Citrix NetScaler Deployment Guide for Microsoft Exchange 2010
Table of Contents
Citrix NetScaler Deployment Guide for Microsoft Exchange 2010 ............................................. 1
Introduction ............................................................................................................................................ 3
Solution Requirements .......................................................................................................................... 3
Prerequisites .......................................................................................................................................... 3
Deployment Overview .......................................................................................................................... 4
Network Diagram .................................................................................................................................. 7
NetScaler Deployment .......................................................................................................................... 7
Client Access Server ............................................................................................................................ 7
  Configuring NetScaler for Outlook Web App (OWA) ......................................................................... 9
  Configuring NetScaler for Microsoft Exchange ActiveSync (AS) ....................................................... 22
  Configuring NetScaler for Microsoft Outlook Anywhere (OA) .......................................................... 23
  Configuring NetScaler for IMAP4 ......................................................................................................... 24
  Configuring NetScaler with POP3 ......................................................................................................... 28
  Configuring NetScaler for RPC Client Access .................................................................................... 32
Edge Transport Servers ....................................................................................................................... 34
  Configuring NetScaler for Edge Transport Servers ........................................................................... 34
  Configuring NetScaler GSLB with Edge Transport Servers in multiple Data Centers ....................... 36
NetScaler Management Pack Deployment .......................................................................................... 43
  Introduction ......................................................................................................................................... 43
  Dependencies ....................................................................................................................................... 44
  Prerequisites ....................................................................................................................................... 44
  Installing Citrix NetScaler Management Pack .................................................................................... 44
  Importing Management Packs ........................................................................................................... 46
  Setting Up Security ............................................................................................................................. 46
  Override MP for Customizations ......................................................................................................... 47
  How it Works ....................................................................................................................................... 48
Introduction
Citrix® NetScaler® optimizes the delivery of Web applications—increasing security, improving performance, and expanding Web server capacity. This approach ensures the best total cost of ownership (TCO), security, availability, and performance for Web applications. The Citrix NetScaler solution is a comprehensive network system that combines high-speed load balancing and content switching with state-of-the-art application acceleration, layer 4-7 traffic management, data compression, dynamic content caching, SSL acceleration, network optimization, and robust application security to provide a single, tightly integrated solution. Deployed in front of application servers, the NetScaler significantly reduces processing overhead on application and database servers, resulting in reduced hardware and bandwidth costs.

The purpose of this guide is to help you deploy NetScaler for load balancing Microsoft® Exchange 2010 Client Access servers. Configuration can be performed by using the web-based configuration utility or the command-line interface (CLI).

Within the Exchange 2010 server architecture, a NetScaler is located in front of the Client Access servers with one single virtual IP address and balances the traffic across the Client Access server pool. Exchange client traffic is bound to a Client Access server through NetScaler. Each Client Access server within the Client Access server pool handles the server applications, security, authentication, and connection and protocol processing. The Mailbox server at the back end handles the mailbox data, such as mail and contacts. Therefore, the same client can be processed by any Client Access server in the pool at any given time.

For readers less familiar with the architecture of Exchange 2010, Microsoft provides a useful overview at http://www.msteched.com/resources/Content_Files/exchange2010.pptx.

Solution Requirements
- Citrix NetScaler or Citrix NetScaler VPX
- Microsoft Exchange 2010 Client Access Server, Server, Edge Transport Server and Hub Transport Server. (Note: One Exchange 2010 system can implement multiple server roles.)

Prerequisites
- Citrix NetScaler running version 9.0 build 61.9 or later (Quantity x 2 for HA)
- Client laptop/workstation running various Microsoft Exchange clients. ActiveSync will require Apple iPhone, handheld running Microsoft Windows Mobile or other Exchange-compatible software.
In cases where it is impractical to deploy actual clients, you may be able to use Microsoft’s online Microsoft Exchange Server Remote Connectivity Analyzer to simulate the end-user protocols. That service can be found at https://www.testexchangeconnectivity.com/.

Deployment Overview
This deployment guide provides the NetScaler configuration for the front-end Microsoft Exchange 2010 Client Access servers and Edge Transport servers. This guide does not explain Microsoft Exchange server deployment or the components in the Client Access server or Edge Transport server deployments. Be sure to follow the Microsoft Exchange 2010 Planning guide to deploy the Exchange components.

In accordance with the Microsoft Exchange Planning Guide, the NetScaler will parse the headers of all the incoming requests and decide which Client Access or Edge Transport servers to send the request. In addition, NetScaler provides security and protection for the Client Access or Edge Transport systems and increases server performance and efficiency.

NetScaler can provide the following key benefits:

- Improved L4 through L7 Performance. Provides 15+ gigabits per second (Gbps) throughput.
- Maximum Feature Concurrency. Supports complex policies by using features such as compression, content switching, and application firewall.
- Accelerated Application Response. Provides advanced compression, TCP optimization, and static and dynamic caching to speed application performance.
- Integrated Application Security. Provides an application firewall feature to block attacks against Web applications.
- Improved Datacenter Efficiency. Accelerates datacenter performance by offloading compute-intensive TCP connection set-up and teardown operations. NetScaler supports Secure Socket Layer (SSL) key generation and bulk encryption to improve server efficiency.

Follow the specific instructions in this guide for configuring a load balancing setup for the Client Access server components. Load balancing improves server fault tolerance and end-user response time. The load balancing feature distributes client requests across multiple servers to optimize resource utilization and improve server performance. NetScaler uses load balancing criteria to accelerate the application response time by forwarding each client request to the server best suited to handle the request when it arrives. The load balancing feature provides traffic management from Layer 4 (TCP and UDP) through Layer 7 (FTP, HTTP, and HTTPS).

The basic building blocks of a typical load balancing configuration are services and load balancing virtual servers. The services represent the applications on the servers. The virtual servers abstract the servers by providing a single IP address to which the clients connect. To ensure that client requests are sent to a server, you must create services for every server and bind the services to the virtual server. To connect to a NetScaler appliance, clients use the IP address of the virtual server and the virtual IP address (VIP). When the NetScaler appliance receives client requests on the VIP, it sends the requests to a server determined by the load balancing algorithm. Load balancing uses a virtual entity called a monitor to track whether a specific service (server plus application) is available to receive requests. By default, the NetScaler binds a monitor to each service. Alternatively, you can create customized monitors to suit your requirements.

To configure load balancing, you typically need to perform the following steps:

- Create customized monitors to track the health of the back-end servers (optional).
- Create services that represent applications on the back-end servers.
- Create a virtual server to abstract the back-end servers.

A load balancing setup can be configured by using the following NetScaler user interfaces:

- Configuration utility. You connect to the configuration utility using a web browser. The Java Runtime Environment (JRE) 1.4 or greater is required on the client system running the web-based configuration utility. The configuration utility runs as a Java application.
- Command-line interface (CLI). You connect a workstation or laptop computer to the NetScaler by using the supplied serial cable, and then connect to the CLI by using terminal emulation software. You can also use
secure shell (SSH) to access the CLI via IP when configuring a physical or virtual NetScaler.

**Note:** This guide provides configuration instructions by using the configuration utility. Many configuration sections also include a summary of NetScaler commands.

To launch the configuration utility

- Connect the NetScaler to a management workstation or network.
- Open a browser and type: http://<IP address of the NetScaler>
- Type the appropriate user name and password in User Name and Password, respectively. By default, the user name and password are nsroot.
- In Start in, select Configuration.
- Click Login.
Network Diagram

A NetScaler appliance resides between the clients and the Client Access and Edge Deployment servers, so that client requests and server responses pass through it. The NetScaler ensures optimal distribution of client traffic by the way it directs client requests. You can segment application traffic according to information in the body of an HTTP or TCP request, and on the basis of L4-L7 header information, such as URL, application data type, or cookie. Numerous load balancing algorithms and extensive server health checks provide greater application availability by ensuring that client requests are directed to the appropriate servers. The following network diagram illustrates the Citrix NetScaler deployment in a typical Exchange 2010 enterprise deployment. Requests originate from the clients and go through the NetScaler to the Client Access servers. Client Access servers get all the information from the backend Exchange components and respond to the incoming request.

NetScaler Deployment

The following sections provide instructions for configuring the NetScaler for Client Access servers and Edge Transport servers.

Client Access Server

The Client Access server role is one of five distinct server roles for Exchange 2010. The Client Access server role accepts connections to your Exchange 2010 server from different clients. Software clients such as Microsoft Outlook Express and Eudora use POP3 or IMAP4 connections to communicate with the
Exchange server. Hardware clients, such as mobile phones, use ActiveSync, POP3, or IMAP4 to communicate with the Exchange server. You must install the Client Access server role in every Exchange organization and every Active Directory site that has the Mailbox server role installed.

This deployment guide provides instructions on how to configure NetScaler to handle connections from the following clients to the Client Access servers:

- **Outlook Web App in Exchange 2010.** Provides access to e-mail from any Web browser. Outlook Web App has been redesigned in Exchange 2010. Features such as chat, text messaging, mobile phone integration, and enhanced conversation view, provide an enhanced user experience from any computer that has a web browser.

- **Microsoft Exchange ActiveSync client applications.** Synchronizes data between your mobile phone and Exchange 2010. You can synchronize e-mail, contacts, calendar information, and tasks.

- **Microsoft Outlook Anywhere.** Allows Exchange access through the Microsoft Outlook 2010 client by tunneling Outlook’s MAPI protocol over an HTTP connection. (This was formerly known as RPC over HTTP. The protocol still functions by wrapping remote procedure calls inside the HTTP layer, only the name has changed.)

- **Post Office Protocol (POP3) and Internet Message Access Protocol (IMAP4).** Allows online and offline access to mail by non-Outlook mail clients.

- **RPC Client Access.** Provides access to Exchange mailboxes through MAPI (Messaging API), but in Exchange 2010, moves the connectivity point from the Mailbox server role to the Client Access server. Note: The Mailbox and Client Access server roles may be implemented in the same Exchange machine.

The following table from the Microsoft planning guide provides information on the ports that are utilized for Client Access servers. The VIP Port is the virtual IP address that you choose to assign to your NetScaler. This is the address that client systems will communicate with. It is NOT the physical IP address of the Exchange system.
Ports and Protocols Used by Exchange 2010 Clients

<table>
<thead>
<tr>
<th>Client Access server role</th>
<th>VIP Port</th>
<th>Server Port</th>
<th>Protocol</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Outlook Web App</td>
<td>443</td>
<td>80</td>
<td>HTTPS</td>
<td></td>
</tr>
<tr>
<td>Active Sync</td>
<td>443</td>
<td>80</td>
<td>HTTPS</td>
<td></td>
</tr>
<tr>
<td>POP3</td>
<td>995</td>
<td>110</td>
<td>TCP</td>
<td></td>
</tr>
<tr>
<td>IMAP4</td>
<td>993</td>
<td>143</td>
<td>TCP</td>
<td></td>
</tr>
<tr>
<td>RPC Client Access</td>
<td>Any</td>
<td>Any</td>
<td>TCP</td>
<td></td>
</tr>
<tr>
<td>Outlook Anywhere</td>
<td>443</td>
<td>80</td>
<td>HTTPS</td>
<td></td>
</tr>
</tbody>
</table>

Configuring NetScaler for Outlook Web App (OWA)

This section covers the configuration steps for load balancing Client Access servers for OWA clients. As illustrated in the earlier “Network Diagram” section, a typical OWA request comes in from the Internet through the DMZ and gets terminated at the NetScaler.

NetScaler performs the following functions on the request:

- Terminates SSL connection and performs SSL decryption. This reduces CPU load on the Access Client servers enabling them to handle more client requests. (Exchange will need to be reconfigured so as NOT to require SSL when processing traffic via NetScaler.)
- Check health of the Access Client servers. This increases availability of the servers.
- Load balances multiple Access Client servers to handle OWA requests efficiently to ensure high availability of the Access Client servers.
- Compresses traffic to decrease response times.

Creating Services for OWA

If any of the menu items are unavailable, be sure the appropriate features are selected by navigating to System > Settings and click Change basic features. The NetScaler should have at least the roles indicated in the following screen shot.
The first step in the configuration process is to identify Client Access servers that are ready to handle OWA connections and add them as services as shown below.

Navigate to Load Balancing > Services, click Add, and enter the values as shown in the screen shot. Please note that the IP address that you enter for “Server” will be the IP address of your Exchange Server. Select the monitor and click Add to bind the http monitor to the service.

Enable compression on each service by clicking advanced tab and selecting the Compression check box.

You will need to repeat the steps above for each Exchange Client Access server that you want to load balance.
Import SSL certificate

Because the NetScaler will be terminating the SSL connections on behalf of the Exchange system (offloading that burden), the NetScaler will need an SSL certificate imported into its system for use in this role. We assume that the certificate is available to the user.

If you are planning to utilize a certificate from the Exchange system, follow these instructions to export the certificate file.

On your Exchange System, open the Exchange Management Shell and input the command “Get-ExchangeCertificate.” This will output a description of all SSL certificates for the specified Exchange services.

Use these three commands to generate a file “htcert.pfx” from the certificate with the thumbprint specified by the hex string. When prompted, enter a user name and password, which will be used for importing into the NetScaler. Then,

transfer the file to the system being used to access the NetScaler.

On the NetScaler, navigate to SSL, and click Import PKCS#12 in the details pane. Provide the required information. The output file name being its representation on the NetScaler.
Click **OK**, and then navigate to **SSL > Certificates** and click **Add**. Provide the information, using the above screen shot as a guide, and click **Install**. The Certificate should appear on the NetScaler.

Create a Content Rewrite Policy

To point the NetScaler virtual servers to the correct URL for Outlook Web App access, create a content rewrite policy for the request from the NetScaler to the Exchange 2010 Client Access server.

On the NetScaler, navigate to **Rewrite > Actions** and click **Add**. Copy the information from the following screen shot, and click **Create**.
Then, navigate to Rewrite > Policies and click Add. Copy the content from the following screen shot, and click OK.

These steps allow the virtual server to add “/owa” to the clients request.

**Create an SSL virtual server**

Create a virtual server and bind the services that we created previously and enable a persistence scheme and a load balancing algorithm.
Navigate to **Load Balancing > Virtual Servers** and click **Add**. Enter the values as shown in the following screen shots. Note that each service that you created in the first step of the OWA configuration will appear as an available service name in the Services screen. The IP address that you enter in the upper-right corner of the dialog box is the virtual IP (VIP) address that OWA clients will use to access OWA.

This virtual server will handle all https requests, that is, requests that arrive over SSL sessions.

Click **Method and Persistence** and choose the load balancing algorithm and persistence scheme as shown in the screen shot. Choose **Round Robin** (recommended by Microsoft) or least connection for load balancing and choose cookie insert for persistence.
Click **SSL Settings** and add the imported certificate to this virtual server by highlighting on *e2010-cert* (or whatever the name was of the certificate that you imported earlier) and clicking **Add**.

Click **Policies > Content Rewrite**, and apply the policy created earlier to the virtual server.
Click OK and it will create a virtual server that is ready to accept incoming OWA requests encrypted via https. NetScaler will then send these requests to the back end server in clear text using http.

This could cause a problem for OWA deployments as the server is not aware of SSL offload and responds to the queries with redirects that are in http mode. Therefore subsequent requests from the clients show up in the clear on port 80 on NetScaler. There are two ways to mitigate this problem. First method requires the user to re-configure Exchange servers indicating to them that SSL has been offloaded. Following (http://technet.microsoft.com/en-us/library/bb885060(EXCHG.80).aspx) are the steps to do that –

1. Start Registry Editor.
2. Locate the following registry key: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\MSExchange OWA.
3. On the Edit menu, click New, and then click DWORD Value.
4. In the details pane, name the DWORD value SSLOffloaded.
5. In the details pane, right-click SSLOffloaded, and then click Modify.
6. In the Edit DWORD Value dialog box, in Value data, type 1.
7. Restart the IIS Admin Service (IISAdmin). To do this, open a Command Prompt window, and then type iisreset /noforce.
Second way is to configure NetScaler to redirect any traffic that comes to OWA server on port 80 to port 443. For this, we need to create another virtual server that will respond to requests that might arrive, unencrypted, via http on port 80.

In Load Balancing > Virtual Servers, click Add. This time, select HTTP as the protocol. You will note that the SSL Settings tab is disabled as HTTP does not use SSL. As before, the IP address in the upper-right corner should be the VIP that you have allocated as the external address for OWA users. Be sure not to bind any services to the server.
On the **Method and Persistence** tab, use **Least Connection** LB method and **None** for persistence. On the **Advanced** tab, in **Redirect URL**, enter the VIP of the https virtual server.

Finally, you will need to log on to your Exchange Client Access servers with administrative privileges to modify the SSL settings of several components to allow Exchange and NetScaler to communicate properly.

You can access the Exchange Server system either through a physical console or Microsoft Remote Desktop. The Exchange OWA service makes use of Internet Information Services (IIS) co-resident with Exchange. It is within the IIS configuration where we need to reconfigure the system so that SSL connections are not mandatory between the Exchange Client Access server system and the NetScaler.
Launch IIS Manager on the Exchange Client Access server system. (It is found in the sub-folder of Applications called Administrative Tools.) Expand the menus, as shown below, until the nodes below Default Web Site are visible.

There are several web site elements that you will need to modify: EWS, Exchange, Exchweb and OWA. The configuration change is the same for all of these. You can apply these changes in any order.

Highlight one of the folders, EWS is highlighted in our example, and scroll down on the middle scroll bar until you see IIS Settings (near the bottom).
Double-click the **SSL Settings** icon to bring up the detailed settings. As a default, you will see **Require SSL** is selected. Clear that check box (as show in our example), and click the radio button for **Accept** client certificates. Once you have done this, be sure to click the **Apply** action in the upper-right corner of the screen.

You will need to repeat the change to the SSL configuration in each of the other three folders referenced above.
enable ns feature WL LB CMP SSL REWRITE
add server 192.168.1.154 192.168.1.154
add server 192.168.1.164 192.168.1.164
add service Exchange_2010_owa 192.168.1.154 HTTP 80 -gslb NONE -maxClient 0 -maxReq 0 -cip DISABLED -usip NO -useproxyport YES -sp OFF -cltTimeout 180 -svrTimeout 360 -CKA NO -TCPB NO -CMP YES
add service Exchange_2010_owa_2 192.168.1.164 HTTP 80 -gslb NONE -maxClient 0 -maxReq 0 -cip DISABLED -usip NO -useproxyport YES -sp OFF -cltTimeout 180 -svrTimeout 360 -CKA NO -TCPB NO -CMP YES
add rewrite action owa_rewrite replace http.REQ.URL "/owa/"
add rewrite policy owa_rewrite_policy "http.req.url.eq("/owa")" owa_rewrite
add lb vserver Exchange_2010_owa_vserver SSL 192.168.1.171 443 -persistenceType COOKIEINSERT -cltTimeout 180
add lb vserver Exchange_2010_owa_http_responder HTTP 192.168.1.171 80 -persistenceType NONE -redirectURL "https://192.168.1.171" -cltTimeout 180
bound lb vserver Exchange_2010_owa_vserver Exchange_2010_owa
bound lb vserver Exchange_2010_owa_vserver Exchange_2010_owa_2
bound lb vserver Exchange_2010_owa_vserver -policyName owa_rewrite_policy -priority 100 -gotoPriorityExpression END -type REQUEST
bound lb monitor http Exchange_2010_owa_2
bound lb monitor ping Exchange_2010_owa
add ssl certKey Exchange_2010_cert /nsconfig/ssl/exchange_2010_cert -key /nsconfig/ssl/exchange_2010_cert
bind ssl vserver Exchange_2010_owa_vserver -certKeyName Exchange_2010
Configuring NetScaler for Microsoft Exchange ActiveSync (AS)

Exchange ActiveSync® lets devices such as a cellular telephone or a Microsoft Windows Mobile® powered device access corporate information on a server that is running Exchange. Exchange ActiveSync is a data synchronization service that enables mobile users to access their e-mail, calendar, and contacts and retain access to this information while they are offline.

This section covers the configuration steps for load balancing Client Access servers that are enabled in ActiveSync mode. As illustrated in the earlier “Network Diagram” section, a typical ActiveSync request comes in from the Internet through the DMZ and gets terminated at the NetScaler. NetScaler performs the following functions on the request:

- SSL termination to decryption
- Health monitoring of the Client Access servers
- Source-IP persistence or Rule based persistence
- Compression
- Load balancing based on the Round Robin algorithm

**Import SSL certificate**

Follow the same instructions that were used to import SSL certificate for OWA.

**Creating Services for AS**

Follow the same instructions that were used for creating services for OWA client and use the appropriate IP addresses for the Client Access servers.

**Create an SSL virtual server**

Follow the same instructions that were used for creating OWA virtual server. Select HTTP health monitor and use the Round Robin load balancing algorithm. Source IP address can be used for persistence, but this could pose a problem with clients coming from behind a NAT service. Alternatively, if basic authentication is being used by ActiveSync, NetScaler rule based persistence can be used using the Authorization header as shown in the following screenshot.
Configuring NetScaler for Microsoft Outlook Anywhere (OA)

In Microsoft Exchange Server 2010, the Outlook Anywhere feature, formerly known as RPC over HTTP, allows clients that use Microsoft Office Outlook 2010, Outlook 2007, or Outlook 2003 connect to their Exchange servers over the Internet using the RPC over HTTP Windows networking component.

This section covers the configuration instructions for load balancing Client Access servers that are enabled in Outlook Anywhere mode. As illustrated in the earlier “Network Diagram” section, a typical OA request comes in from the Internet through the DMZ and gets terminated at the NetScaler. NetScaler performs the following functions on the request:

- SSL termination to decryption
- Health monitoring of the Client Access servers
- Source-IP or Rule based persistence
- Compression
• Load balancing based on Round Robin algorithm

**Import SSL certificate**

Follow the same instructions that were used to import SSL certificate for OWA. If you plan to use the same certificate as used for OWA, you may skip this step.

**Creating Services for OA**

Follow the same instructions that were used for creating services for the OWA client and use the appropriate IP addresses for the Client Access servers.

**Create an SSL virtual server**

Follow the same instructions that were used for creating the OWA virtual server. Select HTTP health monitor and use the Round Robin load balancing algorithm. Source IP address can be used for persistence, but this could pose a problem with clients coming from behind a NAT service. Alternatively, if basic authentication is being used, NetScaler rule based persistence can be used using the Authorization header as shown in the ActiveSync section.

**Configuring NetScaler for IMAP4**

Internet Message Access Protocol (IMAP4) is an Application Layer Internet protocol operating on port 143 that allows an e-mail client to access e-mail on a remote mail server. Within Microsoft Exchange, IMAP4 clients are serviced by the Client Access server component.

IMAP4 does not offer advanced collaboration features, such as calendaring, contacts, and tasks. IMAP4 is commonly used in e-mail clients, such as Windows Mail, Windows Live Mail, and Mozilla Thunderbird.

IMAP4 cannot be used to send messages from a client application to the e-mail server. E-mail applications that use IMAP4 to send messages rely on the SMTP protocol to send messages. The connector for receiving e-mail submissions from client applications that use IMAP4 is created automatically on every Hub Transport server.

This section covers the instructions for load balancing Client Access servers that are enabled for IMAP4 protocol. As illustrated in the earlier “Network Diagram” section, a typical IMAP4 request comes in from the Internet through the DMZ and gets terminated at the NetScaler. NetScaler performs the following functions on the request:

• SSL termination for decryption
• Health monitoring of the target servers using TCP-based health monitor
• Load balancing based on Least Connection algorithm

**Import SSL certificate**

Follow the same instructions that were used to import SSL certificate for OWA. If you plan to use the same certificate as used for OWA, you may skip this step.

**Create a TCP level monitor for IMAP4 (optional)**

NetScaler can create an extended TCP level monitor that can monitor the availability of the IMAP4 server banner through a TCP connection.

Navigate to Load Balancing > Monitors and click Add. Use the values in the following screen shots to create a TCP level monitor.
Click **Special Parameters**, and use the values in the following screen shot to create a TCP-level ECV monitor. Click **Create** to create a TCP level monitor for IMAP4.

Create **Services for IMAP4**

Follow the same instructions that were used to create services for the OWA client. Navigate to **SSL Offload > Services > Add** and use appropriate IP addresses for the Client Access servers. Set the port to **143**. Use the **e2010_imap4** monitor that was created in the previous section.
Create an SSL virtual server

Follow the same instructions that were used for creating the OWA virtual server. Use port number 993 (standard SSL IMAP4 port). Use the Least Connection load balancing algorithm.

In SSL Settings, once again add the Exchange Certificate to the virtual server. Click OK, and the NetScaler will be ready to forward IMAP requests.
Troubleshooting

If the monitor created for IMAP services does not go up when there is physical connectivity to the Exchange Server, you may need to customize the application monitor.

On the Exchange server, ensure that the services for IMAP4 and POP3 are started. Log on to the Exchange Management Server and navigate to Server Configuration > Client Access > POP3 and IMAP4. Open the IMAP4 Properties dialog box and note the banner string. This should match the string inputted into the Special Parameters section of the IMAP4 monitor.

Summary of Commands

```
add service Exchange_2010_IMAP4 192.168.1.154 TCP 143 -gslb NONE -maxClient 0 -maxReq 0 -cip DISABLED -usip NO -useproxyport YES -sp OFF -crtTimeout 9000 -srtTimeout 9000 -CKA NO -TCPB NO -CMP NO
add lb vserver Exchange_2010_IMAP_vserver SSL_TCP 192.168.1.171 993 -persistenceType NONE -crtTimeout 9000
bind lb vserver Exchange_2010_IMAP_vserver Exchange_2010_IMAP4
add lb monitor e2010_IMAP4_monitor TCP -send "GET /" -recv "The Microsoft Exchange IMAP4 service is ready." -LRTM ENABLED -interval 30 -resptimeout 5 -downTime 2 MIN -destIP 192.168.1.154 -destPort 143
bind lb monitor e2010_IMAP4_monitor Exchange_2010_IMAP4
set ssl vserver Exchange_2010_IMAP_vserver -ciphersv2Redirect DISABLED -sslv2Redirect DISABLED
set aaa parameter -maxAAAUsers 10
set aaa preauthenticationparameter -preauthenticationaction ALLOW -rule ns_true
bind ssl vserver Exchange_2010_IMAP_vserver -certKeyName Exchange_2010
```

Configuring NetScaler with POP3

Post Office Protocol (POP) is an application-layer Internet standard protocol used by local e-mail clients to retrieve e-mail from a remote server over a TCP/IP connection. POP and IMAP (Internet Message Access Protocol) are the
two most prevalent Internet standard protocols for e-mail retrieval. Virtually all modern e-mail clients and servers support both. The POP protocol has been developed through several versions, with version 3 (POP3) being the current standard. Within Microsoft Exchange, IMAP4 clients are serviced by the Client Access server component.

POP3 was designed to support offline mail processing. With POP3, e-mail messages are removed from the server and stored on the local POP3 client, unless the client has been set to leave mail on the server. This puts the data management and security responsibility in the hands of the user. POP3 does not offer advanced collaboration features, such as calendaring, contacts, and tasks. POP3 cannot be used to send messages from a client application to the e-mail server. E-mail applications that use POP3 to send messages rely on the SMTP protocol to send messages. The connector for receiving e-mail submissions from client applications that use POP3 is created automatically on every Hub Transport server.

This section covers the configuration steps for load balancing Client Access servers that are enabled for POP3 protocol. As illustrated in the earlier “Network Diagram” section, a typical POP3 request comes in from the Internet through the DMZ and gets terminated at the NetScaler. NetScaler performs the following functions on the request:

- SSL termination for decryption
- Health monitoring of the target servers using TCP-based health monitor
- Load balancing based on the Least Connection algorithm

**Import SSL certificate**

Follow the same procedure that was used to import SSL certificate for OWA. If you plan to use the same certificate as used for OWA, you may skip this step.

**Create an application level monitor for POP3 (optional)**

NetScaler provides two options for monitoring POP3 servers. The first one uses a POP3 user name and password to log on to a POP3 server and the second one uses a TCP level monitor to verify the banner string from the POP3 server. The second monitor can be configured the same way as the IMAP4 monitor. In this section, the following instructions will help you create a POP3 monitor.

Navigate to **Load Balancing > Monitors** and click **Add**. Use the values in the following screen shots to create a POP3 monitor.
Click **Special Parameters** and enter the values as shown in the following screen shot. Click **Create**. It is assumed that the administrator has created a POP3 user and password on the POP3 server. This concludes creation of a POP3 monitor.
Creating Services for POP3

Follow the same instructions that were used to create services for the OWA client and use the appropriate IP addresses for the Client Access servers by navigating to Load Balancing > Services > Add. Set the port to 110. Bind the POP3 monitor that was created in the previous section.

Create an SSL virtual server for POP3

Follow the same procedure that was used for creating an OWA virtual server by navigating to Load Balancing > Virtual Servers > Add. Use port number 995 (standard POP3 over SSL port). Use the Least Connection load balancing algorithm, no persistence, and bind the desired SSL Certificate to the server.
Summary of Commands

add service Exchange_2010_POP3 192.168.1.154 TCP 110 -gslb NONE -maxClient 0 -maxReq 0 -cip DISABLED -usip NO -useproxyport YES -sp OFF -clTimeout 9000 -svrTimeout 9000 -cka NO -TCPB NO -CMP NO
add lb vserver Exchange_2010_POP3_vserver SSL_TCP 192.168.1.171 995 -persistenceType NONE -clTimeout 9000
bind lb vserver Exchange_2010_POP3_vserver Exchange_2010_POP3
add lb monitor e2010_POP3_monitor POP3 -scriptName nspop3.pl -dispatcherIP 127.0.0.1 -dispatcherPort 3013 -userName itest -password cc2e035357d02d31f5cb -encrypted -LRTM ENABLED -interval 30 -retrytimeout 5 -downTime 2 MIN -destIP 192.168.1.154 -destPort 110
bind lb monitor e2010_POP3_monitor Exchange_2010_POP3
set ssl vserver Exchange_2010_POP3_vserver -cipherRedirect DISABLED -sslv2Redirect DISABLED
set aaa parameter -maxAAAUsers 10
set aaa preauthenticationparameter -preauthenticationaction ALLOW -rule ns_true
bind ssl vserver Exchange_2010_POP3_vserver -certkeyName Exchange_2010 POP3

Configuring NetScaler for RPC Client Access

Among the architectural changes made in Exchange Server 2010 is the introduction of the new RPC Client Access service. This new service moves Outlook MAPI mailbox connections from the back-end Mailbox server and moves directory access from domain controllers/global catalog servers in the data tier to the Client Access servers in the middle tier. This section covers the configuration instructions for load balancing Client Access servers that are enabled for RPC Client Access. As illustrated in the earlier “Network Diagram” section, a typical RPC Client Access request comes in from the Internet through the DMZ and gets terminated at the NetScaler. NetScaler performs the following functions on the request:

- Health monitoring of the Client Access servers using TCP-based health monitor
- Load balancing based on the least connection algorithm

Creating Monitor for RPC Client Access

Create a TCP Monitor for port 22902 (may vary depending on specific deployment) by navigating to Load Balancing > Monitor > Add and use the values in the following screen shot as a guide.
Creating Services for RPC Client Access

Follow the same instructions that were used for creating services for the OWA client and use the appropriate IP addresses for the Client Access servers. Set the port to wild card (*).

Create a virtual server for RPC Client Access

Follow the same procedure that was used for creating OWA virtual server. Use the wild card port value denoted by an asterisk (*).
Select the TCP health monitor and use the Round Robin load balancing algorithm. Select source IP address based persistence.

**Summary of Commands**

```bash
add service Exchange_2010_RPC 192.168.1.154 TCP * -gslb NONE -maxClient 0 -maxReq 0 -cip DISABLED -usip NO -useproxyport YES -sp OFF -cltTimeout 9000 -srvTimeout 9000 -CKA NO -TCPB NO -CMP NO
add lb vserver Exchange_2010_RPC_vserver TCP 192.168.1.172 * -persistenceType SOURCEIP -cltTimeout 9000
bind lb vserver Exchange_2010_RPC_vserver Exchange_2010_RPC
add lb monitor e2010_SMTP_monitor SMTP -scriptName nssmtp.pl -dispatcherIP 127.0.0.1 -dispatcherPort 3013 -LRTM ENABLED -interval 30 -resptimeout 5 -downTime 2 MIN -destIP 0.0.0.0
add lb monitor e2010_RPC_monitor TCP -LRTM ENABLED -destIP 192.168.1.154 -destPort 22902
bind lb monitor e2010_RPC_monitor Exchange_2010_RPC
```

**Edge Transport Servers**

The Edge Transport server role is an important role in Microsoft Exchange Server 2010. It handles all Internet-facing mail flow, which provides SMTP relay and smart host services for the Exchange organization. It also provides message protection and security through a series of agents that act on messages as they are processed by the message transport components. These agents support the features that provide protection against viruses and spam and apply transport rules to control message flow.

In this deployment guide, learn how to configure NetScaler to load balance connections to Edge Transport servers. Also, learn how to provide high availability for deployments spanning multiple data centers through global server load balancing (GSLB).

**Configuring NetScaler for Edge Transport Servers**
This section shows how NetScaler can be used to load balance traffic across multiple Edge Transport servers.

**Create an application level monitor for SMTP**

NetScaler provides application specific monitoring for SMTP servers. Navigate to Load Balancing > Monitors and click Add. Use the values in the following screen shots to create a SMTP monitor.

![Create Monitor Screen Shot](image1)

**Creating Services**

Follow the same instructions that were used for creating services for OWA client and use the appropriate IP addresses for the Edge Transport servers. Set the protocol to TCP and port number to 25. Select the SMTP monitor that was just created as the monitor for each of these services.

![Configure Service Screen Shot](image2)
Create a virtual server

Follow the same procedure that was used for creating OWA virtual server. Use port number 25 (which is the port used for SMTP) and protocol TCP. Select the SMTP monitor and use the Least Connection load balancing algorithm.

Summary of Commands

```
add service Exchange_2010_SMTP 192.168.1.154 TCP 25 -gslb NONE -maxClient 0 -maxReq 0 -cip DISABLED -usip NO -useproxyport YES -sp OFF
  -cltTimeout 9000 -svrTimeout 9000 -CKA NO -TCPB NO -CMP NO
add lb monitor e2010_SMTP_monitor SMTP
  -scriptName nssmtp.pl
  -dispatcherIP 127.0.0.1
  -dispatcherPort 3013
  -LRTM ENABLED
  -interval 30
  -resptimeout 5
  -downTime 2 MIN
  -destIP 0.0.0.0
add lb vserver Exchange_2010_SMTP_vserver TCP 192.168.1.171 25
  -persistenceType NONE
  -cltTimeout 9000
bind lb vserver Exchange_2010_SMTP_vserver Exchange_2010_SMTP
bind lb monitor e2010_SMTP_monitor Exchange_2010_SMTP
```

Configuring NetScaler GSLB with Edge Transport Servers in multiple Data Centers

Global server load balancing (GSLB) is a DNS-based technology that uses an authoritative DNS service to direct users to an appropriate instance of an application using its Fully Qualified Domain Name (FQDN). It enables NetScaler to distribute network traffic and server load across multiple sites based upon service availability.

The following diagram shows GSLB in operation.
This section shows how NetScaler can be configured to load balance traffic across Edge Transport server banks in multiple data centers.

**Create GSLB services**

Follow the instructions **described in Configuring NetScaler for Edge Transport Servers** to create virtual servers for Edge Transport servers in each of the data center. Use the GSLB wizard to create GSLB services. The following information should be obtained before creating GSLB services:

- Local GSLB Site IP – 192.168.1.141
- Local GSLB Name - GSLB_local
- Local GSLB Service – 192.168.1.171
- Remote GSLB Site IP – 192.168.1.142
- Remote GSLB Name - GSLB_remote
- Remote GSLB Service – 192.168.1.164
- ADNS IP – 192.168.1.154
- GSLB FQDN – gslb.contoso.com

*Create GSLB sites and services prior to launching wizard (optional)*
Though it can be done in the wizard, you will have more freedom in your configuration if you first take the following steps. Navigate to GSLB > Services > Add. Provide the relevant information as specified in the following screen shot. For Site Name, click New and you will be directed to another configuration page.

Create the new site, providing the basic information and location and then click Create.

Repeat this process for each site to be handled by the GSLB policy.
To start configuring GSLB, navigate to GSLB and click the GSLB wizard.

Click **Next** and specify the domain name and service type.

Click **Next** and set the GSLB method to Round Robin.
Configure local and remote site IP addresses and add the corresponding services as specified in the table above. Or, if the services were created manually, simply bind them by selecting the check boxes.

Click **Next** for the configuration summary. Click **Finish** to apply the configuration.
The second page prompts whether or not additional services are required for the proposed configuration.
If there is no prior ADNS service on the NetScaler, click the link to enter the configuration.

Create the ADNS service and replicate the same configuration on the other site.
Summary of Commands

```
add ns 192.168.1.141 255.255.255.255 -type GSLBsiteIP -vServer DISABLED -telnet DISABLED -ftp DISABLED -gui DISABLED -ssh DISABLED -smtp DISABLED
add server 192.168.1.171 192.168.1.171
add server 192.168.1.154 192.168.1.154
add server "gslb remote" 192.168.1.164
add service "GSLB_ADNS" 192.168.1.154 ADNS 53 -gslb NONE -maxClient 0 -maxReq 0 -cip DISABLED -usp NO -useproxyport NO -sp OFF -cltTimeout 120 -svrTimeout 120 -cKA NO -TCPB NO -CMP NO
add lb vserver Exchange_2010_GSLB_vserver TCP -persistenceType NONE -cltTimeout 9000
add gslb vserver Exchange_2010_GSLB_vserver TCP -lbMethod ROUNDROBIN -tolerance 0
add gslb vserver "SMTP GSLB" TCP -lbMethod ROUNDROBIN -tolerance 0
set gslb vserver "SMTP GSLB" -lbMethod ROUNDROBIN
add gslb site GSLB_Local 192.168.1.141
add gslb site "GSLB_Remote" 192.168.1.142
set ns rpcNode 192.168.1.141 -password 8a7b474124957776a0cd31b862cbeb4d72b8c5d5f986a1364d8d6528 -encrypted
set ns rpcNode 192.168.1.142 -password 8a7b474124957776a0cd31b862cbeb4d72b8c5d5f986a1364d8d6528 -encrypted
add gslb service GSLB_local 192.168.1.171 TCP 25 -publicIP 192.168.1.171 -publicPort 25 -maxClient 0 -siteName GSLB_Local -cltTimeout 9000 -svrTimeout 9000 -downStateFlush DISABLED
add gslb service smtp_159 "gslb remote" TCP -publicIP 192.168.1.165 -publicPort 25 -maxClient 0 -siteName GSLB_Remote -cltTimeout 9000 -svrTimeout 9000 -downStateFlush DISABLED
bind gslb vserver Exchange_2010_GSLB_vserver -serviceName smtp_159
bind gslb vserver Exchange_2010_GSLB_vserver -serviceName GSLB_local
bind gslb vserver "SMTP GSLB" -serviceName GSLB_local
bind gslb vserver "SMTP GSLB" -domainName gslb.contoso.com -TTL 5
set ssl service nskrpcs 192.168.1.141 3009 -sessReuse ENABLED -sessTimeout 120 -cipherRedirect DISABLED -sslv2Redirect DISABLED
set ssl service nshttps fe80::6819:b4ff:fe43:ebc8 443 -sessReuse ENABLED -sessTimeout 120
bind ssl service nskrpcs 192.168.1.141 3009 -certkeyName ns-server-certificate
bind ssl service nshttps fe80::6819:b4ff:fe43:ebc8 443 -certkeyName ns-server-certificate
```

This concludes the configuration of the GSLB services for Edge Transport Servers.

### NetScaler Management Pack Deployment

#### Introduction

The Citrix NetScaler Management Pack (MP) provides monitors and rules to monitor the health of the virtual servers configured on the managed NetScaler systems and initiate corrective actions using Performance and Resource Optimization (PRO) feature of SCVMM when the virtual servers become unhealthy.

As an example, SCOM could monitor a virtual IP on NetScaler for the health of all the Exchange 2010 Client Access services bound to it. If all the services attached to the virtual server are healthy, then the virtual server is 100% healthy, and health keeps reducing as the number of servers in a healthy state goes down.

SCOM MP monitors the health of all virtual servers on the NetScaler and raises an event should the health drop below a configured threshold. This event could trigger a workflow that could start the process of creating a virtual machine for the application that caused the health alert. Once the VM is created and is running on the Hyper-V host, its IP address is attached on the NetScaler, as an additional server to which the user traffic can be directed, thus clearing the event that triggered this corrective action.

NetScaler Management Pack therefore is a very powerful tool to manage virtual environments in the context of a NetScaler deployment.
Dependencies
This management pack is dependent on the following management packs:

- Microsoft.SystemCenter.Library
- Microsoft.Windows.Library
- System.Health.Library
- System.Library

Prerequisites
Before you import the management pack(s) in the SCOM Operations Console, ensure that the following prerequisites are met:

- Dependent management packs, as mentioned in the above section, are imported into SCOM.
- Windows SNMP Service Component is installed.

Installing Citrix NetScaler Management Pack
The Citrix NetScaler management pack solution is packaged as Windows installer, .msi.

To install the management pack

2. In the Welcome dialog box, click Next.
3. In the **License Agreement** dialog box, read the agreement, click **I Agree**, and then click **Next**.

4. In the **Confirm Installation** dialog box, click **Next** to start installation of this solution. Note that all the components are installed under `C:\Program Files\Citrix\NetScaler\SystemCenter`.

5. In the **Installation Complete** dialog box, click **Close**.
To verify the installation

1. Click Start > Settings > Control Panel > Add or Remove Programs.
2. In the Add or Remove window, check for Citrix NetScaler Management Pack for System Center Operations Manager 2007 entry.

Importing Management Packs

To import management packs

1. Open the SCOM Operations Console by clicking Start > Programs > System Center Operations Manager 2007 > Operations Console.
2. In the Operations view, click the Administration button.
3. Under Security node, right-click the Management Packs node, and then select Import Management Pack.
4. Navigate to C:\Program Files\Citrix\NetScaler\SystemCenter\mp folder and select all the .mp files, and then click Open.
5. In the Import Management Packs screen, click Import.
Note: The system may take few moments to complete the import process.
6. After the import is completed, click Close.

Setting Up Security

This management pack requires the log on credentials of the NetScaler appliances it is managing to be able to take corrective actions when the virtual servers become unhealthy.

To setup security for managing NetScaler systems

1. In the Operations Console, click Administration.
2. Under Security node, right-click Run As Accounts view, and then select the Create Run As Account option.
3. On the General tab, select Simple Authentication as Run as Account Type. Type Display name and description, and then click Next.
4. In Account name, type the NetScaler log on user name and in password, type the password.
5. In confirm password field, type the password again, and then click Create. The account is displayed under Type:Simple Authentication view in the right pane.
6. Click Run As Profiles view, and then double click Citrix NetScaler PRO Authentication Account.
7. On the Run as Profile Properties screen, click Run As Accounts tab.
8. Click +New.
9. On the Run Alternate Run As Account screen, in the Run As Account drop-down list select the account you created in steps 2 - 4 above.
10. Under Matching Computers, select the SCOM system, and then click OK. The security setup is complete.

Override MP for Customizations

This section describes the overrides available at discovery, monitor, and recovery configurations. Note that all the overrides mentioned below are mandatory for the proper functioning of the MP.

Overrides defined at VserverHealth monitor

Following are the overrides defined at the monitor level:

**NetScalerIPAddress**: Specify the IP Address of the NetScaler system whose virtual server health needs to be monitored.

**Threshold**: Define the threshold value of the virtual server health. If the polled value is less than the threshold, then a PRO tip is generated to initiate corrective action.

**IntervalSeconds**: Define the frequency of polling the virtual server health counter.

**Virtual Server Name**: Specify the name of the virtual server whose health needs to be monitored.

Overrides defined at VServerHealth Discovery

Following are the overrides defined at the discovery level:

**IntervalSeconds**: Define NetScaler device discovery interval.

**VMMServer**: Specify the host name of the Virtual Machine Machine (VMM) server which would receive the PRO tip and also initiate corrective actions once a PRO tip is generated.

Overrides defined at VServerHealth recovery

Following are the overrides defined at the recovery level:

**HyperVHostname**: Specify the host name of the HyperV system into which a VM needs to be provisioned as part of corrective action.

**Protocol**: Specify the protocol of the service that will be configured on the NetScaler system as part of the corrective action. This usually should be same as
the protocol of the virtual vserver that is being monitored by the management pack.

**Port:** Specify the port of the service to be configured on the NetScaler system.

**LibraryServer:** Specify the host name of the library server that contains the VMs that need to be deployed in the HyperV host.

**How it Works**

The following steps describe how the MP solution works.
1) At the configured poll interval, the PRO MP polls and compares the value of the virtual server’s health counter with that of the threshold value. If the polled value is less than the configured threshold value, it generates a warning alert.

2) This warning alert triggers a PRO tip to be generated in the VMM PRO console.

3) On clicking the Implement button in the PRO window in the VMM console, corrective actions per definition in the PRO MP are initiated.

4) The first step of corrective action is to provision a VM from the defined Library Sever. This step deploys a VM available in the library Server on the HyperV host.

5) After step 4 is complete, the MP picks the computer name of the provisioned VM and resolves it to its IP address. It is mandatory that the computer name of the new VM resolves to a proper IP address for the corrective action to be fully functional.

6) After step 5 is complete, the next probe for the health of the monitored virtual server should become healthy with a new service bound to it. For proper functioning of the MP, ensure that the overrides as mentioned in the section “Override MP for Customizations” are defined properly.
Worldwide Headquarters
Citrix Systems, Inc.
851 West Cypress Creek Road
Fort Lauderdale, FL 33309, USA
T +1 800 393 1888
T +1 954 267 3000

Americas
Citrix Silicon Valley
4988 Great America Parkway
Santa Clara, CA 95054, USA
T +1 408 790 8000

Europe
Citrix Systems International GmbH
Rheinweg 9
8200 Schaffhausen, Switzerland
T +41 52 635 7700

Asia Pacific
Citrix Systems Hong Kong Ltd.
Suite 3201, 32nd Floor
One International Finance Centre
1 Harbour View Street
Central, Hong Kong
T +852 2100 5000

Citrix Online Division
6500 Hollister Avenue
Goleta, CA 93117, USA
T +1 805 690 6400
www.citrix.com

About Citrix
Citrix Systems, Inc. (NASDAQ:CTXS) is the leading provider of virtualization, networking and software as a service technologies for more than 230,000 organizations worldwide. Its Citrix Delivery Center, Citrix Cloud Center (C3) and Citrix Online Services product families radically simplify computing for millions of users, delivering applications as an on-demand service to any user, in any location on any device. Citrix customers include the world’s largest Internet companies, 99 percent of Fortune Global 500 enterprises, and hundreds of thousands of small businesses and prosumers worldwide. Citrix partners with over 10,000 companies worldwide in more than 100 countries. Founded in 1989, annual revenue in 2008 was $1.6 billion.

©2009 Citrix Systems, Inc. All rights reserved. Citrix, NetScaler, nCore, Citrix Application Firewall and Access Gateway are trademarks of Citrix Systems, Inc. and/or one or more of its subsidiaries, and may be registered in the United States Patent and Trademark Office and in other countries. All other trademarks and registered trademarks are property of their respective owners.

0609/PDF