Microsoft Office Communication Server 2007 with NetScaler
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.

There are several ways to configure the NetScaler to load balance the Microsoft Office Communication Server 2007. NetScalers can be configured through their configuration utility or through the CLI. This guide describes both scenarios, using the Microsoft OCS 2007 Consolidated Enterprise Edition as an example. Microsoft OCS 2007 has Standard and Enterprise Editions available. However, the Enterprise Edition is the one that requires a hardware load balancer at the front end of a large deployment with multiple servers in order to scale to the maximum number of users for the Enterprise customers. For large-scale deployments, OCS 2007 Enterprise Edition (EE) can scale up to 50,000 users.

NetScaler will front end the OCS servers with one single Virtual IP address and balance the load across the OCS Server pool. After OCS clients register on an active directory or Enterprise pool, the client traffic is bound to an OCS-specific server through the NetScaler. Each OCS server within the Enterprise pool directory handles the server applications, security, authentication, and connection and protocol processing. The SQL database in the back end handles the persistent data, such as contact lists and Access Control Lists. Therefore, the same client can be processed by any OCS server in the pool at any given time.

Solution Requirements

- Application Front-End Switch – Citrix NetScaler
- Microsoft Office Communicator Server 2007

Prerequisites

- Citrix NetScaler appliance, running version 9.0 build 61.9 or later (Quantity x 2 for HA)
- Microsoft Office Communication Servers
- Client laptop/workstation running Microsoft Office Communicators

• Active Directory deployment; information is available at http://technet2.microsoft.com/windowsserver/en/technologies/featured/ad/default.mspx
  — SQL Server 2000/20005 – and if required SQL server cluster deployment available in the following; information is available at http://support.microsoft.com/kb/842192
  — For more information on SQL version and service packs, please go to http://support.microsoft.com/kb/321185
  — Know the Pool FQDN/Server FQDN/port services configured during the Microsoft OCS deployments – these details will not be covered in this guide.
• Domain and Forest Trust Tools and Settings; information is available at http://technet.microsoft.com/en-us/library/cc756944.aspx
• Domain Name Services
  — DNS server is recommended for the OCS domain.
  — Assign DNS Host Records for the VIP, SQL database and OCS servers.

Deployment Overview
This deployment guide provides the NetScaler configuration for the front-end Microsoft OCS 2007 servers. This guide does not explain Microsoft OCS server deployment or the components in the OCS server deployments. Be sure to follow the Microsoft OCS Planning guide to deploy the following OCS components:

• **Active Directory Server.** Stores the user and server information. To increase performance, OCS servers usually cache this information. Single or multiple forest topologies can also be deployed, depending on the size of the enterprise users. For simplicity most enterprises deploy single forest for their network infrastructure. The following diagram illustrates the OCS components as described in the Microsoft OCS Planning guide.
- OCS 2007 Enterprise Edition Servers. These servers should already be connected in a Microsoft OCS pool with back-end services identified and activated as described in the Microsoft Planning Guide.

The following screen shot shows the Microsoft OCS 2007 setup deployed at Citrix.

As shown in the above screen shot, a single forest is created with multiple domains for Citrix employees. Fully qualified domain names (FQDNs) and services are configured for the Federation settings.
The following table from the Microsoft planning guide provides information on the ports that are utilized for OCS servers.

### Ports and Protocols Used by Office Communications Server and Clients

<table>
<thead>
<tr>
<th>Component (Server role or client)</th>
<th>Port</th>
<th>Protocol</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Front End Servers</td>
<td>5060/5061</td>
<td>TCP and MTLS</td>
<td>Used by Standard Edition Servers and Enterprise pools for all internal SIP communications between servers and between servers and Office Communicator.</td>
</tr>
<tr>
<td>Front End Servers</td>
<td>443</td>
<td>HTTPS</td>
<td>Communication from front-end servers to the Web farm FQDNs (the URLs used by Web Components).</td>
</tr>
<tr>
<td>Front End Servers</td>
<td>444</td>
<td>HTTPS</td>
<td>Communication between the focus (Office Communications Server component that manages conference state) and the conferencing servers.</td>
</tr>
<tr>
<td>Front End Servers</td>
<td>135</td>
<td>DCOM and RPC</td>
<td>Used when a load balancer is deployed, port 135 is used by the Front End Servers for WMI operations and moving users (a remote DCOM-based database operation).</td>
</tr>
<tr>
<td>Web Components</td>
<td>443</td>
<td>TCP</td>
<td>HTTPS traffic to the pool URLs.</td>
</tr>
<tr>
<td>Web Conferencing Server</td>
<td>443</td>
<td>TLS</td>
<td>HTTPS communications to Web Components Servers.</td>
</tr>
<tr>
<td>Web Conferencing Server</td>
<td>8057</td>
<td>TLS</td>
<td>Used to listen to direct PSOM connections from Live Meeting client.</td>
</tr>
<tr>
<td>A/V Conferencing Server</td>
<td>5063</td>
<td>TCP</td>
<td>Used for incoming SIP listening requests.</td>
</tr>
<tr>
<td>A/V Conferencing Server</td>
<td>49152 – 65535 media port range</td>
<td>UDP</td>
<td>Port range used for media requests sent.</td>
</tr>
<tr>
<td>Reverse Proxy</td>
<td>443</td>
<td>TCP</td>
<td>Used for SIP/TLS communications from external users on both the internal and external firewalls for external user access.</td>
</tr>
<tr>
<td>Access Edge Server</td>
<td>5061</td>
<td>TCP</td>
<td>Used for SIP/MTLS communication for remote user access or federation.</td>
</tr>
<tr>
<td>Access Edge Server</td>
<td>443</td>
<td>TCP</td>
<td>Used for SIP/TLS communication for remote user access.</td>
</tr>
<tr>
<td>Web Conferencing Edge Server</td>
<td>8057</td>
<td>TCP</td>
<td>Used to listen for PSOM/MTLS communications from the Web Conferencing Server on the internal interface of the Web Conferencing Edge Server.</td>
</tr>
<tr>
<td>Web Conferencing Edge Server</td>
<td>443</td>
<td>TCP</td>
<td>Used for inbound communications for access of remote, anonymous and federated users to access internal Web conferences.</td>
</tr>
<tr>
<td>A/V Edge Server</td>
<td>443</td>
<td>TCP</td>
<td>Used for STUN/TCP inbound and outbound media communications to allow external users to access media and A/V sessions.</td>
</tr>
<tr>
<td>A/V Edge Server</td>
<td>5062</td>
<td>TCP</td>
<td>Used for SIP/MTLS authentication of A/V users. Communications flow outbound through the internal firewall.</td>
</tr>
<tr>
<td>A/V Edge Server</td>
<td>3478</td>
<td>UDP</td>
<td>Used for STUN/UDP inbound and outbound media communications.</td>
</tr>
<tr>
<td>A/V Edge Server</td>
<td>50,000-59,999</td>
<td>RTP/TCP</td>
<td>Used for inbound and outbound media transfer through the external firewall.</td>
</tr>
<tr>
<td>Office Communicator</td>
<td>5060</td>
<td>TCP (SIP)</td>
<td>Used by Office Communicator for SIP communications internally.</td>
</tr>
<tr>
<td>Live Meeting 2007 client</td>
<td>443</td>
<td>TCP</td>
<td>Used by Live Meeting 2007 clients connecting from outside the intranet for: SIP traffic sent to the Access Edge Server. PSOM traffic sent to the Web Conferencing Edge Server.</td>
</tr>
<tr>
<td>Live Meeting 2007 client</td>
<td>8057</td>
<td>TCP</td>
<td>Used for outgoing PSOM traffic sent to the Web Conferencing Server.</td>
</tr>
<tr>
<td>Live Meeting 2007 client</td>
<td>5061</td>
<td>TCP</td>
<td>Used for SIP/TLS communication between Live Meeting and the Front End Servers or the Access Edge Server and for SIP/MTLS authentication of A/V users. Communications flow outbound through the internal firewall.</td>
</tr>
<tr>
<td>Live Meeting 2007 client</td>
<td>1024-65535</td>
<td>UDP/TCP</td>
<td>Port range used for inbound and outbound media transfer through the external firewall.</td>
</tr>
<tr>
<td>Live Meeting 2007 client</td>
<td>6891-6901</td>
<td>TCP</td>
<td>Port ranged used by Live Meeting for file transfer.</td>
</tr>
</tbody>
</table>
As described later in this guide, the preceding ports can be used and deployed with the NetScaler to provide load balancing for the OCS servers. The following screen shot shows the hardware details of the deployed OCS servers as recommended by Microsoft.

Hardware Details

- **SQL database server.** SQL Server 2000 with SP4 or SQL Server 2005 with SP1 or higher is recommended. To provide redundancy, you can additionally configure a cluster of SQL servers. For more information on how to deploy an SQL database server, see [http://support.microsoft.com/kb/842192](http://support.microsoft.com/kb/842192)

- **OCS Clients.** Can be used on any desktop, personal computer, or laptop and provide features such Instant Messaging, presence integration including voice and video functionalities as shown in the following screen shot.
Network Diagram

A NetScaler resides between the clients and the front-end OCS servers, so that client requests and server responses pass through it. The NetScaler ensures optimal distribution of client traffic by the way in which 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 for the OCS servers.
NetScaler Deployment

In accordance with the Microsoft OCS Planning Guide, the NetScaler need not parse SIP messages, and therefore can easily be deployed to provide TCP load balancing for SIP traffic on port 5060 and port 5061. In addition, the NetScaler provides security and protection for the OCS servers and increases server performance and efficiency.

A NetScaler can provide the following key benefits:

- **Improved L4 through L7 Performance.** Provides 15+ Gbps throughput.
- **Maximum Feature Concurrency.** Supports complex policies by using features such as compression, content switching, and application firewall.
- **Accelerates Application Response.** Provides advanced compression, TCP optimization, and static and dynamic caching to speed application performance.
- **Integrates Application Security.** Provides application firewall feature to block attacks against Web applications.
- **Improves 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.

This deployment guide provides instructions to configure a load balancing setup for the OCS 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. A 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 vservers. The services represent the applications on the servers. The vservers 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 vserver. Clients use the IP address of the vserver, the VIP, to connect to a NetScaler. When the NetScaler receives client requests on the VIP, it sends them 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 create customized monitors to suit your requirements.
To configure load balancing, you typically need to perform the following steps:

- Step 1. Creating customized monitors to track the health of the back-end servers.
- Step 2. Creating Services that represent applications on the back-end servers.
- Step 3. Creating Vservers to abstract the back-end servers.

A load balancing setup can be configured by using:

- **Configuration Utility.** You connect to the configuration utility using a web browser.
- **Command Line Interface (CLI).** You connect a workstation or laptop computer to the NetScaler by using the serial cable supplied with it, and then connect to the CLI using terminal emulation software.

Note: In this guide, the procedures to configure a load balancing setup are described for using the configuration utility and CLI.

**To launch the configuration utility**
1. Connect the NetScaler to a management workstation or network.
2. Open a browser and type: http://<IP address of the NetScaler>
3. Type the appropriate user name and password in the User Name and Password fields respectively.
4. In Start in, select Configuration.
5. Click Login to log on. The configuration utility is displayed.
6. Then, navigate to NetScaler > Load Balancing. The Load Balancing page appears as shown in the following diagram.
Load Balancing Front End Servers

This section covers the configuration steps for load balancing Front End servers. As illustrated in the “Network Diagram” section, a typical OCS configuration comprises of the following front end servers:

- Front end server for Windows Management Instrumentation (WMI) operations and for moving users (a remote DCOM-based database operation)
- Front end server for communication between the focus (Office Communications Server component that manages conference state) and the conferencing servers

The NetScaler provides load balancing for DCOM-based front end servers on port 135 and conferencing servers on port 444.

Step 1. Creating Customized Monitors for Front-end Servers

In the load balancing setup for front-end servers, you need to create a monitor to track the health of DCOM-based applications. You need a customized TCP monitor with destination port set to 5061. This setting enables the monitor to track the health of the TLS service listening on port 5061.

Navigate to Load Balancing > Monitors, click Add, and enter the values as shown in the screen shot.

Click Create and then click Close.

To create a TCP monitor using the NetScaler command line

At the NetScaler command prompt, type:

```
add lb monitor OCS_Custom_TCP TCP -LRTM DISABLED -destPort 5061
```
Step 2. Creating Services for DCOM and Conferencing Servers

You need to create services for each front end server and bind monitors to the services. The DCOM servers listen on port 135. Therefore, you need to create a service with port 135 and bind a customized monitor to track the health of the server, as shown in the following screen shot.

Because the SIP traffic uses long-lived connections, the maximum client time-out and server time-out values need to be high. In this case, we set them to 1200 seconds, as shown in the following screen shot.

To create DCOM service using the NetScaler command line

At the NetScaler command prompt, type:

```
add service OCSE_DCOM_01 10.18.182.251 TCP 135 -svrTimeout 1200
add service OCSE_DCOM_02 10.18.12.253 TCP 135 -svrTimeout 1200
```

To bind a monitor to the DCOM services using the NetScaler command line

At the NetScaler command prompt, type:

```
bind lb monitor OCS_Custom_TCP OCSE_DCOM_02
bind lb monitor OCS_Custom_TCP OCSE_DCOM_01
```

The conferencing servers listen on port 444. Therefore, you need to create a service with port 444 and bind a customized monitor to track the health of the server, as shown in the following screen shot.

Navigate to Load Balancing > Services, click Add and enter the values as shown in the screen shot.

Select the monitor and click Add to bind the monitor to the service.
To create services and bind monitor using the NetScaler command line
At the NetScaler command prompt, type:

```
add service OCSE_Conf_01 10.18.182.251 TCP 444 -svrTimeout 1200
add service OCSE_Conf_02 10.18.12.253 TCP 444 -svrTimeout 1200
bind lb monitor OCS_Custom_TCP OCSE_Conf_02
bind lb monitor OCS_Custom_TCP OCSE_Conf_01
```

Step 3. Creating Vservers for DCOM and Conferencing Services
This section covers the steps to configure vservers for DCOM and conferencing services.

Create a vserver for the DCOM services and bind the DCOM services to the vserver.

Navigate to Load Balancing > Vservers, click Add and enter the values as shown in the screen shot.

To bind services to the vserver, select the services in the Services tab.

Click the Advanced tab.

Because the SIP traffic uses long-lived connections, the maximum client time-out value must be high. In this case, it is set to set to 1200 seconds as shown in the following screen shot.
To create DCOM vservers using the NetScaler command line
At the NetScaler command prompt, type:

```
add lb vserver VIP_OCS_DCOM_135 TCP 10.102.29.35 135 -persistenceType NONE -cltTimeout 1200
```

To bind DCOM services to DCOM vservers using the NetScaler command line
At the NetScaler command prompt, type:

```
bind lb vserver VIP_OCS_DCOM_135 OCSE_DCOM_01
bind lb vserver VIP_OCS_DCOM_135 OCSE_DCOM_02
```

Similarly, create a vserver for the conferencing services and bind the conferencing services to the vserver.
To create conferencing vservers and bind conferencing services using the NetScaler command line

At the NetScaler command prompt, type:

```
add lb vserver VIP_OCS_Conf_444 TCP 10.102.29.40 444 -clt -Timeout 1200
```

```
bind lb vserver VIP_OCS_Conf_444 OCSE_Conf_01
bind lb vserver VIP_OCS_Conf_444 OCSE_Conf_02
```
Load Balancing SIP-TLS Traffic

The Standard Edition Servers and Enterprise pools use SIP-TLS for all internal SIP communications between servers and Office Communicator. Office Communicator uses SIP-TLS for SIP communications internally and for SIP/MTLS authentication of Audio and Video users. Communications flow outbound through the internal firewall. Therefore, the NetScaler provides load balancing for SIP-TLS traffic.

Navigate to Load Balancing > Vservers click Add, and enter the values shown in the screenshot.

Select the services that must be bound to the vserver and click the Advanced tab.

Enter the Client Time-out (secs) value as shown in the screen shot.

Click Create, and then click Close.
To configure load balancing for SIP-TLS traffic using the NetScaler command line
At the NetScaler command prompt, type:

```
add lb vserver VIP_OCS_TLS_5061 TCP 10.102.29.36 5061 clt-Timeout 1200
add service OCSE_SIP_TLS_TCP_01 10.18.182.251 TCP 5061 -svr-Timeout 1200
add service OCSE_SIP_TLS_TCP_02 10.18.12.253 TCP 5061 -svr-Timeout 1200
bind lb vserver VIP_OCS_TLS_5061 OCSE_SIP_TLS_TCP_01
bind lb vserver VIP_OCS_TLS_5061 OCSE_SIP_TLS_TCP_02
```

Load Balancing HTTPS Traffic
Front-end servers communicate to the Web farm FQDNs (the URLs used by Web Components) by using HTTPS. HTTPS traffic is also used to the pool URLs and to communicate to the Web Components Servers.

Navigate to Load Balancing > Vservers, click Add, and enter the values shown in the screen shot.

Select the services that must be bound to the vserver and click the Advanced tab.
To configure load balancing for HTTPS traffic using the NetScaler command line

At the NetScaler command prompt, type:

```
add lb vserver VIP_OCS_SSL_443 SSL_BRIDGE 10.102.29.37 443
add service OCSE_SSL_01 10.18.182.251 SSL_BRIDGE 443
add service OCSE_SSL_02 10.18.12.253 SSL_BRIDGE 443
bind lb vserver VIP_OCS_SSL_443 OCSE_SSL_01
bind lb vserver VIP_OCS_SSL_443 OCSE_SSL_02
```

Enter the Client Time-out (secs) value as shown in the screen shot.

Click Create, and then click Close.
Navigate to Load Balancing > Vservers; click Add.

Enter the values as shown in the screenshot.

Select the services that must be bound to the vserver and click the Advanced tab.

Enter the Client Time-out (secs) value as shown in the screenshot.

Click Create, and then click Close.

To configure load balancing for SIP traffic using the NetScaler command line:

At the NetScaler command prompt, type:

```
add lb vserver VIP_OCS_SIP_5060 TCP 10.102.29.38 5060 -persistenceType NONE -cltTimeout 1200
add service OCSE_SIP_TCP_01 10.18.182.251 TCP 5060 -svrTimeout 1200
add service OCSE_SIP_TCP_02 10.18.12.253 TCP 5060 -svrTimeout 1200
bind lb vserver VIP_OCS_SIP_5060 OCSE_SIP_TCP_01
bind lb vserver VIP_OCS_SIP_5060 OCSE_SIP_TCP_02
```
Appendix A – Configuration Summary

#NS9.0 Build 68.1

# File contains user comments

# To use the load balancing feature, first enable load balancing.

enable ns feature LB

# Configure the modes of packet forwarding

enable ns mode FR L3 CKA MBF Edge

# Configure the link aggregate channel protocol

# Enables network devices to exchange link aggregation information

set lacp -sysPriority 12

# Customize the interface settings for your network interfaces

set interface 1/1 -flowControl ON -haMonitor OFF -lacpMode DISABLED
-throughput 0 -bandwidthHigh 0 -bandwidthNormal 0

set interface 1/2 -lacpMode DISABLED -throughput 0 -bandwidthHigh 0
-bandwidthNormal 0

set interface 1/3 -flowControl ON -haMonitor OFF -lacpMode DISABLED
-throughput 0 -bandwidthHigh 0 -bandwidthNormal 0

set interface 1/4 -haMonitor OFF -lacpMode DISABLED -throughput 0
-bandwidthHigh 0 -bandwidthNormal 0

set interface 1/5 -flowControl ON -haMonitor OFF -lacpMode ACTIVE
-lacpKey 2 -throughput 0 -bandwidthHigh 0 -bandwidthNormal 0

set interface 1/6 -haMonitor OFF -lacpMode DISABLED -throughput 0
-bandwidthHigh 0 -bandwidthNormal 0

set interface 1/7 -flowControl RXTX -haMonitor OFF -lacpMode DISABLED
-throughput 0 -bandwidthHigh 0 -bandwidthNormal 0

set interface 1/8 -speed 100 -duplex FULL -flowControl RXTX -haMonitor
OFF -lacpMode DISABLED -throughput 0 -bandwidthHigh 0
-bandwidthNormal 0

# Configure link aggregate channels

# Increases the capacity and availability of the communication channel

add channel LA/1 -ifnum 1/2 1/3 -Mode MANUAL -connDistr ENABLED
-macDistr BOTH -speed 10 -flowControl OFF -haMonitor ON -trunk OFF
-throughput 0 -bandwidthHigh 0 -bandwidthNormal 0

set channel LA/2 -Mode AUTO -connDistr ENABLED -macDistr BOTH
-haMonitor OFF -trunk OFF -throughput 0 -bandwidthHigh 0
-bandwidthNormal 0

# Configure Server Objects

# The server object is usually created when you create a service

add server 10.18.182.251 10.18.182.251

add server 10.18.12.253 10.18.12.253

# Configure services

add service OCSE_DCOM_01 10.18.182.251 TCP 135 -svrTimeout 1200

add service OCSE_DCOM_02 10.18.12.253 TCP 135 -svrTimeout 1200
add service OCSE_Conf_01 10.18.182.251 TCP 444 -svrTimeout 1200
add service OCSE_Conf_02 10.18.12.253 TCP 444 -svrTimeout 1200
add service OCSE_SIP_TLS_TCP_01 10.18.182.251 TCP 5061 -svrTimeout 1200
add service OCSE_SIP_TLS_TCP_02 10.18.12.253 TCP 5061 -svrTimeout 1200
add service OCSE_SIP_TLS_TCP_01 10.18.182.251 TCP 5060 -svrTimeout 1200
add service OCSE_SIP_TLS_TCP_02 10.18.12.253 TCP 5060 -svrTimeout 1200
#Configure Vservers
add lb vserver VIP_OCS_DCOM_135 TCP 10.102.29.35 135 -cltTimeout 1200
add lb vserver VIP_OCS_Conf_444 TCP 10.102.29.40 444 -cltTimeout 1200
add lb vserver VIP_OCS_TLS_5061 TCP 10.102.29.36 5061 -cltTimeout 1200
add lb vserver VIP_OCS_TLS_5061 TCP 10.102.29.36 5061 -cltTimeout 1200
add lb vserver VIP_OCS_SSL_443 SSL_BRIDGE 10.102.29.37 443 -cltTimeout 180
add lb vserver VIP_OCS_SIP_5060 TCP 10.102.29.38 5060 -cltTimeout 1200
#Bind services to vservers
bind lb vserver VIP_OCS_DCOM_135 OCSE_DCOM_01
bind lb vserver VIP_OCS_DCOM_135 OCSE_DCOM_02
bind lb vserver VIP_OCS_Conf_444 OCSE_Conf_01
bind lb vserver VIP_OCS_Conf_444 OCSE_Conf_02
bind lb vserver VIP_OCS_TLS_5061 OCSE_SIP_TLS_TCP_01
bind lb vserver VIP_OCS_TLS_5061 OCSE_SIP_TLS_TCP_02
bind lb vserver VIP_OCS_TLS_5061 OCSE_SIP_TLS_TCP_02
bind lb vserver VIP_OCS_SIP_5060 OCSE_SSL_01
bind lb vserver VIP_OCS_SIP_5060 OCSE_SIP_TFTP_02
bind lb vserver VIP_OCS_SIP_5060 OCSE_SIP_TFTP_01
bind lb vserver VIP_OCS_SIP_5060 OCSE_SIP_TFTP_02
# Create custom monitor
add lb monitor OCS_Custom_TCP TCP -LRTM DISABLED -destPort 5061
#Bind the custom monitors to services
bind lb monitor OCS_Custom_TCP OCSE_Conf_02
bind lb monitor OCS_Custom_TCP OCSE_Conf_01
bind lb monitor OCS_Custom_TCP OCSE_DCOM_02
bind lb monitor OCS_Custom_TCP OCSE_DCOM_01
#Set SIP parameters for SIP traffic
set lb sipParameters -addRportVip ENABLED
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®, and NetScaler® 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.