



Microsoft Internet Information Services (IIS) Deployment Guide

Copyright © 2012 Loadbalancer.org, Inc.





Table of Contents

About This Guide.....	4
Appliances Supported.....	4
Microsoft IIS Software Versions Supported.....	4
Loadbalancer.org Software Versions Supported.....	4
Microsoft Internet Information Services (IIS).....	5
Load Balancing IIS.....	5
The Basics.....	5
Sharing the Load.....	5
Providing Resilience.....	5
Ports & Protocols.....	5
SSL & Certificates.....	5
Persistence (aka Server Affinity).....	5
Load Balancer Deployment Methods.....	6
Layer 4.....	6
Direct Server Return (DR Mode).....	6
Network Address Translation (NAT Mode).....	6
Layer 7.....	7
Source Network Address Translation (HAProxy).....	7
Loadbalancer.org Recommended Method.....	7
Loadbalancer.org Web User Interface.....	8
Accessing the WUI.....	8
Implementing IIS in DR Mode.....	9
Overview.....	9
Load Balancer Configuration.....	9
Configure the Network Interface.....	9
Configure the Virtual Server.....	9
Configure the Real Servers.....	11
IIS Server Configuration.....	11
Solve the 'ARP Problem'.....	11
Configure IIS Bindings.....	11
DR Mode - Key Points.....	12
Implementing IIS in NAT Mode.....	13
Overview.....	13
Load Balancer Configuration.....	13
Configure the Network Interfaces.....	13
Configure the Virtual Server.....	14
Configure the Real Servers.....	16
IIS Server Configuration.....	17
Default Gateway.....	17
NAT Mode - Key Points.....	17
Implementing IIS in SNAT (HAProxy) Mode.....	18
Overview.....	18
Load Balancer Configuration.....	18
Configure the Network Interface(s).....	18
Configure the Virtual Server.....	18
Configure the Real Servers.....	19
IIS Server Configuration.....	20
HAProxy - Key Points.....	20

Additional Configuration Options & Settings.....	21
SSL Certificates.....	21
Installed on IIS.....	21
Installed on the Load balancer (aka SSL off-loading).....	24
Grouping Multiple Ports on a Single Virtual Server (VIP).....	29
Layer 4 – Using Firewall Marks.....	29
Layer 7 – Using Extra Ports Field.....	30
IIS Health Checks.....	31
Layer 4.....	31
Layer 7.....	34
Using Server Feedback Agents.....	36
Layer 4.....	36
Load Balancer Transparency.....	39
Layer 4 – DR & NAT Mode.....	39
Layer 7 - TPROXY.....	39
Layer 7 – X-Forwarded-For Headers.....	39
Testing & Validation.....	40
Monitoring Connections.....	40
Layer 4.....	40
Layer 7.....	40
Technical Support.....	41
Conclusion.....	41

About This Guide

This guide details the configuration of Loadbalancer.org appliances for deployment with Microsoft Internet Information Services (IIS).

For an introduction to setting up the appliance as well as more detailed technical information, please refer to our quick-start guide and administration manual which are available at the following link :

<http://www.loadbalancer.org/downloads.php>

(the documentation links are at the bottom of the page)

Appliances Supported

All our products can be used with Microsoft IIS. The complete list of models is shown below:

- Enterprise R16
- Enterprise
- Enterprise MAX
- Enterprise 10G
- Enterprise VA
- Enterprise VA R16

For a full specification comparison of these models please refer to : <http://www.loadbalancer.org/matrix.php>

Microsoft IIS Software Versions Supported

- V5.0
- V6.0
- V7.0
- V7.5

Loadbalancer.org Software Versions Supported

- v6.9, v6.10, v6.11, v6.12, v6.13, v6.14, v6.15, v6.16, v6.17, v6.18
- v7.2, v7.3, v7.3.1, v7.3.2

Microsoft Internet Information Services (IIS)

IIS is one of the components of Microsoft Windows and is Microsoft's implementation of a web server. The protocols supported include HTTP, HTTPS, FTP, FTPS, SMTP & NNTP. The latest release is v7.5 which is part of Windows 2008 R2. IIS 7.5 is built on an open and modular architecture that allows users to customize and add new features through free IIS Extensions. It's estimated that around 25% of all websites utilize IIS.

Load Balancing IIS

The Basics

Sharing the Load

The primary function of the load balancer is to distribute inbound connection requests across multiple IIS servers. This allows administrators to setup multiple servers and easily share the load between them. Adding additional capacity as demand grows is straight forward and can be achieved by simply adding additional IIS servers to the virtual cluster.

Providing Resilience

Typically, two load balancer appliances are deployed. This ensures that a single point of failure is not introduced. A heartbeat signal between the pair is used to ensure that should the active unit fail, the passive unit takes over. IIS server monitoring is also used to ensure that failed servers are removed from the cluster and client requests are only directed to functional servers.

Ports & Protocols

The following table shows the ports that are normally used with IIS for website applications using HTTP and HTTPS:

80	HTTP Protocol
443	HTTPS Protocol

SSL & Certificates

For secure websites & web pages, SSL is used. This ensures that data is encrypted between client and server. SSL certificates can be installed on the load balancer (aka SSL off-loading) or on the IIS servers. When terminating SSL on the load balancer, it is important to consider that data is not secured between the load balancer and the backend IIS servers and is transmitted unencrypted.

Persistence (aka Server Affinity)

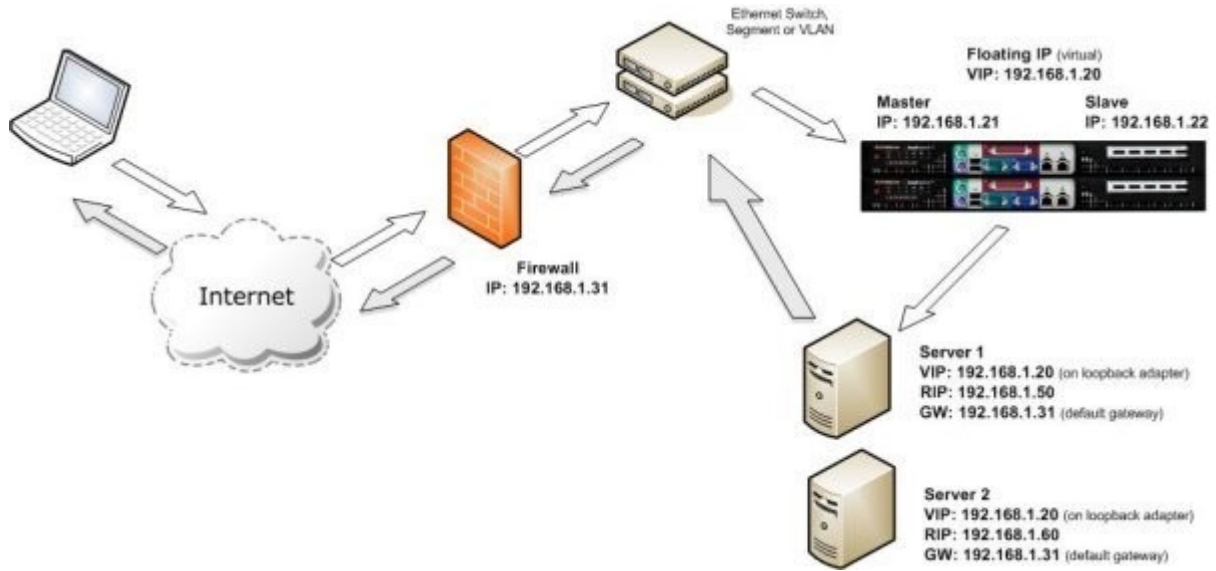
Ideally, persistence should be considered at the start of any IIS project. A database is typically used to maintain session information. This information is then available to all IIS servers so that whenever a user connects, any previous session details can be accessed. If this structure is not in place, persistence can be implemented on the load balancer. For HTTP, this can be either based on source IP address or cookies - both ensure that repeated connections within a session are always sent to the same backend IIS server.

Load Balancer Deployment Methods

Layer 4

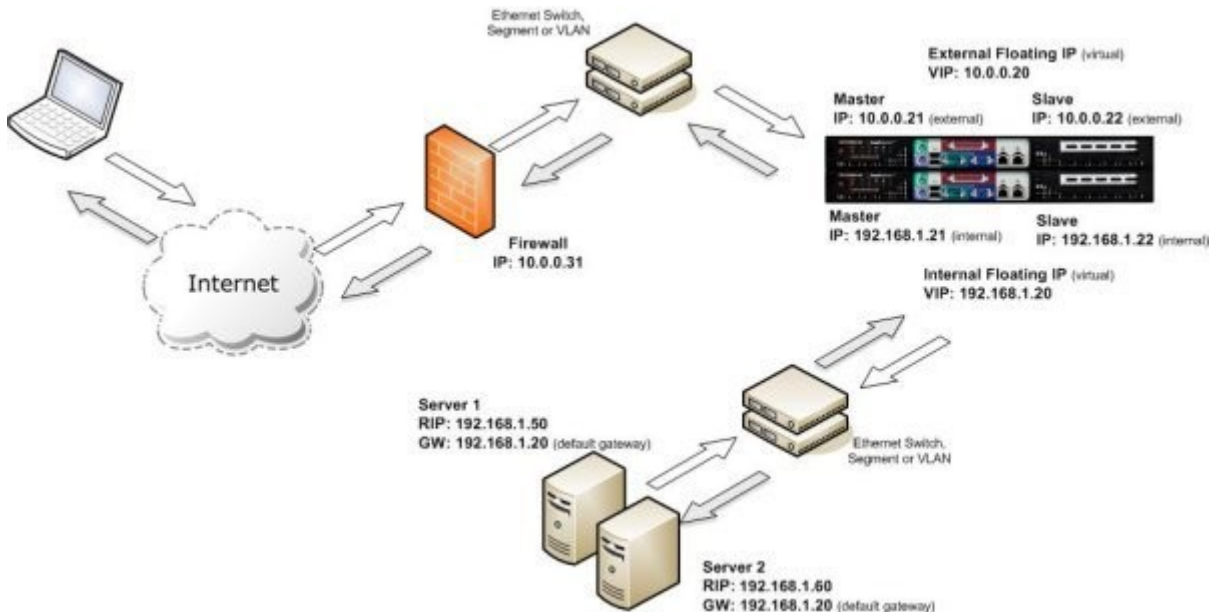
Direct Server Return (DR Mode)

In this mode, traffic from the client to the Web Proxy passes via the load balancer, return traffic passes directly back to the client which maximizes performance. Direct routing works by changing the destination MAC address of the incoming packet on the fly, which is very fast. This mode is transparent by default meaning that the proxy sees the real client IP address and not the IP address of the load balancer.



Network Address Translation (NAT Mode)

This mode requires the implementation of a two-arm infrastructure with an internal and external subnet to carry out the translation (the same way a firewall works). The real servers (i.e. the web proxies) must have their default gateway configured to point at the load balancer. It also offers high performance and like DR mode is transparent by default.

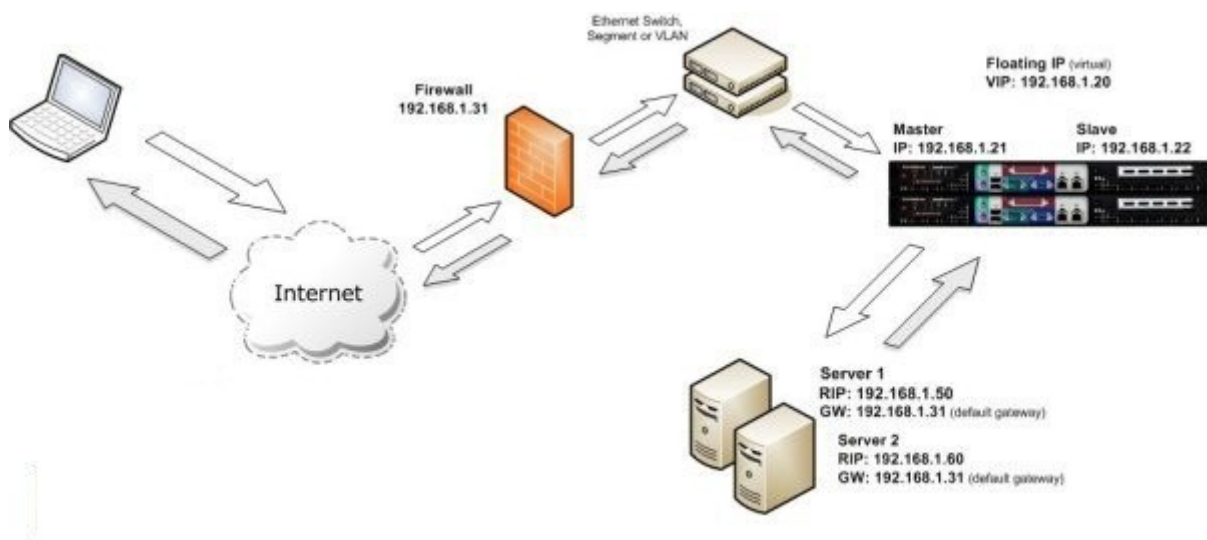


Layer 7

Layer 7 load balancing using a proxy at the application layer. HTTP requests are terminated on the load balancer, and the proxy generates a new request to the chosen real server. As a result, Layer 7 tends to be a slower technique than Direct Routing or NAT at Layer 4. Layer 7 is generally chosen when cookie-based persistence is required.

Source Network Address Translation (HAProxy)


Using HAProxy in SNAT mode means that the load balancer is acting as a full proxy and therefore doesn't have the same raw throughput as the layer 4 methods. Also, this method is not transparent by default so the real servers will see the source address of each request as the load balancer's IP address. Methods exist to address this and are covered on page 39 on this guide.



Loadbalancer.org Recommended Method

Where possible, Loadbalancer.org recommends that Layer 4 Direct Routing (DR) mode is used. DR mode provides the best possible performance with minimal change to your existing infrastructure. Ultimately, the final choice will depend on your specific requirements and infrastructure.

Loadbalancer.org Web User Interface

 It's important to have a working IIS system first before implementing the load balancer

Accessing the WUI

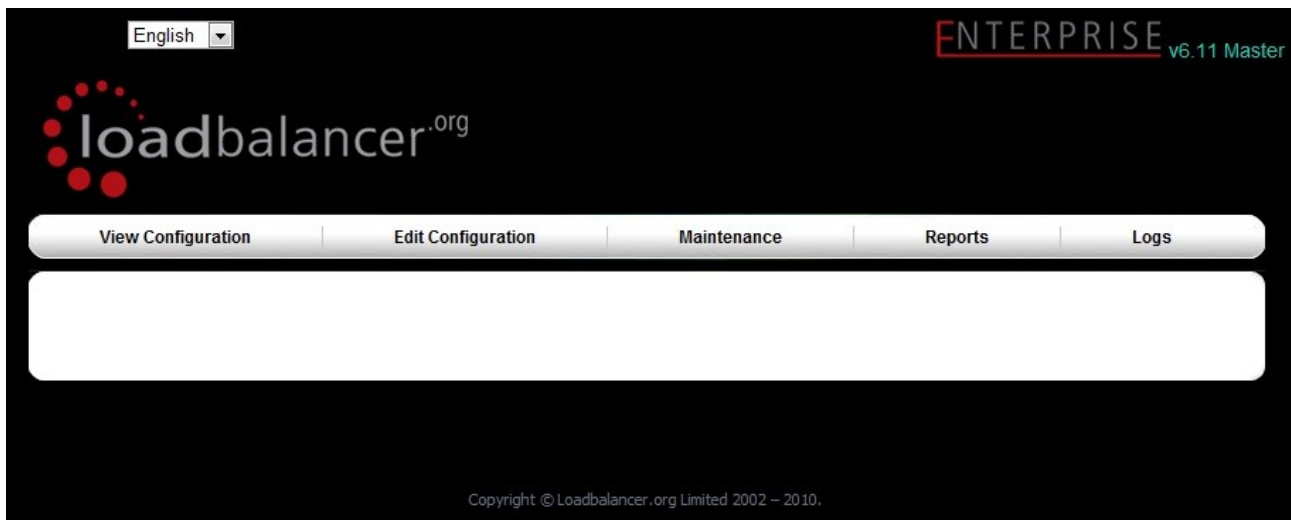
(All configuration is completed via the Web User Interface)

The WUI can be accessed from a browser at: ***http://192.168.2.21:9080/lbadmin***
(replace 192.168.2.21 with the IP address of your load balancer if this has been changed)

Username: loadbalancer

Password: loadbalancer

Once you have entered the logon credentials the Loadbalancer.org web interface will be displayed:



Implementing IIS in DR Mode

Overview

- **Configure the Network Interface** – A single Interface is needed, eth0 is normally used
- **Configure the Virtual Server** – All IIS servers are accessed via this IP address
- **Configure the Real Servers** – Define the servers that make up the IIS cluster
- **Configure the IIS servers** – In DR mode, the ARP issue must be solved

Load Balancer Configuration

Configure the Network Interface

- Go to *Edit Configuration > Network Interface Configuration*
- Set the IP Address, Netmask & Gateway for eth0 as required

Configure the Virtual Server

- Go to *Edit Configuration > Virtual Servers*
- Click [**Add a new Virtual Server**]
- Type an appropriate name (label) for the Virtual Server, e.g. IIS-Cluster
- Enter an IP address followed by :80 (e.g. 192.168.2.180:80)
- If required, change Persistent to Yes
- Click the **Update** button
- Now click [**Modify**] next to the newly created Virtual Server
- Set the Scheduler (the load balancing algorithm) mode according to your needs (recommended: 'wlc' = weighted least connection)
- Ensure that the Forwarding Method is set to 'DR'
- Click the **Update** button

The Configured Virtual Server:

EDIT CONFIGURATION > VIRTUAL SERVERS

Label	<input type="text" value="IIS-Cluster"/>	?
Virtual Server (ipaddress:port)	<input type="text" value="192.168.2.180:80"/>	?
Persistent	<input type="text" value="no"/>	?
Persistence Timeout	<input type="text" value="300"/>	?
Scheduler	<input type="text" value="wrr"/>	?
Fallback Server	<input type="text" value="127.0.0.1:80"/>	?
Check Type	<input type="text" value="connect"/>	?
Service to check	<input type="text" value="http"/>	?
Check Port	<input type="text"/>	?
Check Command	<input type="text"/>	?
Virtual Host	<input type="text"/>	?
Login	<input type="text"/>	?
Password	<input type="text"/>	?
Protocol	<input type="text" value="tcp"/>	?
Granularity	<input type="text" value="255.255.255.255"/>	?
Request to send	<input check.txt\""="" type="text" value="\"/>	?
Response expected	<input ok\""="" type="text" value="\"/>	?
Database	<input type="text"/>	?
Secret	<input type="text"/>	?
Email Alerts	<input type="text"/>	?
Forwarding Method	<input type="text" value="DR"/>	?
Feedback Method	<input type="text" value="none"/>	?

Configure the Real Servers

- Go to *Edit Configuration > Real Servers*
- Click **[Add a new Real Server]** next to the newly created Virtual Server
- Type an appropriate name for the server, e.g. IIS1
- Enter the IP address of the first IIS server followed by :80 (e.g. 192.168.2.190:80)
- Ensure that the Forwarding Method is set to 'DR'
- Click the Update button
- Repeat for your remaining IIS servers

The Configured Real Servers:

EDIT CONFIGURATION > REAL SERVERS

<i>IIS-Cluster</i>	(192.168.2.180:80)	[Add a new Real Server]	
<i>IIS2</i>	192.168.2.191:80	1	[Modify] [Delete]
<i>IIS1</i>	192.168.2.190:80	1	[Modify] [Delete]

[Virtual Servers]

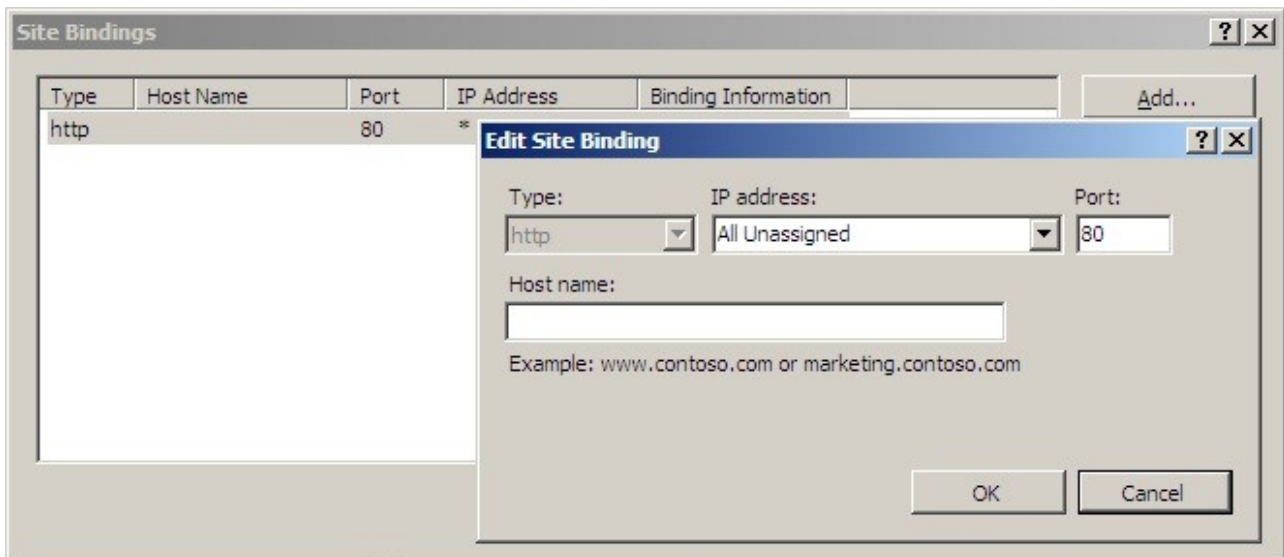
IIS Server Configuration

Solve the 'ARP Problem'

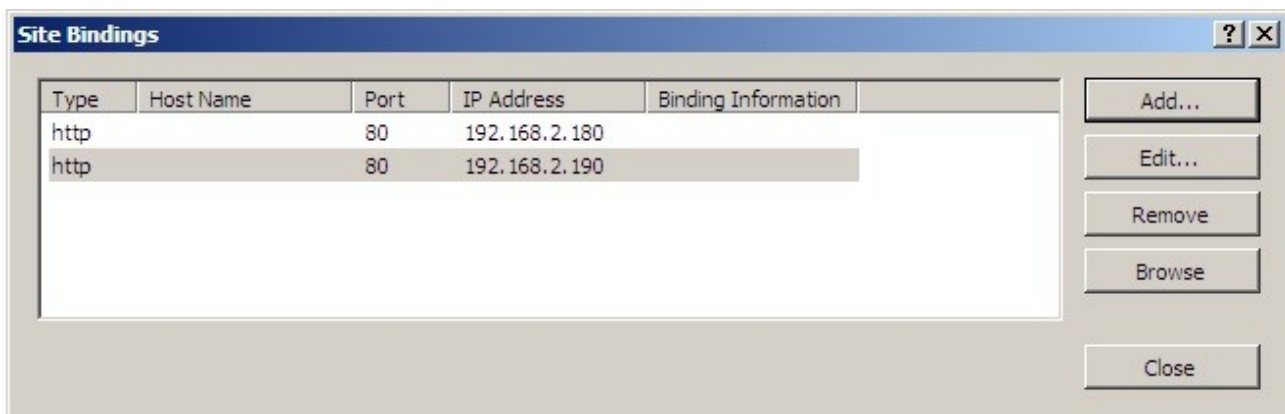
As mentioned previously, DR mode works by changing the MAC address of the incoming packet. Therefore the load balancer and the IIS servers must both be configured to accept traffic for the same IP address. However, only the load balancer should respond to ARP requests. To achieve this, a loopback adapter is added to the IIS servers. The IP address is then set to be the same as the Virtual server and is also configured so that it does not respond to ARP requests. For specific configuration steps for Windows 2003 and Windows 2008, please refer to pages 58-62 of the full administration guide which is available here: <http://loadbalancer.org/pdffiles/loadbalanceradministration.pdf>

Configure IIS Bindings

By default, IIS listens on all configured IP addresses as shown below:



If the default configuration is left, no further IIS configuration is required. If you do change the IP address in the bindings from "All Unassigned" to a specific IP address, then you need to make sure that you also add a binding for the Virtual Server IP address (VIP) as shown below:



In this example, 192.168.2.180 is the main NIC interface for the IIS server and 192.168.2.190 is the Virtual Server's IP address (assigned to the loopback Interface). This ensures that IIS responds to both the RIP and the VIP.

DR Mode - Key Points

- You must solve the ARP problem on the IIS servers
- Virtual servers & real servers (the IIS servers) must be on the same subnet
- Port translation is not possible, e.g. VIP:80 ----> RIP:82 is not allowed. The port used for the VIP & RIP must be the same
- IIS bindings must include the Virtual Server IP address

Implementing IIS in NAT Mode

Overview

- **Configure the Network Interfaces** – Two Interfaces are needed, this can be either two physical interfaces such as eth0 and eth1, or one physical interface and an alias/secondary interface such as eth0:0
- **Configure the Virtual Server** – All IIS servers are accessed via this IP address
- **Configure the Real Servers** – Define the servers that make up the IIS cluster
- **Configure the IIS servers** – In NAT mode, the IIS servers default gateway must be the load balancer

Load Balancer Configuration

Configure the Network Interfaces

- Go to *Edit Configuration > Network Interface Configuration*
- Set the IP Address, Netmask & Gateway for eth0 as required. If using two physical interfaces configure eth1 in the same way. Normally eth0 is used for the internal subnet, eth1 for the external subnet

EDIT CONFIGURATION > NETWORK INTERFACE CONFIGURATION

IP Address (eth0) :	192.168.2.170	IP Address (eth1) :	192.168.23.170
Netmask :	255.255.255.0	Netmask :	255.255.255.0
Default Gateway :	192.168.2.1		

- If using an alias, expand **Aliases**, click [**add new Alias**] and enter the required IP address and netmask

EDIT CONFIGURATION > NETWORK INTERFACE CONFIGURATION

IP Address (eth0) :	<input type="text" value="192.168.2.170"/>	IP Address (eth1) :	<input type="text"/>
Netmask :	<input type="text" value="255.255.255.0"/>	Netmask :	<input type="text"/>
Default Gateway :	<input type="text" value="192.168.2.1"/>		
Bond eth0+eth1 (bond0) :	<input type="checkbox"/>		
IP Address (eth2) :	<input type="text"/>	IP Address (eth3) :	<input type="text"/>
Netmask :	<input type="text"/>	Netmask :	<input type="text"/>
Bond eth1+eth2 (bond1) :	<input type="checkbox"/>		

- Aliases 

[add new Alias]

Interface	IP	Netmask	
eth0:250	192.168.23.170	255.255.255.0	[edit] [delete]

Configure the Virtual Server

- Go to *Edit Configuration > Virtual Servers*
- Click **[Add a new Virtual Server]**
- Type an appropriate name (label) for the Virtual Server, e.g. IIS-Cluster
- Enter an IP address followed by :80 (e.g. 192.168.2.180:80)
- If required, change Persistent to Yes
- Click the **Update** button
- Now click **[Modify]** next to the newly created Virtual Server
- Set the Scheduler (the load balancing algorithm) mode according to your needs (recommended: 'wlc' = weighted least connection)
- Ensure that the Forwarding Method is set to 'NAT'
- Click the **Update** button

The Configured Virtual Servers:

EDIT CONFIGURATION > VIRTUAL SERVERS

Label	<input type="text" value="IIS-Cluster"/>	
Virtual Server (ipaddress:port)	<input type="text" value="192.168.2.180:80"/>	
Persistent	<input type="text" value="no"/>	
Persistence Timeout	<input type="text" value="300"/>	
Scheduler	<input type="text" value="wrr"/>	
Fallback Server	<input type="text" value="127.0.0.1:9081"/>	
Check Type	<input type="text" value="connect"/>	
Service to check	<input type="text" value="http"/>	
Check Port	<input type="text"/>	
Check Command	<input type="text"/>	
Virtual Host	<input type="text"/>	
Login	<input type="text"/>	
Password	<input type="text"/>	
Protocol	<input type="text" value="tcp"/>	
Granularity	<input type="text" value="255.255.255.255"/>	
Request to send	<input check.txt\""="" type="text" value="\"/>	
Response expected	<input ok\""="" type="text" value="\"/>	
Database	<input type="text"/>	
Secret	<input type="text"/>	
Email Alerts	<input type="text"/>	
Forwarding Method	<input type="text" value="NAT"/>	
Feedback Method	<input type="text" value="none"/>	

Configure the Real Servers

- Go to *Edit Configuration > Real Servers*
- Click **[Add a new Real Server]** next to the newly created Virtual Server
- Type an appropriate name for the server, e.g. IIS1
- Enter the IP address of the first IIS server followed by :80 (e.g. 192.168.23.190:80)
- Ensure that the Forwarding Method is set to 'NAT'
- Click the **Update** button
- Repeat for your remaining IIS servers

The Configured Real Servers:

EDIT CONFIGURATION > REAL SERVERS

<i>IIS-Cluster</i>	(192.168.2.180:80)	[Add a new Real Server]	
<i>IIS2</i>	192.168.23.191:80	<i>1</i>	[Modify] [Delete]
<i>IIS1</i>	192.168.23.190:80	<i>1</i>	[Modify] [Delete]

[Virtual Servers]

IIS Server Configuration

Default Gateway

It is possible to use the internal IP address on eth0 for the default gateway, although it's recommended that an additional floating IP is created for this purpose. This is required if two load balancers (our recommended configuration) are used. Then, if the master unit fails, the floating IP will be brought up on the slave and failover will be seamless. To create a floating IP address on the load balancer:

- Go to *Edit Configuration > Floating IP(s)*
- Enter the required IP address and click **Update**. Once added, there will be two floating IP's, one for the Virtual Server (192.168.2.180) and one for the default gateway (192.168.23.250) as shown below

EDIT CONFIGURATION > EDIT FLOATING IP

192.168.2.180	[Delete]
192.168.23.250	[Delete]

EDIT CONFIGURATION > ADD NEW FLOATING IP

NAT Mode - Key Points

- Virtual Servers & Real Servers (The IIS servers) must be on different subnets
- The default gateway on the IIS servers should be an IP address on the load balancer
- Port translation is possible, e.g. VIP:80 ----> RIP:8010 is allowed

Implementing IIS in SNAT (HAProxy) Mode

Overview

- **Configure the Network Interface(s)** – Using HAProxy, it's possible to use a single interface on a single subnet or use two interfaces across different subnets. As with NAT mode, it's possible to use either a physical interface or an alias/secondary interface for the second subnet
- **Configure the Virtual Server** – All IIS servers are accessed via this IP address
- **Configure the Real Servers** – Define the servers that make up the IIS cluster
- **Configure the IIS servers** – NO real server changes are required

Load Balancer Configuration

Configure the Network Interface(s)

- Go to *Edit Configuration > Network Interface Configuration*
- Set the IP Address, Netmask & Gateway for eth0 as required. If the IIS servers are in the same subnet as the VIP, there is no need to use a second interface. If in a different subnet, either setup eth1 or create an alias on eth0 as per NAT mode described previously. Again, eth0 is normally used for the internal subnet (i.e. the IIS servers) and eth1 for the external subnet (i.e. the VIP)

Configure the Virtual Server

- Go to *Edit Configuration > Virtual Servers (HAProxy)*
- Click [**Add a new Virtual Server**]
- Type an appropriate name (label) for the Virtual Server, e.g. IIS-Cluster
- Enter an IP address followed by :80 (e.g. 192.168.2..180:80)
- If not required, change the persistence mode to None
- Click the **Update** button
- Now click [**Modify**] next to the newly created Virtual Server
- Set the balance mode according to your needs (recommended: Least Connections)
- Click the **Update** button

The Virtual Server configuration:

EDIT CONFIGURATION > VIRTUAL SERVERS (HAProxy)

Label	<input type="text" value="IIS-Cluster"/>	?
Virtual Server (ipaddress:port)	<input type="text" value="192.168.2.180:80"/>	?
Extra Ports	<input type="text"/>	?
Persistence mode	<input type="text" value="None"/>	?
Balance mode	<input type="text" value="Least Connections"/>	?
Timeout	<input type="text" value="30"/>	?
Table Size	<input type="text" value="10240"/>	?
Fallback	<input type="text" value="127.0.0.1:9081"/>	?
Check Port	<input type="text"/>	?
Request to send	<input type="text"/>	?
Response expected	<input type="text"/>	?
Maximum Connections	<input type="text"/>	?

Configure the Real Servers

- Go to *Edit Configuration > Real Servers (HAProxy)*
- Click **[Add a new Real Server]**
- Type an appropriate name for the server, e.g. IIS1
- Enter the IP address followed by :80 (e.g. 192.168.23.20:80)
- Click the **Update** button
- Now repeat for your remaining real servers

Configured Real Servers:

EDIT CONFIGURATION > REAL SERVERS (HAPROXY)

<i>IIS-Cluster</i>	(192.168.2.180:80)	[Add a new Real Server]		
<i>IIS2</i>	192.168.2.191:80	1	[Modify]	[Delete]
<i>IIS1</i>	192.168.2.190:80	1	[Modify]	[Delete]

[Virtual Servers]

IIS Server Configuration

In SNAT (HAProxy) mode, no IIS server changes are required.

HAProxy - Key Points

- Virtual Servers & Real Servers (The IIS servers) can be on the same or different subnets
- Port translation is possible, e.g. VIP:80 ----> RIP:8010 is allowed
- No configuration changes are required to the IIS servers
- Not as fast as Layer 4 DR mode or NAT mode

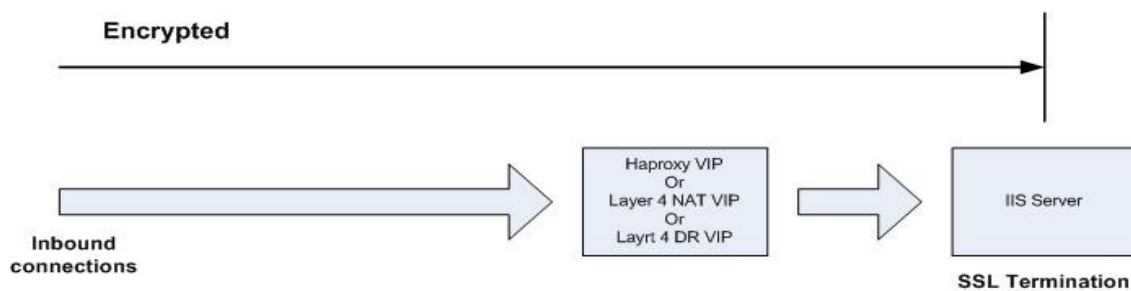
Additional Configuration Options & Settings

SSL Certificates

Installed on IIS

When certificates are installed on the IIS server:

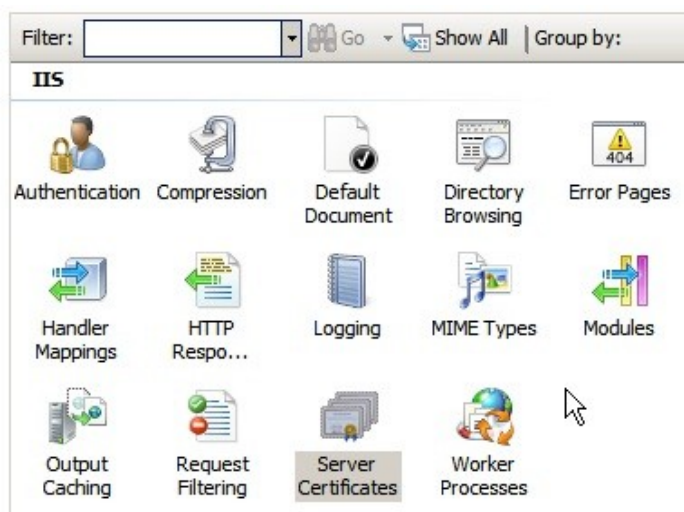
- It's not possible to use HTTP cookie persistence since the packet is encrypted and therefore the cookie cannot be read. If persistence via the load balancer is required, IP persistence must be used
- Data is encrypted from client to server. This provides full end-to-end data encryption as shown in the diagram below:



Creating a CSR

To generate a certificate for IIS the first step is to create a Certificate Signing Request (CSR)

1. Select the IIS server in IIS Manager then double-click Server Certificates



- In the actions section on the right hand side of the screen, select Create Certificate Request, fill in the relevant details as per the example below, then click Next

The screenshot shows a Windows dialog box titled "Request Certificate" with a sub-header "Distinguished Name Properties". Below the sub-header is an icon of a certificate and a paragraph of instructions: "Specify the required information for the certificate. State/province and City/locality must be specified as official names and they cannot contain abbreviations." The form contains several input fields: "Common name:" with the value "www.loadbalancer.org"; "Organization:" with the value "loadbalancer.org"; "Organizational unit:" with the value "support"; "City/locality:" with the value "portsmouth"; "State/province:" with the value "hampshire"; and "Country/region:" with a dropdown menu showing "GB". At the bottom of the dialog are four buttons: "Previous", "Next" (which is highlighted with a dotted border), "Finish", and "Cancel".

- Leave the default settings and click Next

The screenshot shows a Windows dialog box titled "Request Certificate" with a sub-header "Cryptographic Service Provider Properties". Below the sub-header is an icon of a certificate and a paragraph of instructions: "Select a cryptographic service provider and a bit length. The bit length of the encryption key determines the certificate's encryption strength. The greater the bit length, the stronger the security. However, a greater bit length may decrease performance." The form contains two dropdown menus: "Cryptographic service provider:" with the value "Microsoft RSA SChannel Cryptographic Provider" and "Bit length:" with the value "1024". At the bottom of the dialog are four buttons: "Previous", "Next" (which is highlighted with a dotted border), "Finish", and "Cancel".

- Where prompted on the following screen enter a suitable filename , e.g. c:\csr.txt and click Finish
- Use this saved CSR with your chosen Certificate Authority to obtain your certificate
- Once you've received your certificate from the CA, save it as a text file

7. To install the certificate on the IIS server select Complete Certificate Request in the action section of Server Certificates in IIS Manager, then specify the filename and a friendly name and click OK



8. At this point you may receive the message shown below. This is a known issue that occurs because the friendly certificate name entered in step 7 above is not being read correctly. For more details please refer to <http://support.microsoft.com/kb/959216>. Note that the certificate has been installed and can be seen in IIS Manager under Server Certificates

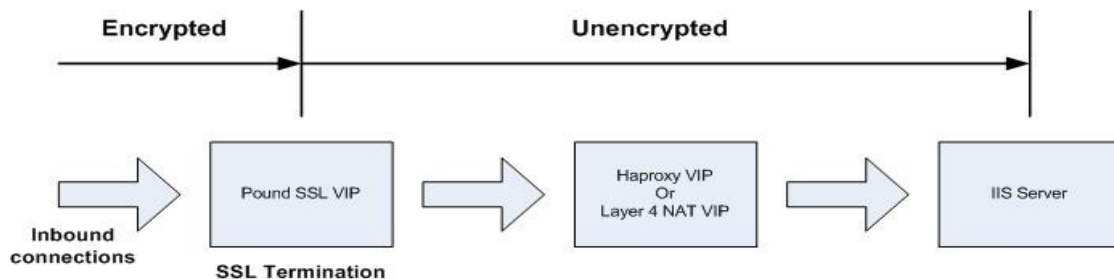


9. Now amend the site bindings to include https and the newly installed certificate

Installed on the Load balancer (aka SSL off-loading)

When certificates are installed on the load balancer:

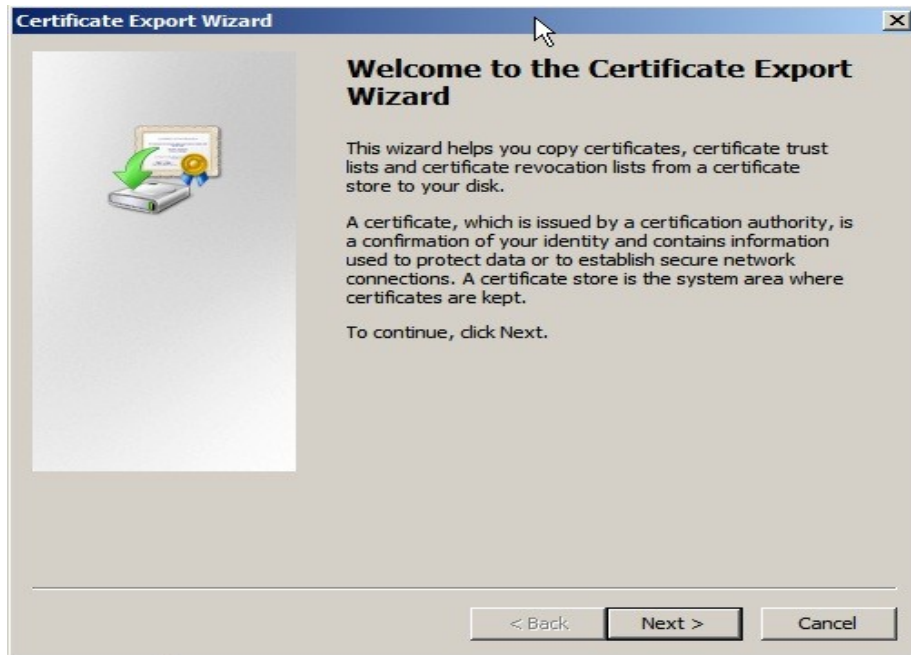
- It's possible to use HTTP cookie based persistence
- Since SSL is terminated on the load balancer, data from the load balancer to the IIS servers is not encrypted as shown in the diagram below. This may or may not be an issue depending on the network structure between the load balancer and IIS servers and your security requirements.
- A Pound SSL Virtual Server is used to terminate SSL. The backend for this Virtual Server can be either a Layer 4 NAT mode Virtual Server or a Layer 7 HAProxy Virtual Server. The following diagram shows this. Note that it's not possible to use a layer 4 DR mode virtual server in this scenario.



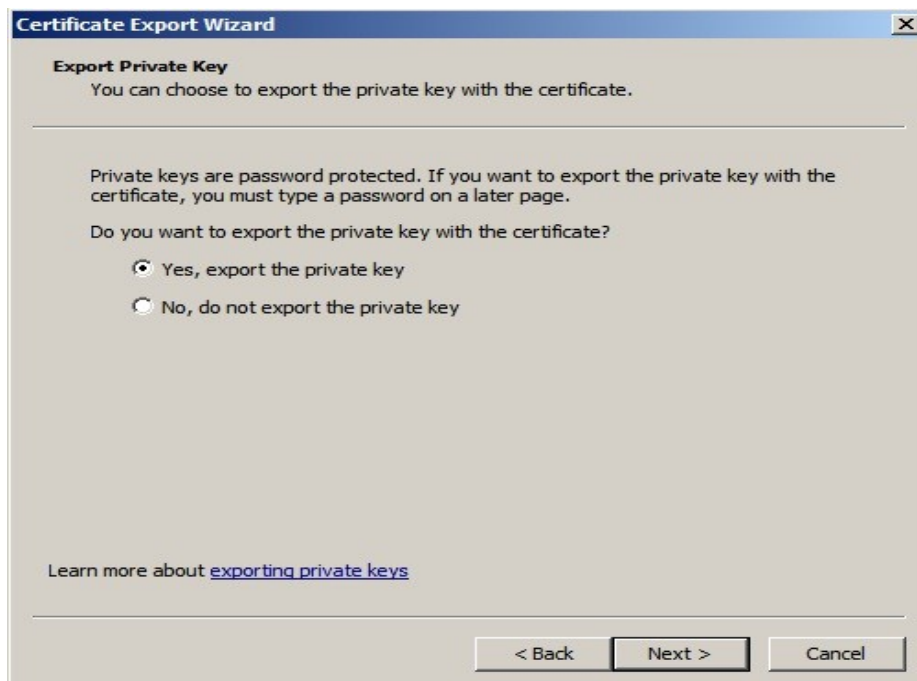
Exporting Certificates from Windows & Importing to the load balancer

Its often easiest to get the certificate working on the IIS server first, then export the certificate and import this to the load balancer. The steps for this process are:

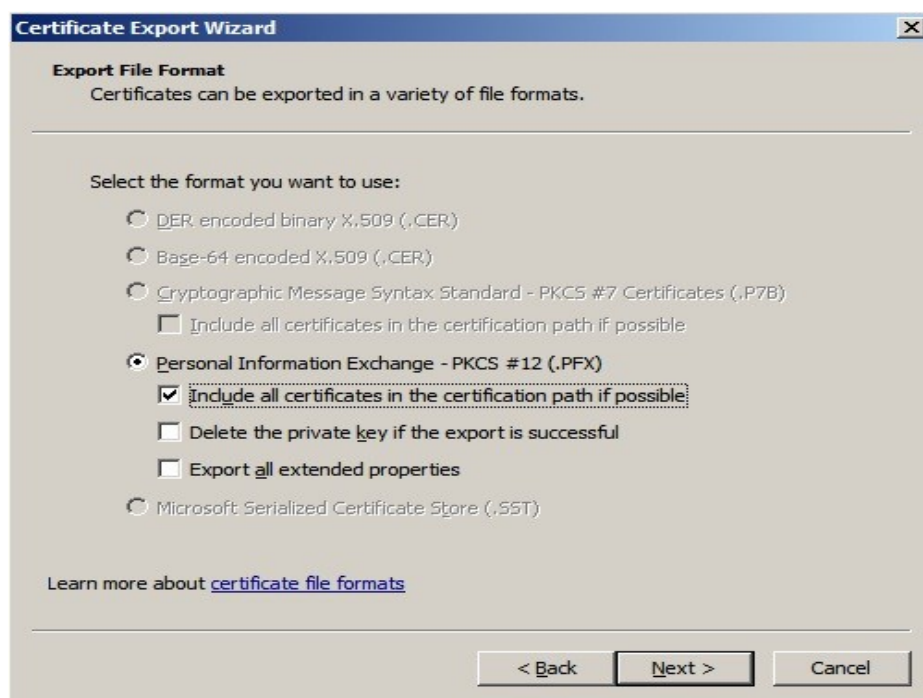
1. Once the certificate is working correctly on your Windows server, run mmc, and add the certificates snap-in. Expand the Personal folder and click on Certificates – your certificate should be here. Right-click the certificate and select All Tasks > Export. This will start the Certificate Export Wizard as shown below:



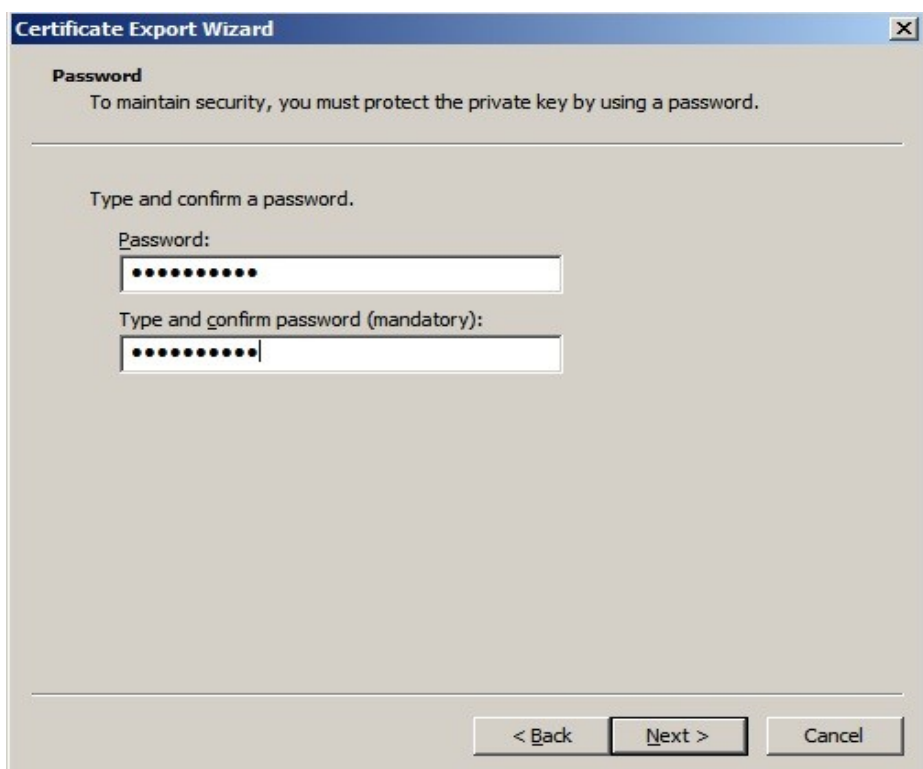
2. Click Yes to export the private key and click Next



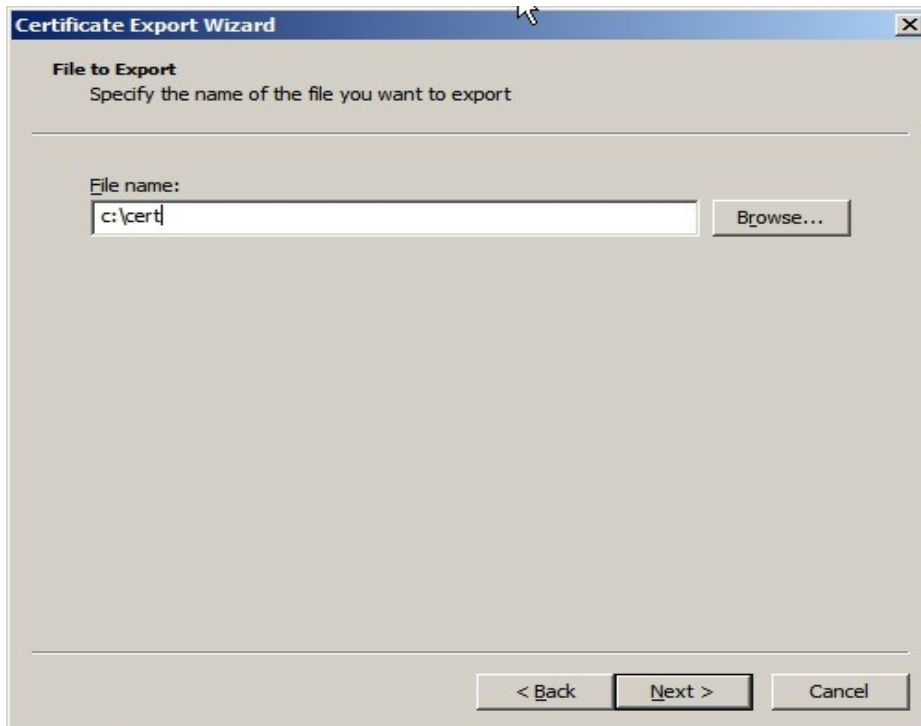
3. Check *Include all Certificates in the certification path if possible* and click Next



4. Enter a password to secure the private key and click Next



5. Enter a folder & filename for the exported certificate and click Next



6. Now click Finish to complete the wizard, the following confirmation should be shown



7. To convert the pfx file to pem format (the format required by the load balancer) download openssl from the following link and install on your PC:

http://www.slproweb.com/download/Win32OpenSSL_Light-1_0_0c.exe

8. In a command window, browse to C:\openssl\bin and run the following command to convert the pfx file to a pem file:

```
openssl pkcs12 -in drive:\path to cert\cert.pfx -nodes -out drive:\path to cert\cert.pem
```

(You will be prompted for the password used to create the pfx file in step 4 above)

- Using *Edit Configuration > SSL Termination (Pound)* create a Pound Virtual Server. For the Virtual Server you can use the same IP address as your HAProxy or NAT Virtual Server created earlier with port 443 for HTTPS. The IP address:Port for the Backend Cluster should be set the same as your HAProxy or NAT Virtual Server as shown below. Click Update to create the new Pound Virtual Server.

EDIT CONFIGURATION > ADD A NEW VIRTUAL SERVER SSL TERMINATION (POUND)

Virtual Server (ipaddress:port)	<input type="text" value="192.168.2.180:443"/>	
Backend Cluster	<input type="text" value="192.168.2.180:80"/>	
Ciphers to use	<input type="text"/>	

- To upload your certificate to the Pound Virtual Server, Click Modify, then browse to the new .pem file created in step 8 above and click Upload PEM file

EDIT CONFIGURATION > VIRTUAL SERVERS SSL TERMINATION (POUND)

Virtual Server (ipaddress:port)	<input type="text" value="192.168.2.180:443"/>	
Backend Cluster	<input type="text" value="192.168.2.180:80"/>	
Ciphers to use	<input type="text"/>	

- Now restart Pound (*Maintenance > Restart Pound-SSL*). Your secure website should now be accessible at: <https://<Virtual IP Address>>

Grouping Multiple Ports on a Single Virtual Server (VIP)

In certain circumstances it may be desirable to combine multiple ports in a single Virtual Server. For example, if your IIS server has both HTTP and HTTPS content, you may want clients to connect to the same IIS server for both. This is especially useful if you need persistence as clients move from HTTP to HTTPS, e.g. an e-commerce web site without a proper back end database for session state.

Layer 4 – Using Firewall Marks

The concept is to create a firewall rule that matches incoming packets to a particular IP and port, and mark them with an arbitrary integer. A Virtual Server is then configured or modified, specifying the firewall mark instead of an IP and port.

Step 1 – Modify the firewall script

The *Maintenance > Firewall Script* page in the WUI includes some examples under the "FIREWALL MARKS" section as shown below. The example firewall mark shown can be uncommented and edited to suit your requirements. This example marks incoming packets to both port 80 and 443 with the same value.

MAINTENANCE > FIREWALL SCRIPT

```
##### FIREWALL MARKS #####

# Now setup any Firewall marks that are required
# Firewall marks allows you to associate multiple ports with one VIP
# This is useful if you need to keep HTTP & HTTPS persistent

# This example marks HTTP & HTTPS connections only

#VIP1="10.0.0.66"
# iptables -t mangle -A PREROUTING -p tcp -d $VIP1 --dport 80 -j MARK --set-mark 1
# iptables -t mangle -A PREROUTING -p tcp -d $VIP1 --dport 443 -j MARK --set-mark 1

# If you then add a virtual service with an address of '1' rather
# than 'IP:port' it will balance HTTPS & HTTP,
# this would usually be set as persistent...
```

Update

Step 2 – Create / modify the Virtual Server

Then, a new Virtual Server must be created or an existing one must be modified – entering the mark value "1" in the *Virtual Server* field. All the other fields can be set as usual, and real servers can be associated with the VIP in the normal way. With a firewall mark Virtual Server, the load balancer forwards traffic to the selected real server without changing the destination port. So, incoming traffic to port 80 on the Virtual IP will be forwarded to port 80 on one of the IIS servers and likewise, incoming traffic to port 443 will be forwarded to port 443 on the same IIS server.

e.g. to configure firewall mark '1', a standard Virtual Server as shown below:

EDIT CONFIGURATION > VIRTUAL SERVERS

Label	<input type="text" value="VIP1"/>	?
Virtual Server (ipaddress:port)	<input type="text" value="192.168.2.165:80"/>	?

would be changed to:

EDIT CONFIGURATION > VIRTUAL SERVERS

Label	VIP1	?
Virtual Server (ipaddress:port)	1	?

Then, any incoming packets marked with a '1' will be associated with that VIP.

Also ensure that:

- The Protocol for the VIP is set to 'fwm'
- Persistence is set to 'Yes'

Layer 7 – Using Extra Ports Field

For Layer 7 Virtual Servers, you can add additional ports in the *Extra Ports* field as shown below.

EDIT CONFIGURATION > VIRTUAL SERVERS (HAPROXY)

Label	IIS-Cluster	?
Virtual Server (ipaddress:port)	192.168.2.180:80	?
Extra Ports	443	?

IIS Health Checks

Layer 4

At layer 4, IIS server health checking is provided by Ldirectord. This allows a full range of options to check that the IIS servers are operational, and if not what steps to take.

Edit Configuration > Virtual Servers > [Modify]

Check Type	connect ▾	?
Service to check	http ▾	?
Check Port	<input type="text"/>	?
Check Command	<input type="text"/>	?
Virtual Host	<input type="text"/>	?
Login	<input type="text"/>	?
Password	<input type="text"/>	?
Protocol	tcp ▾	?
Granularity	255.255.255.255	?
Request to send	"check.txt"	?
Response expected	"OK"	?
Database	<input type="text"/>	?
Secret	<input type="text"/>	?
Email Alerts	<input type="text"/>	?
Forwarding Method	DR ▾	?
Feedback Method	none ▾	?

Check Types

Connect - Just do a simple connect to the specified port/service & verify that its able to accept a connection

Negotiate – Sends a request and looks for a specific response (see service to check below)

Ping – Check by sending an ICMP echo request packet

External - Use a custom file for the health check. Specify the file path in the 'Check Command' field.

- Off** - All real servers are off
- On** - All real servers are on (no checking)
- 5** - Do 5 connect checks and then 1 negotiate
- 10** - Do 10 connect checks and then 1 negotiate

Service to check

If negotiate is selected as the check type, the following methods are available:

- http** – use http as the negotiate protocol (also requires file name, path + text expected)
- https** – use https as the negotiate protocol (also requires file name, path + text expected)
- ftp** – use ftp as the negotiate protocol (optional username/password, filename in the default folder)
- imap** – use imap as the negotiate protocol (requires username/password)
- pop** – use pop as the negotiate protocol (requires username/password)
- ldap** – use ldap as the negotiate protocol
- smtp** – use smtp as the negotiate protocol
- nntp** – use nntp as the negotiate protocol
- dns** – use dns as the negotiate protocol
- mysql** – use mysql as the negotiate protocol
- sip** – use sip as the negotiate protocol
- telnet** – use telnet as the negotiate protocol
- none**

Check Port

This can be used if you require the health check to connect to a different port than that used by the Virtual Server.

Check Command

Location of the custom check file relative to root. For use with check type = external.

Virtual Host

If the real server will only respond to a URL or 'virtualhost' rather than an IP address. You can specify the virtualhost to request here.

Login

The login name to use for IMAP, POP3 or FTP accounts (used for negotiate checks)

Password

The password to use for negotiate checks that require a password.

Request to Send

Specify the name of the file to check if you are using 'negotiate'.

Response Expected

This is the response that must be received for the negotiate to be a success. The negotiate check will succeed if the specified text (response) is found anywhere in the response from the web server when the file specified in the File to Check field is requested.

For example, a file called 'check.txt' could be placed in the default folder of the web server. This text file could just have the text "OK" in the file, then, when the negotiate check runs, it would look for a file called 'check.txt' containing "OK". If found, the test would succeed. If not found, it would fail and no new sessions would be sent to that server.

Additional Layer 4 health check settings

Edit Configuration > Global Settings > Layer 4

Layer 4:		
Check Interval	<input type="text" value="6"/>	?
Check Timeout	<input type="text" value="3"/>	?
Negotiate Timeout	<input type="text" value="5"/>	?
Quiescent	<input type="text" value="no"/> ▼	?
Default Forwarding Method	<input type="text" value="DR"/> ▼	?
Email Alerts	<input type="text"/>	?
Auto NAT	<input type="text" value="off"/> ▼	?

Check Interval

Layer 4 (Ldirectord) health check interval in seconds. If this setting is too low, you may induce unexpected real server downtime. For slower servers, this may need to be increased.

Check Timeout

Layer 4 (Ldirectord) health check timeout in seconds. If this setting is too low, you may induce unexpected real server downtime. For slower servers, this may need to be increased.

Negotiate Timeout

Layer 4 (Ldirectord) negotiate health check timeout in seconds. The negotiate checks may take longer to process as they involve more server side processing than a simple TCP socket connect check. If this setting is too low, you may induce unexpected real server downtime. For slower servers, this may need to be increased.

Quiescent

Yes - When an IIS server is determined to be down, its not actually removed from the kernel's LVS table. Instead, the weight is set to zero which means that no new connections will be accepted.

No – When an IIS server is determined to be down, the real server will be removed from the kernel's LVS table.

Email Alerts

This is the default global setting for email alerts and is used if not specified at the individual VIP level.

Layer 7

By default layer 7 (HAProxy) Virtual Servers use a connect type health check on the same port used specified in the Virtual Server.

Edit Configuration > Virtual Servers (HAProxy) > [Modify]

Check Port	<input type="text"/>	
File to check	<input type="text"/>	
Response expected	<input type="text"/>	

Check Port

This field can be used if you require the health check to connect to a different port than that used by the Virtual Server.

File to check




To change the connect check to a negotiate check, specify a file in the *File to Check* field. The health check will then attempt to open the specified file and check for the text specified in the *Response expected* field.

Response expected

The content expected for a valid health check on the specified file. The response expected can be any valid regular expression statement.

Additional Layer 7 health check settings

Edit Configuration > Global Settings > Layer 7 (HAProxy)

Interval	<input type="text" value="2000"/>	
Rise	<input type="text" value="2"/>	
Fall	<input type="text" value="3"/>	

Interval

This is the time interval between real server health checks in milliseconds.

Rise

The number of positive health checks required before re-activating an IIS server.

Fall

The number of negative health checks required before de-activating an IIS server.

Using Server Feedback Agents

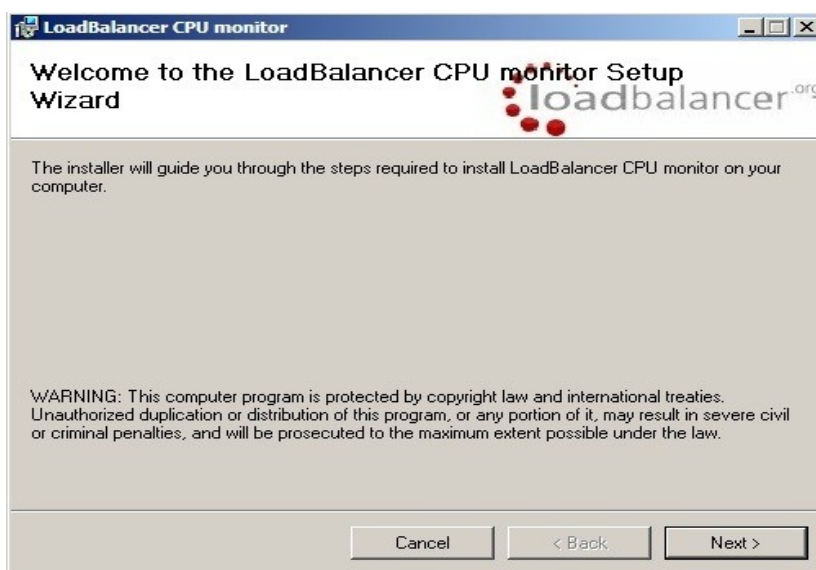
Layer 4

To enable the load balancer to be aware of the actual load on the IIS servers, it's possible to install a feedback agent on each IIS server that provides CPU utilization information back to the load balancer via TCP port 3333. If CPU utilization on one of the IIS server goes up, the weighting is dynamically adjusted so that less connections are sent to that server.

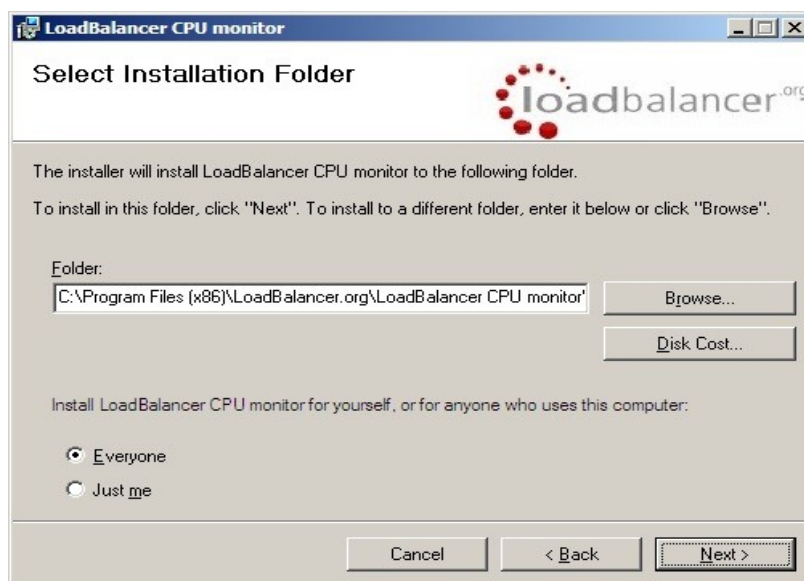
The feedback agent can be downloaded from:

<http://www.loadbalancer.org/download/agent/Windows/LBCPUMonInstallation.msi>

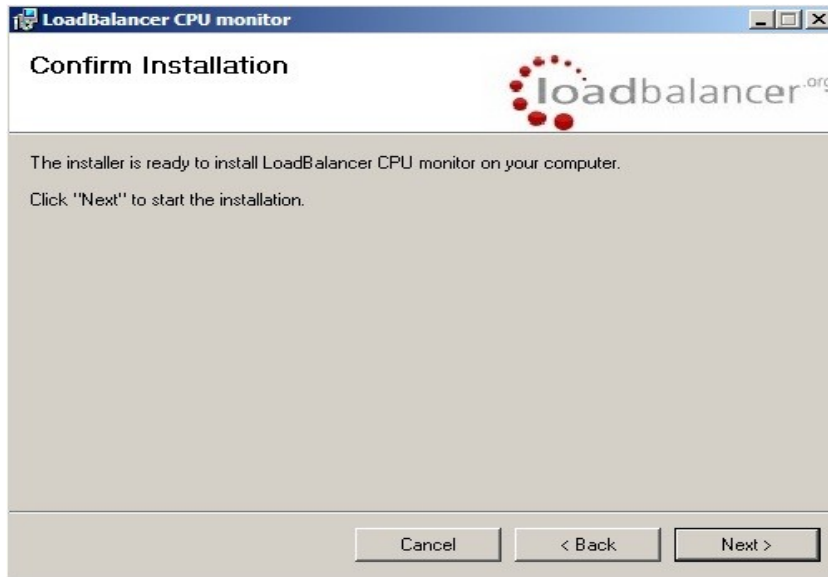
To install the agent, run LBCPUMonInstallation.msi



click next



select the installation folder and click next



click next to start the installation

Once the installation has completed, you'll need to start the service on the real servers. The service is called "Loadbalancer CPU Monitor".

Also, the Feedback Method for the Layer 4 Virtual Server must be changed:

- Go to *Edit Configuration > Virtual Servers*
- Click [**Modify**] next to the Virtual Server
- Change the Feedback Method to 'agent'



- Click Update

Prior to installing & activating the agent, *View Configuration > System Overview* would look similar to the following (server weights are set to the default of 1) :

Key cluster healthy cluster may need attention cluster is down real server deliberately offline

WEB1-192.168.23.165:80		total connections - active: 0 inactive: 0			
Label	IP	Method	Weight	Active conns	Inactive conns
IIS1	192.168.23.20:80	DR	1	0	0 take offline
IIS2	192.168.23.21:80	DR	1	0	0 take offline

Once the agents are installed on the terminal server and the feedback method is changed, the weights for the IIS servers are updated :

Key cluster healthy cluster may need attention cluster is down real server deliberately offline

WEB1-192.168.23.165:80		total connections - active: 0 inactive: 0			
Label	IP	Method	Weight	Active conns	Inactive conns
IIS1	192.168.23.20:80	DR	10	0	0 take offline
IIS2	192.168.23.21:80	DR	10	0	0 take offline

If one of the real servers is heavily loaded, the weighting is adjusted accordingly - a lower weight causes less sessions for that server. Here, CPU utilization on IIS1 is high so the weight has been reduced to 1 :

Key cluster healthy cluster may need attention cluster is down real server deliberately offline

WEB1-192.168.23.165:80		total connections - active: 1 inactive: 0			
Label	IP	Method	Weight	Active conns	Inactive conns
IIS1	192.168.23.20:80	DR	1	230	0 take offline
IIS2	192.168.23.21:80	DR	10	1	0 take offline

Load Balancer Transparency

Layer 4 – DR & NAT Mode

By default both Layer 4 modes are transparent. This means that IIS will log the actual IP address of the client rather than the IP address of the load balancer.

Layer 7 - TPROXY

When using HAProxy, the load balancer is not transparent by default. This means that the IP address of the load balancer will be captured and stored in the IIS logs. To get around this, TPROXY can be enabled in *Edit Configuration > Global Settings > Layer 7 (HAProxy)*. TPROXY enables the IIS servers behind a layer 7 HAProxy configuration to see the client source IP address. For this to work, the load balancer must be in a NAT configuration (i.e. both internal and external subnets) and the IIS servers must be configured to use the load balancer as their default gateway.

Layer 7 – X-Forwarded-For Headers

Since the load balancer must be in a NAT configuration (i.e. the Virtual Server and the IIS servers in different subnets) to utilize TPROXY, it is not always an appropriate solution. In situations such as this, it's possible to use the X-forwarded-for header that is included by default in all layer 7 Virtual Servers. To enable IIS to log this information, a 3rd party application must be installed on the IIS server – several are available.

Testing & Validation

Monitoring Connections

Layer 4

For Layer 4 Virtual Servers, the following monitoring options are available:

- **System Overview** – accessible from *View Configuration > System Overview*
shows the total active and inactive connections for each VIP
- **Status** – accessible from *Reports > Status*
shows similar details to system overview
- **Current Connections** – accessible from *View Configuration > Current Connections*
shows a detailed breakdown of all current connections

Layer 7

For Layer 7 Virtual Servers, the following monitoring options are available:

- **System Overview** – accessible from *View Configuration > System Overview*
shows the total connections for each VIP
- **Status (HAProxy)** – accessible from *Reports > Status*
displays a detailed real-time statistics page for all Layer 7 VIPS (requires username & password – use the default credentials)

Technical Support

For more details or assistance with your deployment please don't hesitate to contact the support team :

support@loadbalancer.org

Conclusion

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