Microsoft Exchange 2010 Deployment Guide

Copyright © 2011 Loadbalancer.org, Inc.
Table of Contents

Exchange Server 2010.................................................................................................................................................. 3
Exchange 2010 Server Roles........................................................................................................................................ 3
Client Access Server.................................................................................................................................................. 3
Hub Transport Server.................................................................................................................................................. 3
Mailbox Server / Database Availability Group’s (DAG).................................................................................................. 4
Load Balancing Exchange......................................................................................................................................... 4
The Basics.................................................................................................................................................................. 4
  Which Roles?.......................................................................................................................................................... 4
  One VIP Per Role.................................................................................................................................................. 4
  Persistence (aka Server Affinity)........................................................................................................................... 4
Port Requirements....................................................................................................................................................... 5
Deployment Architecture........................................................................................................................................ 6
Exchange Configuration........................................................................................................................................ 6
CAS Array............................................................................................................................................................... 6
Static RPC Ports........................................................................................................................................................ 7
  RPC Client Access Service................................................................................................................................... 7
  Exchange Address Book Service.......................................................................................................................... 7
Send & Receive Connectors....................................................................................................................................... 9
  Send Connector.................................................................................................................................................... 9
  Receive Connector............................................................................................................................................... 9
Outlook Client Configuration..................................................................................................................................... 10
Loadbalancer.org Appliance Configuration............................................................................................................ 11
Accessing the WUI.................................................................................................................................................... 11
Configuring the Virtual Servers................................................................................................................................ 12
  CAS Virtual Server (VIP)....................................................................................................................................... 12
  HT Virtual Server (VIP)....................................................................................................................................... 13
Configure the Real Servers....................................................................................................................................... 14
  CAS Real Servers............................................................................................................................................... 14
  HT Real Servers............................................................................................................................................... 14
Configure Global Settings......................................................................................................................................... 15
Finalizing the Configuration...................................................................................................................................... 16
3rd Party Testing Tool................................................................................................................................................. 16
Conclusion................................................................................................................................................................. 16
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.</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

The Basics

Which Roles?

The CAS 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.

One VIP Per Role

There are several different ways to configure the load balancer for the CAS & HT roles. The method used in this guide is to have one Virtual Server (VIP) per role. This allows health check ports to be defined per role. It is possible to divide Exchange services between a larger number of VIPs although this can be an unnecessary complication. However, in some circumstances it may be required to do this. For example, if a different persistence method is needed for a particular client type, e.g. Outlook Web App may require cookie persistence, then a separate VIP would need to be configured to allow a different method to be specified.

Persistence (aka Server Affinity)

Some Exchange 2010 protocols require affinity and others don’t. For those that do, the recommended method to provide affinity between clients and servers is by using source IP persistence. If multiple clients come from the same IP address, then this method of persistence would not be appropriate and an alternative would need to be used. In these cases, cookie persistence is a good candidate for most client types. This guide uses IP persistence throughout.
Port Requirements

The following table shows the ports that must be load balanced for the CAS and HT roles:

<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>SSL - 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>6001</td>
<td>CAS</td>
<td>RPC related - outlook anywhere (RPC client access service)</td>
</tr>
<tr>
<td>6002</td>
<td>CAS</td>
<td>RPC related - Outlook anywhere (NspiHTTPPort)</td>
</tr>
<tr>
<td>6004</td>
<td>CAS</td>
<td>RPC related - outlook anywhere (RfrHTTPPort)</td>
</tr>
<tr>
<td>60200*</td>
<td>CAS</td>
<td>RPC client access service</td>
</tr>
<tr>
<td>60201*</td>
<td>CAS</td>
<td>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 (see the Static RPC Ports section on page 7 & 8).

Deployment Architecture

There are multiple ways to deploy Exchange, but in this example 2 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.

Exchange Configuration

CAS Array

To enable multiple CAS servers to work with the load balancer, a CAS array must be configured. The steps to do this are 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 Server's IP address, e.g. cas.domain.com (also refer to the Load Balancer configuration section below)
- 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 “site1”
- 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”
**Static RPC Ports**

To enable the load balancer to have a predefined set of ports to load balancer, static ports need to be configured on all Client Access Servers in the CAS array. Once RPC port changes have been made, it's recommended to restart the Exchange servers to make sure changes have been applied.

**RPC Client Access Service**

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

To set a static port for the RPC CA service on a CAS server, you need to open the registry on the respective CAS server in the CAS array 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 `REG_DWORD` named `TCP/IP Port`. 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 any one AD site. In this deployment guide, the port used is 60200.

**Exchange Address Book Service**

By default the Exchange Address Book service on the Client Access server in Exchange 2010 uses the TCP End Point Mapper (TCP/135) and the dynamic RPC port range (6005-59530) for outgoing connections, when an Outlook client establish a connection to Exchange. To set a static port for the Exchange Address Book service, using notepad open the file `microsoft.exchange.addressbook.service.exe.config` located in:

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

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.

**NOTE – Exchange 2010 SP1**

With Exchange 2010 SP1, you no longer edit `Microsoft.exchange.addressbook.service.exe.config` to assign the static RPC port for the Exchange Address Book Service. Instead, you do so by creating a new `REG_SZ` registry key named “RpcTcpPort” under:
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\MSExchangeAB\Parameters

Then define the port within the registry key. i.e. for this guide, set to 60201.

N.B. For more information please refer to the following Microsoft link:


IMPORTANT : Verify that both static RPC ports have been opened correctly by using the following command in a command window on each Exchange server: `netstat -an -p tcp`
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 Exchange Management Shell:

- Open Exchange Management Shell and run below mentioned command.
- `New-SendConnector -Name "<Name for this send connector>" -Usage Internet -AddressSpaces "*" -SourceTransportServers "<Hub Transport Server Name>" -DNSRoutingEnabled:$true -UseExternalDNSServersEnabled:$true`

Receive Connector

Using the Exchange Management Shell:

- Open Exchange Management Shell and run below mentioned command.
- `Set-ReceiveConnector -Name "Default Server Name" -Server "<Hub Transport Server Name>" -PermissionGroups AnonymousUsers,ExchangeUsers,ExchangeServers,ExchangeLegacyServers`

_N.B. The exact configuration steps required depend on your environment. The steps listed here are meant as an example._
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. Just set the Exchange Server to the array name, in this guide this is cas.domain.com.

For example:
Loadbalancer.org Appliance Configuration

As per Microsoft's recommendation, the load balancer is configured in SNAT mode (Source Network Address Translation). This is accomplished by configuring a Layer 7 Virtual Service using HAproxy.

All configuration is completed via the Web User Interface.

Accessing the WUI

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)

Username: loadbalancer
Password: loadbalancer

Once you have entered the logon credentials the Loadbalancer.org Web User Interface will be displayed.
Configuring the Virtual Servers

CAS Virtual Server (VIP)

- Go to Edit Configuration > Virtual Servers (HAProxy)
- Click [Add a new Virtual Server]
- Type an appropriate name for the Virtual Server, e.g. CAS
- Enter an IP address for the VIP followed by :80 (e.g. 192.168.2.179:80), the other ports will be specified later
- Change the persistence mode to Source IP
- Click the Update button
- Now click [Modify] next to the newly created Virtual Server
- In the Extra Ports field enter the additional ports separated by commas: 110,135,143,443,993,995,6001,6002,6004,60200,60201
- Set the balance mode according to your needs (recommended: Round Robin)

*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.*

- Set the Check Port to 80
- Click the Update button

<table>
<thead>
<tr>
<th>Label</th>
<th>CAS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual Server (ipaddress:port)</td>
<td>192.168.2.179:80</td>
</tr>
<tr>
<td>Extra Ports</td>
<td>110,135,143,443,993,995,6001,6002,6004,60200,60201</td>
</tr>
<tr>
<td>Persistence mode</td>
<td>Source IP</td>
</tr>
<tr>
<td>Balance mode</td>
<td>Round Robin</td>
</tr>
<tr>
<td>Timeout</td>
<td>30</td>
</tr>
<tr>
<td>Table Size</td>
<td>10240</td>
</tr>
<tr>
<td>Fallback</td>
<td>127.0.0.1:9081</td>
</tr>
<tr>
<td>Check Port</td>
<td>80</td>
</tr>
<tr>
<td>F ) to check</td>
<td></td>
</tr>
<tr>
<td>Response expected</td>
<td></td>
</tr>
<tr>
<td>Maximum Connections</td>
<td></td>
</tr>
</tbody>
</table>
**HT Virtual Server (VIP)**

- Go to *Edit Configuration > Virtual Servers (HAProx)*
- Click [*Add a new Virtual Server*]
- Type an appropriate name for the Virtual Server, e.g. HT
- Enter an IP address for the VIP followed by :25 (e.g. 192.168.2.180:25), the other ports will be specified later
- Change the persistence mode to Source IP
- Click the Update button
- Now click [*Modify*] next to the newly created Virtual Server
- Set the balance mode according to your needs (recommended: Least Connection)
- Set the Check Port to 25
- Click the Update button
Configure the Real Servers

CAS Real Servers

- Go to Edit Configuration > Real Servers (HAProxy)
- Click [Add a new Real Server] next to the CAS Virtual Server
- Type an appropriate name for the server, e.g. CAS-Real-1
- Enter the IP address without specifying a port (e.g. 10.20.1.1)
- Click the Update button
- Now repeat for your other real servers

HT Real Servers

- Go to Edit Configuration > Real Servers (HAProxy)
- Click [Add a new Real Server] next to the HT Virtual Server
- Type an appropriate name for the server, e.g. HT-Real-1
- Enter the IP address without specifying a port (e.g. 10.20.1.1)
- Click the Update button
- Now repeat for your other real server(s)

Once all servers have been configured, the list should look something similar to the following:

<table>
<thead>
<tr>
<th>CAS</th>
<th>(192.168.2.179:60)</th>
<th>[ Add a new Real Server ]</th>
</tr>
</thead>
<tbody>
<tr>
<td>CAS-Real-2</td>
<td>10.20.1.2</td>
<td>1</td>
</tr>
<tr>
<td>CAS-Real-1</td>
<td>10.20.1.1</td>
<td>1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>HT</th>
<th>(192.168.2.180:25)</th>
<th>[ Add a new Real Server ]</th>
</tr>
</thead>
<tbody>
<tr>
<td>HT-Real-2</td>
<td>10.20.1.2</td>
<td>1</td>
</tr>
<tr>
<td>HT-Real-1</td>
<td>10.20.1.1</td>
<td>1</td>
</tr>
</tbody>
</table>

Note: Because SNAT is a full proxy any server in the cluster can be on any accessible subnet including across the Internet or WAN
Configure Global Settings

Change the clitimeout and srvtimeout values from 43000 to 3600000 (i.e. 1 hour) as follows:

- Go to Edit Configuration > Global Settings
- Change clitimeout to 3600000
- Change srvtimeout to 3600000
- Click the Update button

This sets the maximum client & server inactivity (idle) timeouts.
Finalizing the Configuration

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

- Go to Maintenance > Restart HAProxy

3rd Party 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.

Conclusion

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

If you have further questions please don't hesitate to contact us at support@loadbalancer.org.