

MS Lync 2010

Deployment Guide

UPDATED: 28 July 2023

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

These materials and all Progress® software products are copyrighted and all rights are reserved by Progress Software Corporation. The information in these materials is subject to change without notice, and Progress Software Corporation assumes no responsibility for any errors that may appear therein. The references in these materials to specific platforms supported are subject to change.

#1 Load Balancer in Price/Performance, 360 Central, 360 Vision, Chef, Chef (and design), Chef Habitat, Chef Infra, Code Can (and design), Compliance at Velocity, Corticon, Corticon.js, DataDirect (and design), DataDirect Cloud, DataDirect Connect, DataDirect Connect64, DataDirect XML Converters, DataDirect XQuery, DataRPM, Defrag This, Deliver More Than Expected, DevReach (and design), Driving Network Visibility, Flowmon, Inspec, Ipswitch, iMacros, K (stylized), Kemp, Kemp (and design), Kendo UI, Kinvey, LoadMaster, MessageWay, MOVEit, NativeChat, OpenEdge, Powered by Chef, Powered by Progress, Progress, Progress Software Developers Network, SequeLink, Sitefinity (and Design), Sitefinity, Sitefinity (and design), Sitefinity Insight, SpeedScript, Stylized Design (Arrow/3D Box logo), Stylized Design (C Chef logo), Stylized Design of Samurai, TeamPulse, Telerik, Telerik (and design), Test Studio, WebSpeed, WhatsConfigured, WhatsConnected, WhatsUp, and WS_FTP are registered trademarks of Progress Software Corporation or one of its affiliates or subsidiaries in the U.S. and/or other countries.

Analytics360, AppServer, BusinessEdge, Chef Automate, Chef Compliance, Chef Desktop, Chef Workstation, Corticon Rules, Data Access, DataDirect Autonomous REST Connector, DataDirect Spy, DevCraft, Fiddler, Fiddler Classic, Fiddler Everywhere, Fiddler Jam, FiddlerCap, FiddlerCore, FiddlerScript, Hybrid Data Pipeline, iMail, InstaRelinker, JustAssembly, JustDecompile, JustMock, KendoReact, OpenAccess, PASOE, Pro2, ProDataSet, Progress Results, Progress Software, ProVision, PSE Pro, Push Jobs, SafeSpaceVR, Sitefinity Cloud, Sitefinity CMS, Sitefinity Digital Experience Cloud, Sitefinity Feather, Sitefinity Thunder, SmartBrowser, SmartComponent, SmartDataBrowser, SmartDataObjects, SmartDataView, SmartDialog, SmartFolder, SmartFrame, SmartObjects, SmartPanel, SmartQuery, SmartViewer, SmartWindow, Supermarket, SupportLink, Unite UX, and WebClient are trademarks or service marks of Progress Software Corporation and/or its subsidiaries or affiliates in the U.S. and other countries. Java is a registered trademark of Oracle and/or its affiliates. Any other marks contained herein may be trademarks of their respective owners.

Please refer to the NOTICE.txt or Release Notes – Third-Party Acknowledgements file applicable to a particular Progress product/hosted service offering release for any related required third-party acknowledgements.

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

Table of Contents

1 Introduction **7**

1.1 Document Purpose 7

1.2 Prerequisites 8

2 Microsoft Lync Server 2010 Overview **9**

2.1 Server Roles 9

2.1.1 Standard Edition Server 9

2.1.2 Enterprise Edition - Front End Server and Back End Server 10

2.1.3 A/V Conferencing Server 11

2.1.4 Edge Server 11

2.1.5 Mediation Server 11

2.1.6 Monitoring Server 12

2.1.7 Archiving Server 12

2.1.8 Director Server 12

2.1.9 File Server 12

2.2 High Availability Concepts 13

2.2.1 Standard Edition Server 13

2.2.2 Front-End Server and Back-End Server 13

2.2.3 A/V Conferencing Server 13

2.2.4 Edge Server 13

2.2.5 Mediation Server 14

2.2.6 Monitoring & Archiving Server 14

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

2.2.7 Director 14
2.3 Overview of High Availability options per Lync Server Role 14
2.4 Advantages to using a Kemp LoadMaster 15
2.5 Optimizing the Kemp LoadMaster for Microsoft Lync 2010 15
2.5.1 Microsoft Terminology vs Kemp Terminology 15
2.5.1.1 Microsoft Terminology 15
2.5.2 Load Balancer Deployment Options 16
2.5.2.1 Lync Internal Server Deployment Options 16
2.5.2.2 Lync External Edge Server Deployment Options 17
2.5.3 SSL Acceleration (SSL Offloading) 17
2.5.4 L7 Transparency 19
2.5.5 Persistence 19
2.5.6 Idle Connection Timeout 20
2.5.7 Port Configuration 20
2.5.8 Connection Scaling 20
3 Hardware Load Balancing vs DNS Load Balancing for Lync 2010 21
3.1 Hardware Load Balancing 21
3.2 DNS Load Balancing 21
3.3 DNS Load Balancing Matrix 22
4 Network Deployment Examples 23
4.1 Typical Deployment Option 24
4.2 Alternative Deployment Option 1 25

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

4.3 Alternative Deployment Option 2 27

5 General Configuration 29

5.1 Disable Global SNAT 29

5.2 Subnet Originating Requests 29

5.3 Change Drop Connections Settings 30

5.4 Increase the Connection Timeout 31

5.5 Connection Scaling For Large Scale Deployments 31

6 Load Balancing Lync Front-End Servers 34

6.1 Required Services for Front-End Pools 34

6.2 Optional Services for Front-End pools 35

6.3 Configuring a Virtual Service for SIP services on the Lync Front-End Servers 36

6.4 Configuring Virtual Services for Additional Services on the Lync Front-End Servers 38

6.5 Configuring a Virtual Service for Internal HTTPS-based Services for the Front-End Servers 39

6.6 Configuring a Virtual Service for External HTTPS-based Services for the Front-End Servers 40

7 Load Balancing Lync Director Servers 43

7.1 Required Services for Director Pools 43

7.2 Configuring a Virtual Service for SIP Services on the Director Servers 44

8 Load Balancing Internal Lync Edge Servers 46

8.1 Required Services for Internal-Facing Edge Pools 46

8.2 Configuring a Virtual Service for SIP Services on the Internal EDGE Servers 47

8.3 Configuring Virtual Services for Additional Services on the Lync Internal Edge Servers 49

8.4 Configuring a Virtual Service for Audio & Video Services on the Internal EDGE Servers 49

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

9 Load Balancing External Lync Edge Servers 51

9.1 Required Services for External-Facing Edge Pools 51

9.2 Optional Services for External-Facing Edge Pools 51

9.3 Configuring a Virtual Service for SIP Services on the External EDGE Servers 53

9.4 Configuring a Virtual Service for Remote User Services on the External EDGE Servers 54

9.5 Configuring a Virtual Service for Conferencing Services on the External EDGE Servers 55

9.6 Configuring a Virtual Service for TCP Audio/Video Services on the External EDGE Servers 57

9.7 Configuring a Virtual Service for UDP Audio/Video Services on the External EDGE Servers 58

10 Using the LoadMaster as a Reverse Proxy 61

10.1 Lync Reverse Proxy HTTP Virtual Service 61

10.2 Lync Reverse Proxy HTTPS Virtual Service 62

References 64

Last Updated Date 65

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

1 Introduction

An enterprise, high available deployment of Lync Server requires deploying multiple servers in Front End pools, Director pools, and or Edge Server pools. Load balancing is necessary when using multiple servers in a pool as the load balancer distributes traffic among the servers.

Microsoft Lync Server 2010 supports two load balancing solutions: DNS load balancing and hardware load balancing. You can choose different load balancing solutions for each pool in your deployment. Hardware load balancers are also required to provide load balancing for the internal and external web services when DNS load balancing is used.

The Kemp LoadMaster combines versatility with ease-of-use to speed deployment of the complete portfolio of advanced messaging applications and protocols used by Microsoft Lync Server 2010. Layer 7 health checking at the LoadMaster ensures that should one of the servers become inaccessible, the load balancer will take that server off-line, while automatically re-routing and reconnecting users to other functioning servers.

The entire Kemp LoadMaster product family, including the Virtual LoadMaster (VLM) supports Microsoft Lync 2010.

For more information about Kemp, visit us online at www.kemptechnologies.com.

1.1 Document Purpose

This manual addresses how to deploy and configure a LoadMaster appliance with Microsoft Lync Server 2010. Specifically, configuration information applies to Front-End pools, Director pools and Edge pools.

Kemp's LoadMaster family of products is available in various models to support networks of different throughput requirements.

Images used in this manual are samples to help you determine if you are "in the right place" when actually performing the configuration.

Certain procedures contain instructions that refer to a website. If you are configuring your LoadMaster and at the same time you need to access a website, you should do so in a new and different browser session (that is, do not use your web browser to access/configure the LoadMaster and then prior to finishing your configuration, browse to a different page and then use the **Back** button or other method to return to the LoadMaster).

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

1.2 Prerequisites

It is assumed that the reader is a network administrator or a person otherwise familiar with networking and general computer terminology. It is further assumed that you have set up your Microsoft Lync Server 2010 environment and have installed your Kemp LoadMaster.

At a minimum, you should have:

- At least LoadMaster firmware 5.1-74
- Configured and published Microsoft Lync Server architecture with Lync Topology builder
- Installed your Microsoft Servers, Active Directories and followed other Microsoft requirements
- Configured Internal and External DNS entries for Front-End, Director and Edge pools
- Established access to the LoadMaster Web User Interface (WUI)
- Tested the Microsoft Lync 2010 Server on voice, Instant Messaging (IM), Presence, Desktop Collaboration and Audio Visual (AV) conferencing applications. Testing should have been performed for both internal and external users
- Tested using Microsoft Lync Server 2010 Enterprise Server with the 64-bit Microsoft SQL Server Enterprise Edition Version 2008 R2.
- Ensured that all Lync 2010 Server Components are running on Windows 2008 R2 (64-bit) Standard Edition Server Operating System.
- Ensured that Lync Clients are running on a Windows 7 Operating System

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

2 Microsoft Lync Server 2010 Overview

2.1 Server Roles

Lync server 2010 supports distinct server roles:

- Standard Edition Server
- Front End Server and Back End Server
- A/V Conferencing Server
- Edge Server
- Mediation Server
- Monitoring Server
- Archiving Server
- Director

For most server roles, for scalability and high availability, pools of multiple servers can be deployed. Each server in a pool must run an identical server role or roles. For some types of pools in Lync Server, a load balancer must be deployed to spread traffic between the various servers in the pool. The table below provides a scalability overview for all server roles when installed on physical servers.

2.1.1 Standard Edition Server

The Standard Edition server is designed for small organizations, and for pilot projects of large organizations. It enables many of the features of Lync Server 2010, including the necessary databases, to run on a single server thus combining many of the server roles on one server.

Standard Edition server offers instant messaging (IM), presence, conferencing, and Enterprise Voice, all from one server. One Standard Edition server supports as many as 5,000 users if deployed as a physical server.

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

2.1.2 Enterprise Edition - Front End Server and Back End Server

The Front End server is the core server role, and runs many basic Lync Server functions. The Front End servers, along with the Back End Servers that provide the database, are the only server roles required to be in any Lync Server Enterprise Edition deployment.

Front End server includes the following functionality:

- User authentication and registration
- Presence information and contact card exchange
- Address book services and distribution list expansion
- IM functionality, including multiparty IM conferences
- Web conferencing and application sharing (if deployed)
- Application hosting services, for both applications included with Lync Server (for example, Conferencing Attendant and Response Group application) and third-party applications
- Application services for application hosting and hosts applications (for example, Response Group application, and several others)

Additionally, one Front End pool in the deployment also runs the Central Management Server, which manages and deploys basic configuration data to all servers running Lync Server 2010. The Central Management Server also provides the Lync Server Management Shell and file transfer capabilities.

The Back End Servers are database servers running Microsoft SQL Server that provide the database services for the Front End pool. Back End Servers do not run any Lync Server software. If a SQL Server cluster is already deployed for other applications, this cluster can be used for Lync Server 2010, if performance allows.

Information stored in the Back End Server databases includes presence information, users' Contacts lists, conferencing data including persistent data about the state of all current conferences, and conference scheduling data.

Front End Server Scalability

A Front End pool, if deployed on physical hardware, should have one Front End server for every 10,000 users homed in the pool, plus an additional Front End server to provide good performance when one server is unavailable. The maximum number of users in one Front End pool is 80,000. If the number of users exceeds 80,000 users at a site, additional Front End pools can be deployed. To provide High Availability at least two Front End servers are required.

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

The additional Front End server ensures good performance in case one server is unavailable. When an active server is unavailable, its connections are transferred automatically to the other servers in the pool.

2.1.3 A/V Conferencing Server

The A/V Conferencing Server provides A/V conferencing functionality to the deployment. It can be collocated with Front End server, or deployed separately as a single server or A/V Conferencing Server pool. If a site has more than 10,000 users, it is recommended to deploy a separate A/V Conferencing pool.

A/V Conferencing Server Scalability

If A/V Conferencing Server is deployed separately, one physical A/V Conferencing Server for each 20,000 users at a site is needed.

2.1.4 Edge Server

The Edge Server enables the users to communicate and collaborate with users outside the organization's firewalls. These external users can include the organization's own users who are currently working offsite, users from federated partner organizations, and outside users who have been invited to join conferences hosted on your Lync Server deployment. Edge Server also enables connectivity to public IM connectivity services, including Windows Live, AOL, and Yahoo!.

Edge Server Scalability

For performance, one physical Edge Server should be deployed for every 15,000 users that are expected to access a site remotely.

2.1.5 Mediation Server

A Mediation Server is a necessary component for implementing Enterprise Voice and dial-in conferencing. The Mediation Server translates signalling and, in some configurations, media between the internal Lync Server infrastructure and a public switched telephone network (PSTN) gateway, IP-Private Branch Exchange (PBX), or a Session Initiation Protocol (SIP) trunk.

Mediation Server Scalability

A co-located Mediation server scales to a maximum of 226 concurrent calls. If the call volume exceeds this maximum number a dedicated Mediation server can be deployed. A dedicated server scales to, depending of the hardware and the ration remote vs. internal users, to a maximum of 1,200 concurrent calls per server.

For full details refer to: http://technet.microsoft.com/en-us/library/gg615015.aspx

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

2.1.6 Monitoring Server

The Monitoring Server collects data about the quality of the network media, in both Enterprise Voice calls and A/V conferences. This information can help to provide the best possible media experience for the users. It also collects Call Error Records (CERs), which can be used to troubleshoot failed calls. Additionally, it collects usage information in the form of Call Detail Records (CDRs) about various Lync Server features. These metrics can be used to calculate return on investment of the Lync deployment, and plan the future growth.

Monitoring Server Scalability

One physical Monitoring Server can support up to 250,000 users if not collocated with Archiving Server. If collocated, it can support up to 100,000 users.

2.1.7 Archiving Server

The Archiving Server enables archiving of IM communications and meeting content for compliance reasons.

Archiving Server Scalability

One physical Archiving Server can support up to 500,000 users if not collocated with Monitoring Server. If collocated, it can support up to 100,000 users.

2.1.8 Director Server

Directors can be used to authenticate Lync Server user requests, but do not home user accounts, or provide presence or conferencing services. Directors are most useful in deployments that enable external user access, where the Director can authenticate requests before sending them on to internal servers. Directors can also improve performance in organizations with multiple Front End pools.

Director Server Scalability

For performance, one physical Director should be deployed for every 15,000 users who will access a site remotely. At a minimum it is recommend deploying two Directors for high availability.

2.1.9 File Server

Lync Server 2010 requires a file share for several services including the address book service, conferencing data and device update files. The file share is supported on either Direct Attached Storage (DAS) or a Storage Area Network (SAN), including Distributed File System (DFS), and on a Redundant Array of Independent Disks (RAID).

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

Lync Server 2010 supports the use of a shared cluster for the file shares in the Lync deployment. If a shared cluster for the file shares is used in the Lync deployment, the Cluster Administrator should be used to create the file shares.

2.2 High Availability Concepts

With the exception of the Archiving and Monitoring role and the standard edition server, all other Lync server roles can be deployed for high availability. The following sections describe the required additional components.

2.2.1 Standard Edition Server

The Standard Edition server combines many of the server roles on one server. High availability options are not available for the Standard Edition server therefore it is recommended to use Lync Server 2010 Enterprise Edition if a highly available solution is required.

2.2.2 Front-End Server and Back-End Server

To improve availability, Front-End servers are deployed in a pool. A Front-End pool is a set of Front-End servers configured identically, that work together to provide services for a common group of users. A pool provides scalability and failover capability to the users. If multiple servers are configured in a pool configuration, Hardware and or DNS load balancing is required to distribute the load and enable failover.

Increasing the availability of the Back-End servers can be achieved by deploying a cluster of two or more servers.

2.2.3 A/V Conferencing Server

Conferencing servers can either be deployed co-located on the Front End servers in a pool or as one or more dedicated servers. A co-located pool setup ensures high availability. In the case of a dedicated server deployment it is recommended to deploy at least two A/V Conferencing Servers for high availability.

2.2.4 Edge Server

For further details refer to: http://technet.microsoft.com/en-us/library/gg425716.aspx

If high availability is required, at least two Edge Servers should be deployed in a pool. A single Edge pool will support up to ten Edge Servers. If multiple servers are configured in a pool configuration, hardware and or DNS load balancing is required to distribute the load and enable failover.

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

2.2.5 Mediation Server

To improve availability, multiple Mediation servers can be deployed. The Enterprise Voice routing component will reroute voice traffic in the case of server or connection failure.

2.2.6 Monitoring & Archiving Server

A Monitoring and/or Archiving server outage will not negatively affect overall Lync service availability. Both server roles use Microsoft message queuing for data exchange and are therefore less susceptible to failure. If an Archiving or Monitoring server fails, messages will remain in the queue until the server is available again. The availability of the server role can be improved by upgrading the hardware specifications and clustering the Back-End database server. It is possible to configure the archiving service as critical for the Lync deployment; this will cause the Lync services to pause if the archiving service is unavailable for a longer period of time and prevent messages from not being archived. For this mode of operation a standby sever could be considered to improve availability.

2.2.7 Director

Similar to the Front End server, Director server availability can be increased by deploying multiple director servers in a pool. A pool of Directors must be load balanced by either a hardware load balancer or by implementing Domain Name System (DNS) load balancing to take care of the SIP traffic.

2.3 Overview of High Availability options per Lync Server Role

Role	High Availability	Load Balancer	DNS Load Balancing
Standard Edition Server	Not Available	N/A	N/A
Enterprise Edition Front-End server	Deploy multiple servers in a Pool and use load balancing	Yes	Yes
Back End Server	SQL Server uses Windows Clustering for High Availability	No	No
A/V Conferencing Server	Deploy Multiple Servers in a pool. load balancing not required	N/A	N/A
Edge Server	Deploy Multiple Servers in a pool and use load balancing	Yes	Yes
Mediation Server	Deploy Multiple Servers in a pool and use	Yes	Yes

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

Role	High Availability	Load Balancer	DNS Load Balancing
	load balancing		
Monitoring	Standby Server (MSMQ on the Front-End queues messages in the event of a failure)	No	No
Archiving	Standby Server (MSMQ on the Front-End queues messages in the event of a failure)	No	No
Director	Deploy Multiple Servers in a pool and use load balancing	Yes	Yes
File Server	Use Windows Clustering or Distributed File System	No	No

2.4 Advantages to using a Kemp LoadMaster

The Kemp LoadMaster offers performance, security and functional advantages that combine versatility with ease-of-use to speed deployment of the Microsoft Lync infrastructure. Layer 7 health checking at the LoadMaster ensures that should one of the servers become inaccessible, the LoadMaster will take that server off-line.

2.5 Optimizing the Kemp LoadMaster for Microsoft Lync 2010

The Kemp LoadMaster has features and capabilities in addition to those described in this manual, however, these features and capabilities in particular can be used to optimize the configuration of LoadMaster to work best with your Lync 2010 server load balancing requirements.

2.5.1 Microsoft Terminology vs Kemp Terminology

2.5.1.1 Microsoft Terminology

Load balancers can be configured to support Network Address Translation (NAT) using one of the following modes:

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

- **Full-NAT (SNAT) mode** (also known as proxy, secure NAT, source NAT, or SNAT mode): In full-NAT mode, both the source and IP destinations are changed as packets pass through the load balancer.
- **Half-NAT (DNAT) mode** (also known as transparency, destination NAT, DNAT mode or Load Balancers Default Gateway LBDG): In half-NAT mode, the destination IP address is changed as packets pass through the load balancer, but the source IP address remains intact.

> Load balancing using Direct Server Return configuration is not supported.

The following table describes the supported configurations for full-NAT and half-NAT modes.

Load-Balanced Pools	Supported NAT Modes	Notes
Enterprise pools and Communicator Web Access	Full-NAT (SNAT)	Half-NAT is not supported for load balancing of internal pools because inter-server communications within an internal pool fail when servers in the pool try to connect to their own VIP
Edge pools	Full-NAT (SNAT) and Half-NAT (DNAT)	The VIP for the external interface of Edge Servers should be set to half-NAT or full-NAT only for traffic to the edge (for each VIP that is used for Edge Servers and HTTP). Also, NAT is not supported for the IP address of the external interface of the A/V Edge Server of an Edge Server, so the IP address of the external interface of the A/V Edge service on each Edge Server must be publicly routable (no NAT).

2.5.2 Load Balancer Deployment Options

The supported deployments of the Lync Server and the Kemp LoadMaster are described in the following sections. Multiple load balancers can be deployed for the Internal Pools, Internal Edge Server and External Edge Server. Single Load Balancers can be used to support both internal and external servers.

2.5.2.1 Lync Internal Server Deployment Options

Non-Transparent (Microsoft SNAT)

- **One-armed topology**

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

This is the typical deployment method allowing the Load Balancer to be in the same network segment as the Real Servers.

- **Two-armed topology**

This topology requires a separate network for the Load Balancer and a separate network for the Real Servers. This requires more configurations networking wise and is considered not a typical deployment.

Transparent (Microsoft DNAT)

- **One-armed topology and two-armed topology**

If you require that the client IP Addresses are retained when the LoadMaster forwards requests to the Lync servers, the transparent mode must be used.

> This topology is not supported as per Microsoft.

2.5.2.2 Lync External Edge Server Deployment Options

One-armed topology & two-armed topology

Transparency must be used when working with load balancers (at least for the Audio and Video EDGE Server).

2.5.3 SSL Acceleration (SSL Offloading)

The Kemp LoadMaster offers SSL acceleration (also referred to as “SSL offloading”) for Virtual Services. With SSL acceleration, the SSL session is terminated at the LoadMaster. Some of the benefits to using SSL acceleration are that the LoadMaster migrates the SSL workload from the Real Servers (which can be hardware accelerated by LoadMaster), can perform Layer 7 processing (such as persistence or content switching), SSL security hardening, and a central point of management of SSL certificates.

With SSL Acceleration, the SSL session is terminated at the LoadMaster and sent to the Real Servers un-encrypted. In some security situations, it may be necessary to encrypt the connection between the LoadMaster and Real Servers. This can be achieved with reverse SSL. Review the LoadMaster manual to configure a reverse SSL deployment.

With reverse SSL, the SSL session is first terminated at the LoadMaster. Persistence and other Layer 7 functionality can then be performed. After that, the traffic is re-encrypted in a new SSL session between the LoadMaster and the Real Server.

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

Without terminating the SSL session at the LoadMaster, the headers and content cannot be read, so persistence cannot be done. The only consistently reliable persistence method available when the SSL session is not terminated at the LoadMaster is Source IP.

Hardware SSL and Software SSL are the two types of SSL termination capabilities available in your LoadMaster. Functionally, hardware and software SSL are the same. The difference is in what part of the LoadMaster handles the actual cryptographic functions associated with SSL operations.

With software SSL, the LoadMaster's general processor handles encryption/decryption tasks. These tasks are shared with other tasks that the LoadMaster performs, such as server load balancing, health checking, and other administrative tasks. Because SSL operations are CPU-intensive, software SSL is sufficient for low levels of SSL traffic but insufficient for higher levels of SSL traffic. Higher connection rates of SSL on a software SSL LoadMaster may degrade overall performance of the LoadMaster.

With hardware SSL, the LoadMaster has a separate specialized processor, which handles all SSL functions. No matter the level of SSL connections, the LoadMaster's general processor is not burdened. This specialized hardware is purpose-built for SSL, and can handle extremely high connection rates (TPS) of SSL traffic.

An SSL certificate is required for all SSL transactions, and as such is required for all SSL-enabled Virtual Services. With the LoadMaster, there are two types of SSL certificates: self-signed certificates generated by the LoadMaster or the administrator and certificates that are signed by a trusted CA (Certificate Authority) such as Digicert, Verisign or Thawte. In addition, with LoadMaster you are managing only one certificate instead of multiple certificates on each Real Server.

When an SSL-enabled Virtual Service is configured on the LoadMaster, a self-signed certificate is installed automatically. Both self-signed and CA signed certificates provide encryption for data in motion. A CA-signed certificate also provides authentication -- a level of assurance that the site is what it reports to be, and not an impostor.

The primary operational difference between a self-signed certificate and a CA certificate is that with a self-signed, certificate cannot be used in conjunction with Lync Server 2010. As such, the Lync 2010 configuration instructions indicate that you would first need to export an appropriately signed certificate from Lync Server 2010 that you may import it into the LoadMaster.

SSL termination is required for load balanced connections to external Lync Web Services, SSL offloading (relieving a web server of all SSL processing) is not supported because Front End servers do not accept unencrypted HTTP requests for Lync Web Services.

By definition, Super HTTP persistence requires SSL termination on the load balancer, otherwise the load balancer would be unable to inspect HTTP traffic to look at the SSL and header Information. Both client_ssl and server_ssl profiles are required for this to work correctly. The client_ssl profile

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

is used to decrypt the request, and as such, the certificate assigned to the client_ssl profile must contain the external web service FQDNs for the Lync Pool. The server_ssl profile is used to re-encrypt the request before routing it on to the Lync Pool.

The following are the requirements and recommendations regarding encryption:

- You must use TLS/MTLS for all communications between Lync Web App and servers that are running Microsoft Lync Server 2010.
- You should always use HTTPS unless SSL offloading is used for performance reasons and other effective security safeguards are in place.
- You may use HTTP for communications between a hardware load balancer or other device and the Lync Web App if SSL offloading is used for performance reasons. In this case, the physical link should be secured.
- Do not use HTTP between the client and the Lync Web App.

2.5.4 L7 Transparency

Newly created Virtual Services on a LoadMaster are set Transparent on a LoadMaster by default. In Transparent mode, the LoadMaster will forward traffic towards the Lync External EDGE Server while retaining the source IP address with which it arrived at the LoadMaster.

For L7 transparency for Lync External EDGE Servers to work properly:

a) The Real Server settings must ensure that all server replies to client requests are routed through the LoadMaster. Typically, this is achieved by making the LoadMaster the Real Server's default gateway.

b) No clients may be located in the same IP subnet with the Real Servers. If necessary, you can use additional ports on the LoadMaster to ensure that Real Servers and Clients are located on distinct IP subnets.

2.5.5 Persistence

Session persistence (a.k.a. Session Affinity or Stickiness) is the ability of the LoadMaster to make sure a given Client always gets to the same Real Server, even across multiple connections. Persistence can make sure that all requests from a client are sent to the same server in a Server Load Balancer (SLB) array or server farm.

Source IP Address persistence is used for all Lync Services except the External Web Services which need to use Super HTTP Persistence.

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

2.5.6 Idle Connection Timeout

If there is no traffic for the period of time specified the connection is timed out and disconnected. The global default is 660 seconds (11 minutes). This value should be adjusted per service type.

For each Virtual Service you can set idle connection timeout values for the connections. In order to make optimal use of your Kemp LoadMaster you should not set these timeout values too low as this could result in clients needing to reestablish a connection, which typically results in the end user is informed to re-authenticate. It is recommended you test which timeout values works best in your specific scenario before the solution goes into production.

> Setting the **Idle Connection Timeout** to **0** ensures that the default L7 connection timeout is used. You can modify the default **Connection Timeout** value by going to **System Configuration > Miscellaneous Options > Network Options**.

2.5.7 Port Configuration

There are many different types of possible data paths. It is recommended that your port configuration stay within the realm of default protocol RFC. However, your Kemp LoadMaster may be configured to use whichever port happens to be most appropriate for your particular network. For more information regarding port definitions, refer to Microsoft documentation at http://technet.microsoft.com/en-us/library/gg398833.aspx

2.5.8 Connection Scaling

LoadMaster is a scalable load balancer, allowing for more than 64,000 client connections to a single Virtual Service at one time. If this is required, you should execute the Connection Scaling for Large Scale Deployments procedure located in the Appendix of this manual.

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

3 Hardware Load Balancing vs DNS Load Balancing for Lync 2010

Microsoft Lync Server 2010 supports two load balancing solutions: DNS load balancing and hardware load balancing. You can choose different load balancing solutions for each pool in your deployment.

3.1 Hardware Load Balancing

Hardware load balancing was the only supported way to deploy a high available Office Communications Server solution. The same functionality is available in Lync Server 2010.

A hardware load balancer is used in an Enterprise pool that has more than one Enterprise Edition server. The load balancer performs the critical role of delivering scalability and high availability across multiple servers that are connected to a centralized database on the Lync Server Back-End Database.

3.2 DNS Load Balancing

DNS load balancing is introduced in Microsoft Lync Server 2010 communications software. The objective of DNS load balancing is to provide a native load balancing mechanism option in Lync Server 2010. A Hardware Load Balancer is still required for Load Balancing the Web traffic.

Domain Name System (DNS) load balancing uses DNS as a way to load-balance across multiple servers. DNS load balancing is implemented at the application level in both servers and clients. They both participate in the load-balancing logic.

Hardware Load Balancer is still required for web traffic. Both HTTP and HTTPS are session-state–oriented protocols. With DNS load balancing, there is no sticky-session state that can be set up. As a result, there is no way to ensure that a session is going to be continued on the correct server. Hardware Load Balancing specifically addresses this session problem by caching the client-server state information. For web-based traffic DNS load balancing is not a solution.

DNS load balancing is not supported in all scenarios.

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

DNS load balancing supports automatic failover only for servers running Lync Server 2010 and Lync Server 2010 clients. Earlier versions of clients and Office Communications Server can still connect to pools running DNS load balancing, but if they cannot make a connection to the first server that DNS load balancing refers them to, they are unable to fail over to another server in the pool.

Additionally, if Exchange Unified Messaging (UM) is used, only Exchange 2010 SP1 has built-in support for Lync Server 2010 DNS load balancing. If an earlier version of Exchange is used, failover capabilities for the following Exchange UM scenarios will not be available:

- Playing their Enterprise Voice mail on their phone
- Transferring calls from an Exchange UM Auto-Attendant

All other Exchange UM scenarios will work properly.

3.3 DNS Load Balancing Matrix

Situation	DNS load balancing supported?	DNS load balancing recommended?	Hardware load balancer (only) recommended?
All or most users homed in the pool run Lync Server 2010 clients	Yes	Yes	
Many users homed in the pool still running older clients	Yes		Yes
Interoperates only with other servers running Lync Server 2010	Yes	Yes	
Interoperates with many servers running earlier versions of Office Communications Server	Yes		Yes
Running Exchange UM with Exchange 2010 SP1 (or not running Exchange UM)	Yes	Yes	

DNS Load Balancing and Hardware Load Balancing setup for web traffic only is not included in this guide.

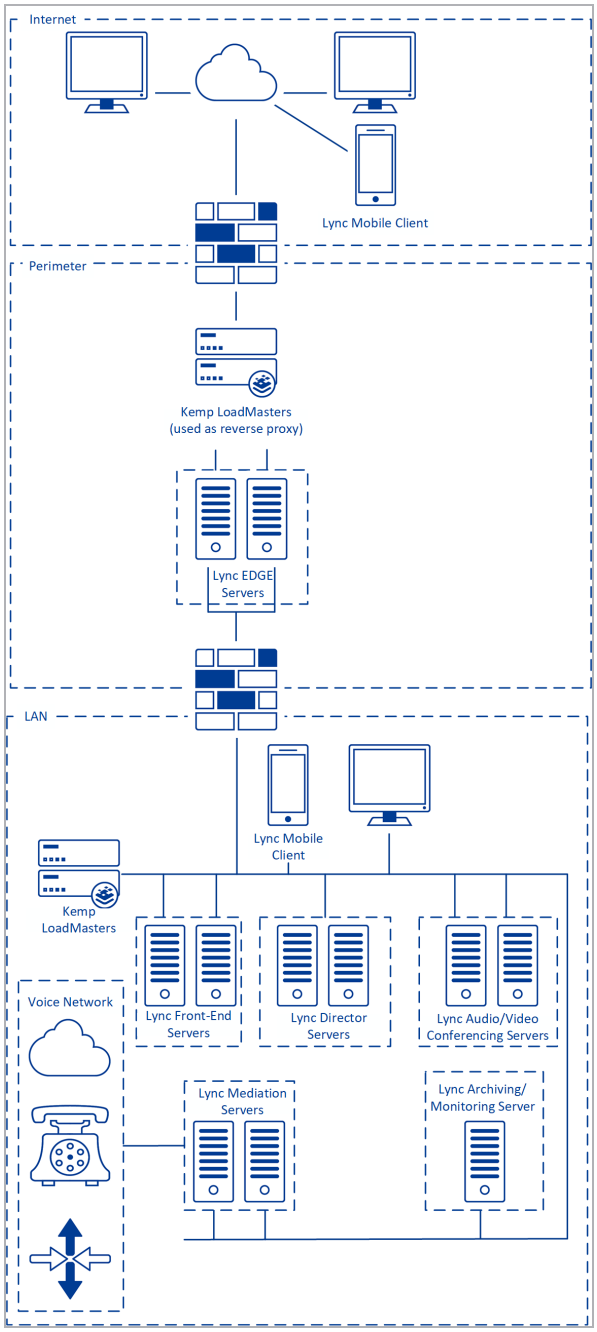
© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

4 Network Deployment Examples

Some network deployment examples are in the sections below.

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

4.1 Typical Deployment Option



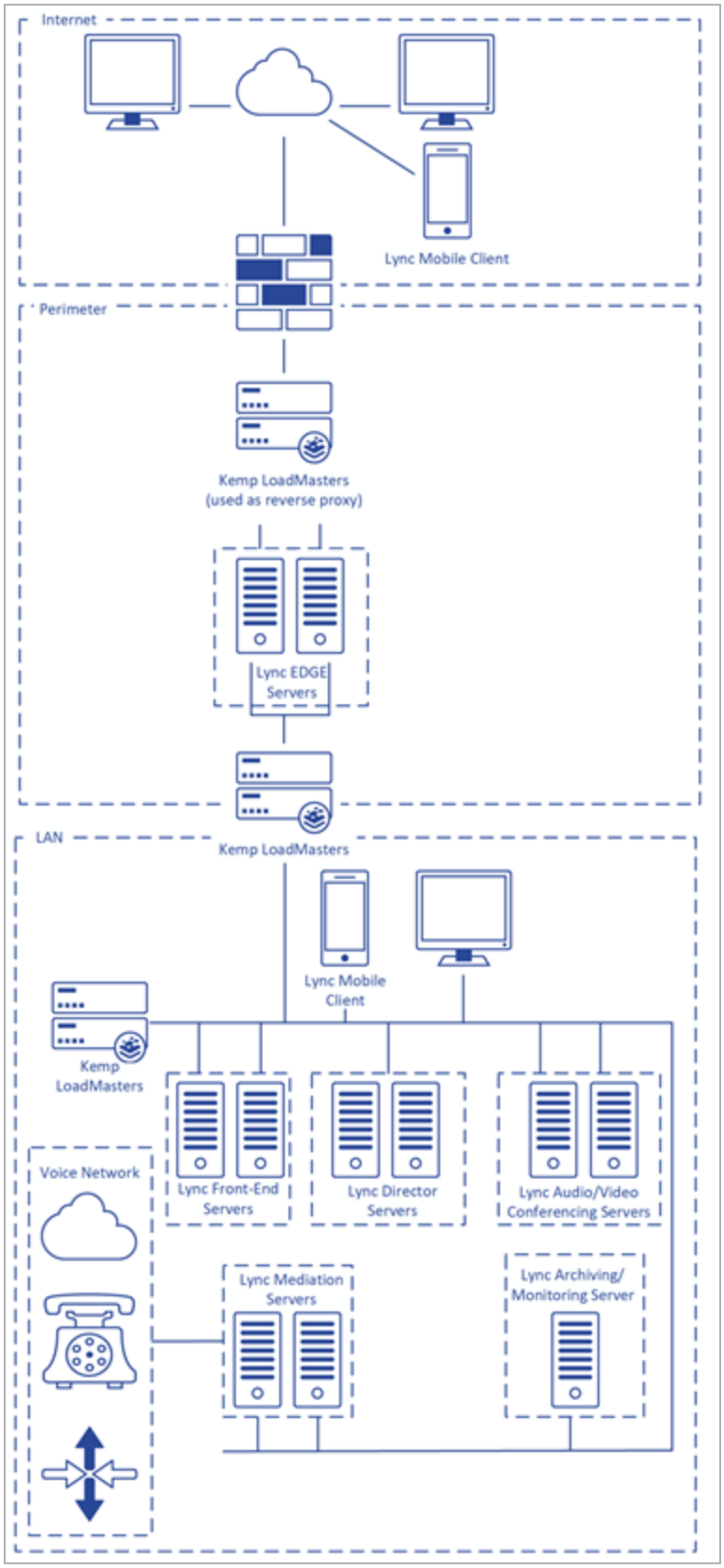
© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

4.2 Alternative Deployment Option 1

One (pair of) Loadmaster(s) is deployed for load balancing all of the Internal Lync Servers (including the internal facing Lync Edge Server Interface) and one (pair of) Loadmaster(s) for load balancing all of the External-facing interfaces for Lync Edge Servers.

> This deployment option departs from the Microsoft recommended standard, as described in http://technet.microsoft.com/en-us/library/gg398478(v=ocs.14).aspx, and may cause some issues in certain network configurations.

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.



© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

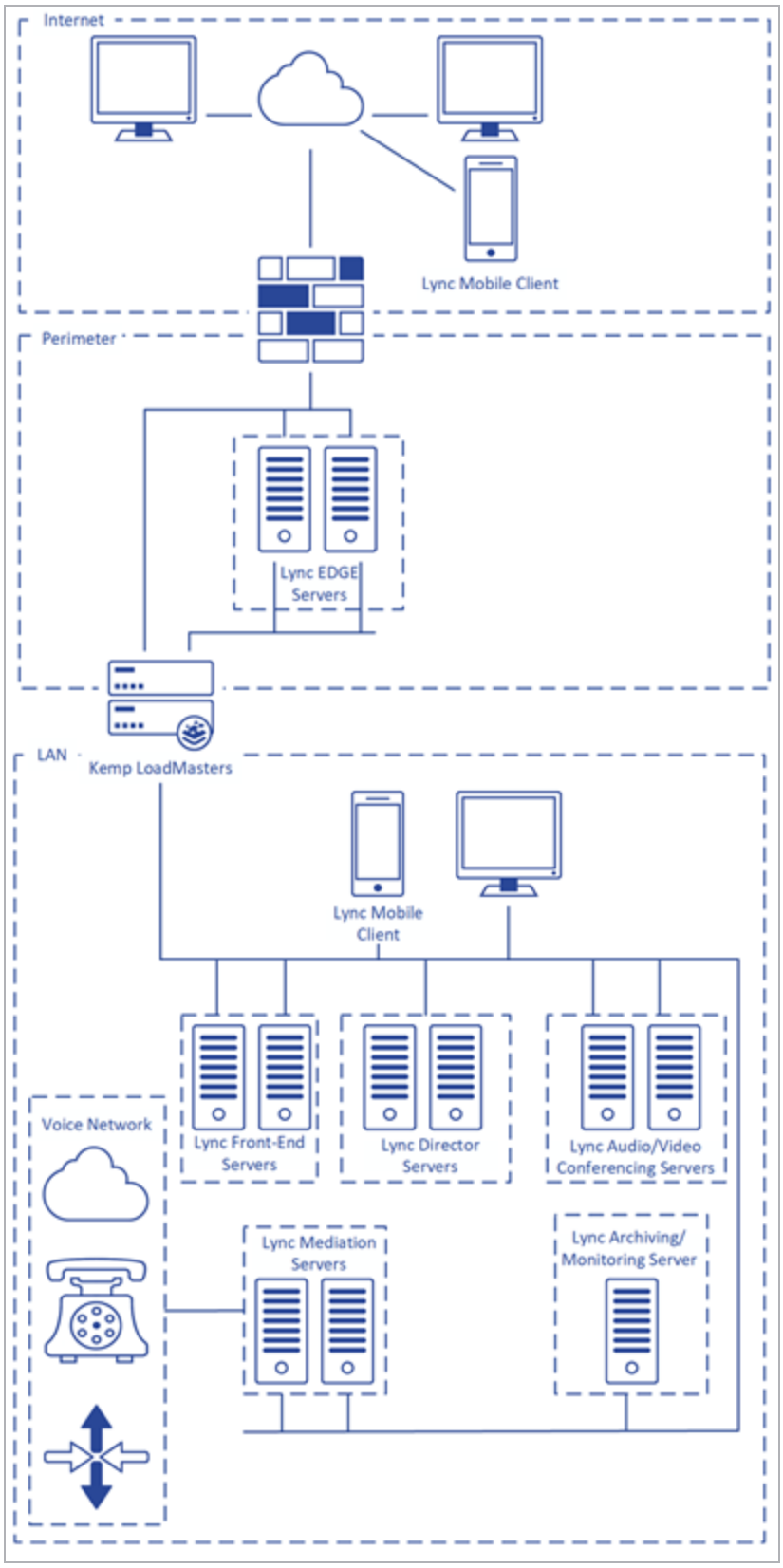
4.3 Alternative Deployment Option 2

One (pair of) Loadmaster(s) is deployed for load balancing all of the Internal Lync Servers and External Lync Edge Servers.

This means that Internal and External traffic traverses the same LoadMaster unit. As a result, a denial of service could impact both the internal and external Lync Server deployment.

This deployment option departs from the Microsoft recommended standard, as described in http://technet.microsoft.com/en-us/library/gg398478(v=ocs.14).aspx, and may cause some issues in certain network configurations.

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.



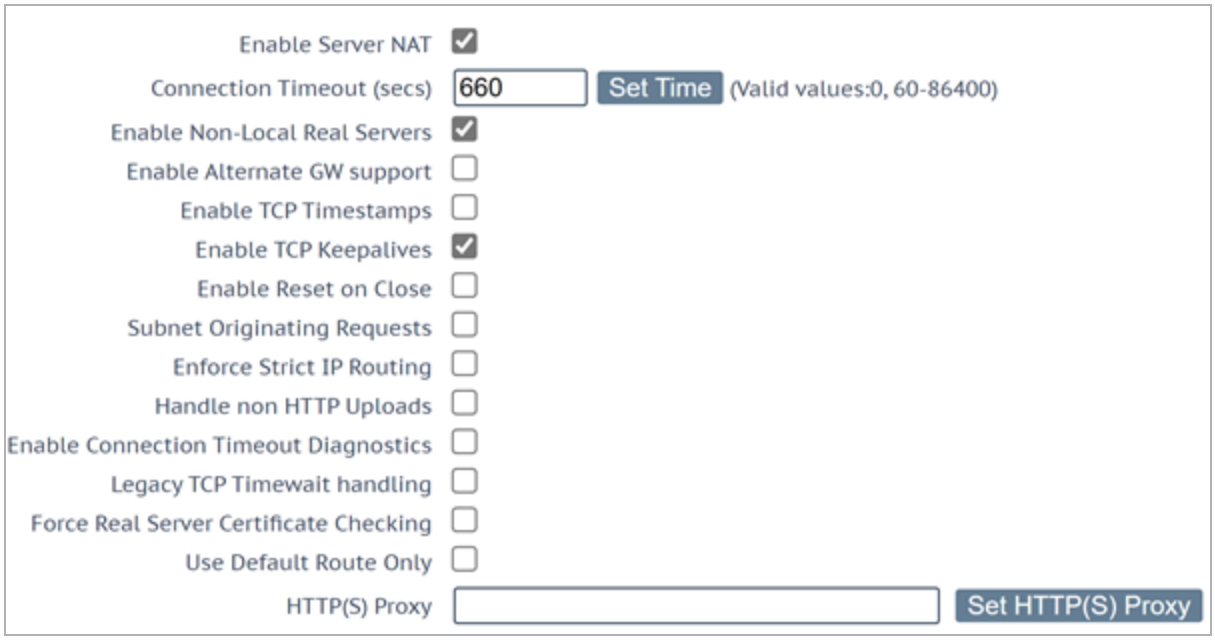
© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

5 General Configuration

5.1 Disable Global SNAT

By default, global Server Network Address Translation (SNAT) is enabled in the LoadMaster settings. Kemp recommends disabling SNAT globally when using the LoadMaster with a Lync 2010 environment. To disable SNAT globally, follow the steps below:

1. In the main menu, select **System Configuration**.
2. Select **Miscellaneous Options**.
3. Select **Network Options**.



4. Remove the check from the **Enable Server NAT** check box.

5.2 Subnet Originating Requests

When the LoadMaster is deployed in a two-armed configuration, Kemp recommends enabling **Subnet Originating Requests**. When this option is enabled, the LoadMaster will use its local IP address, instead of the IP address of the Virtual Service, when communicating to the Real Servers.

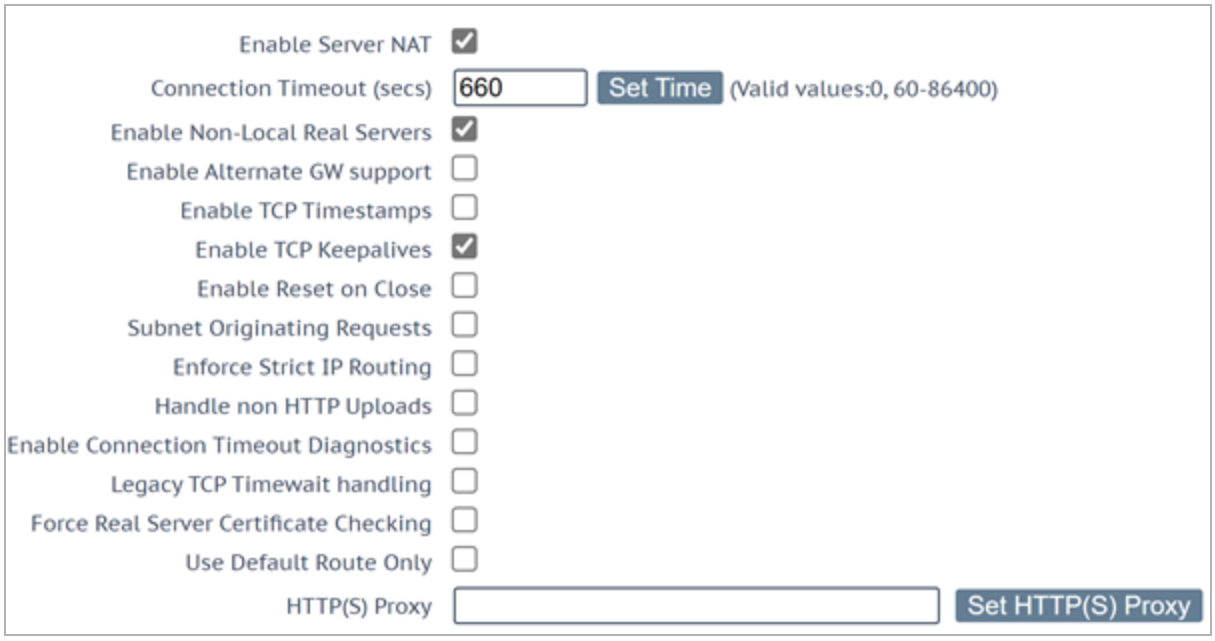
Subnet Originating Requests can be enabled on a per-Virtual Service or a global basis.

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

> It is recommended that the **Subnet Originating Requests** option is enabled on a per-Virtual Service basis.

To enable **Subnet Originating Requests** globally, follow the steps below:

1. In the main menu of the LoadMaster WUI, select **System Configuration > Miscellaneous Options > Network Options.**



2. Select the **Subnet Originating Requests** check box.

5.3 Change Drop Connections Settings

The LoadMaster must be configured to drop connections on Real Server failure in order to have fast failover for clients to another Real Server. To enable this setting, follow the steps below:

1. In the main menu, select **System Configuration**.
2. Select **Miscellaneous Options**.
3. Select **L7 Configuration**.
4. Select the **Drop Connections on RS failure** check box.

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

5.4 Increase the Connection Timeout

The LoadMaster **Connection Timeout** should be set to one day. The reason why this value can be set so high is because the LoadMaster monitors client connection to Real Servers and if a server fails then the LoadMaster can drop the associated client connections to that Real Server. Clients are disconnected from the LoadMaster and then they reconnect to the LoadMaster in order to connect to another Real Server.

One day is the maximum value for this setting and it must be used in conjunction with the **Drop Connections on RS failure** option. To set this option, follow the steps below:

1. In the main menu, select **System Configuration**.
2. Select **Miscellaneous Options**.
3. Select **L7 Configuration**.
4. Set the **L7 Connection Drain Time (secs)** to **86400 (1 day)** and click **Set Time**.

5.5 Connection Scaling For Large Scale Deployments

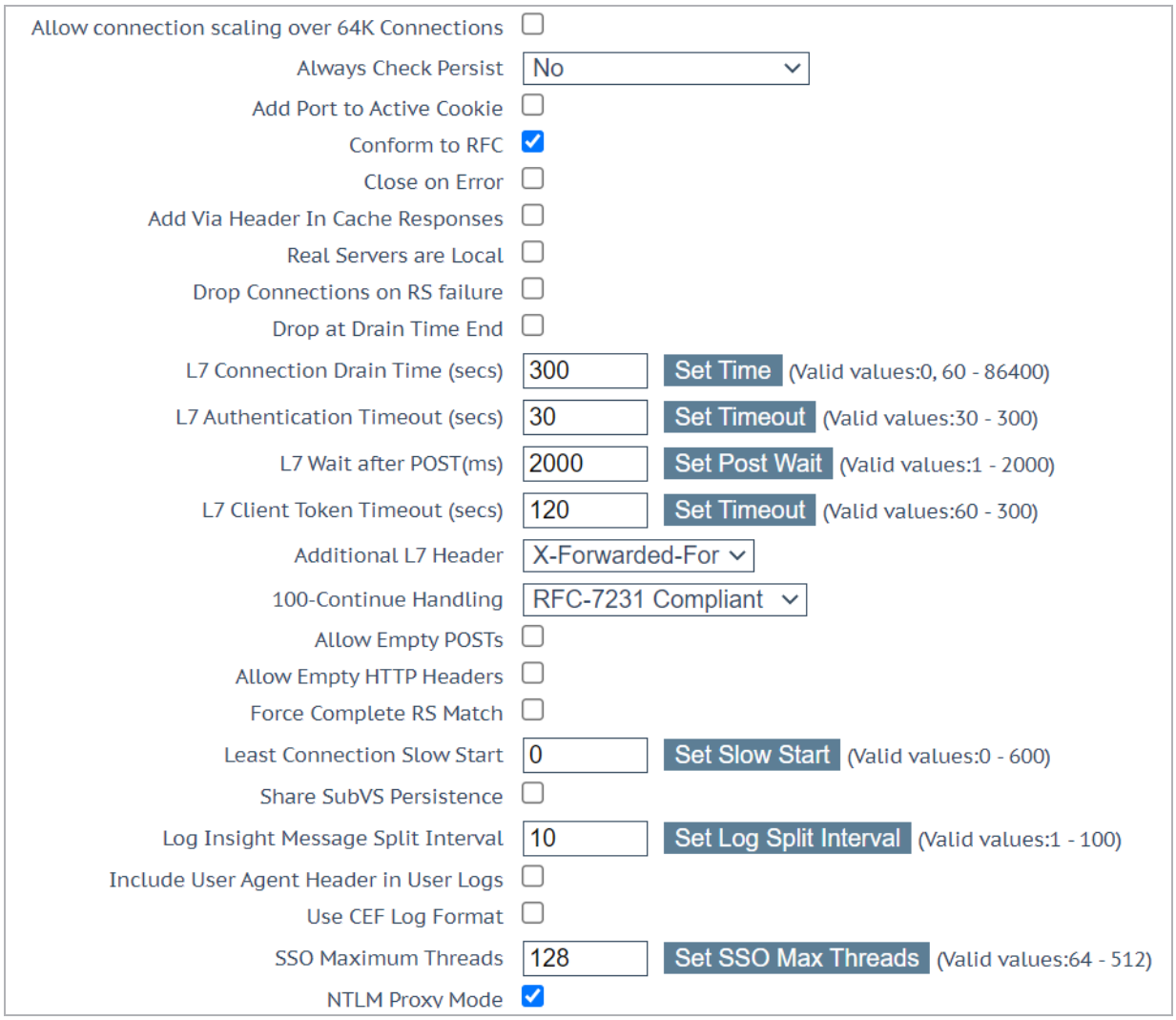
This is optional and should be used only in cases where you expect your network traffic to be greater than 64,000 server connections at any one particular time.

You must disable L7 Transparency in order to use connection scaling.

To use connection scaling, follow the steps below:

1. In the main menu, select **System Configuration**.
2. Select **Miscellaneous Options**.
3. Select **L7 Configuration**.

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.



4. Select the **Allow connection scaling over 64K Connections** check box.
5. In the main menu, select **Virtual Services**.
6. Select **View/Modify Services**.
7. Click the **Modify** button on the relevant **Virtual Service**.
8. Expand the **Advanced Properties** section.
9. In the **Alternate Source Addresses** text box, enter a list of **Alternate Source Addresses**. Multiple IPv4 addresses must be separated with a space; each must be unallocated and allow 64K connections.

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

10. Click the **Set Alternate Source Addresses** button.

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

6 Load Balancing Lync Front-End Servers

This section provides step -by-step instructions on how to configure the Kemp LoadMaster to load balance the various services of a Microsoft Lync 2010 Front-End pool.

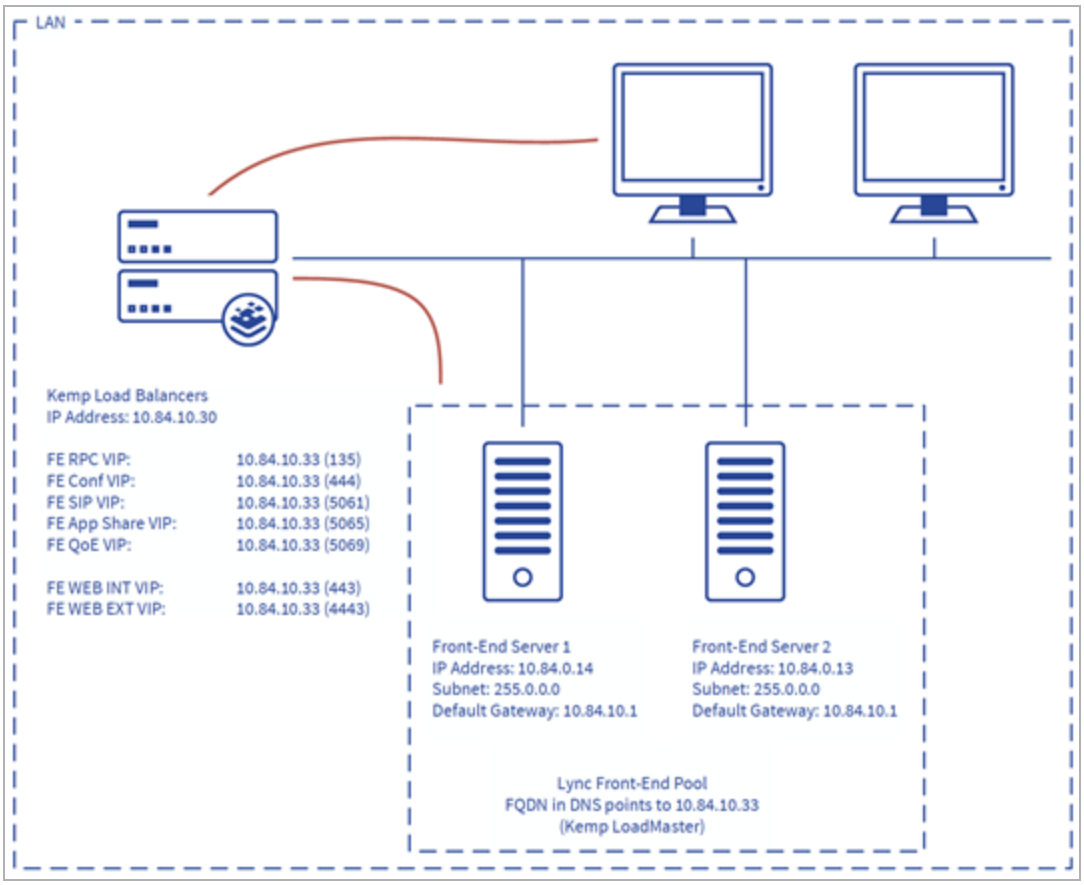
These instructions are for a typical deployment type: one-armed topology and non-transparent (Microsoft SNAT).

6.1 Required Services for Front-End Pools

Pool IP = Enterprise Front-End Pool FQDN IP Address
Server IPs = IP Addresses of Front-End Servers

Name	Protocol	Port	VIP	Real Servers	Persistence	Scheduling	Transparency	Layer	Notes
FE DCOM	TCP	135	Pool IP	Server IP	Source IP	Least Connection	Disabled	L7	RPC/DCOM based operations
FE SIP	TCP	5061	Pool IP	Server IP	Source IP	Least Connection	Disabled	L7	SIP/TLS
FE App Share	TCP	5065	Pool IP	Server IP	Source IP	Least Connection	Disabled	L7	Application Sharing
FE QoE	TCP	5069	Pool IP	Server IP	Source IP	Least Connection	Disabled	L7	QoE Agent
FE Conf	TCP	444	Pool IP	Server IP	Source IP	Least Connection	Disabled	L7	Conferencing
FE Web Int	TCP	445	Pool IP	Server IP	Source IP	Least Connection	Disabled	L7	HTTPS Internal Web Services
FE Web Ext	TCP	4445	Pool IP	Server IP	Active Cookies	Least Connection	Disabled	L7	HTTPS External Web Services

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.



6.2 Optional Services for Front-End pools

Pool IP = Enterprise Front-End Pool FQDN IP Address
Server IPs = IP Addresses of Front-End Servers

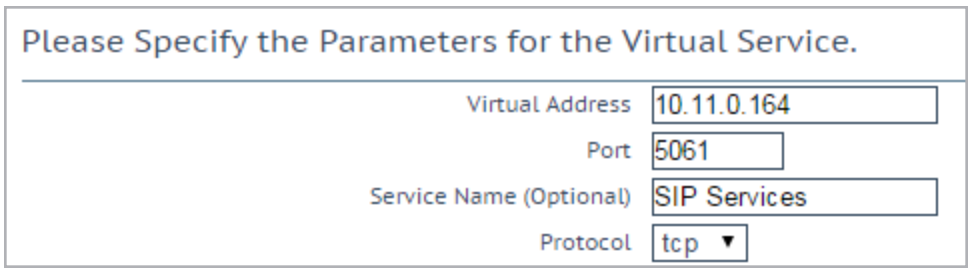
Name	Protocol	Port	VIP	Real Servers	Persistence	Scheduling	Transparency	Layer	Notes
FE Web 80	TCP	80	Pool IP	Server IPs	Source IP	Least Connection	Disabled	L7	HTTP Root Cert
FE CAC	TCP	448	Pool IP	Server IPs	Source IP	Least Connection	Disabled	L7	Retrieval for Lync Phones
FE SIPU	TCP	5060	Pool IP	Server IPs	Source IP	Least Connection	Disabled	L7	SIP unsecured
FE MED	TCP	5067	Pool IP	Server IPs	Source IP	Least Connection	Disabled	L7	Mediation Server

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

									SIP/TLS
FE MED	TCP	5068	Pool IP	Server IPs	Source IP	Least Connection	Disabled	L7	Mediation Server SIP/TCP
FE MED	TCP	5070	Pool IP	Server IPs	Source IP	Least Connection	Disabled	L7	Mediation Server FE
FE RSG	TCP	5071	Pool IP	Server IPs	Source IP	Least Connection	Disabled	L7	Response Groups
FE CAA	TCP	5072	Pool IP	Server IPs	Source IP	Least Connection	Disabled	L7	Conferencing Attendant
FE CA	TCP	5073	Pool IP	Server IPs	Source IP	Least Connection	Disabled	L7	Conferencing Announcement
FE OV	TCP	5074	Pool IP	Server IPs	Source IP	Least Connection	Disabled	L7	Outside Voice Control
FE	TCP	5075	Pool IP	Server IPs	Source IP	Least Connection	Disabled	L7	
FE	TCP	5076	Pool IP	Server IPs	Source IP	Least Connection	Disabled	L7	
FE	TCP	5080	Pool IP	Server IPs	Source IP	Least Connection	Disabled	L7	
FE Web 8080	TCP	8080	Pool IP	Server IPs	Source IP	Least Connection	Disabled	L7	HTTP Root Cert Retrieval for Lync Phones

6.3 Configuring a Virtual Service for SIP services on the Lync Front-End Servers

1. In the main menu of the LoadMaster WUI, select **Virtual Services**.
2. Select **Add New**.



© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

3. Enter the **Virtual Address** of the Lync Server Front-End Pool using the format **###.###.###.###**.
4. Enter **5061** as the **Port**.
5. Enter a recognizable **Service Name**.
6. Select **tcp** as the **Protocol**.

> The combination of Virtual Address, Port and Protocol must be unique within LoadMaster.

7. Click **Add this Virtual Service**.
8. Configure the settings as recommended in the following table:

Section	Option	Value	Comments
Standard Options	Force L4	Disabled	
	Transparency	Disabled	
	Persistence Options	Source IP Address	
	Timeout	20 minutes	.
	Scheduling Method	least connection	
	Idle Timeout	1800 (30 minutes)	Click **Set Idle Timeout**.
Real Servers	Real Server Check Method	TCP Connection Only	
	Checked Port	5061	Click the **Set Checked Port** button. Click the **Add New** button.

9. Add the Real Servers.
   a) Enter the relevant address in the **Real Server Address** text box.
   b) Type 5061 as the port.

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

c) Click **Add This Real Server**.

d) Click **OK** in response to the confirmation that the Real Server was added.

e) Add any other Front-End Real Servers as needed.

6.4 Configuring Virtual Services for Additional Services on the Lync Front-End Servers

Additional Services need to be configured for at least the following ports:

- **135** (RPC)
- **444** (Conferencing)
- **5065** (Application Sharing)
- **5069** (QoE Agent)

> Other ports may be required. Review all the ports in the following table and add Additional Services as required.

Configure the Additional Services for the Front-End Servers by following the steps in the **Configuring a Virtual Service for SIP services on the Lync Front-End Servers** section but changing the settings as per the table below.

You only have to replace the values in **Step 4** (**Port** configuration), **Step 16** (**Checked Port** configuration), **Step 5** (**Service Nickname)** and **Step 19** (**Port** on Real Server) according to the following table:

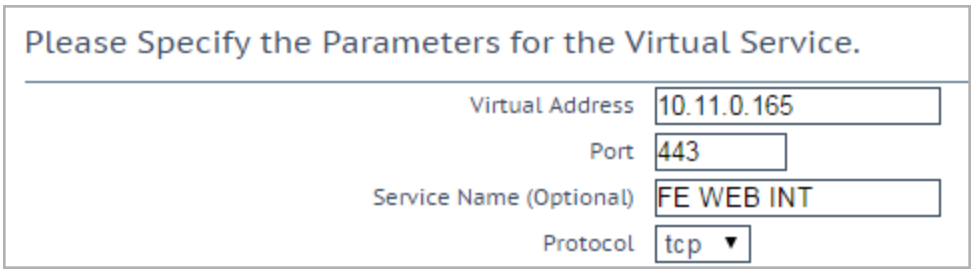
Step 4 (Port)	Step 16 (Checked Port)	Step 5 (Service Name)	Step 19 (Port)	Notes
135	5061	FE RPC	135	Port checking on port **135** does not work as this is a Windows RPC Port and always returns alive also when Lync is not running so checking on a Lync port is required - **5061** in this case.
444	444	FE Conf	444	
5065	5065	FE App Share	5065	
5069	5069	FE QoE	5069	

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

6.5 Configuring a Virtual Service for Internal HTTPS-based Services for the Front-End Servers

To configure a Virtual Service for internal, HTTPS-based services for the front-end servers, follow the steps below:

1. In the main menu of the LoadMaster WUI, click **Virtual Services** and then click **Add New**.



2. Enter the **Virtual Address** using the format **###.###.###.###**, for example **10.84.10.33**.
3. Enter **443** as the **Port**.
4. Enter a recognizable **Service Name**, for example **FE WEB INT**.
5. Select **tcp** as the **Protocol**.

> The combination of Virtual Address, Port and Protocol must be unique within LoadMaster.

6. Click **Add this Virtual Service**.
7. Configure the settings as recommended in the following table:

Section	Option	Value	Comments
Standard Options	Force L4	Disabled	
	Transparency	Disabled	
	Persistence Mode	Source IP Address	
	Timeout	20 Minutes	
	Scheduling Method	least	

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

Section	Option	Value	Comments
		connection	
	Idle Connection Timeout	1800 (30 minutes)	Click **Set Idle Timeout.**
Real Servers	Real Server Check Method	HTTPS Protocol	
	Checked Port	443	Click the **Set Checked Port** button.
	URL	/abs/handler	Click the **Set URL** button. Click the **Add New** button.

8. Add the Real Servers.

   a) Enter the relevant address in the **Real Server Address** text box.

   b) Enter **443** as the **Port**.

   c) Click the **Add This Real Server** button.

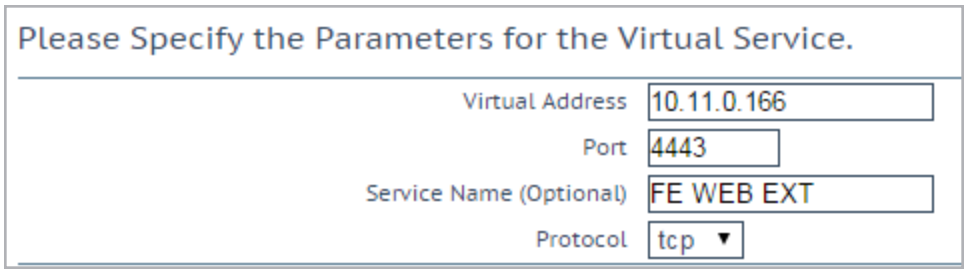
   d) Click **OK** in response to the confirmation that the Real Server was added.

   e) Add any other Real Servers as needed.

6.6 Configuring a Virtual Service for External HTTPS-based Services for the Front-End Servers

To configure a Virtual Service for external HTTPS-based services for the front-end servers, follow the steps below:

1. In the main menu of the LoadMaster WUI, select **Virtual Services**.
2. Select **Add New**.



© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

3. Enter the relevant IP address in the **Virtual Address** text box using the format **###.###.###.###**, for example **10.84.10.33**.
4. Enter **4443** as the **Port**.
5. Enter a recognizable **Service Name**, for example **FE WEB EXT**.
6. Select **tcp** as the **Protocol**.

> The combination of Virtual Address, Port and Protocol must be unique within the LoadMaster.

7. Click **Add this Virtual Service**.
8. Configure the settings as recommended in the following table:

Section	Option	Value	Comments
Basic Properties	Service Type	HTTP/HTTPS	
Standard Options	Force L4	Disabled	
	Transparency	Disabled	
	Persistence Mode	Active Cookie	The cookie must be named **MS-WSMAN** because this is the value that the web services expect, and cannot be changed.
	Timeout	20 Minutes	
	Scheduling Method	least connection	
	Idle Timeout	1800 (30 minutes)	Click **Set Idle Timeout**.
SSL Properties	SSL Acceleration	Enabled	Click **OK** to the warning that appears.
	Reencrypt	Enabled	Re-encryption is required. SSL Offloading is not supported for Lync Web Services. Click the **Manage Certificates** button and click **Import Certificate**.*

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

Section	Option	Value	Comments
Real Servers	Real Server Check Method	HTTPS Protocol	
	Checked Port	4443	Click **Set Check Port**.
	URL	/abs/handler	Click the **Set URL** button. Click the **Add New** button.

The **Active Cookies** option is not available in release 6.0-28. If you are using version 6.0-28, please upgrade to a more recent release to correctly configure this service.

9. *Click the **Choose File** button next to the **Certificate File**.
10. Locate and open the PFX file.
11. Import a **Key File** if needed.
12. Enter the **Pass Phrase**.
13. Enter a name in the **Certificate Identifier** text box.
14. Click the **Save** button.
15. Select the relevant Virtual Service(s) on the left.
16. Click the right arrow to assign the certificate to the Virtual Service.
17. Click **Save Changes**.
18. Add the Real Servers.
    a) Enter the relevant **Real Server Address**.
    b) Enter **4443** as the **Port**.
    c) Click **Add This Real Server**.
    d) Click **OK** in response to the confirmation that the Real Server was added.
    e) Add any other Real Servers as needed.

If you wish to view, modify, or delete any Virtual Services or Real Servers that have been added, select **Virtual Services** and **View/Modify Services** in the main menu of the LoadMaster WUI.

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

7 Load Balancing Lync Director Servers

This section provides step-by-step instructions on how to configure the Kemp LoadMaster to load balance the various services of a Microsoft Lync 2010 Director pool.

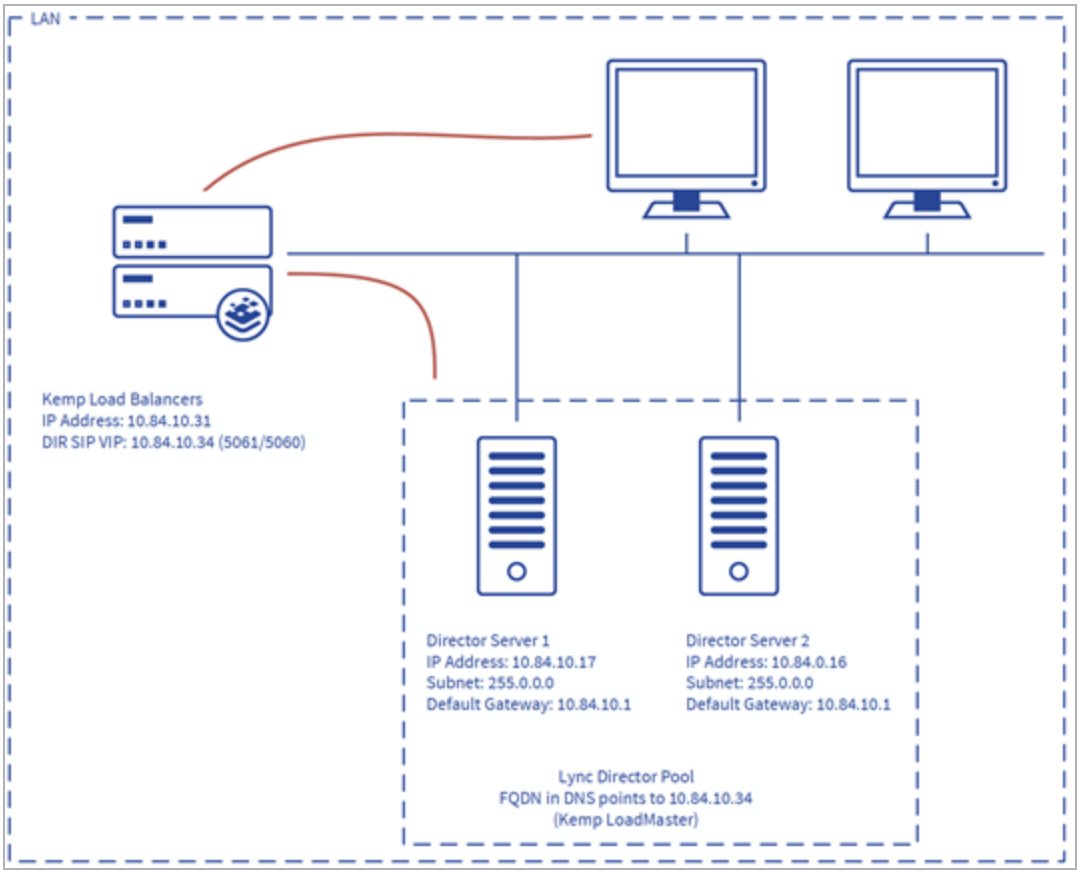
Typical Deployment Type: One-armed Topology and Non transparent (Microsoft SNAT)

7.1 Required Services for Director Pools

Pool IP = Enterprise Front-End Pool FQDN IP Address
Server IPs = IP Addresses of Front-End Servers

Name	Protocol	Port	VIP	Real Servers	Persistence	Scheduling	Transparency	Layer	Notes
DIR SIP	TCP	5061	Pool IP	Server IPs	Source IP	Least Connection	Disabled	L7	SIP/TLS
DIR SIPU	TCP	5060	Pool IP	Server IPs	Source IP	Least Connection	Disabled	L7	SIP Unsecured
DIR Web Com	TCP	443	Pool IP	Server IPs	Source IP	Least Connection	Disabled	L7	HTTPS comms between DIRs and FEs
DIR FE	TCP	444	Pool IP	Server IPs	Source IP	Least Connection	Disabled	L7	HTTPS comms between DIRs and web farm FQDNs

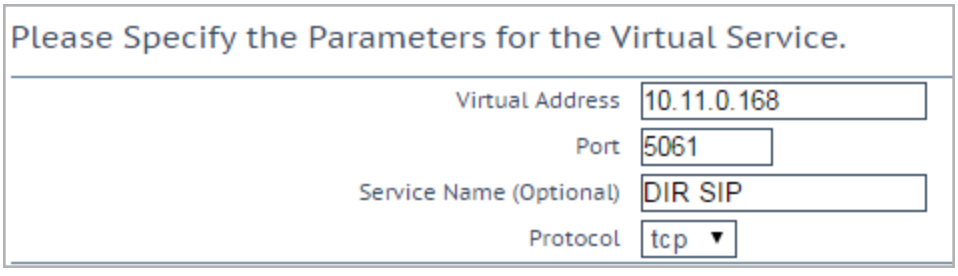
© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.



7.2 Configuring a Virtual Service for SIP Services on the Director Servers

To configure a Virtual Service for SIP services on the Director Servers, follow the steps below:

1. In the main menu of the LoadMaster WUI, select **Virtual Services**.
2. Select **Add New**.



© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

3. Enter the relevant **Virtual Address**, using the format **###.###.###.###**,.Enter **5061** as the **Port**.

4. Enter a recognizable **Service Name**, for example **DIR SIP**.

5. Select **tcp** as the **Protocol**.

> The combination of Virtual Address, Port and Protocol must be unique within the LoadMaster.

6. Click **Add this Virtual Service**.

7. Configure the settings as recommended in the following table:

Section	Option	Value	Comments
Standard Options	Extra Ports	5060	Click **Set Extra Ports**.
	Transparency	Disabled	
	Persistence Mode	Source IP Address	
	Timeout	20 Minutes	
	Scheduling Method	least connection	
	Idle Connection Timeout	1800 (30 minutes)	Click **Set Idle Timeout**.
Real Servers	Real Server Check Method	TCP Connection Only	
	Checked Port	5061	Click **Set Check Port**.

8. Click the **Add New...** button.

9. Add the Real Servers.

   a) Enter the relevant **Real Server Address**.

   b) Enter **5061** as the **Port**.

   c) Click the **Add This Real Server** button.

   d) Click **OK** in response to the confirmation that the Real Server was added.

   e) To view, modify, or delete any Virtual Services or Real Servers, select the **Virtual Services** > **View/Modify Services** option from the main menu of the LoadMaster WUI.

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

8 Load Balancing Internal Lync Edge Servers

This section provides step–by-step instructions on how to configure the Kemp LoadMaster to load balance the various services of a Microsoft Lync 2010 Edge pool.

Typical Deployment Type:

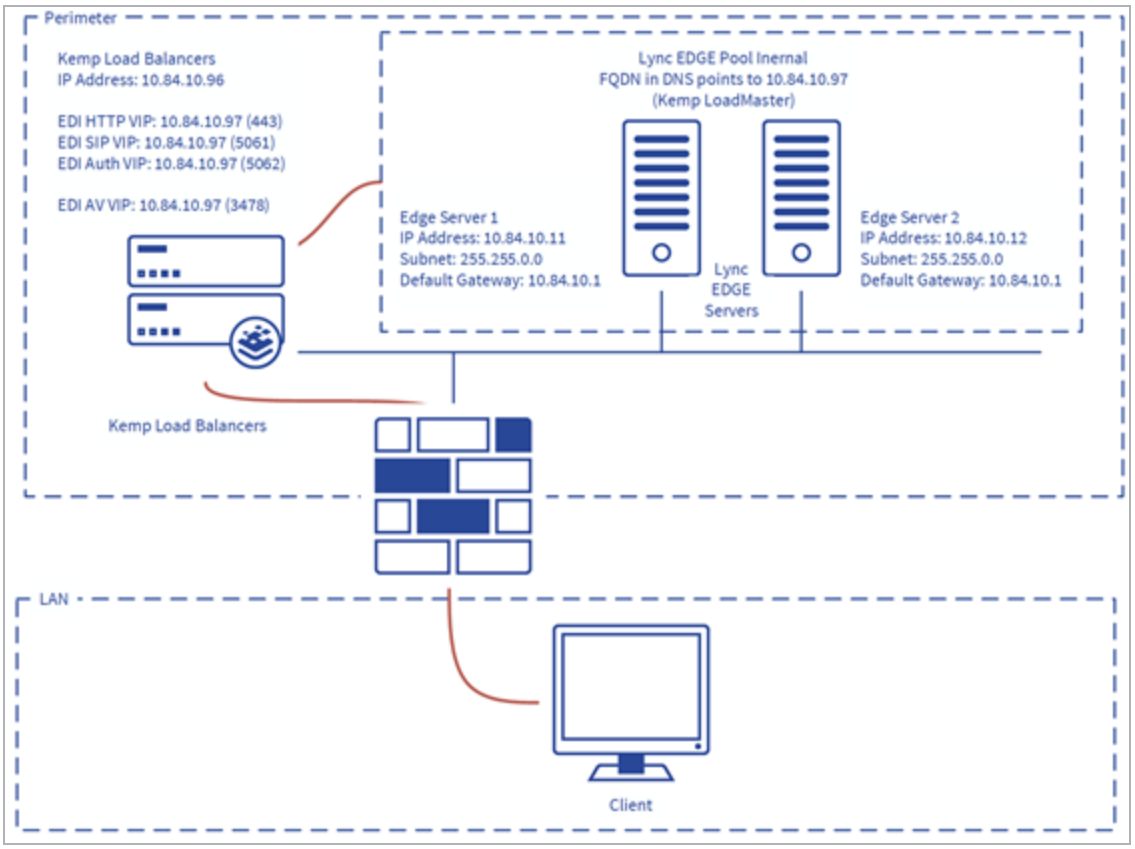
- One-armed Topology and None transparent (Microsoft SNAT)
- (Optional) One or Two-armed Transparency using a Layer 4 Service

8.1 Required Services for Internal-Facing Edge Pools

Pool IP = Enterprise Front-End Pool FQDN IP Address
Server IPs = IP Addresses of Front-End Servers

Name	Protocol	Port	VIP	Real Servers	Persistence	Scheduling	Transparency	Layer	Notes
EDI SIP	TCP	5061	Pool IP	Server IPs	Source IP	Least Connection	Disabled	L7	SIP/TLS
EDI Auth	TCP	5062	Pool IP	Server IPs	Source IP	Least Connection	Disabled	L7	A/V Authentication
EDI HTTP	TCP	443	Pool IP	Server IPs	Source IP	Least Connection	Disabled	L7	TCP Audio, Video, Sharing & Files
EDI Conf	UDP	3478	Pool IP	Server IPs	Source IP	Least Connection	Disabled	L4	Audio/Video

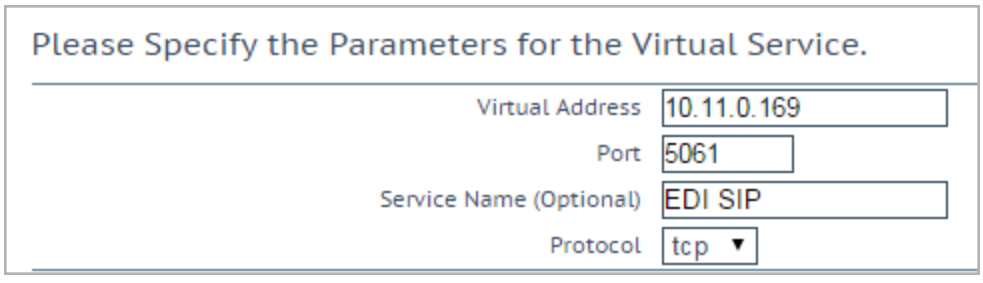
© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.



8.2 Configuring a Virtual Service for SIP Services on the Internal EDGE Servers

To configure a Virtual Service for SIP services on the internal EDGE servers, follow the steps below:

1. In the main menu of the LoadMaster WUI, select **Virtual Services**.
2. Select **Add New**.



© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

3. Enter the relevant **Virtual Address** using the format **###.###.###.###**, for example **10.84.10.97**.
4. Enter **5061** as the **Port**.
5. Enter a recognizable **Service Name**, for example **EDI SIP**.
6. Select **tcp** as the **Protocol**.

> The combination of **Virtual Address**, **Port** and **Protocol** must be unique within the LoadMaster.

7. Click **Add this Virtual Service**.
8. Configure the settings as recommended in the following table:

Section	Option	Value	Comments
Standard Options	Force L4	Disabled	
	Transparency	Disabled	
	Persistence Mode	Source IP Address	
	Timeout	20 Minutes	
	Scheduling Method	least connection	
	Idle Connection Timeout	1800 (30 minutes)	Click **Set Idle Timeout.**
Real Servers	Real Server Check Method	TCP Connection Only	
	Checked Port	5061	Click **Set Check Port**.

9. Add the Real Servers.
    a) Click the **Add New...** button.
10. Click the **Add New...**button.
    b) Enter the relevant **Real Server Address**.
    c) Enter **5061** as the **Port**.
    d) Click the **Add This Real Server** button.
    e) Click **OK** in response to the confirmation that the Real Server was added.

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

8.3 Configuring Virtual Services for Additional Services on the Lync Internal Edge Servers

Additional Services need to be configured for at least the following ports:

- **443** (TCP Media)
- **5062** (Authentication)

Configure the Additional Services for the Internal Edge Servers by following the steps in the **Configuring a Virtual Service for SIP Services on the Internal EDGE Servers** section but with a few small differences.

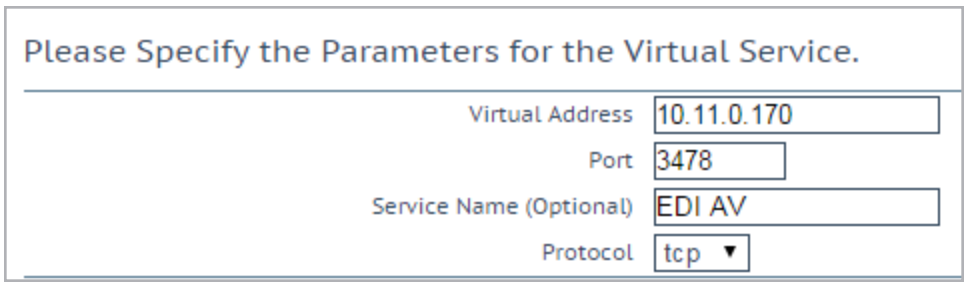
The values in **Step 4** (**Port** configuration), **Step 9** (**Checked Port** configuration), **Step 10** (**Service Nickname)** and **Step 15** (**Port** on Real Server) need to be replaced according to the following table:

Service	Step 4 (Port)	Step 9 (Checked Port)	Step 10 (Service Name)	Step 15 (Port)
Media	443	443	EDI HTTP	443
Authentication	5062	5062	EDI Auth	5062

8.4 Configuring a Virtual Service for Audio & Video Services on the Internal EDGE Servers

To configure a Virtual Service for Audio & Video Services on the Internal EDGE Servers, follow the steps below:

1. In the main menu of the LoadMaster WUI, select **Virtual Services**.
2. Select **Add New**.



© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

3. Enter the **Virtual Address**, using the format **###.###.###.###**, for example **10.84.10.97**.
4. Enter **3478** as the **Port**.
5. Enter a recognizable **Service Name**, for example **EDI AV**.
6. Select **udp** as the **Protocol**.

   The combination of **Virtual Address**, **Port** and **Protocol** must be unique within the LoadMaster.

7. Click **Add this Virtual Service**.
8. Configure the settings as recommended in the following table:

Section	Option	Value
Standard Options	Persistence Mode	Source IP Address
	Timeout	30 Minutes
	Scheduling Method	least connection

9.
10. Add the Real Servers.
    a) Expand the **Real Servers** section.
    b) Click the **Add New...** button.
    c) Enter the relevant **Real Server Address**.
    d) Enter **3478** as the port.
    e) Click **Add This Real Server**.
    f) Click **OK** in response to the confirmation that the Real Server was added.

To view, modify, or delete any existing Virtual Services or Real Servers, go to the **Virtual Services** > **View/Modify Services** option in the main menu of the LoadMaster WUI.

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

9 Load Balancing External Lync Edge Servers

This section provides step–by-step instructions on how you configure the Kemp LoadMaster to load balance the various services of a Microsoft Lync 2010 Edge pool.

Typical Deployment Type: One or Two-armed Transparent using a Layer 4 Service

9.1 Required Services for External-Facing Edge Pools

Pool IP = Enterprise Front-End Pool FQDN IP Address
Server IPs = IP Addresses of Front-End Servers

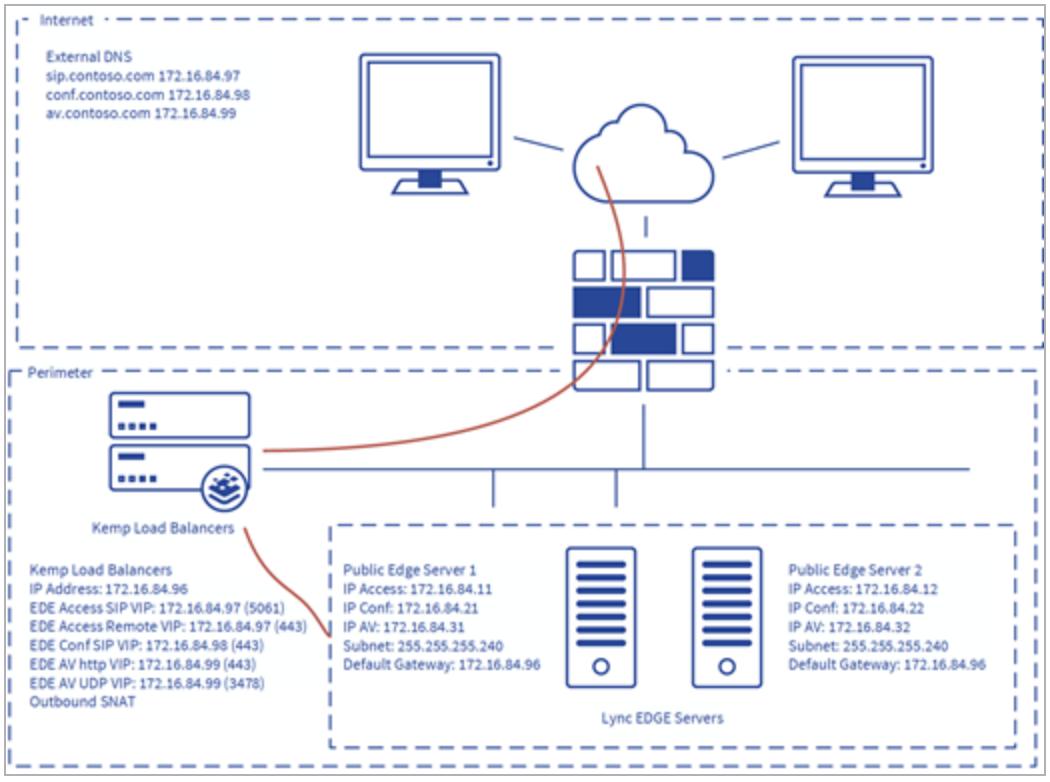
Name	Protocol	Port	VIP	Real Servers	Persistence	Scheduling	Transparency	Layer	Notes
EDE Access SIP	TCP	5061	Pool IP	Server IPs	Source IP	Least Connection	Disabled	L7	SIP/TLS
EDE Access Remote	TCP	443	Pool IP	Server IPs	Source IP	Least Connection	Disabled	L7	Remote Users
EDE Conf	TCP	443	Pool IP	Server IPs	Source IP	Least Connection	Disabled	L7	Conferencing
EDE AV TCP	TCP	443	Pool IP	Server IPs	Source IP	Least Connection	Enabled	L7	Fallback port TCP Audio, Video, Sharing & Files
EDI AV UDP	UDP	3478	Pool IP	Server IPs	Source IP	Least Connection	Enabled	L4	Audio/Video

9.2 Optional Services for External-Facing Edge Pools

Pool IP = Enterprise Front-End Pool FQDN IP Address
Server IPs = IP Addresses of Front-End Servers

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

Name	Protocol	Port	VIP	Real Servers	Persistence	Scheduling	Transparency	Layer	Notes
EDE AV TCP High	TCP	50.000 - 59.999	Pool IP	Server IPs	Source IP	Least Connection	Enabled	L7	Fallback port Audio/Video. High port range. Desktop sharing/CWA
EDI AV UDP High	UDP	50.000 - 59.999	Pool IP	Server IPs	Source IP	Least Connection	Enabled	L4	Audio/Video. High port range. Federation/ remote users

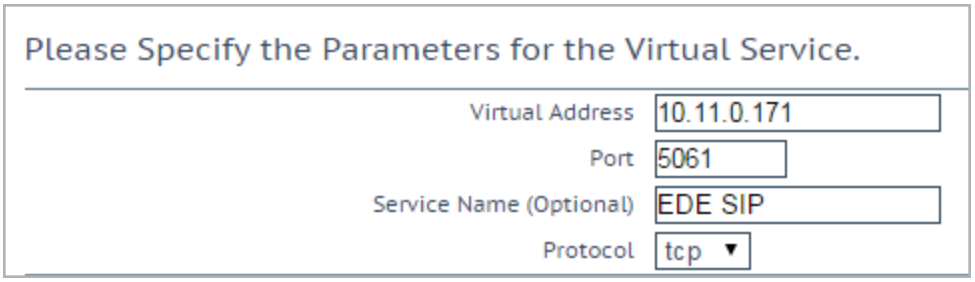


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

9.3 Configuring a Virtual Service for SIP Services on the External EDGE Servers

To configure a Virtual Service for SIP Services on the External EDGE Servers, follow the steps below:

1. In the main menu of the LoadMaster WUI, select **Virtual Services**.
2. Select **Add New**.



3. Enter the **Virtual Address** using the format **###.###.###.###**, for example **172.16.84.97**.
4. Enter **5061** as the **Port**.
5. Select **tcp** as the **Protocol**.

> The combination of **Virtual Address**, **Port** and **Protocol** must be unique within the LoadMaster.

6. Click **Add this Virtual Service**.
7. Configure the settings as recommended in the following table:

Section	Option	Value	Comments
Standard Options	Force L4	Disabled	
	Transparency	Disabled	
	Persistence Mode	Source IP Address	
	Timeout	20 Minutes	
	Scheduling Method	least connection	
	Idle Connection Timeout	1800 (30 minutes)	Click **Set Idle Timeout**.
Real Servers	Real Server Check Method	TCP Connection Only	

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

Section	Option	Value	Comments
	Checked Port	5061	Click **Set Check Port**.

8. Add the Real Servers.

   a) Click the **Add New...** button.

   b) Enter the **Real Server Address**.

   c) Enter **5061** as the **Port**.

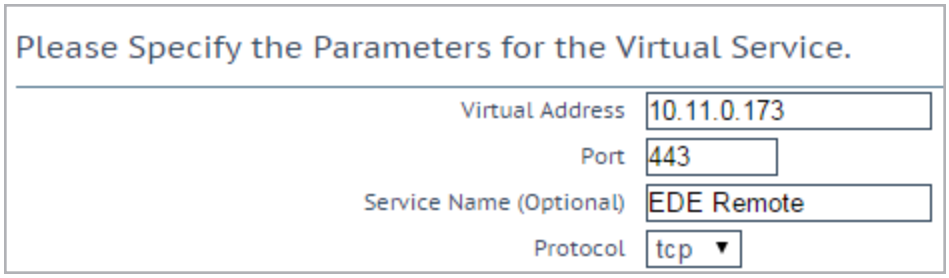
   d) Click **Add This Real Server**.

9. Click **OK** in response to the confirmation that the Real Server was added.

9.4 Configuring a Virtual Service for Remote User Services on the External EDGE Servers

To configure a Virtual Service for Remove User Services on the external EDGE servers, follow the steps below:

1. In the main menu of the LoadMaster WUI, select **Virtual Services**.
2. Select **Add New**.



3. Enter the **Virtual Address** using the format **###.###.###.###**.
4. Enter **443** as the **Port**.
5. Select **tcp** as the **Protocol**.

   The combination of **Virtual Address**, **Port** and **Protocol** must be unique within the LoadMaster.

6. Click **Add this Virtual Service**.

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

7. Configure the settings as recommended in the following table:

Section	Option	Value	Comments
Standard Options	Force L4	Disabled	
	Transparency	Disabled	
	Persistence Mode	Source IP Address	
	Timeout	20 Minutes	
	Scheduling Method	least connection	
	Idle Connection Timeout	1800 (30 minutes)	Click **Set Idle Timeout**.
Real Servers	Real Server Check Method	TCP Connection Only	
	Checked Port	443	Click **Set Check Port**.

8. Add the Real Servers.

   a) Click the **Add New...** button.

   b) Enter the **Real Server Address**.

   c) Enter **443** as the **Port**.

   d) Click **Add This Real Server**.

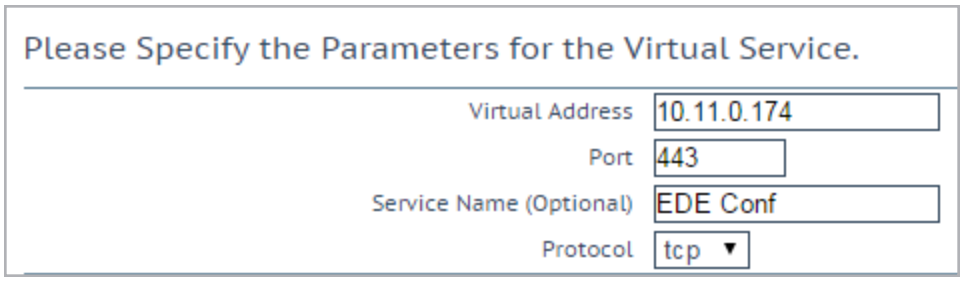
   e) Click **OK** in response to the confirmation that the Real Server was added.

9.5 Configuring a Virtual Service for Conferencing Services on the External EDGE Servers

To configure a Virtual Service for conferencing services on the external EDGE servers, follow the steps below:

1. In the main menu of the LoadMaster WUI, select **Virtual Services**.
2. Select **Add New**.

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.



3. Enter the **Virtual Address** using the format **###.###.###.###**.
4. Enter **443** as the **Port**.
5. Select **tcp** as the **Protocol**.

   The combination of **Virtual Address**, **Port** and **Protocol** must be unique within the LoadMaster.

6. Click **Add this Virtual Service**.
7. Configure the settings as recommended in the following table:

Section	Option	Value	Comments
Standard Options	Force L4	Disabled	
	Transparency	Disabled	
	Persistence Mode	Source IP Address	
	Timeout	20 Minutes	
	Scheduling Method	least connection	
	Idle Connection Timeout	1800 (30 minutes)	Click **Set Idle Timeout**.
Real Servers	Real Server Check Method	TCP Connection Only	
	Checked Port	443	Click **Set Check Port**.

8. Add the Real Servers.
   a) Click the **Add New...** button.
   b) Enter the **Real Server Address**.
   c) Enter **443** as the **Port**.

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

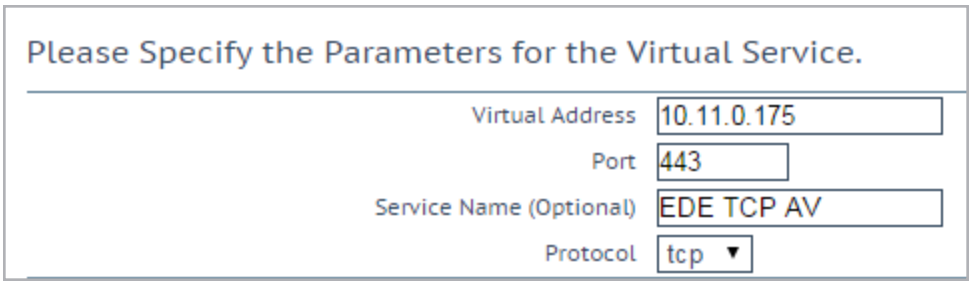
d) Click **Add This Real Server**.

e) Click **OK** in response to the confirmation that the Real Server was added.

9.6 Configuring a Virtual Service for TCP Audio/Video Services on the External EDGE Servers

To configure a Virtual Service for TCP audio/video services on the External EDGE servers, follow the steps below:

1. In the main menu of the LoadMaster WUI, select **Virtual Services**.
2. Select **Add New**.



3. Enter the **Virtual Address** using the format **###.###.###.###**.
4. Enter **443** as the **Port**.
5. Select **tcp** as the **Protocol**.

> The combination of **Virtual Address**, **Port** and **Protocol** must be unique within the LoadMaster.

6. Click **Add this Virtual Service**.
7. Configure the settings as recommended in the following table:

Section	Option	Value	Comments
Standard Options	Force L4	Disabled	
	Transparency	Enabled	This is a requirement for the External Audio/Video EDGE server only.
	Persistence Mode	Source IP	

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

Section	Option	Value	Comments
		Address	
	Timeout	20 Minutes	
	Scheduling Method	least connection	
	Idle Connection Timeout	1800 (30 minutes)	Click **Set Idle Timeout**.
Real Servers	Real Server Check Method	TCP Connection Only	
	Checked Port	443	Click **Set Check Port**.

8. Add the Real Servers.

    a) Click the **Add New...** button.

    b) Enter the **Real Server Address**.

    c) Enter **443** as the **Port**.

    d) Click **Add This Real Server**.

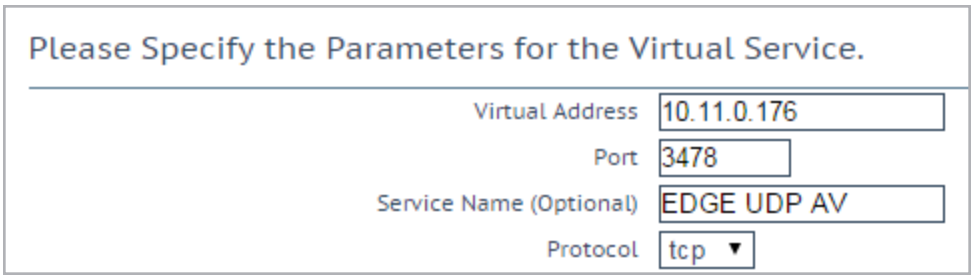
    e) Click **OK** in response to the confirmation that the Real Server was added.

9.7 Configuring a Virtual Service for UDP Audio/Video Services on the External EDGE Servers

To configure a Virtual Service for UDP audio/video services on the External EDGE servers, follow the steps below:

1. In the main menu of the LoadMaster WUI, select **Virtual Services**.
2. Select **Add New**.

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.



3. Enter the **Virtual Address**.
4. Enter **3478** as the **Port**.
5. Enter a recognizable **Service Name**, for example **EDE UDP AV**.
6. Select **udp** as the **Protocol**.

> The combination of **Virtual Address**, **Port** and **Protocol** must be unique within the LoadMaster.

7. Click **Add this Virtual Service**.
8. Configure the settings as recommended in the following table:

Section	Option	Value	Comments
Standard Options	Persistence Mode	Source IP Address	
	Timeout	2 Minutes	
	Scheduling Method	least connection	
Real Servers	Real Server Check Method	ICMP Ping	Click the **Add New...** button and type the Real Server address.
	Port	3478	Click **Set Check Port**.

9. Add the Real Servers.
10. Click the **Add New...** button.
    a) Enter the **Real Server Address**
    b) Enter **3478** as the **Port**.

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

c) Click **Add This Real Server**.

d) Click **OK** in response to the confirmation that the Real Server was added.

To view, modify, or delete any existing Virtual Services or Real Servers, select **Virtual Services** > **View/Modify Services** from the main menu of the LoadMaster WUI.

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

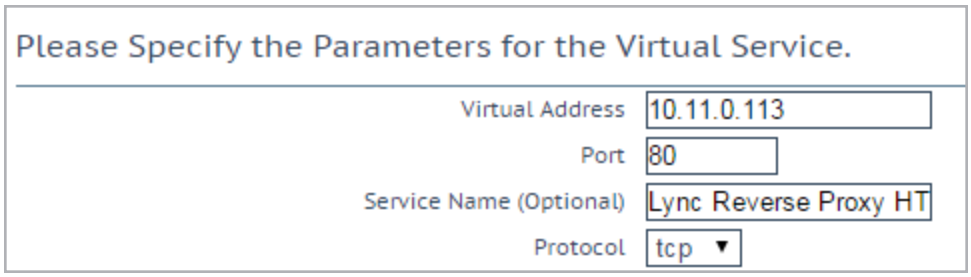
10 Using the LoadMaster as a Reverse Proxy

The LoadMaster can be used as a reverse proxy. To configure the LoadMaster to be used as a reverse proxy, follow the steps in the sections below.

10.1 Lync Reverse Proxy HTTP Virtual Service

To configure a Virtual Service for Lync Reverse Proxy HTTP, follow the steps below:

1. Click the **Add New** button.



2. Enter a **Virtual Address**.
3. Enter **80** in the **Port** field.
4. Enter a recognisable **Service Name**, for example **Lync Reverse Proxy HTTP**.
5. Ensure that **TCP** is set as the **Protocol**.
6. Click **Add This Virtual Service**.
7. Configure the settings as recommended in the following table:

Section	Option	Value	Comments
Standard Options	Force L4	Disabled	
	Transparency	Disabled	
	Persistence Mode	Source IP Address	

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

Section	Option	Value	Comments
	Persistence Timeout	20 Minutes	
	Idle Connection Timeout	1800	Click **Set Idle Timeout**.
Real Servers	Real Server Check Method	TCP Connection Only	
	Checked Port	5061	Click **Set Checked Report**.

8. Add the Real Servers.

   a) Click the **Add New ...** button to add a Real Server.

   b) Enter the **Real Server Address**.

   c) Enter **8080** as the **Port**.

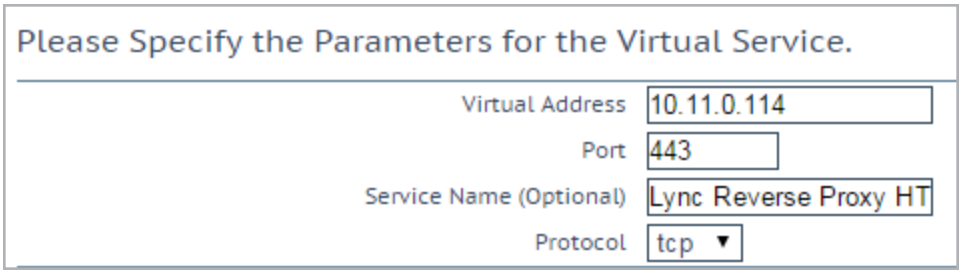
   > Ensure to not use **80** as the Real Server **Port**.

   d) Click the **Add This Real Server** button.

10.2 Lync Reverse Proxy HTTPS Virtual Service

To configure a Virtual Service for Lync Reverse Proxy HTTPS, follow the steps below:

1. Click the **Add New** button.



2. Enter a **Virtual Address**.
3. Enter **443** in the **Port** field.
4. Enter a recognisable **Service Name**, for example **Lync Reverse Proxy HTTPS**.
5. Ensure that **TCP** is set as the **Protocol**.
6. Click **Add This Virtual Service**.
7. Configure the settings as recommended in the following table:

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

Section	Option	Value	Comments
SSL Properties	SSL Acceleration	Enabled	
	Reencrypt	Enabled	
Standard Options	Persistence Mode	Source IP Address	
	Persistence Timeout	20 Minutes	
Real Servers	Real Server Check Method	TCP Connection Only	
	Checked Port	5061	Click **Set Checked Port**.

8. Expand the **Real Servers** section and select the following options:

   a) Click the **Add New** button.

   b) Enter the **Real Server Address**.

   c) Enter **4443** as the **Port**.

   Ensure to not use **443** as the Real Server **Port**.

   d) Click the **Add This Real Server** button.

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

References

Unless otherwise specified, the following documents can be found at http://kemptechnologies.com/documentation.

WUI, Configuration Guide

Kemp LoadMaster, Product Overview

Virtual Services and Templates, Feature Description

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

Last Updated Date

This document was last updated on 28 July 2023.

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.