About this Guide

This guide details the configuration of Loadbalancer.org appliances for deployment with Microsoft Exchange 2010. It includes details of ports/services that must be load balanced, topology considerations for the various Exchange 2010 server roles and also steps on how to configure the appliances.

For an introduction on setting up the appliance as well as more technical information, please also refer to our quick-start guides and full administration manuals which are available at the following links:

**Version 7 Documentation**


**Version 8 Documentation**


Loadbalancer.org Appliances Supported

All our products can be used with Exchange 2010. The complete list of models is shown below:

<table>
<thead>
<tr>
<th>Discontinued Models</th>
<th>Current Models *</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enterprise R16</td>
<td>Enterprise R20</td>
</tr>
<tr>
<td>Enterprise VA R16</td>
<td>Enterprise MAX</td>
</tr>
<tr>
<td>Enterprise VA</td>
<td>Enterprise 10G</td>
</tr>
<tr>
<td></td>
<td>Enterprise R320</td>
</tr>
<tr>
<td></td>
<td>Enterprise VA R20</td>
</tr>
<tr>
<td></td>
<td>Enterprise VA MAX</td>
</tr>
<tr>
<td></td>
<td>Enterprise AWS **</td>
</tr>
<tr>
<td></td>
<td>Enterprise AZURE **</td>
</tr>
</tbody>
</table>

* For full specifications of these models please refer to: [http://www.loadbalancer.org/products](http://www.loadbalancer.org/products)

** Some features may not be supported, please check with Loadbalancer.org support

Loadbalancer.org Software Versions Supported

- v7.3.2 and later

  *N.B. this guide includes configuration steps for v7.6 & later. For older versions of the appliance please contact Loadbalancer.org sales or support*

Microsoft Exchange Software Versions Supported

- Microsoft Exchange 2010 – all versions
Exchange Server 2010

Exchange 2010 is Microsoft’s enterprise level messaging and collaboration server.

Exchange 2010 Server Roles

System functionality is split into five role as shown in the following table. Mandatory roles are Mailbox, Client Access and Hub Transport. The Edge Transport and Unified Messaging roles are optional and depend on the infrastructure and operational requirements.

<table>
<thead>
<tr>
<th>Role</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mailbox Server</td>
<td>This server hosts mailboxes and public folders.</td>
</tr>
<tr>
<td>Client Access Server</td>
<td>This is the server that hosts the client protocols, such as Post Office Protocol 3 (POP3), Internet Message Access Protocol 4 (IMAP4), Secure Hypertext Transfer Protocol (HTTPS), Outlook Anywhere, Availability service, and Autodiscover service. The Client Access Server also hosts Web services. N.B. A number of issues have been seen with IOS-7 on the iPhone when used with ActiveSync. Upgrading to IOS-8 resolved these issues.</td>
</tr>
<tr>
<td>Unified Messaging Server</td>
<td>This is the server that connects a Private Branch exchange (PBX) system to Exchange 2010.</td>
</tr>
<tr>
<td>Hub Transport Server</td>
<td>This is the mail routing server that routes mail within the Exchange organization.</td>
</tr>
<tr>
<td>Edge Transport Server</td>
<td>This is the mail routing server that typically sits at the perimeter of the topology and routes mail in to and out of the Exchange organization.</td>
</tr>
</tbody>
</table>

Client Access Server

The Client Access Server Role also known as CAS, provides Exchange connectivity for all clients regardless of client type or protocol including Outlook Web App (aka OWA), ActiveSync, POP3, IMAP4, RPC Client Access (MAPI) and Outlook Anywhere (previously known as RPC over HTTP). Exchange now has a single common path through which all data access occurs.

Therefore, due to the critical nature of this role, it's common practice to implement load balancing and redundancy technologies to ensure availability.

Hub Transport Server

For internal server to server mail traffic, HT servers are automatically load balanced by Exchange 2010 and there is no need to configure any type of load balancing mechanism to load balance the mail submission traffic among Exchange servers.

However, some sites may decide not to deploy an ET server. In this scenario, inbound SMTP mail is typically forwarded from a third party smart host directly to the HT server. Also, internal applications and systems often need to send email via Exchange and typically are only able to do so using an SMTP connection. To provide redundancy in these cases, additional load balancing & HA techniques are required to ensure availability of the HT role.
Mailbox Server / Database Availability Group's (DAG)

Exchange 2010 brings the ability to combine both CAS and HT roles on a mailbox server that is also configured as a DAG member. This permits a highly available solution using just two Exchange servers and one or two (configured as a clustered pair for added redundancy) Loadbalancer.org appliances. Another server is needed to act as the witness server, but this doesn’t need to be an Exchange server. It could be any Windows 2003/2008 file server within the environment.

DAG’s utilize Microsoft Clustering Services which cannot be enabled on the same server as Microsoft Network Load Balancing (NLB). Therefore, using Microsoft NLB is not an option in this case. Using a Loadbalancer.org hardware appliance provides an ideal solution.

Load Balancing Exchange 2010

The Basics

Which Roles?
The CAS role does not have any built-in load balancing functionality. The HT role does provide load balancing functionality for server to server mail traffic, but not external SMTP traffic that arrives from other applications or from outside the organization directly to the HT server. Therefore, it is a common requirement to load balance both the CAS and HT roles. In some cases only the CAS role is load balanced. The exact load balancing requirements depend on the number of servers in use and how / where the roles are deployed.

Persistence (aka Server Affinity)

Some Exchange 2010 protocols require affinity and others do not. For more details please refer to the following Microsoft Technet article: http://technet.microsoft.com/en-us/library/ff625248.aspx

For additional information on the various affinity options, please refer to the following Microsoft Technet article: http://technet.microsoft.com/en-us/library/ff625247.aspx#affinity

Summary of Persistence Requirements:

<table>
<thead>
<tr>
<th>Persistence – Required</th>
<th>Persistence – Recommended</th>
<th>Persistence – Not Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>Outlook Web App</td>
<td>Outlook Anywhere</td>
<td>Offline Address Book</td>
</tr>
<tr>
<td>Exchange Control Panel</td>
<td>ActiveSync</td>
<td>AutoDiscover</td>
</tr>
<tr>
<td>Exchange Web Service</td>
<td>Address Book Service</td>
<td>POP3</td>
</tr>
<tr>
<td>RPC Client Access Service</td>
<td>Remote PowerShell</td>
<td>IMAP4</td>
</tr>
</tbody>
</table>

For simplicity and consistency we recommend that source IP persistence is used for all protocols that require persistence between client and back-end server.

N.B. If your Outlook Web App users pass through a NAT device to reach the load balancer then IP based persistence may not be appropriate since the source IP address may be the same for all users. This would
cause all OWA sessions to be directed to the same backend CAS. In this situation, HTTP cookie persistence can be used. This requires the HTTPS traffic to be terminated on the load balancer to allow the cookie to be read. For more details on this, please refer to the Appendix.

Virtual Service (VIP) Requirements

There are a number of options when deciding on the number of VIPs required for the CAS and HT roles. This deployment guide presents two options as shown below:

Option 1 – Four VIPs (Used for the example configuration in this guide)

This method uses three VIPs for the CAS role, and one VIP for the HT role as follows:

1. CAS role – HTTPS & HTTP services
2. CAS role – RPC services
3. CAS role – IMAP4 or POP3 services (if used / required)
4. HT role – SMTP services

This method allows the settings for each VIP to be customized (e.g. persistence/affinity options) to suit the service being load balanced and also ensures more granular health-checks.

**i** IMAP4 and POP3 are not typically used. Therefore the IMAP4 and POP3 VIPs are not generally required.

Option 2 – Two VIPs (NOT recommended for production deployments)

This method uses two VIPs - one VIP for all CAS services, and one VIP for the HT role. This is useful for rapid deployments and is only recommended for evaluation & testing purposes. For details of this, please refer to section 1 in the Appendix.
Port Requirements

The following table shows the port list that must be load balanced for the CAS and HT roles. Note that some services such as IMAP4 or POP3 may not be used in your environment.

<table>
<thead>
<tr>
<th>TCP Port</th>
<th>Role(s)</th>
<th>Uses</th>
</tr>
</thead>
<tbody>
<tr>
<td>25</td>
<td>HT</td>
<td>SMTP</td>
</tr>
<tr>
<td>80</td>
<td>CAS</td>
<td>HTTP – various</td>
</tr>
<tr>
<td>110</td>
<td>CAS</td>
<td>POP3 clients</td>
</tr>
<tr>
<td>135</td>
<td>CAS</td>
<td>RPC end point mapper</td>
</tr>
<tr>
<td>143</td>
<td>CAS</td>
<td>IMAP4 clients</td>
</tr>
<tr>
<td>443</td>
<td>CAS</td>
<td>HTTPS – various</td>
</tr>
<tr>
<td>993</td>
<td>CAS</td>
<td>Secure IMAP4 clients</td>
</tr>
<tr>
<td>995</td>
<td>CAS</td>
<td>Secure POP3 clients</td>
</tr>
<tr>
<td>60200*</td>
<td>CAS</td>
<td>Static port for RPC client access service</td>
</tr>
<tr>
<td>60201*</td>
<td>CAS</td>
<td>Static port for Exchange address book service</td>
</tr>
</tbody>
</table>

HT = Hub Transport Server, CAS = Client Access Server

* These ports have been chosen as the static RPC ports. Microsoft recommends that any port within the range 59531 to 60554 should be used, and that the same ports should be used on all Client Access Servers within the same AD site.

For a full Exchange Server 2010 port list, please refer to the following Microsoft Technet article: http://technet.microsoft.com/en-us/library/bb331973.aspx

NOTE: If you use Microsoft ISA Server or TMG, you may need to disable the RPC Filter to allow Outlook client RPC related communication to work correctly.
Deployment Overview

There are multiple ways to deploy Exchange, but in this example two servers are used. Each server hosts the CAS & HT roles, as well as the Mailbox role in a DAG configuration. This provides high availability for these three key Exchange roles and uses a minimum number of Exchange servers.

Clients then connect to the Virtual Services (VIPs) on the load balancer rather than connecting directly to one of the Exchange servers. These connections are then load balanced across the Exchange servers to distribute the load according to the load balancing algorithm selected.

The load balancer can be deployed as a single unit, although Loadbalancer.org strongly recommends a clustered pair for resilience & high availability.
Initial Network Configuration

The IP address, subnet mask, default gateway and DNS settings can be configured in several ways as detailed below:

**Method 1 - Using the Network Setup Wizard at the console**

After boot up, follow the instructions on the console to configure the IP address, subnet mask, default gateway and DNS settings.

**Method 2 - Using the WUI:**

Using a browser, connect to the WUI on the default IP address/port: [http://192.168.2.21:9080](http://192.168.2.21:9080)

To set the IP address & subnet mask, use: Local Configuration > Network Interface Configuration

To set the default gateway, use: Local Configuration > Routing

To configure DNS settings, use: Local Configuration > Hostname & DNS

**Method 3 - Using Linux commands:**

At the console, set the initial IP address using the following command:

```
ip addr add <IP address>/mask dev eth0
e.g.
ip addr add 192.168.2.10/24 dev eth0
```

At the console, set the initial default gateway using the following command:

```
route add default gw <IP address> <interface>
e.g.
rout add default gw 192.168.2.254 eth0
```

At the console, set the DNS server using the following command:

```
echo nameserver <IP address> >> /etc/resolv.conf
e.g.
echo nameserver 192.168.2.250 >> /etc/resolv.conf
```

_N.B. If method 3 is used, you must also configure these settings using the WUI, otherwise the settings will be lost after a reboot_
Accessing the Web User Interface (WUI)

The WUI can be accessed from a browser at:  http://192.168.2.21:9080/lbadmin

* Note the port number → 9080

(replace 192.168.2.21 with the IP address of your load balancer if its been changed from the default)

username: loadbalancer
password: loadbalancer

Once you have entered the logon credentials the Loadbalancer.org Web User Interface will be displayed as shown below:
The screen shot below shows the v7.6 WUI once logged in:

**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 6 of the Appendix.

**Load Balancer Deployment Method**

As with several other Microsoft applications, the load balancer for Exchange 2010 is deployed in one-arm SNAT mode (Source Network Address Translation) at layer 7 using HAProxy. This mode is recommended by Microsoft and also has the advantage that it requires no changes to the Exchange 2010 servers.
**NOTE: Source IP Address Transparency**

It's important to remember that when using HAProxy, the source IP address of packets reaching the Exchange servers will be the IP address of the load balancer and not the source IP address of the client.

If this is an issue, please refer to section 4 in the Appendix for details on using Tproxy. Tproxy enables the original source IP address to be maintained, but requires that separate subnets are used, and also requires that the load balancer becomes the default gateway for the Exchange Servers. Enabling Tproxy is a global setting and therefore effects all Virtual Services configured on the load balancer which may not always be desirable.

Transparency is normally only an issue for SMTP traffic at the receive connector. System Administrators typically want to lock down receive connectors to accept SMTP connections only from a controlled set of devices such as external smart mail hosts, printers, networked photocopiers etc.

If transparency for SMTP is the only issue, there are a couple of options available to address this:

**Option 1** – Use a Layer 7 VIP for SMTP as detailed on page 28 of this guide and also enable the load balancers on-board firewall to lock down inbound SMTP connections rather than the receive connector. This is covered in section 2 of the Appendix.

**Option 2** – Configure a layer 4 Virtual Service for SMTP rather than a layer 7 (HAProxy) based Virtual Service. Layer 4 is transparent by default so the source IP address is maintained. This is covered in section 5 of the Appendix.
Exchange 2010 – Configuring for Load Balancing

Step 1 – Configure the CAS Array & Internal / External URL’s

The CAS Array
To enable multiple CAS servers to work with the load balancer, a CAS array must be configured in your Exchange environment using the ‘New-ClientAccessArray’ command as detailed below. Exact configuration details obviously depend on the specific environment.

- Install the CAS 2010 servers
- Create a DNS record for the CAS Array, this should be the same as the Virtual Service’s IP address, e.g. cas.domain.com (also refer to the Load Balancer configuration section starting on page 21)
- Create a new CAS array object using the New-ClientAccessArray command in the Exchange 2010 management shell:

  New-ClientAccessArray –Name "CAS-array" –FQDN "cas.domain.com" -Site “YourSiteName”

  N.B. change “YourSiteName” to the AD site appropriate for your Client Access Servers
  N.B. change “cas.domain.com” to the FQDN of the CAS array
  N.B. to determine your site name:
  ◦ On an Exchange server use: get-adsite
  ◦ On a Domain Controller use: nltest /server:<servername> /dsgetsites
- If the mail database already existed before creating the array, you’ll also need to run the following command to relate the new CAS array to the database:

  Set-MailboxDatabase "NameofDatabase" -RpcClientAccessServer "cas.domain.com"

  N.B. change “cas.domain.com” to the FQDN of the CAS array

To verify the configuration of the CAS array, use the following commands from the Exchange Shell:

- to list the available Client Access Servers:
  get-ClientAccessServer

- to list the Client Access Array and its members:
  get-ClientAccessArray
The Internal & External URL's

Once the CAS Array has been created it's important to remember that clients should then connect using the CAS Array based address rather than individual CAS servers. This applies to both internal and external URL's. The following list provides a number of examples that illustrate how the various URL's can be checked / configured:

Get-OABVirtualDirectory | fl identity, internalurl, externalurl
Set-OABVirtualDirectory -Identity "CAS01\OAB (Default Web Site)" -ExternalUrl "https://cas.domain.com/OAB"

Get-ActiveSyncVirtualDirectory | fl identity, internalurl, externalurl

Get-ClientAccessServer | fl Identity, AutoDiscoverServiceInternalUri
Set-ClientAccessServer -Identity CAS01 -AutoDiscoverServiceInternalUri https://cas.domain.com/Autodiscover/Autodiscover.xml

Get-WebServicesVirtualDirectory | fl identity, internalurl, externalurl
Set-WebServicesVirtualDirectory -Identity "CAS01\EWS (Default Web Site)" -ExternalUrl https://cas.domain.com/ews/exchange.asmx

Get-OWAVirtualDirectory | fl identity, internalurl, externalurl
Set-OWAVirtualDirectory -Identity "CAS01\owa (Default Web Site)" -ExternalUrl https://cas.domain.com/owa

Get-ECPVirtualDirectory | fl identity, internalurl, externalurl
Set-ECPVirtualDirectory -Identity "CAS01\ECP (default web site)" -Externalurl https://cas.domain.com/ecp

Get-ActiveSyncVirtualDirectory | fl identity, internalurl, externalurl
Set-ActiveSyncVirtualDirectory -Identity "CAS01\Microsoft-Server-ActiveSync (Default Web Site)" -ExternalUrl https://cas.domain.com/Microsoft-Server-ActiveSync

Please refer to the following Microsoft article for further details:

Step 2 – Configure Static RPC Ports

By default the RPC Client Access service and the Address Book Service on an Exchange 2010 Client Access Server uses the TCP End Point Mapper port (TCP/135) and the dynamic RPC port range (6005-59530) for outgoing connections when an Outlook clients establishes a connection to Exchange.

Since this would add complexity to the load balancers configuration, and would also uses substantially more on-board memory, it's recommended to configure static ports as described below.

If you later apply a service pack to your Exchange servers, re-check that the settings described in this section are still valid and if required re-configure them.

RPC Client Access Service

To set a static port for the RPC Client Access Service, open the registry on each CAS and navigate to:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\MSExchangeRPC

Here, you need to create a new key named ParametersSystem, and under this key create a new DWORD (32-bit) Value named TCP/IP Port as shown below. The Value for the DWORD should be the port number you want to use. Microsoft recommends you set this to a unique value between 59531 and 60554 and use the same value on all CAS.

In this deployment guide, the port used is 60200.

IMPORTANT!! Make sure you use a DWORD Value for this key

N.B. Once this registry change has been made, restart the RPC Client Access Service to apply the new setting. This process must be completed on all CAS.

If there is a possibility that these ports are already in use, for example if the server was serving clients prior to implementing these changes, then a reboot is recommended rather than a service restart.

N.B. If you have separate Mailbox Servers, the above steps must also followed on these servers. This ensures that static ports are also used for the RPC Client Access service that runs on the Mailbox Servers.

A list of services running on the various roles can be found here:
Exchange Address Book Service (SP1 & later)

To set a static port for the Address Book Service, open the registry on each CAS and navigate to:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\MSExchangeAB

Here, you need to create a new key named Parameters, and under this key create a new String Value named RpcTcpPort as shown below. Microsoft recommends you set this to a unique value between 59531 and 60554 and use the same value on all CAS.

In this deployment guide, the port used is 60201.

IMPORTANT!! Make sure you use a STRING Value for this key

![Registry Editor](image)

N.B. Once this registry change has been made, restart the Address Book Service to apply the new setting. This process will need to be completed on all CAS.

If there is a possibility that these ports are already in use, for example if the server was serving clients prior to implementing these changes, then a reboot is recommended rather than a service restart

Exchange Address Book Service (pre SP1)

For Exchange 2010 without SP1, the static port for the Exchange Address Book service is configured in a different way. First, navigate to the following folder:

C:\Program Files\Microsoft\Exchange Server\V14\Bin

Using Notepad, open the file microsoft.exchange.addressbook.service.exe.config

Now change the value for the key RpcTcpPort to the port you want to use. The ports specified must be different than the port used for the RPC Client Access Service. In this deployment guide the port used is 60201.

![IMPORTANT](image)

IMPORTANT: Once the settings listed in this section have been configured and the services have been restarted, verify that all servers are listening on these newly configured ports by using the following command in a command window on each Exchange server:

```bash
netstat -an -p tcp
```
For more information on configuring & verifying static ports, please refer to the following Microsoft Technet article:


**Step 3 – Configure Send & Receive Connectors**

In cases where there is no Edge Transport server, the Hub Transport server must be configured to accept and send mail. It is possible to send and receive directly to / from the Internet, although a more secure and typical configuration would be to use a 3rd party external smart host. To establish mail flow to and from the Internet through a Hub Transport server the basis steps required are:

1) **Create a Send connector on the Hub Transport server to send e-mail to the Internet**
2) **Modify the default Receive connector to allow anonymous connections**

**Send Connector (using the New-SendConnector cmdlet)**

- To configure a new send connector, open the Exchange Management Shell and run the following command on each server:

  ```powershell
  New-SendConnector -Name "<Name for this send connector>" -Usage Internet -AddressSpaces "*" -SourceTransportServers "<Hub Transport Server Name>" -DNSRoutingEnabled:$true -UseExternalDNSServersEnabled:$true
  ```

**Receive Connector (using the Set-ReceiveConnector cmdlet)**

- To change the permissions of the default receive connector, open the Exchange Management Shell and run the following command on each server:

  ```powershell
  Set-ReceiveConnector -Identity "Default <ServerName>" -PermissionGroups AnonymousUsers
  ```

_N.B. The exact configuration steps required depend on your environment. The commands listed above are provided as examples only._
Step 4 – Microsoft Outlook Client Configuration

All Outlook clients must be configured to connect to the CAS array rather than an individual Client Access Server. To do this, the Exchange Server Connection settings must be modified. If Autodiscover is enabled this configuration should occur automatically, if Autodiscover is not enabled specify the FQDN of the CAS array configured and enter a valid email account in the User Name field.

For example:
STEP 1 – CONFIGURE LAYER 7 GLOBAL SETTINGS

To ensure that client connections remain open during periods of inactivity, the Client and Real Server Timeout values must be changed from their default values of 43 seconds and 45 seconds respectively to 1 hour. To do this follow the steps below:

- Using the WUI, go to Cluster Configuration > Layer 7 – Advanced Configuration

  ![Layer 7 Configuration Screen]

  - Change **Client Timeout** to **3600000** as shown above (i.e. 1 hour)
  - Change **Real Server Timeout** to **3600000** as shown above (i.e. 1 hour)
  - Click the **Update** button to save the settings

This step must be completed to avoid Outlook client timeout & reconnection issues that would otherwise occur within around 45 seconds with unchanged default values.
Step 2 – Configuring the Virtual Services & Real Servers

VIP1 – CAS Role HTTP & HTTPS Services

a) Setting up the Virtual Service

- Using the WUI, go to Cluster Configuration > Layer 7 – Virtual Service and click [Add a New Virtual Service]
- Enter the following details:
  
<table>
<thead>
<tr>
<th>Label</th>
<th>CAS-WEB</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual Service IP Address</td>
<td>192.168.30.10</td>
</tr>
<tr>
<td>Ports</td>
<td>80,443</td>
</tr>
<tr>
<td>Layer 7 Protocol</td>
<td>TCP Mode</td>
</tr>
</tbody>
</table>
  
  - Enter an appropriate label for the VIP, e.g. CAS-WEB
  - Set the Virtual Service IP address field to the required IP address, e.g. 192.168.30.10
  - Set the Virtual Service Ports field to 80,443
  - Set Layer 7 Protocol to TCP Mode
  - Click Update
  
- Now click [Modify] next to the newly created VIP
- Set Balance mode to Weighted Round Robin

NOTE: Microsoft recommends that ‘Round Robin’ rather than ‘Least Connection’ should be used to help prevent over loading servers when they are brought online. This could occur if Least Connection was selected, since the load balancer would try to balance the number of connections across all real severs and therefore send all new requests to the new server. The trade off here is that using Round Robin will mean that server load may remain unbalanced for some time after bringing a new server into the active pool.

- Set Persistence mode to Source IP
- Change Persistence Timeout to 60 (i.e. 1 hour)
- Click Update
b) Setting up the Real Servers

- Using the WUI, go to Cluster Configuration > Layer 7 – Real Servers and click [Add a new Real Server] next to the newly created VIP
- Enter the following details:

<table>
<thead>
<tr>
<th>Label</th>
<th>CAS1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Real Server IP Address</td>
<td>192.168.30.20</td>
</tr>
<tr>
<td>Real Server Port</td>
<td></td>
</tr>
<tr>
<td>Weight</td>
<td>100</td>
</tr>
</tbody>
</table>

- Enter an appropriate label for the RIP, e.g. **CAS1**
- Change the **Real Server IP Address** field to the required IP address, e.g. **192.168.30.20**
- Leave the **Real Server Port** field blank
- Click **Update**
- Repeat the above steps to add your other CAS Server(s)

**NOTE:** Because SNAT is a full proxy, any server in the cluster can be on any accessible subnet including across the Internet or WAN.
VIP2 – CAS Role RPC Services

a) Setting up the Virtual Service

- Using the WUI, go to *Cluster Configuration > Layer 7 – Virtual Service* and click *Add a New Virtual Service*
- Enter the following details:

<table>
<thead>
<tr>
<th>Label</th>
<th>CAS-RPC</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual Service IP Address</td>
<td>192.168.30.10</td>
</tr>
<tr>
<td>Ports</td>
<td>135,60200,60201</td>
</tr>
<tr>
<td>Layer 7 Protocol</td>
<td>TCP Mode</td>
</tr>
</tbody>
</table>

  - Enter an appropriate label for the VIP, e.g. **CAS-RPC**
  - Set the *Virtual Service IP address* field to the required IP address, e.g. **192.168.30.10**
  - Set the *Virtual Service Ports* field to **135,60200,60201**
  - Set *Layer 7 Protocol* to **TCP Mode**
  - Click **Update**
  - Now click [Modify] next to the newly created VIP
  - Set *Balance mode* to **Weighted Round Robin**

**NOTE:** Microsoft recommends that 'Round Robin' rather than 'Least Connection' should be used to help prevent over loading servers when they are brought online. This could occur if Least Connection was selected, since the load balancer would try to balance the number of connections across all real servers and therefore send all new requests to the new server. The trade off here is that using Round Robin will mean that server load may remain unbalanced for some time after bringing a new server into the active pool.

- Set *Persistence mode* to **Source IP**
- Change *Persistence Timeout* to 60 (i.e. 1 hour)
- Set *Check Port* to **60200** (i.e. the static port used for the RPC client access service)
- Click **Update**
b) Setting up the Real Servers

• Using the WUI, go to *Cluster Configuration > Layer 7 – Real Servers* and click [Add a new Real Server] next to the newly created VIP
• Enter the following details:

<table>
<thead>
<tr>
<th>Field</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Label</td>
<td>CAS1</td>
</tr>
<tr>
<td>Real Server IP Address</td>
<td>192.168.30.20</td>
</tr>
<tr>
<td>Real Server Port</td>
<td>blank</td>
</tr>
<tr>
<td>Weight</td>
<td>100</td>
</tr>
</tbody>
</table>

• Enter an appropriate label for the RIP, e.g. **CAS1**
• Change the *Real Server IP Address* field to the required IP address, e.g. **192.168.30.20**
• Leave the *Real Server Port* field blank
• Click **Update**
• Repeat the above steps to add your other CAS Server(s)

**NOTE:** Because SNAT is a full proxy, any server in the cluster can be on any accessible subnet including across the Internet or WAN.
VIP3 – CAS Role IMAP4 or POP3 Services

a) Setting up the Virtual Service

N.B. these steps show IMAP4 settings, for POP3 change the port numbers from 143 & 993 to 110 & 995

- Using the WUI, go to Cluster Configuration > Layer 7 – Virtual Service and click [Add a New Virtual Service]
- Enter the following details:

<table>
<thead>
<tr>
<th>Label</th>
<th>CAS-IMAP4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual Service</td>
<td>192.168.30.10</td>
</tr>
<tr>
<td>Ports</td>
<td>143,993</td>
</tr>
<tr>
<td>Layer 7 Protocol</td>
<td>TCP Mode</td>
</tr>
</tbody>
</table>

- Enter an appropriate label for the VIP, e.g. **CAS-IMAP4**
- Set the Virtual Service IP address field to the required IP address, e.g. **192.168.30.10**
- Set the Virtual Service Ports field to **143,993**
- Set Layer 7 Protocol to **TCP Mode**
- Click Update
- Now click [Modify] next to the newly created VIP
- Set Balance mode to **Weighted Round Robin**

![Virtual Service Configuration Table]

**NOTE:** Microsoft recommends that 'Round Robin' rather than 'Least Connection' should be used to help prevent over loading servers when they are brought online. This could occur if Least Connection was selected, since the load balancer would try to balance the number of connections across all real servers and therefore send all new requests to the new server. The trade off here is that using Round Robin will mean that server load may remain unbalanced for some time after bringing a new server into the active pool.

- Click Update

N.B. persistence is not required for IMAP or POP3
b) Setting up the Real Servers

- Using the WUI, go to Cluster Configuration > Layer 7 – Real Servers and click [Add a new Real Server] next to the newly created VIP.
- Enter the following details:

```
<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Label</td>
<td>CAS1</td>
</tr>
<tr>
<td>Real Server IP Address</td>
<td>192.168.30.20</td>
</tr>
<tr>
<td>Real Server Port</td>
<td>Blank</td>
</tr>
<tr>
<td>Weight</td>
<td>100</td>
</tr>
</tbody>
</table>
```

- Enter an appropriate label for the RIP, e.g. **CAS1**.
- Change the **Real Server IP Address** field to the required IP address, e.g. **192.168.30.20**.
- Leave the **Real Server Port** field blank.
- Click **Update**.
- Repeat the above steps to add your other CAS Server(s).

**NOTE:** Because SNAT is a full proxy, any server in the cluster can be on any accessible subnet including across the Internet or WAN.
VIP4 – HT Role SMTP Services

NOTE: Source IP Address Transparency

It’s important to remember that when using HAProxy, the source IP address of packets reaching the Exchange servers will be the IP address of the load balancer and not the source IP address of the client. If this is an issue, please refer to section 4 in the Appendix for details on using Tproxy. Tproxy enables the original source IP address to be maintained, but requires that separate subnets are used, and also requires that the load balancer becomes the default gateway for the Exchange Servers. Enabling Tproxy is a global setting and therefore effects all Virtual Services configured on the load balancer which may not always be desirable.

Transparency is normally only an issue for SMTP traffic at the receive connector. System Administrators typically want to lock down receive connectors to accept SMTP connections only from a controlled set of devices such as external smart mail hosts, printers, networked photocopiers etc. If transparency for SMTP is the only issue, there are a couple of options available to address this:

Option 1 – Use a Layer 7 VIP for SMTP as detailed below and also enable the load balancers on-board firewall to lock down inbound SMTP connections rather than the receive connector. This is covered in section 2 of the Appendix.

Option 2 – Configure a layer 4 Virtual Service for SMTP rather than a layer 7 (HAProxy) based Virtual Service. Layer 4 is transparent by default so the source IP address is maintained. This is covered in section 5 of the Appendix.

a) Setting up the Virtual Service

- Using the WUI, go to Cluster Configuration > Layer 7 – Virtual Service and click [Add a New Virtual Service]
- Enter the following details:

<table>
<thead>
<tr>
<th>Label</th>
<th>HT-SMTP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual Service IP Address</td>
<td>192.168.111.10</td>
</tr>
<tr>
<td>Ports</td>
<td>25</td>
</tr>
<tr>
<td>Layer 7 Protocol</td>
<td>TCP Mode</td>
</tr>
</tbody>
</table>

- Enter an appropriate label for the VIP, e.g. HT-SMTP
- Set the Virtual Service IP address field to the required IP address, e.g. 192.168.30.10
- Set the Virtual Service Ports field to 25
- Set Layer 7 Protocol to TCP Mode
- Click Update

N.B. persistence is not required for SMTP
b) Setting up the Real Servers

- Using the WUI, go to Cluster Configuration > Layer 7 – Real Servers and click [Add a new Real Server] next to the newly created VIP.
- Enter the following details:

  ![Real Server Configuration Table]

  - Enter an appropriate label for the RIP, e.g. HT1
  - Change the Real Server IP Address field to the required IP address, e.g. 192.168.30.20
  - Change the Real Server Port field to 25
  - Click Update
  - Repeat the above steps to add your other HT Server(s)

NOTE: Because SNAT is a full proxy, any server in the cluster can be on any accessible subnet including across the Internet or WAN.
Step 3 – Finalizing the Configuration

To apply the new settings, HAProxy must be restarted as follows:

- Go to Maintenance > Restart Services and click Restart HAPerxy

Microsoft Exchange Testing Tool

The Exchange Remote Connectivity Analyzer tool, available at https://www.testexchangeconnectivity.com/ is a useful Web-based Microsoft tool designed to help IT Administrators troubleshoot connectivity issues with their Exchange Server deployments. The tool simulates several client logon and mail flow scenarios. When a test fails, many of the errors have troubleshooting tips to assist the IT Administrator in correcting the problem.

Technical Support

For more details or assistance with your deployment please don’t hesitate to contact the support team at the following email address: support@loadbalancer.org

Conclusion

Loadbalancer.org appliances provide a very cost effective solution for highly available load balanced Exchange 2010 environments.
Appendix

1 – Configuring the Load balancer using a single VIP for all CAS Services

For testing purposes it's also possible to configure the load balancer with a single VIP for all CAS services. The basic steps to create the VIP & associated RIPS are the same as described previously, the only difference is that all ports would be specified in one VIP as shown below:

N.B. this configuration is not recommended for production deployments

<table>
<thead>
<tr>
<th>Label</th>
<th>CAS-AllServices</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual Service</td>
<td>IP Address 192.168.30.20</td>
</tr>
<tr>
<td>Ports</td>
<td>80,110,135,143,443,993,995,60200,60201</td>
</tr>
<tr>
<td>Layer 7 Protocol</td>
<td>TCP Mode</td>
</tr>
</tbody>
</table>

N.B. the full list of ports in the 'Virtual Service Ports' field is: 80,110,135,143,443,993,995,60200,60201
2 – Limiting inbound SMTP Connections using Firewall Rules

Since layer 7 is not transparent by default, it’s not possible to filter inbound SMTP connections by IP address at the receive connector on the Hub Transport Server. One way to address this is to add firewall rules to the load balancer to limit which hosts can connect inbound on port 25.

Rules can be added using the WUI option: Maintenance > Firewall Script. Simply copy/paste/edit the examples below into the firewall script then click Update.

**EXAMPLES:**

1) to limit inbound SMTP connections to a specific smart host:

VIP1="192.168.30.10"
SRC1="192.168.30.50"

iptables -A INPUT -p tcp --src $SRC1 --dst $VIP1 --destination-port 25 -j ACCEPT
iptables -A INPUT -p tcp --dport 25 -j DROP

*These rules will only allow SMTP traffic from the host 192.168.30.50 to reach the 192.168.30.10 VIP.*

2) to limit inbound SMTP connections to a range of smart hosts:

VIP1="192.168.30.10"
SRC1="192.168.30.50-60"

iptables -A INPUT -p tcp -m iprange --src-range $SRC1 --destination $VIP1 --destination-port 25 -j ACCEPT
iptables -A INPUT -p tcp --dport 25 -j DROP

*These rules will only allow SMTP traffic from hosts in the range 192.168.30.50 through 192.168.30.60 to reach the 192.168.30.10 VIP.*

3 – Using HTTP Cookie Persistence for OWA Users

If IP persistence cannot be used for OWA (e.g. if clients pass through a NAT device), HTTP cookie persistence can be used as an alternative. To use cookie persistence, the SSL stream must be decrypted on the load balancer to enable the cookies to be inserted / read. For more details on setting this up, refer to configuration/deployment example 3 in the administration manual.

---

**i** SSL termination on the load balancer can be very CPU intensive. Therefore this is only advised when IP persistence is not possible. In most cases, for a scalable solution terminating SSL on the real servers is the best option.
4 – Enabling full Transparency using Tproxy

If a fully transparent configuration is required, Tproxy can be used. The main point to note is that two subnets must be used for Tproxy to work correctly.

**Key points to consider:**

- The Exchange servers must be on a different subnet to the VIP – this can achieved by using 2 IP addresses assigned to a single interface, or two separate interfaces (eth0 & eth1)
- The default gateway on the Exchange servers **must** be configured to be an IP address on the load balancer. For a clustered pair of load balancers, it’s best to add an additional floating IP for this to allow failover to the slave
- Tproxy must be enabled. Using the WUI go to *Cluster Configuration > Layer 7 – Advanced Configuration*, check **Transparent Proxy** and click **Update**
5 – Using a Layer 4 Virtual Service for the HT Role

This guide uses Layer 7 HAProxy based Virtual Services for all load balanced services. Layer 7 Virtual Services are not transparent by default which can be an issue for the HT role. In these cases a Layer 4 VIP can be used instead. There are two possibilities: DR (Direct Return) mode and NAT (Network Address Translation) mode.

Layer 4 – DR Mode

DR mode works by changing the MAC address to match one of the real servers on the fly. DR mode requires that the ‘ARP issue’ is solved on each real server. This involves configuring the network stack of each real server to accept packets destined for the VIP address, but not to reply to ARP requests for this address. DR mode requires that the VIP & associated RIP are located in the same switch fabric / logical network. They can be on different subnets, provided there are no router hops between them. If multiple subnets are used, an IP address in each subnet must be defined on the load balancer.

Layer 4 – NAT Mode

NAT mode works by changing the destination address of inbound packets from the VIP address to be one of the load balanced real server IP addresses, and by changing real server response packets from the real address back to the VIP address. NAT mode requires the VIP and associated RIPS to be in different subnets and also the default gateway on each real server must be set to be the load balancer.

For examples of setting up layer 4 Virtual Services, please refer to the configuration/deployment examples in the administration manual.

6 – 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 document referenced below for more details:

Version 7

Please refer to Chapter 8 – Appliance Clustering for HA in the v7 Administration Manual.

Version 8

Please refer to Chapter 9 – Appliance Clustering for HA in the v8 Administration Manual.

Don’t hesitate to contact our support team if you need further assistance: support@loadbalancer.org
# 7 – Company Contact Information

<table>
<thead>
<tr>
<th>Website</th>
<th>URL : <a href="http://www.loadbalancer.org">www.loadbalancer.org</a></th>
</tr>
</thead>
</table>
| **North America (US)** | Loadbalancer.org, Inc.  
270 Presidential Drive  
Wilmington,  
DE 19807  
USA  
Tel : +1 888.867.9504 (24x7)  
Fax : +1 302.213.0122  
Email (sales) : sales@loadbalancer.org  
Email (support) : support@loadbalancer.org |
| **North America (Canada)** | Loadbalancer.org Ltd.  
300–422 Richards Street  
Vancouver, BC  
V6B 2Z4  
Canada  
Tel : +1 855 681.6017 (24x7)  
Fax : +1 302.213.0122  
Email (sales) : sales@loadbalancer.org  
Email (support) : support@loadbalancer.org |
| **Europe (UK)** | Loadbalancer.org Ltd.  
Portsmouth Technopole  
Kingston Crescent  
Portsmouth  
PO2 8FA  
England, UK  
Tel : +44 (0)330 3801064 (24x7)  
Fax : +44 (0)870 4327672  
Email (sales) : sales@loadbalancer.org  
Email (support) : support@loadbalancer.org |
| **Europe (Germany)** | Loadbalancer.org GmbH  
Alt Pempelfort 2  
40211 Düsseldorf  
Germany  
Tel : +49 (0)30 920 383 6494  
Fax : +49 (0)30 920 383 6495  
Email (sales) : vertrieb@loadbalancer.org  
Email (support) : support@loadbalancer.org |