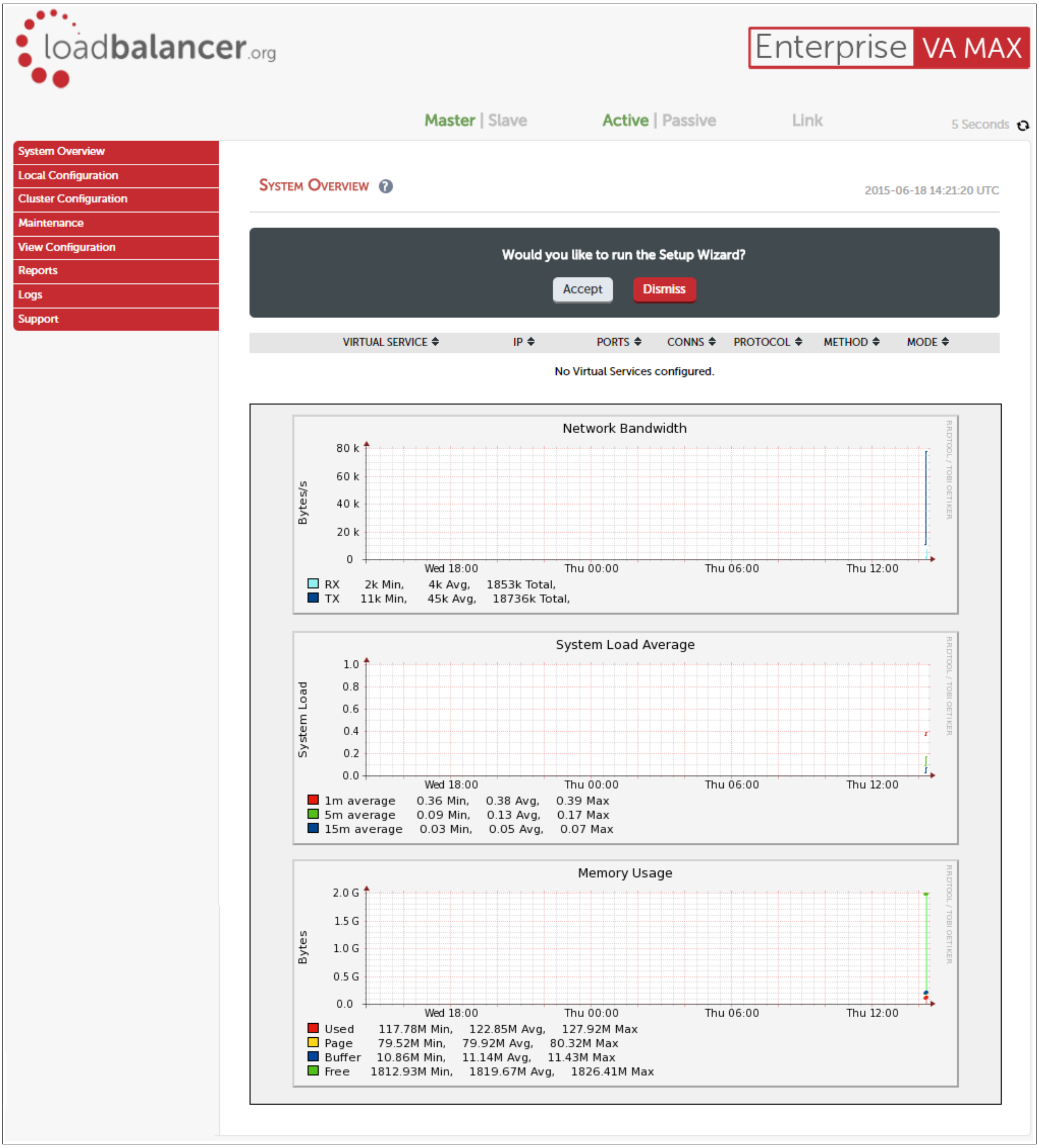
2. Login to the WebUI:

   Username: loadbalancer

   Password: <configured-during-network-setup-wizard>

> Note: To change the password , use the WebUI menu option: *Maintenance > Passwords.*

Once logged in, the WebUI will be displayed as shown below:



SYSTEM OVERVIEW

2015-06-18 14:21:20 UTC

Would you like to run the Setup Wizard?

VIRTUAL SERVICE	IP	PORTS	CONNS	PROTOCOL	METHOD	MODE

No Virtual Services configured.

```
RX      2k Min,    4k Avg,   1853k Total,
TX     11k Min,   45k Avg,  18736k Total,
```

```
1m average    0.36 Min,   0.38 Avg,   0.39 Max
5m average    0.09 Min,   0.13 Avg,   0.17 Max
15m average   0.03 Min,   0.05 Avg,   0.07 Max
```

```
Used     117.78M Min,   122.85M Avg,   127.92M Max
Page      79.52M Min,    79.92M Avg,    80.32M Max
Buffer    10.86M Min,    11.14M Avg,    11.43M Max
Free    1812.93M Min,  1819.67M Avg,  1826.41M Max
```

HA Clustered Pair Configuration

Loadbalancer.org recommend that load balancer appliances are deployed in pairs for high availability. In this guide a single unit is deployed first, adding a secondary slave unit is covered in section 1 of the Appendix on page 26.

9. Appliance Configuration for DirectAccess

Configuring load balancing for DirectAccess is done in 4 steps:

A) Configuring load balancing for DirectAccess Servers

B) Configuring load balancing for Network Location Servers

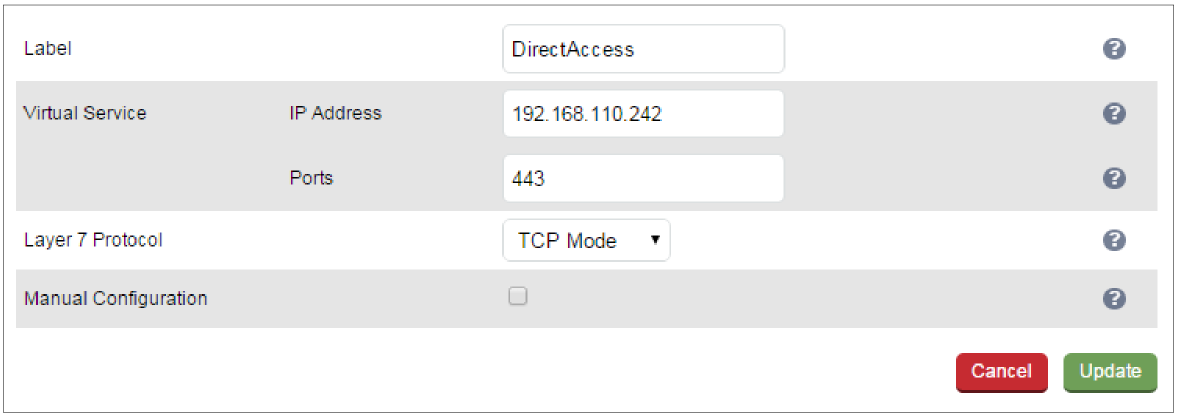
C) Configuring load balancing for Connectivity Verifier (Web Probe) Servers

D) Finalizing Appliance settings

A – Configuring for DirectAccess Servers

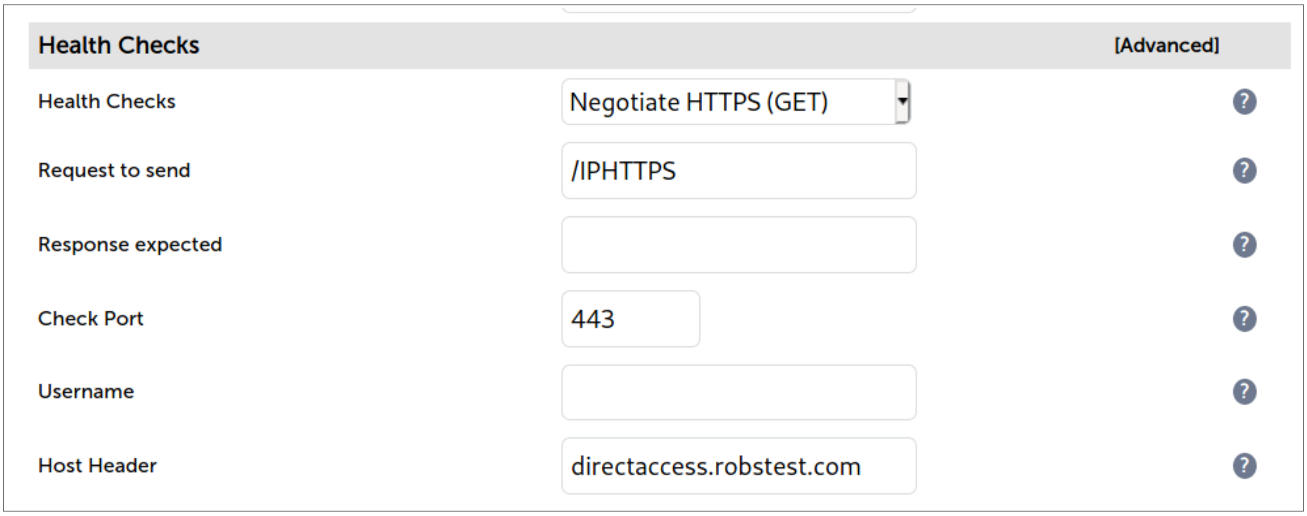
Setting up the Virtual Service (VIP)

1. Using the WebUI, navigate to: *Cluster Configuration > Layer 7 – Virtual Services* and click **Add a New Virtual Service**
2. Enter the following details:



Label		DirectAccess	?
Virtual Service	IP Address	192.168.110.242	?
	Ports	443	?
Layer 7 Protocol		TCP Mode ▾	?
Manual Configuration		□	?

3. Enter an appropriate name (Label) for the Virtual Service, e.g. **DirectAccess**
4. Set the *Virtual Service IP address* field to the required IP address, e.g. **192.168.110.242**
5. Set the *Virtual Service Ports* field to **443**
6. Set the *Layer 7 Protocol* to **TCP Mode**
7. Click **Update**
8. Now click **Modify** next to the newly created Virtual Service
9. Ensure *Persistence Mode* is set to **Source IP**
10. Under *Health Checks*, click **Advanced** to show more options
11. Change *Health Checks* to **Negotiate HTTPS (GET)** as shown below



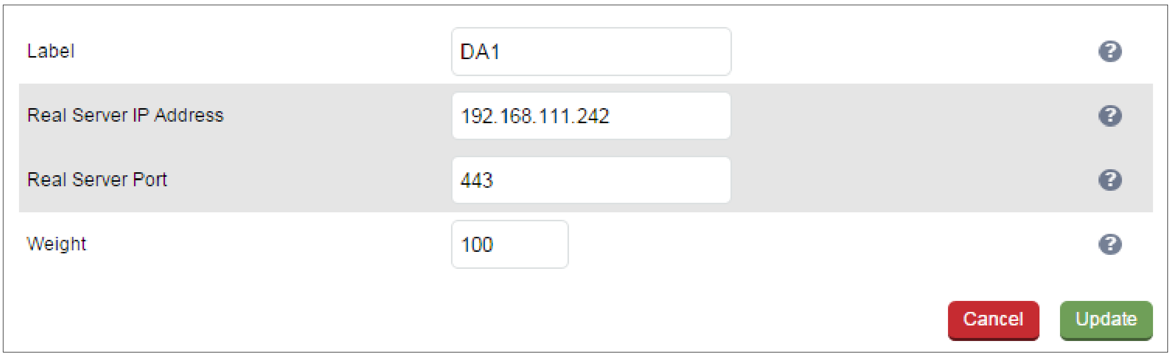
Health Checks [Advanced]

Health Checks	Negotiate HTTPS (GET)
Request to send	/IPHTTPS
Response expected	
Check Port	443
Username	
Host Header	directaccess.robstest.com

12. Set *Check Port* to **443**
13. Set *Request to Send* to **/IPHTTPS**
14. leave *Response Expected* blank
15. Set *Host Header* as appropriate for your environment, e.g. **directaccess.robstest.com**
16. Click **Update**

Setting up the Real Servers (RIPs)

1. Using the WebUI, navigate to: *Cluster Configuration > Layer 7 – Real Servers* and click **Add a new Real Server** next to the newly created Virtual Service
2. Enter the following details:



Label	DA1
Real Server IP Address	192.168.111.242
Real Server Port	443
Weight	100

3. Enter an appropriate name (Label) for the first DirectAccess server, e.g. **DA1**
4. Change the *Real Server IP Address* field to the required IP address, e.g. **192.168.111.242**
5. Set the *Real Server Port* field to **443**
6. Click **Update**
7. Now repeat for your remaining DirectAccess server(s)

DNS Configuration

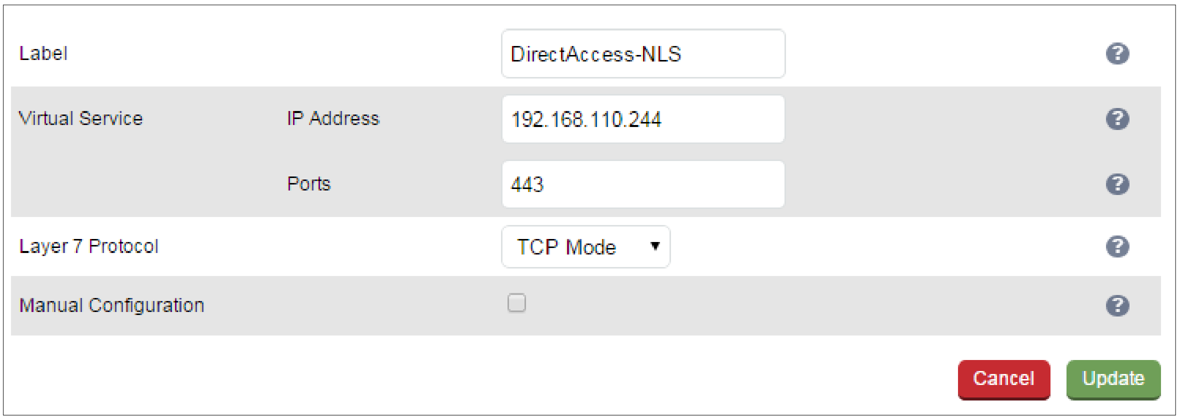
1. Ensure that the external DNS record points at the correct external IP and that the firewall NAT's this to the load balanced VIP address.

   e.g. **directaccess.robstest.com → External IP on NAT firewall → DirectAccess VIP (192.168.110.242)**

B - Configuring for Network Location Servers

Setting up the Virtual Service (VIP)

1. Using the WebUI, navigate to: *Cluster Configuration > Layer 7 – Virtual Services* and click **Add a New Virtual Service**
2. Enter the following details:

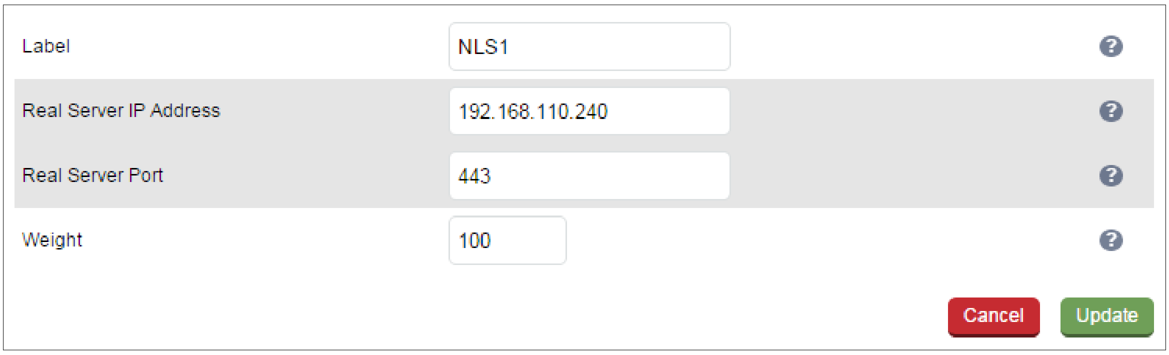


Label		DirectAccess-NLS
Virtual Service	IP Address	192.168.110.244
	Ports	443
Layer 7 Protocol		TCP Mode
Manual Configuration		□

3. Enter an appropriate name (Label) for the Virtual Service, e.g. **DirectAccess-NLS**
4. Set the *Virtual Service IP address* field to the required IP address, e.g. **192.168.110.244**
5. Set the *Virtual Service Ports* field to **443**
6. Set the *Layer 7 Protocol* to **TCP Mode**
7. Click **Update**
8. Now click **Modify** next to the newly created Virtual Service
9. Change *Persistence Mode* to **None**
10. Ensure *Health Checks* is set to **Connect to Port**
11. Click **Update**

Setting up the Real Servers (RIPs)

1. Using the WebUI, navigate to: *Cluster Configuration > Layer 7 – Real Servers* and click **Add a new Real Server** next to the newly created Virtual Service
2. Enter the following details:



Label	NLS1
Real Server IP Address	192.168.110.240
Real Server Port	443
Weight	100

3. Enter an appropriate name (Label) for the first NLS server, e.g. **NLS1**
4. Change the *Real Server IP Address* field to the required IP address, e.g. **192.168.110.240**
5. Set the *Real Server Port* field to **443**
6. Click **Update**
7. Now repeat for your remaining NLS server(s)

DNS Configuration

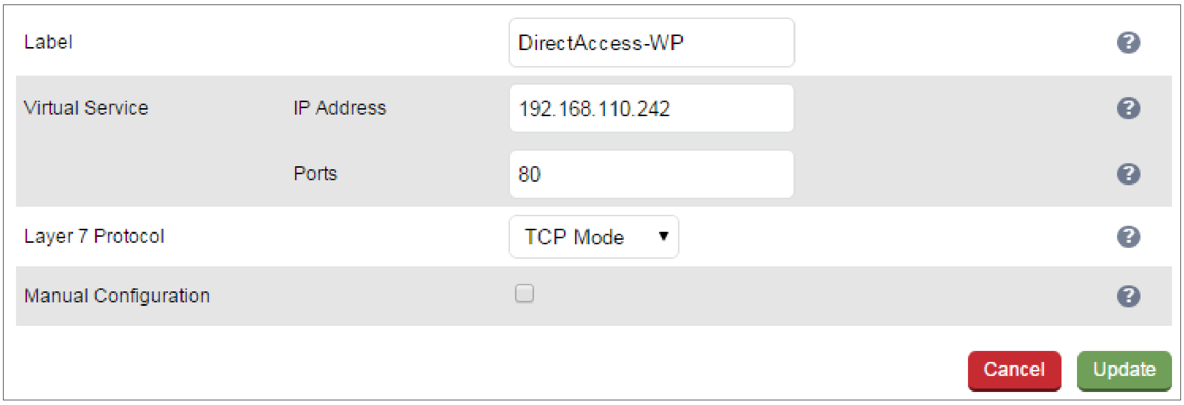
1. Modify the internal DNS entry for the Network Location Server so it points at the load balanced VIP address rather than the IP address of the first NL server.

   i.e. **directaccess-nls.robstest.com → 192.168.110.244**

C - Configuring for Connectivity Verifier (Web Probe) Servers

Setting up the Virtual Service (VIP)

1. Using the WebUI, navigate to: *Cluster Configuration > Layer 7 – Virtual Services* and click **Add a New Virtual Service**
2. Enter the following details:



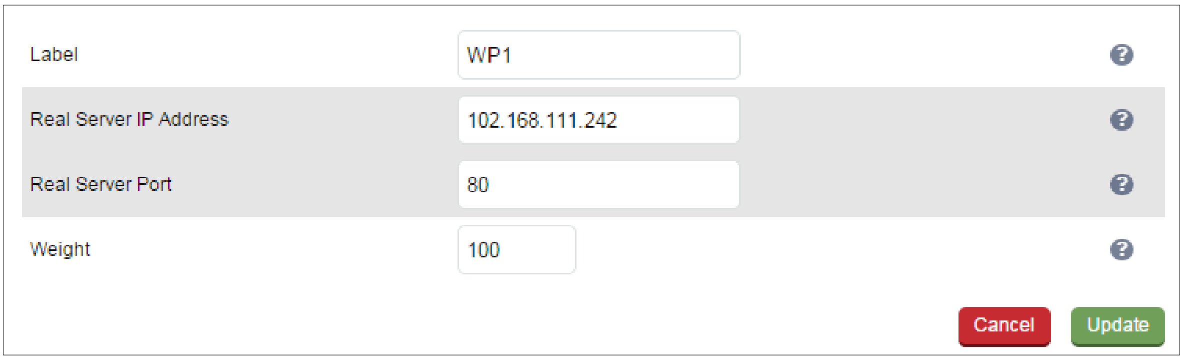
Label		DirectAccess-WP
Virtual Service	IP Address	192.168.110.242
	Ports	80
Layer 7 Protocol		TCP Mode ▾
Manual Configuration		□

3. Enter an appropriate name (Label) for the Virtual Service, e.g. **DirectAccess-WP**
4. Set the *Virtual Service IP address* field to the required IP address, e.g. **192.168.110.242**

5. Set the *Virtual Service Ports* field to **80**
6. Set the *Layer 7 Protocol* to **TCP Mode**
7. Click **Update**
8. Now click **Modify** next to the newly created Virtual Service
9. Change *Persistence Mode* to **None**
10. Ensure *Health Checks* is to **Connect to Port**
11. Click **Update**

Setting up the Real Servers (RIPs)

1. Using the WebUI, navigate to: *Cluster Configuration > Layer 7 – Real Servers* and click **Add a new Real Server** next to the newly created Virtual Service
2. Enter the following details:



Label	WP1
Real Server IP Address	102.168.111.242
Real Server Port	80
Weight	100

3. Enter an appropriate name (Label) for the first Web Probe server, e.g. **WP1**
4. Change the *Real Server IP Address* field to the required IP address, e.g. **192.168.111.242**
5. Set the *Real Server Port* field to **80**
6. Click **Update**
7. Now repeat for your remaining Web Probe server(s)

DNS Configuration

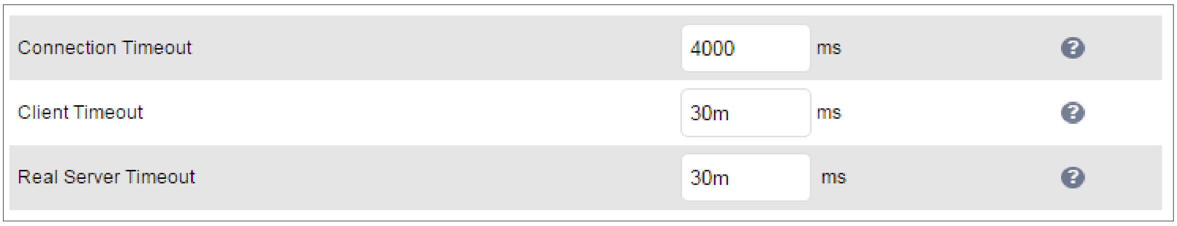
1. The internal DNS entry for the load balanced Connectivity Verifier (web probe) Servers should already exist and refer to the VIP address.

   i.e. **directaccess-webprobehost.robstest.com → 192.168.110.242**

D – Finalizing Appliance Settings

Configure Layer 7 Timeouts

1. Using the WebUI, navigate to: *Cluster Configuration > Layer 7 – Advanced Configuration*



Connection Timeout	4000	ms	?
Client Timeout	30m	ms	?
Real Server Timeout	30m	ms	?

2. Change *Client Timeout* to **30m** as shown above (i.e. 30 minutes)
3. Change *Real Server Timeout* to **30m** as shown above (i.e. 30 minutes)
4. Click the **Update** button to save the settings

Restart HAProxy

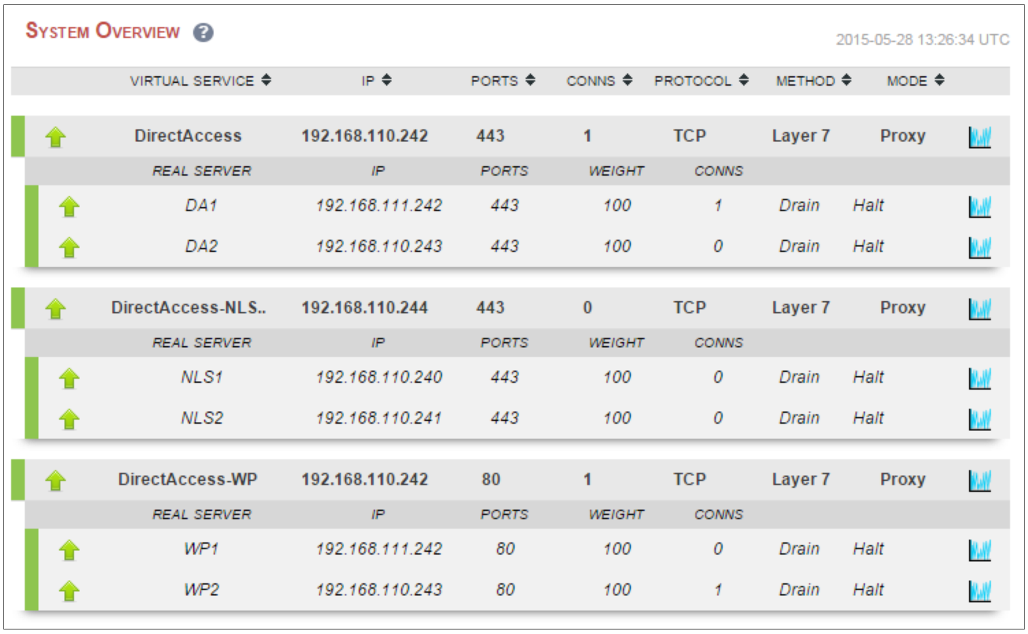
1. To apply the new settings restart HAProxy using the WebUI option: *Maintenance > Restart Services* and clicking **Restart HAProxy**

10. Testing & Verification

> Note: Make sure that the firewall on the clients and servers is enabled. This is a requirement for DirectAccess to work successfully.

Using The System Overview

Verify that all VIPs & associated RIPs are reported as up (green) as shown below:

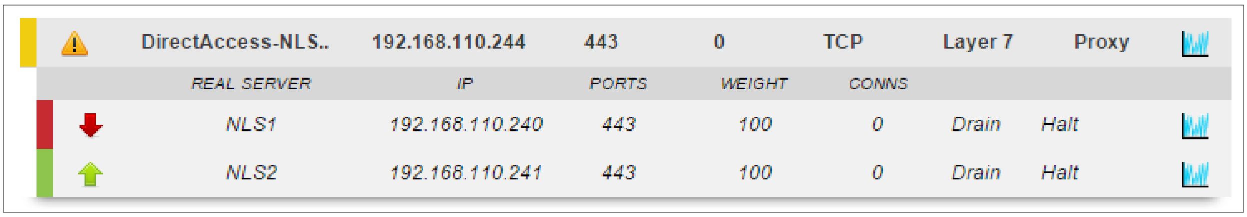


SYSTEM OVERVIEW

2015-05-28 13:26:34 UTC

	VIRTUAL SERVICE	IP	PORTS	CONNS	PROTOCOL	METHOD	MODE
⬆	DirectAccess	192.168.110.242	443	1	TCP	Layer 7	Proxy
	REAL SERVER	IP	PORTS	WEIGHT	CONNS		
⬆	DA1	192.168.111.242	443	100	1	Drain	Halt
⬆	DA2	192.168.110.243	443	100	0	Drain	Halt
⬆	DirectAccess-NLS..	192.168.110.244	443	0	TCP	Layer 7	Proxy
	REAL SERVER	IP	PORTS	WEIGHT	CONNS		
⬆	NLS1	192.168.110.240	443	100	0	Drain	Halt
⬆	NLS2	192.168.110.241	443	100	0	Drain	Halt
⬆	DirectAccess-WP	192.168.110.242	80	1	TCP	Layer 7	Proxy
	REAL SERVER	IP	PORTS	WEIGHT	CONNS		
⬆	WP1	192.168.111.242	80	100	0	Drain	Halt
⬆	WP2	192.168.110.243	80	100	1	Drain	Halt

If certain servers are down, i.e. failing their health check, they will be highlighted red as shown below:

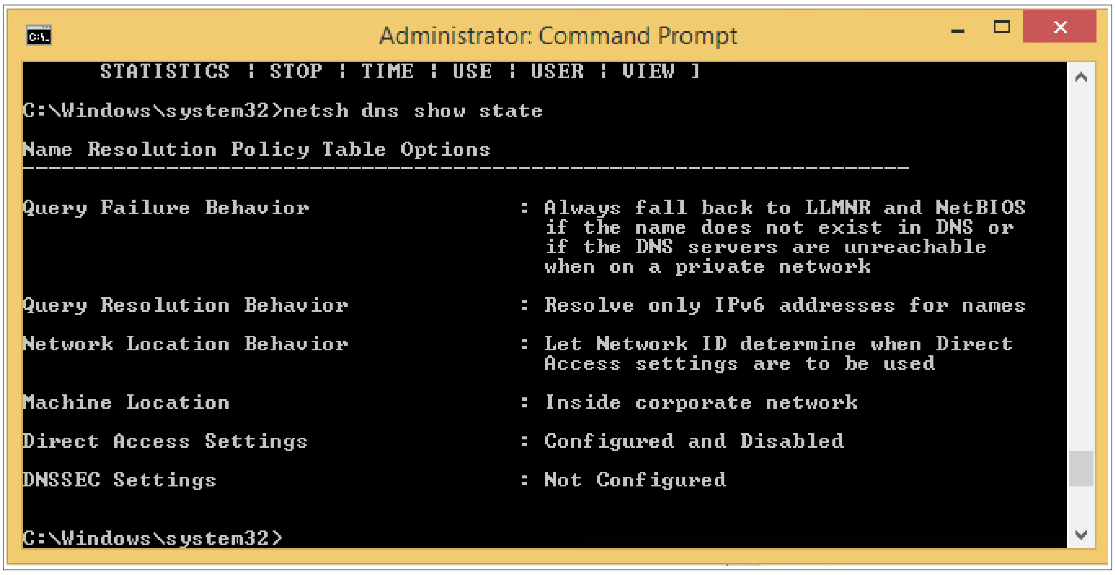


	DirectAccess-NLS..	192.168.110.244	443	0	TCP	Layer 7	Proxy
	REAL SERVER	IP	PORTS	WEIGHT	CONNS		
⬇	NLS1	192.168.110.240	443	100	0	Drain	Halt
⬆	NLS2	192.168.110.241	443	100	0	Drain	Halt

Verify Client Location

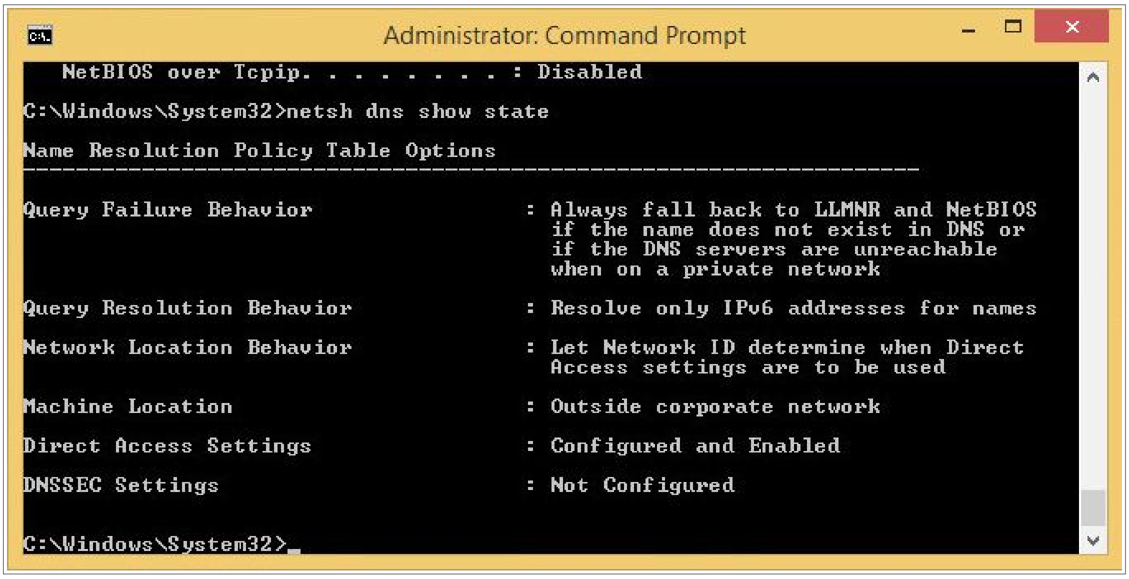
Using **netsh dns show state**

When inside the corporate network it should show:



```
      STATISTICS ¦ STOP ¦ TIME ¦ USE ¦ USER ¦ VIEW ]

C:\Windows\system32>netsh dns show state

Name Resolution Policy Table Options
--------------------------------------------------------------------

Query Failure Behavior                 : Always fall back to LLMNR and NetBIOS
                                         if the name does not exist in DNS or
                                         if the DNS servers are unreachable
                                         when on a private network

Query Resolution Behavior              : Resolve only IPv6 addresses for names

Network Location Behavior              : Let Network ID determine when Direct
                                         Access settings are to be used

Machine Location                       : Inside corporate network

Direct Access Settings                 : Configured and Disabled

DNSSEC Settings                        : Not Configured


C:\Windows\system32>
```

When outside the corporate network it should show:

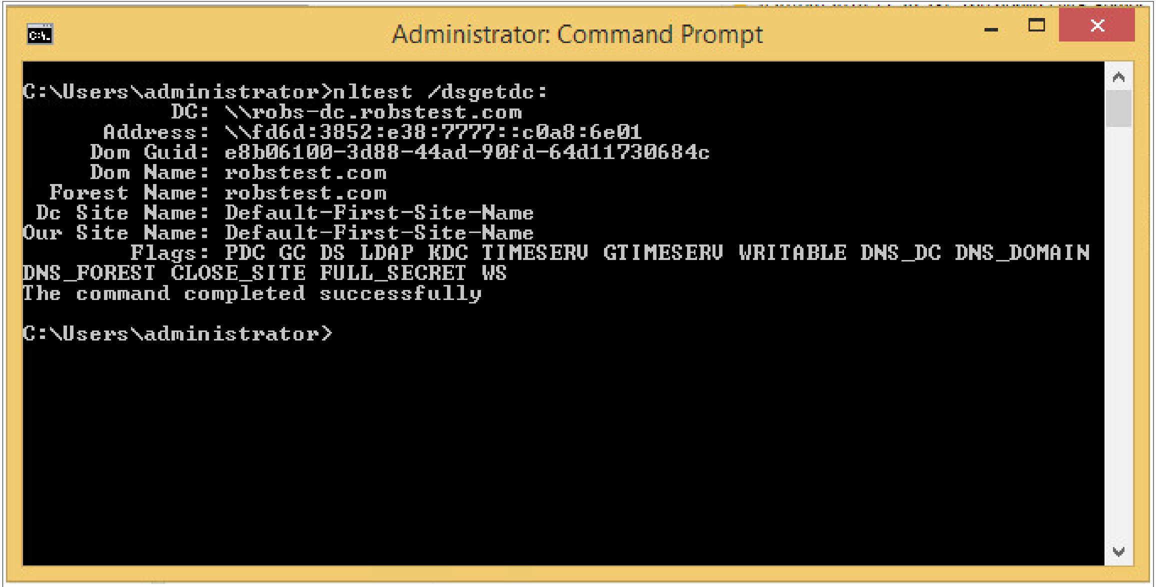


```
   NetBIOS over Tcpip. . . . . . . . : Disabled

C:\Windows\System32>netsh dns show state

Name Resolution Policy Table Options
--------------------------------------------------------------------

Query Failure Behavior                 : Always fall back to LLMNR and NetBIOS
                                         if the name does not exist in DNS or
                                         if the DNS servers are unreachable
                                         when on a private network

Query Resolution Behavior              : Resolve only IPv6 addresses for names

Network Location Behavior              : Let Network ID determine when Direct
                                         Access settings are to be used

Machine Location                       : Outside corporate network

Direct Access Settings                 : Configured and Enabled

DNSSEC Settings                        : Not Configured


C:\Windows\System32>_
```

Verify Domain Connectivity

1) using **nltest /dsgetdc**

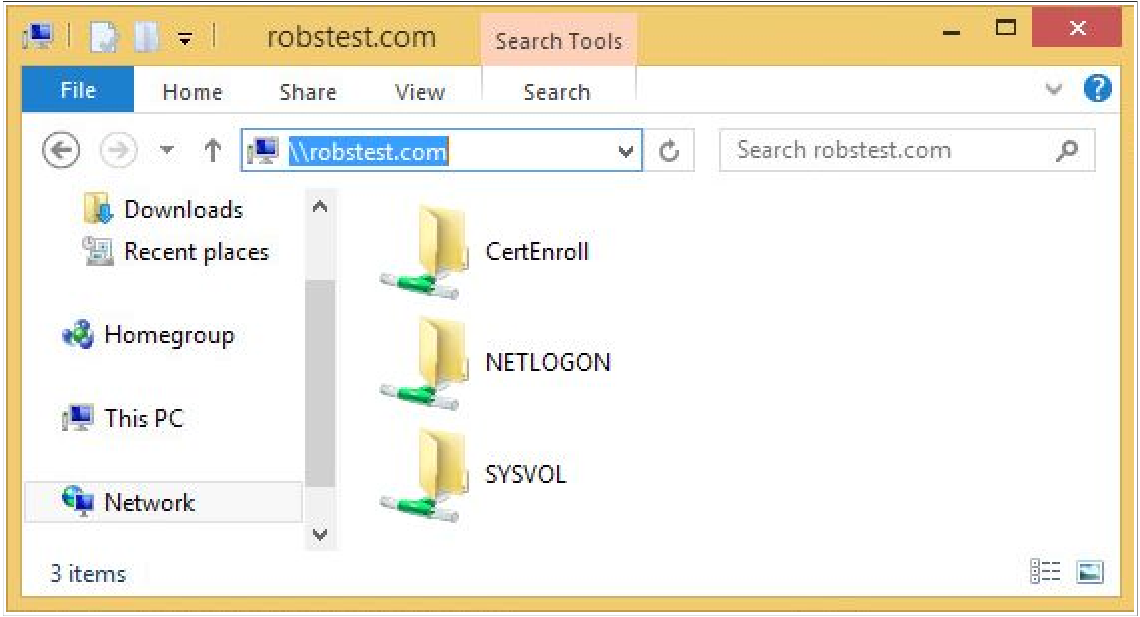
When run internally or externally this command should be able to connect and retrieve domain information:



```
C:\Users\administrator>nltest /dsgetdc:
           DC: \\robs-dc.robstest.com
      Address: \\fd6d:3852:e38:7777::c0a8:6e01
     Dom Guid: e8b06100-3d88-44ad-90fd-64d11730684c
     Dom Name: robstest.com
  Forest Name: robstest.com
 Dc Site Name: Default-First-Site-Name
Our Site Name: Default-First-Site-Name
        Flags: PDC GC DS LDAP KDC TIMESERV GTIMESERV WRITABLE DNS_DC DNS_DOMAIN
DNS_FOREST CLOSE_SITE FULL_SECRET WS
The command completed successfully

C:\Users\administrator>
```

2) browsing to \\domain-name, e.g. \\robstest.com

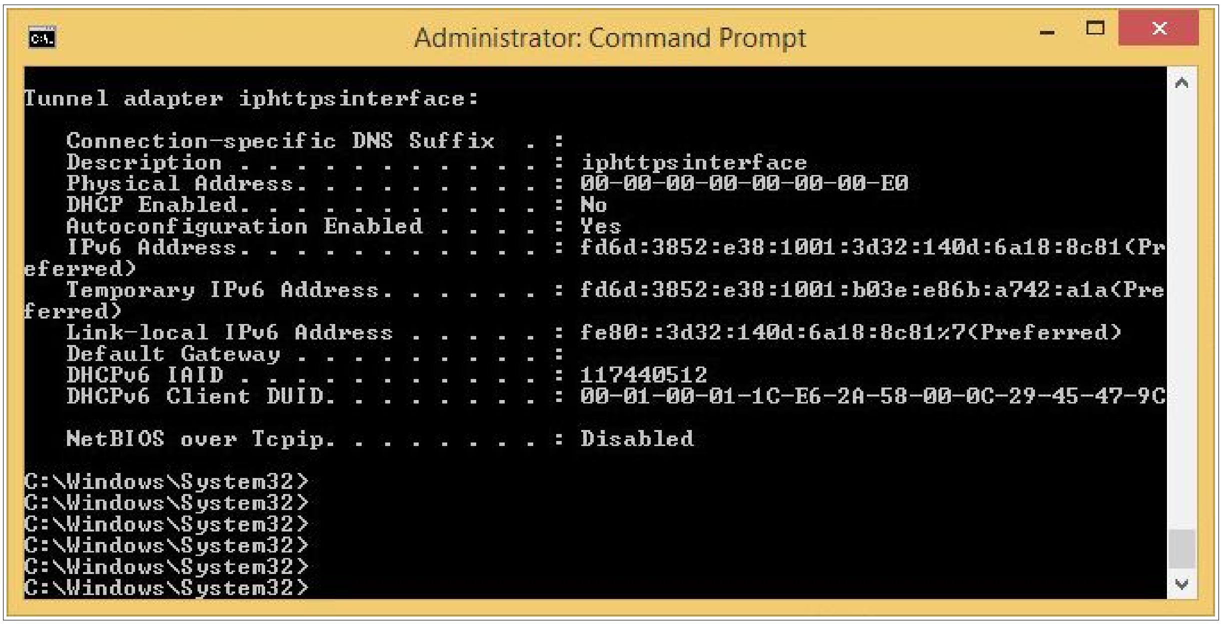
When run internally or externally this should show the list of default shares:



Verify Network Connection

Using **ipconfig /all**

When run externally should show that the IPHTTPS interface is active:



```
Tunnel adapter iphttpsinterface:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : iphttpsinterface
   Physical Address. . . . . . . . . : 00-00-00-00-00-00-00-E0
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   IPv6 Address. . . . . . . . . . . : fd6d:3852:e38:1001:3d32:140d:6a18:8c81(Pr
eferred)
   Temporary IPv6 Address. . . . . . : fd6d:3852:e38:1001:b03e:e86b:a742:a1a(Pre
ferred)
   Link-local IPv6 Address . . . . . : fe80::3d32:140d:6a18:8c81%7(Preferred)
   Default Gateway . . . . . . . . . :
   DHCPv6 IAID . . . . . . . . . . . : 117440512
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-1C-E6-2A-58-00-0C-29-45-47-9C

   NetBIOS over Tcpip. . . . . . . . : Disabled

C:\Windows\System32>
C:\Windows\System32>
C:\Windows\System32>
C:\Windows\System32>
C:\Windows\System32>
C:\Windows\System32>
```

When run internally, it should show that the client is connected using the standard NIC card and that the IPHTTPS interface is no longer active.

DirectAccess Client Troubleshooting Tool

This Microsoft tool is very useful when diagnosing client connection issues. It can be downloaded from the following URL: https://www.microsoft.com/en-us/download/details.aspx?id=41938

11. Technical Support

If you have any questions regarding the appliance or would like assistance designing your deployment, please don't hesitate to contact our support team: support@loadbalancer.org.

12. Further Documentation

The Administration Manual contains much more information about configuring and deploying the appliance. It's available here: http://pdfs.loadbalancer.org/loadbalanceradministrationv8.pdf

13. Conclusion

Loadbalancer.org appliances provide a very cost effective and flexible solution for highly available load balanced DirectAccess Server environments.

14. Appendix

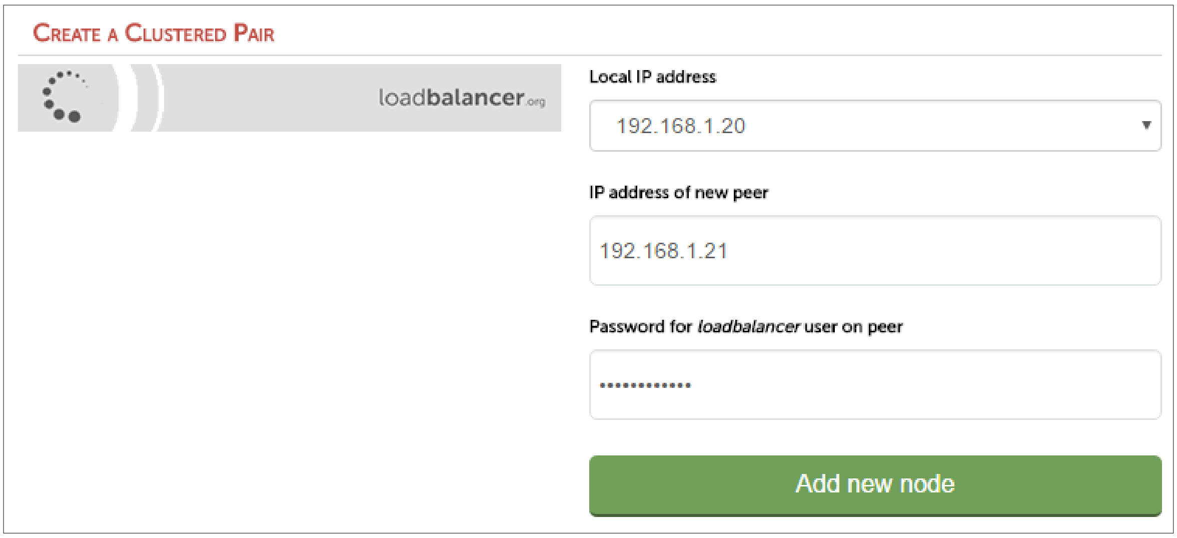
1 - Clustered Pair Configuration – Adding a Slave Unit

If you initially configured just the master unit and now need to add a slave - our recommended procedure, please refer to the relevant section below for more details:

> Note: A number of settings are not replicated as part of the master/slave pairing process and therefore must be manually configured on the slave appliance. These are listed below:
>
> - Hostname & DNS settings
> - Network settings including IP addresses, bonding configuration and VLANs
> - Routing configuration including default gateways and static routes
> - Date & time settings
> - Physical – Advanced Configuration settings including Internet Proxy IP address & port, Firewall table size, SMTP relay and Syslog server
> - SNMP settings
> - Graphing settings
> - Firewall Script & Firewall Lockdown Script settings
> - Software updates

To add a slave node – i.e. create a highly available clustered pair:

- Deploy a second appliance that will be the slave and configure initial network settings
- Using the WebUI, navigate to: *Cluster Configuration > High-Availability Configuration*



CREATE A CLUSTERED PAIR

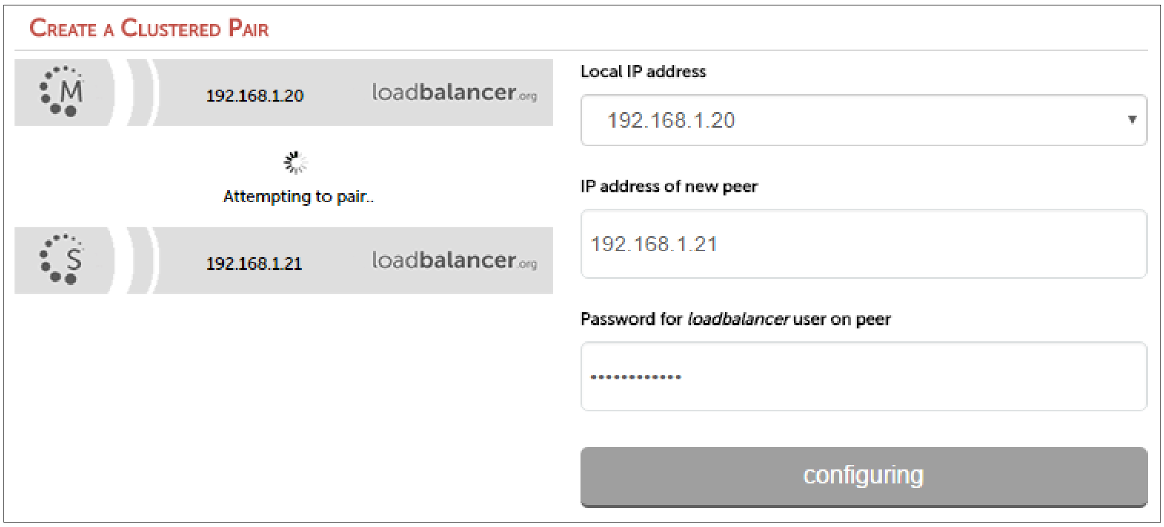
Local IP address: 192.168.1.20

IP address of new peer: 192.168.1.21

Password for *loadbalancer* user on peer: ••••••••••••

- Specify the IP address and the *loadbalancer* users password (the default is 'loadbalancer') for the slave (peer) appliance as shown above

- Click **Add new node**
- The pairing process now commences as shown below:



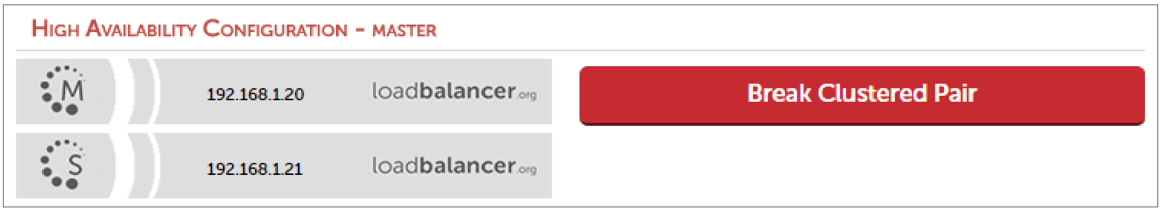
Create a Clustered Pair

Local IP address: 192.168.1.20

IP address of new peer: 192.168.1.21

Password for *loadbalancer* user on peer: ••••••••••••

- Once complete, the following will be displayed:



High Availability Configuration - master

- To finalize the configuration, restart heartbeat and any other services as prompted in the blue message box at the top of the screen

> Note: Clicking the **Restart Heartbeat** button on the master appliance will also automatically restart heartbeat on the slave appliance.

> Note: Please refer to chapter 9 – Appliance Clustering for HA in the Administration Manual for more detailed information on configuring HA with 2 appliances.

2 – Useful Microsoft Resources & References

Microsoft Windows DirectAccess Client Troubleshooting Tool:

https://www.microsoft.com/en-us/download/details.aspx?id=41938

DirectAccess in Windows Server:

https://technet.microsoft.com/en-us/library/dn636118.aspx

Troubleshooting DirectAccess:

https://technet.microsoft.com/en-us/library/dn467926.aspx

Client diagnostic log information:

http://blogs.technet.com/b/jasonjones/archive/2013/11/13/the-evolution-of-collecting-directaccess-client-diagnostic-log-information.aspx

What's new in DirectAccess 2012:

https://technet.microsoft.com/en-GB/library/dn753677.aspx

15. Document Revision History

Version	Date	Change	Reason for Change	Changed By
1.2.0	26 November 2019	Styling and layout	General styling updates	AH
1.2.1	28 August 2020	New title page Updated Canadian contact details Amended instructions and new screenshot for configuring negotiate health check	Branding update Change to Canadian contact details Changes to the appliance WebUI	AH
1.2.2	18 June 2021	Various minor updates		RJC

About Loadbalancer.org

Loadbalancer.org's mission is to ensure that its clients' businesses are never interrupted. The load balancer experts ask the right questions to get to the heart of what matters, bringing a depth of understanding to each deployment. Experience enables Loadbalancer.org engineers to design less complex, unbreakable solutions - and to provide exceptional personalized support.

loadbalancer.org

United Kingdom

Loadbalancer.org Ltd.
Compass House, North Harbour
Business Park, Portsmouth, PO6 4PS
UK:+44 (0) 330 380 1064
sales@loadbalancer.org
support@loadbalancer.org

Canada

Loadbalancer.org Appliances Ltd.
300-422 Richards Street, Vancouver,
BC, V6B 2Z4, Canada
TEL:+1 866 998 0508
sales@loadbalancer.org
support@loadbalancer.org

United States

Loadbalancer.org, Inc.
4550 Linden Hill Road, Suite 201
Wilmington, DE 19808, USA
TEL: +1 833.274.2566
sales@loadbalancer.org
support@loadbalancer.org

Germany

Loadbalancer.org GmbH
Tengstraße 2780798,
München, Germany
TEL: +49 (0)89 2000 2179
sales@loadbalancer.org
support@loadbalancer.org