Microsoft Lync 2013 and Citrix NetScaler Deployment Guide

CITRIX®

Table of contents

Introduction	3
Overview of Microsoft Lync 2013	3
Lync Server Roles	3
Standard Edition Server	3
Front-End Server and Back-End Server	3
Edge Server	4
Mediation Server	5
Director	5
Persistent Chat Front-End Server	5
Workload Types	6
Instant Messaging and Presence	6
Audio/Video & Web Conferencing	6
Enterprise Voice	6
Microsoft Recommended topology for HLB and Reverse Proxy	7
Front End Pool Internal interface load balancer setting	8
Front End Pool External Interface Load Balancer Settings	9
Director Pool Load balancer settings	9
Edge Internal Load Balancer Settings	9
Edge External Load Balancer Settings	10
Port information for Reverse Proxy External interface	10
Port information for Reverse Proxy Internal interface	10
NetScaler Load Balancing Microsoft Lync 2013	11
Recommended Topology	11
Load balancing internal traffic	11
Lync Protocol / Port Information for internal traffic	12
Internal DNS Considerations	19
SSL Certificate Considerations	20
Monitoring Resources	21
Load balancing, Reverse Proxy for External traffic	21
Load Balancing Edge Pool	21
HTTPS Reverse Proxy	22
Mobility	22
Federations & XMPP Partners	22
External DNS Considerations	25
SSL Certificate Considerations	25
Benefits of using a hardware appliance load balancer	27
Conclusion	28
Appendix	28
Product versions used during testing	28
Lync PowerShell Commands	28

Citrix® NetScaler® is the industry's leading Application Delivery Controller (ADC) that optimizes and enhances the performance, availability, scalability and security of Microsoft Lync 2013 deployments. Citrix NetScaler is available both as physical and virtual appliance. This guide will take you through an easy to understand step by step process of deploying Citrix NetScaler for Microsoft Lync 2013.

Overview of Microsoft Lync 2013

Microsoft Lync 2013 is a unified communication product. It offers features like Instant Messaging, VOIP, Online Conferencing, Collaborative development, File Sharing, integration with Exchange UM and federation services to integrate with other enterprises or public IM.

IM clients are available for windows, mac, mobiles; which can work with Lync 2013 servers as well as Lync Online (Office 365).

Lync Server Roles

Standard Edition Server

- The Standard Edition server is designed for small organizations, and for pilot projects in large organizations. It enables many of the features of Lync Server, including the necessary databases, to run on a single server. This enables Lync Server functionality at a lower cost, but does not provide a true high-availability solution.
- Standard Edition server enables instant messaging (IM), presence, conferencing, and Enterprise Voice, to run on a single server.
- The main difference between Lync Server 2013 Enterprise Edition and Lync Server 2013 Standard Edition is that Standard Edition does not support the high-availability features included with Enterprise Edition. For high-availability, multiple Front-End servers must be deployed to a pool and the SQL Server needs to be mirrored. It is not possible to pool Standard Edition servers.

Front-End Server and Back-End Server

- In Lync Server Enterprise Edition, the Front-End Server plays the core server role, and runs many basic Lync Server functions. The Front-End and Back-End Servers are the only server roles required to be in any Lync Server Enterprise Edition deployment.
- 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 of multiple servers running the same role provides scalability and failover capability.
- The Front-End Server includes the following roles:
    - User authentication and registration
    - Presence information and contact card exchange
    - Address book services and distribution list expansion

  - IM functionality, including multi-party IM conferences
  - Web conferencing, PSTN Dial-in conferencing and A/V conferencing (if deployed)
  - Application hosting for applications included with Lync Server (for example,
  - Conferencing Attendant and Response Group application) and third-party applications
  - Optional: monitoring-collection of usage information in the form of call detail records (CDRs) and call error records (CERs). This information provides metrics about the quality of the media (audio and video) traversing the network for both Enterprise voice calls and A/V conferences.
  - Web components of supported web-based tasks such as Web Scheduler and Join Launcher.
  - Option: Archiving - archival of IM communications and meeting content for compliance.
  - Option: Persistent Chat Web Services for Chat Room management and Persistent Chat Web Services for File Upload/Download [if persistent chat is enabled]
  - NOTE: In Lync Server 2010 and prior versions, Monitoring and Archiving were separate server roles, not collocated on Front End Server.
- Front-End Pools are also the primary store for user and conference data. Information about each user is replicated among Front-End Servers in the pool, and backed up on the Back-End Servers.
- 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. The Central Management Server also provides 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. The Back-End Servers serve as backup stores for the pool's user and conference data, and are the primary stores for other databases such as the Response Group database. A deployment with a single Back-End Server is possible but a solution that uses SQL Server mirroring is recommended for failover. Back-End Servers do not run any Lync Server software.

Edge Server

- Edge Server enables users to communicate and collaborate with users outside the organization's core infrastructure. 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 AIM, Yahoo! Messenger, and Google Talk.

- Deploying Edge Servers also enables mobility services, which supports Lync functionality on mobile devices. Users can use supported Apple iOS, Android, Windows Phone, or Nokia mobile devices to perform activities such as sending and receiving instant messages, viewing contacts, and viewing presence. In addition, mobile devices support some Enterprise Voice features, such as click to join a conference, Call via Work, single number reach, voice mail, and missed calls. The mobility feature also supports push notifications for mobile devices that do not support applications running in the background. A push notification is a notification that is sent to a mobile device about an event that occurs while a mobile application is inactive.
- Edge Servers also include a fully-integrated Extensible Messaging and Presence Protocol (XMPP) proxy, with an XMPP gateway included on Front-End Servers. Configuring the XMPP components enables Lync Server 2013 users to add contacts from XMPP-based partners (such as Google Talk) for instant messaging and presence.

Mediation Server

- Mediation Server is a necessary component for implementing Enterprise Voice and dial-in conferencing. Mediation Server translates signaling, and, in some configurations, media or mediates between your internal Lync Server infrastructure and a public switched telephone network (PSTN) gateway, IP-PBX, or a Session Initiation Protocol (SIP) trunk. You can run Mediation Server collocated on the same server as Front-End Server, or separated into a stand-alone Mediation Server pool.

Director

- Director can authenticate Lync Server user requests but they do not store user accounts, provide presence, or conferencing services. Directors are most useful to enhance security in deployments that enable external user access. The Director can authenticate requests before sending them on to internal servers. In the case of a denial-of-service attack, the attack ends with the Director and does not reach the Front-End Servers.

Persistent Chat Front-End Server

- Persistent chat enables users to participate in multiparty, topic-based conversations that persist over time. The Persistent Chat Front-End Server runs the persistent chat service. The Persistent Chat Back-End Server stores the chat history data, and information about categories and chat rooms. The optional Persistent Chat Compliance Back-End Server can store the chat content and events for the purpose of compliance.
- Deployments running Lync Server Standard Edition can also run Persistent chat collocated on the same server. You cannot collocate the Persistent Chat Front-End Server with Enterprise Edition Front-End Server.

Workload Types

Instant Messaging and Presence

- Instant messaging (IM) enables users to communicate with each other in real time on their computers using text-based messages. Both two-party and multiparty IM sessions are supported. A participant in a two-party IM conversation can add a third participant to the conversation at any time. When this happens, the Conversation window changes to support conferencing features.
- Presence provides information to users about the status of other on the network. A user's presence status provides information to help others decide whether they should try to contact the user and whether to use instant messaging, phone, or email. Presence encourages instant communication when possible, but it also provides information about whether a user is in a meeting or out of the office, indicating that instant communication is not possible. This presence status is displayed as a presence icon in Lync and other presence-aware applications, including the Microsoft Outlook messaging and collaboration client, Microsoft SharePoint technologies, Microsoft Word, and Microsoft Excel spreadsheet software. The presence icon represents the user's current availability and willingness to communicate.

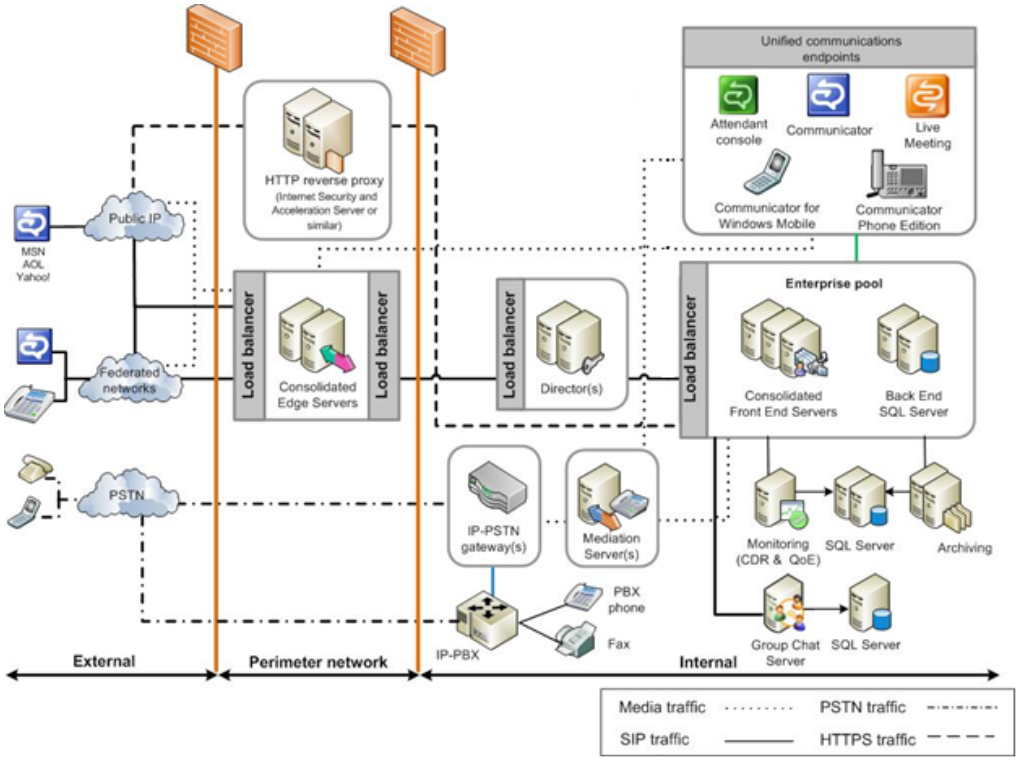
Audio/Video & Web Conferencing

- With web conferencing, users can share and collaborate on documents, such as Microsoft PowerPoint presentations, during their conferences. Additionally, users can share all or part of their desktop with each other in real time.
- A/V conferencing enables real-time audio and video communications between your users (that is, provided they have appropriate client devices such as headsets for audio conferences, and webcams for video conferences).

Enterprise Voice

- Lync Server 2013 supports multiple trunks between Mediation Servers and gateways. A trunk is a logical association between a port number and Mediation Server with a port number and a gateway. This means that a Mediation Server can have multiple trunks to different gateways, and a gateway can have multiple trunks to different Mediation Servers. Inter-trunk routing makes it possible for Lync Server 2013 to interconnect an IP-PBX to a public switched telephone network (PSTN) gateway or to interconnect multiple IP-PBX systems. Lync Server 2013 serves as the glue (that is, the interconnection) between different telephony systems. Microsoft Lync Server 2013 makes improvements in the areas of call forwarding, simultaneous ringing, voice mail handling, and caller ID presentation.

Microsoft Recommended topology for HLB and Reverse Proxy



Front End Pool Internal interface load balancer setting

Server	Port	Node Port	Protocol Type	Protocol	LB method, persistency, & client timeout
Front End	443	443	TCP	Source Address Affinity	Used for internal ports for SIP/TLS communication for remote user access, accessing internal Web conferences, and STUN/TCP inbound and outbound media communications for accessing internal media and A/V sessions.
Front End	135	135	TCP	Source Address Affinity	RPC
Front End	444	444	TCP	Source Address Affinity	HTTPS – Intra and interpool communication
Front End	5061	5061	TCP	Source Address Affinity	SIP/MTLS
Front End	443	4443	TCP	Source Address Affinity	HTTPS
Front End	80	8080	TCP	Source Address Affinity	HTTP
Front End	5065	5065	TCP	Source Address Affinity	Used for incoming SIP listening requests for application sharing.
Front End	5071	5071	TCP	Source Address Affinity	Used for incoming SIP requests for the Response Group application.
Front End	5072	5072	TCP	Source Address Affinity	Used for incoming SIP requests for Attendant (dial in conferencing).
Front End	5073	5073	TCP	Source Address Affinity	Used for incoming SIP requests for the Lync Server Conferencing Announcement service (that is, for dial-in conferencing).
Front End	5075	5075	TCP	Source Address Affinity	Used for incoming SIP requests for the Call Park application.
Front End	5076	5076	TCP	Source Address Affinity	Used for incoming SIP requests for the Audio Test service.
Front End	5080	5080	TCP	Source Address Affinity	Used for call admission control by the Bandwidth Policy service for A/V Edge TURN traffic.
Front End	448	448	TCP	Source Address Affinity	Used for call admission control by the Lync Server Bandwidth Policy Service.

Front End Pool External Interface Load Balancer Settings

Server	Port	Node Port	Protocol Profile	Persistence Profile	Description
Front End	443	443	TCP	Source Address Affinity	Used for internal ports for SIP/TLS communication for remote user access, accessing internal Web conferences, and STUN/TCP inbound and outbound media communications for accessing internal media and A/V sessions.
Front End	443	4443	TCP	Source Address Affinity	HTTP
Front End	80	8080	TCP	No Affinity	HTTP

Director Pool Load balancer settings

Server	Port	Node Port	Protocol Profile	Persistence Profile	Description
Director	443	443	TCP	None	Used for internal ports for SIP/TLS communication for remote user access, accessing internal Web conferences, and STUN/TCP inbound and outbound media communications for accessing internal media and A/V sessions.
Director	443	4443	TCP	None	HTTPS
Director	80	8080	TCP	None	HTTP
Director	5061	5061	TCP	None	Used for internal communications between servers and for client connections.

Edge Internal Load Balancer Settings

Server	Port	Node Port	Protocol Profile	Persistence Profile	Description
Director	443	443	TCP	None	Used for internal ports for SIP/TLS communication for remote user access, accessing internal Web conferences, and STUN/TCP inbound and outbound media communications for accessing internal media and A/V sessions.
Director	443	4443	TCP	None	HTTPS
Director	80	8080	TCP	None	HTTP
Director	5061	5061	TCP	None	Used for internal communications between servers and for client connections.

Edge External Load Balancer Settings

Server	Port	Node Port	Protocol Profile	Persistence Profile	Description
A/V, Access, Web Conf	443	443	TCP	Source Address Affinity	Used for external ports for SIP/TLS communication for remote user access, accessing internal Web conferences, and STUN/TCP inbound and outbound media communications for accessing internal media and A/V sessions.
Access	5061	5061	TCP	Source Address Affinity	Used for external ports for SIP/MTLS communication for remote user access or federation.
A/V	3478	3478	UDP	Source Address Affinity	Used for external ports for STUN/ UDP inbound and outbound media communications.

Port information for Reverse Proxy External interface

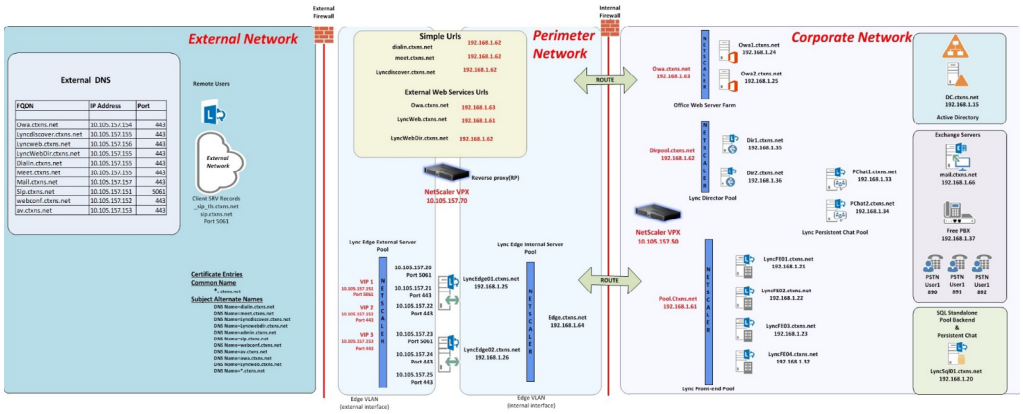
Server	Port	Destination IP	Source IP
Address book downloads, Address Book Web Query service, Autodiscover, client updates, meeting content, device updates, group expansion, Office Web Apps for conferencing, dial-in conferencing, and meetings.	443	Reverse proxy listener (VIP)	Any

Port information for Reverse Proxy Internal interface

Desitnation	Protocol Profile	Destination IP	Source IP
Traffic sent to port 443 on the reverse proxy external interface is redirected to a pool on port 4443 from the reverse proxy internal interface so that the pool web services can distinguish it from internal web traffic.	4443	Front End Server, Front End pool, Director, Director pool	Internal reverse proxy interface

NetScaler Load Balancing Microsoft Lync 2013

Recommended Topology



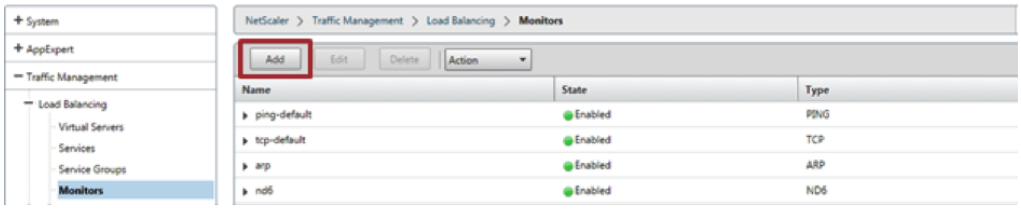
Load balancing internal traffic

In this scenario, the NetScaler® will be the connectivity point to multiple front-end, director and outlook web app servers in an Enterprise pool.

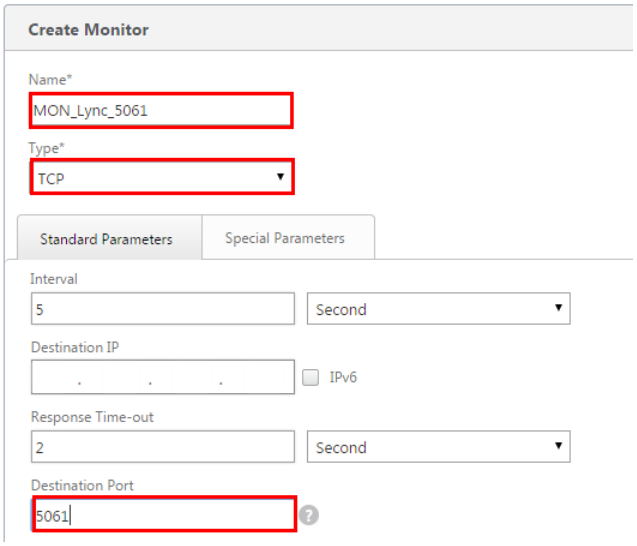
Role	FQDN	IP	Additional
Active Directory	DC.ctxns.net	192.168.1.15	Domain Controller & DNS
SQL Server 2012	LyncSql01.ctxns.net	192.168.1.20	Default Instance for Lync 2013
Lync 2013 Front-End 1	LyncFE01.ctxns.net	192.168.1.21	Pool Name: Pool.Ctxns.net
Lync 2013 Front-End 2	LyncFE02.ctxns.net	192.168.1.22	Pool Name: Pool.Ctxns.net
Lync 2013 Front-End 3	LyncFE03.ctxns.net	192.168.1.23	Pool Name: Pool.Ctxns.net
Lync 2013 Front-End 4	LyncFE04.ctxns.net	192.168.1.32	Pool Name: Pool.Ctxns.net
Lync 2013 Director 1	Dir1.ctxns.net	172.16.99.201	xencloud\user1
Lync 2013 Director 2	Dir2.ctxns.net	172.16.99.202	xencloud\user2
Outlook Web App server	Owa.ctxns.net	172.16.99.203	xencloud\user3
NetScaler		10.105.157.50	
Front End Pool	Pool.Ctxns.net	192.168.1.61	NS VIP 1
Director Pool	Dirpool.ctxns.net	192.168.1.62	NS VIP 2
OWA Pool	Owa.ctxns.net	192.168.1.63	NS VIP 3

Lync Protocol / Port Information for internal traffic

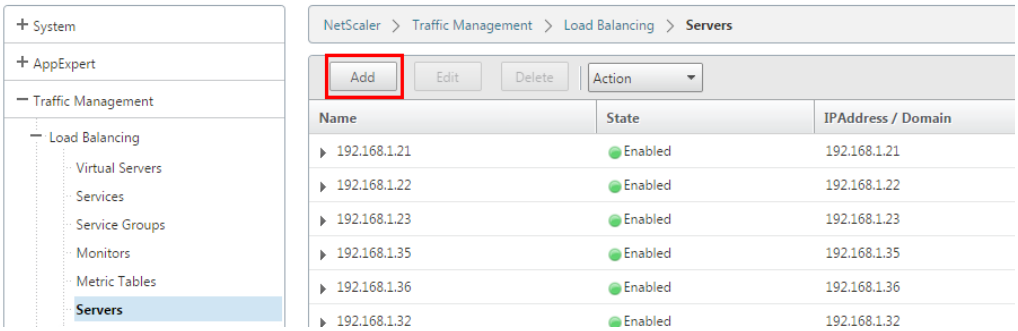
Add Custom Monitors

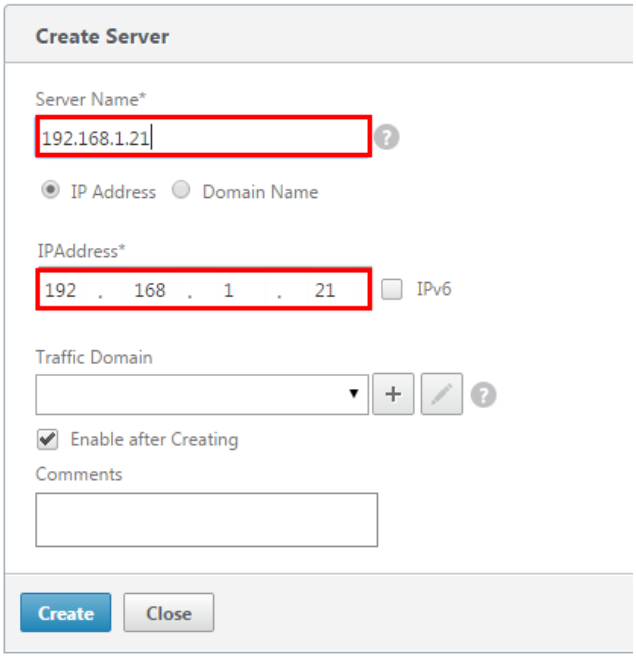


Configure for all the applicable ports in the deployment

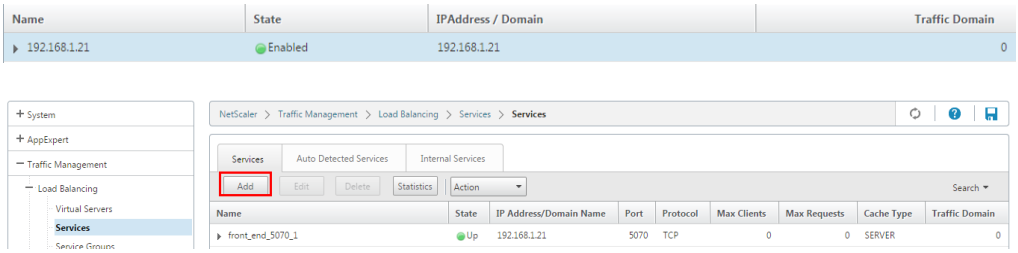


Add Lync application servers

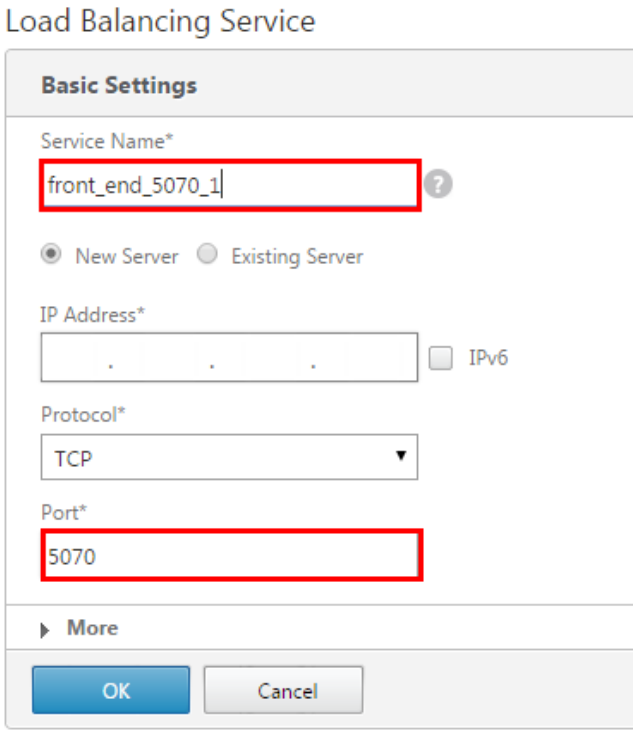




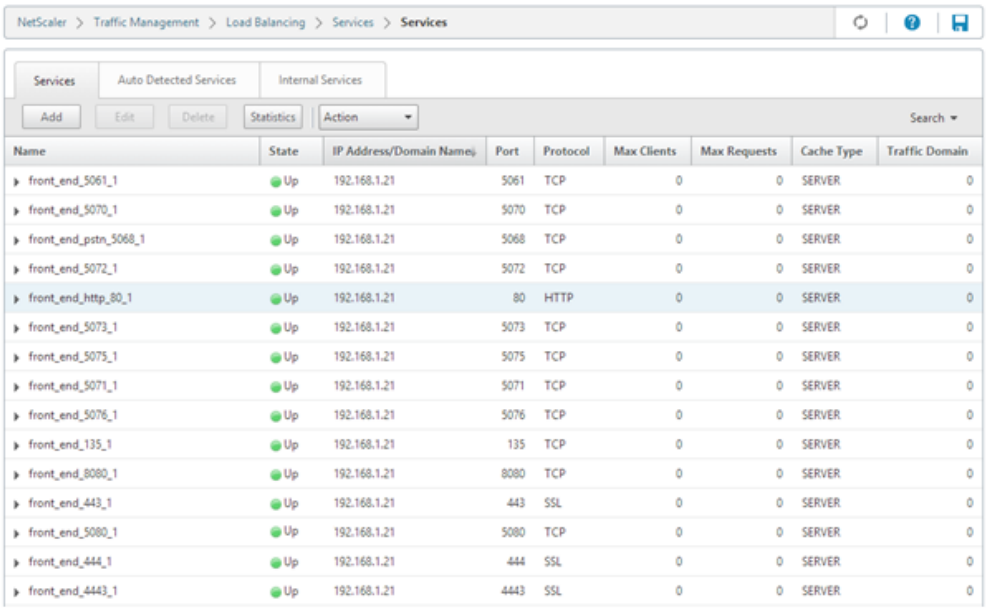
Verify the state is up

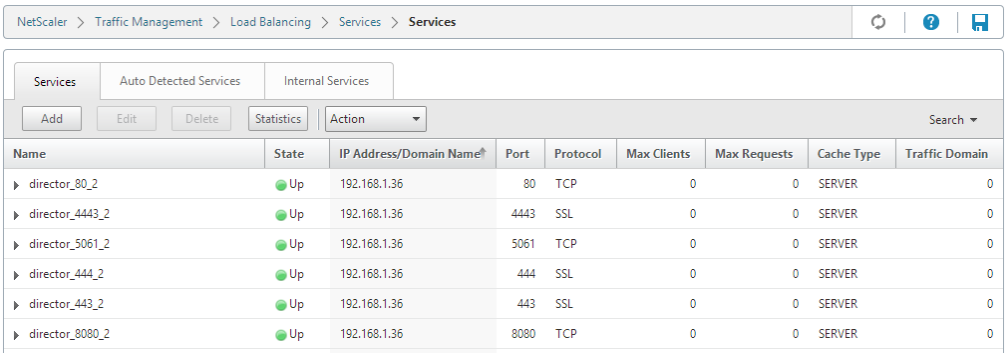


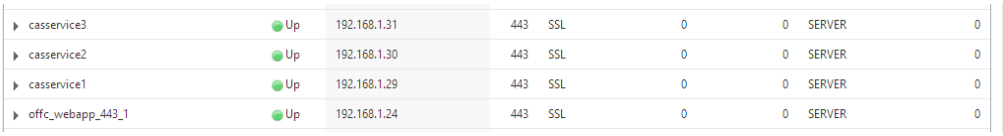
Create Lync Services



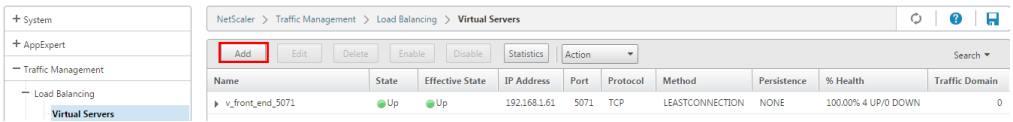
Verify Status of created services. You should have following services created as part of your configuration.

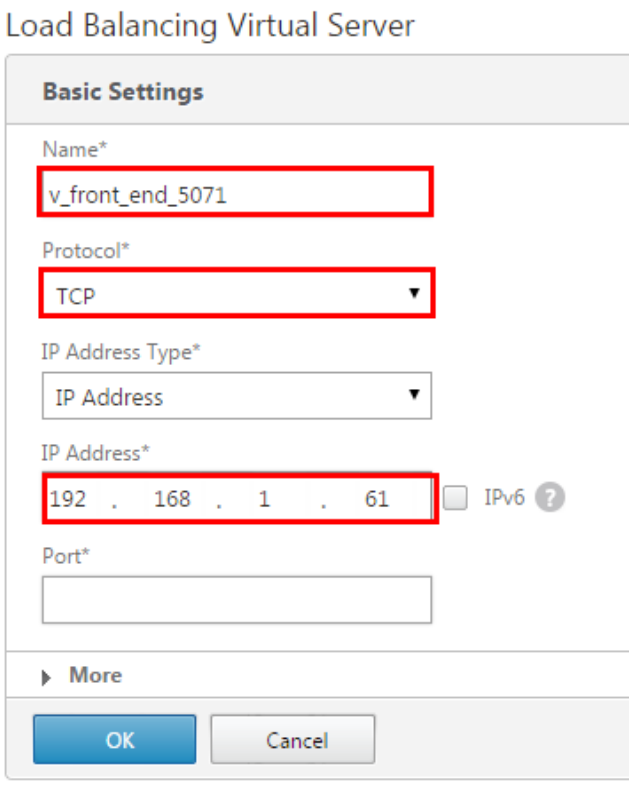


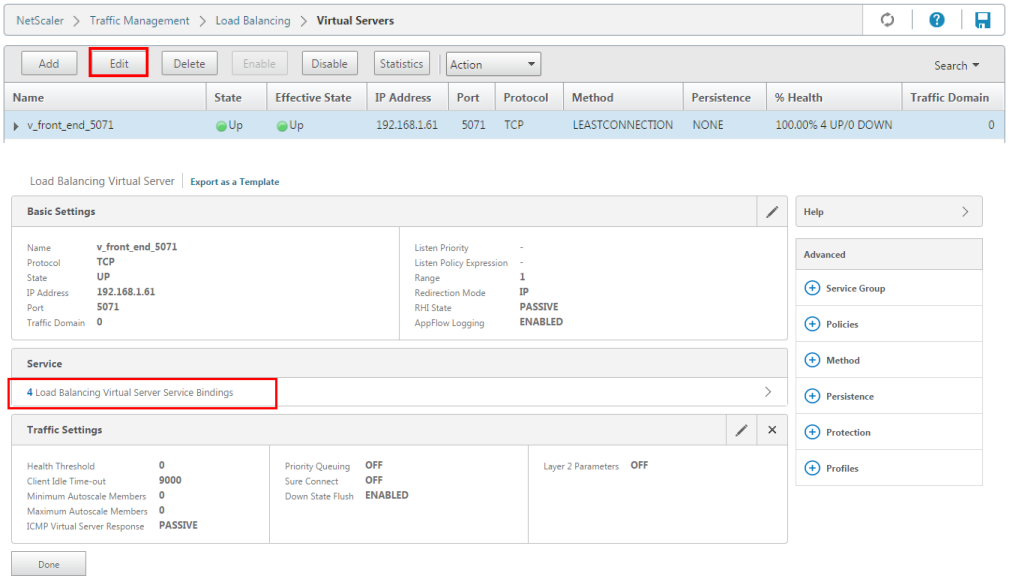


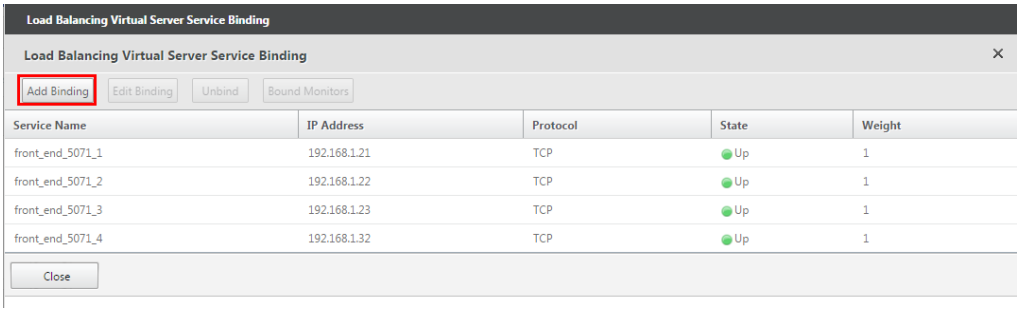


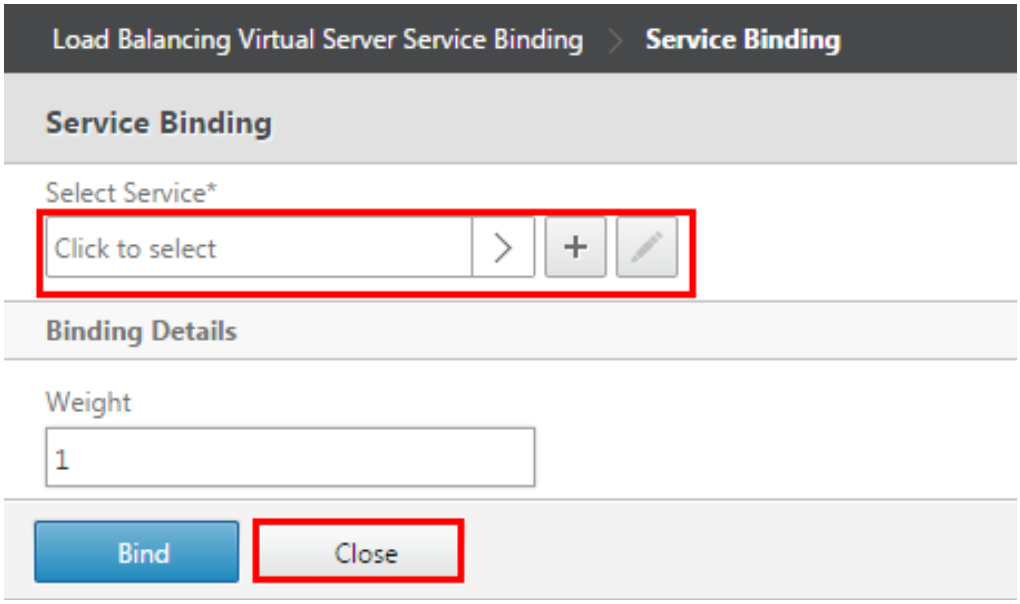
Create virtual servers

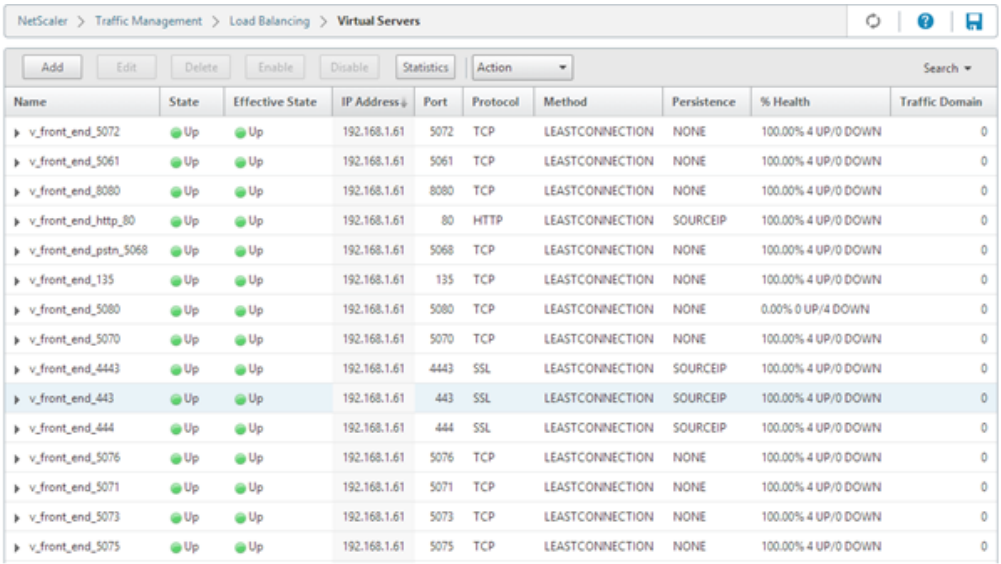



Load Balancing Virtual Server
Basic Settings
Name*
v_front_end_5071
Protocol*
TCP
IP Address Type*
IP Address
IP Address*
192 . 168 . 1 . 61
IPv6
Port*
More
OK
Cancel


NetScaler > Traffic Management > Load Balancing > Virtual Servers
Add
Edit
Delete
Enable
Disable
Statistics
Action
Search
Name
State
Effective State
IP Address
Port
Protocol
Method
Persistence
% Health
Traffic Domain
v_front_end_5071
Up
Up
192.168.1.61
5071
TCP
LEASTCONNECTION
NONE
100.00% 4 UP/0 DOWN
0
Load Balancing Virtual Server
Export as a Template
Basic Settings
Name v_front_end_5071
Protocol TCP
State UP
IP Address 192.168.1.61
Port 5071
Traffic Domain 0
Listen Priority -
Listen Policy Expression -
Range 1
Redirection Mode IP
RHI State PASSIVE
AppFlow Logging ENABLED
Help
Advanced
Service Group
Policies
Method
Persistence
Protection
Profiles
Service
4 Load Balancing Virtual Server Service Bindings
Traffic Settings
Health Threshold 0
Client Idle Time-out 9000
Minimum Autoscale Members 0
Maximum Autoscale Members 0
ICMP Virtual Server Response PASSIVE
Priority Queuing OFF
Sure Connect OFF
Down State Flush ENABLED
Layer 2 Parameters OFF
Done


Load Balancing Virtual Server Service Binding
Load Balancing Virtual Server Service Binding
Add Binding
Edit Binding
Unbind
Bound Monitors
Service Name
IP Address
Protocol
State
Weight
front_end_5071_1
192.168.1.21
TCP
Up
1
front_end_5071_2
192.168.1.22
TCP
Up
1
front_end_5071_3
192.168.1.23
TCP
Up
1
front_end_5071_4
192.168.1.32
TCP
Up
1
Close


Load Balancing Virtual Server Service Binding
Service Binding
Service Binding
Select Service*
Click to select
Binding Details
Weight
1
Bind
Close


NetScaler
Traffic Management
Load Balancing
Virtual Servers
Add
Edit
Delete
Enable
Disable
Statistics
Action
Search
Name
State
Effective State
IP Address
Port
Protocol
Method
Persistence
% Health
Traffic Domain
v_front_end_5072 Up Up 192.168.1.61 5072 TCP LEASTCONNECTION NONE 100.00% 4 UP/0 DOWN 0
v_front_end_5061 Up Up 192.168.1.61 5061 TCP LEASTCONNECTION NONE 100.00% 4 UP/0 DOWN 0
v_front_end_8080 Up Up 192.168.1.61 8080 TCP LEASTCONNECTION NONE 100.00% 4 UP/0 DOWN 0
v_front_end_http_80 Up Up 192.168.1.61 80 HTTP LEASTCONNECTION SOURCEIP 100.00% 4 UP/0 DOWN 0
v_front_end_pstn_5068 Up Up 192.168.1.61 5068 TCP LEASTCONNECTION NONE 100.00% 4 UP/0 DOWN 0
v_front_end_135 Up Up 192.168.1.61 135 TCP LEASTCONNECTION NONE 100.00% 4 UP/0 DOWN 0
v_front_end_5080 Up Up 192.168.1.61 5080 TCP LEASTCONNECTION NONE 0.00% 0 UP/4 DOWN 0
v_front_end_5070 Up Up 192.168.1.61 5070 TCP LEASTCONNECTION NONE 100.00% 4 UP/0 DOWN 0
v_front_end_4443 Up Up 192.168.1.61 4443 SSL LEASTCONNECTION SOURCEIP 100.00% 4 UP/0 DOWN 0
v_front_end_443 Up Up 192.168.1.61 443 SSL LEASTCONNECTION SOURCEIP 100.00% 4 UP/0 DOWN 0
v_front_end_444 Up Up 192.168.1.61 444 SSL LEASTCONNECTION SOURCEIP 100.00% 4 UP/0 DOWN 0
v_front_end_5076 Up Up 192.168.1.61 5076 TCP LEASTCONNECTION NONE 100.00% 4 UP/0 DOWN 0
v_front_end_5071 Up Up 192.168.1.61 5071 TCP LEASTCONNECTION NONE 100.00% 4 UP/0 DOWN 0
v_front_end_5073 Up Up 192.168.1.61 5073 TCP LEASTCONNECTION NONE 100.00% 4 UP/0 DOWN 0
v_front_end_5075 Up Up 192.168.1.61 5075 TCP LEASTCONNECTION NONE 100.00% 4 UP/0 DOWN 0

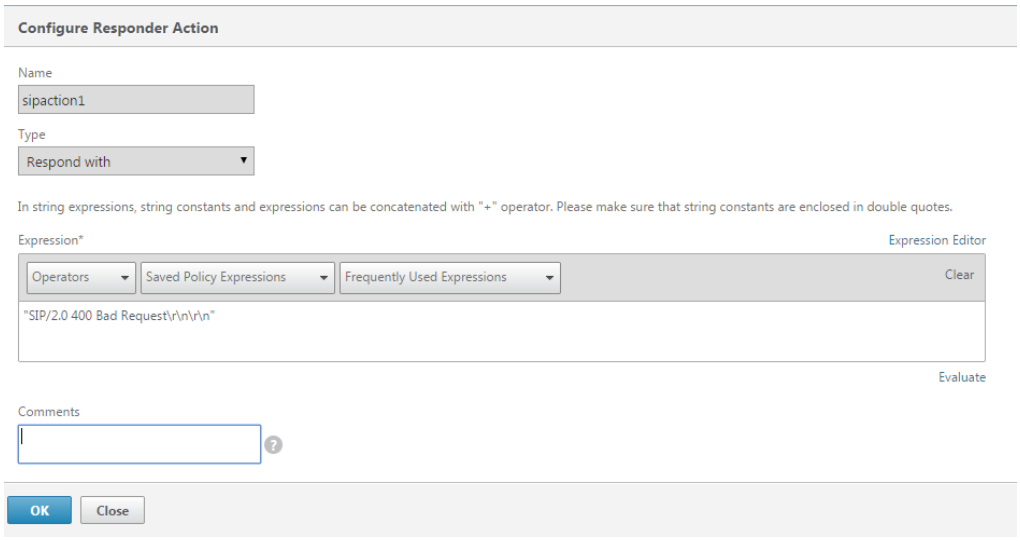
v_director_5061	Up	Up	192.168.1.62	5061	TCP	LEASTCONNECTION	SOURCEIP	100.00% 2 UP/0 DOWN	0
v_director_4443	Up	Up	192.168.1.62	4443	SSL	LEASTCONNECTION	SOURCEIP	100.00% 2 UP/0 DOWN	0
v_director_444	Up	Up	192.168.1.62	444	SSL	LEASTCONNECTION	SOURCEIP	100.00% 2 UP/0 DOWN	0
v_director_443	Up	Up	192.168.1.62	443	SSL	LEASTCONNECTION	SOURCEIP	100.00% 2 UP/0 DOWN	0
v_director_80	Up	Up	192.168.1.62	80	TCP	LEASTCONNECTION	NONE	100.00% 2 UP/0 DOWN	0
v_director_8080	Up	Up	192.168.1.62	8080	TCP	LEASTCONNECTION	NONE	100.00% 2 UP/0 DOWN	0

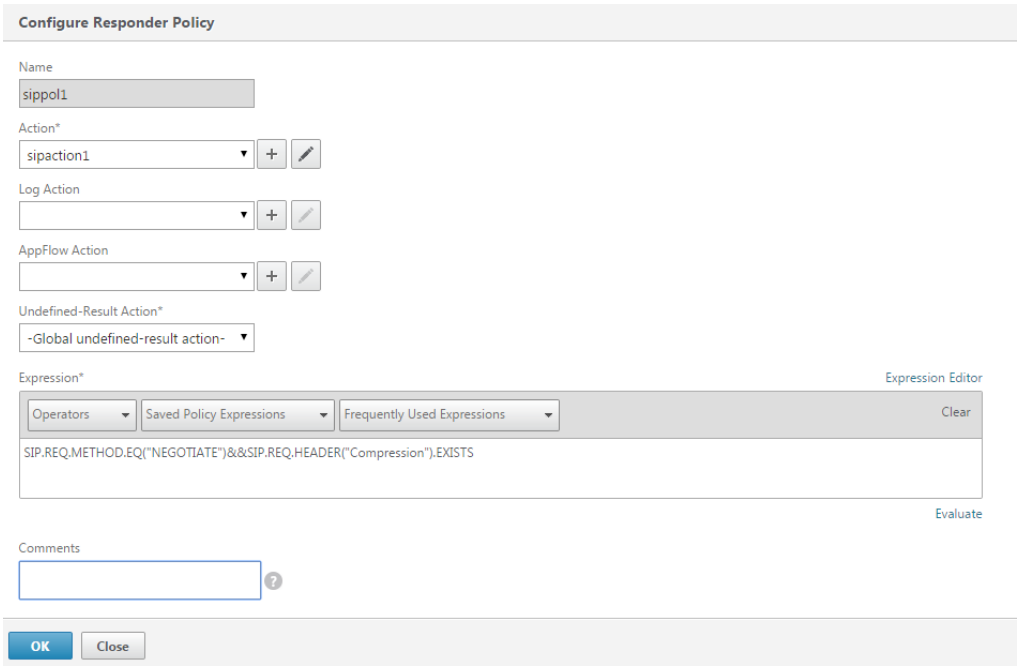
v_offc_webapp_443	Up	Up	192.168.1.63	443	SSL	LEASTCONNECTION	NONE	100.00% 1 UP/0 DOWN	0

v_cas_server	Up	Up	192.168.1.66	443	SSL	LEASTCONNECTION	NONE	100.00% 3 UP/0 DOWN	0

Suggested Optimization: Though Microsoft recommend using a TCP vip for port 5061, this limits supported persistency to "Source IP". If you want to enable "SIP Call ID" as persistency parameter we recommend following changes

- Change v_director_5061 and v_front_end_5061 to type SIP_SSL
- Convert bound service type to Sip_SSL
- A responder Policy is added to respond with bad request if compression is enabled on the client





Internal DNS Considerations

Below is an example of internal DNS Configuration used while testing in the lab:

dialin.ctxns.net	192.168.1.62
meet.ctxns.net	192.168.1.62
Lyncdiscover.ctxns.net	192.168.1.62
Owa.ctxns.net	192.168.1.63
LyncWeb.ctxns.net	192.168.1.61
LyncWebDir.ctxns.net	192.168.1.62

SSL Certificate Considerations

Create the below Server Certificate using an Internal CA with Subject name and Subject alternative name as below

---

Subject: CN=Dirpool.ctxns.net
X509v3 Subject Alternative Name:

DNS:sip.CTXNS.net, DNS:dir2.ctxns.net, DNS:Dirpool.ctxns.net, DNS:Dir1.CTXNS.net, DNS:dialin.ctxns.net, DNS:meet.ctxns.net, DNS:admin.ctxns.net, DNS:LyncdiscoverInternal.CTXNS.net, DNS:Lyncdiscover.CTXNS.net

add ssl certKey lync_cert -cert dirpool.pem -key dirpool.pem -passcrypt Wa4i9NP1Ma0=<password>

bind ssl vserver v_director_443 -certkeyName lync_cert
bind ssl vserver v_director_444 -certkeyName lync_cert
bind ssl vserver v_director_5061 -certkeyName lync_cert

Subject: CN=LyncwebDir.ctxns.net
X509v3 Subject Alternative Name:

DNS:Dirpool.ctxns.net, DNS:dialin.ctxns.net, DNS:meet.ctxns.net, DNS:admin.ctxns.net, DNS:LyncdiscoverInternal.CTXNS.net, DNS:Lyncdiscover.CTXNS.net

add ssl certKey dirwebcert -cert dirweb.pem -key dirwebkey.pem

bind ssl vserver v_director_4443 -certkeyName dirwebcert

X509v3 Subject Alternative Name:

DNS:sip.CTXNS.net, DNS:UCUpdates-r2.ctxns.net, DNS:UCupdates-r2, DNS:Lyncfe01.Ctxns.net, DNS:Lyncfe02.Ctxns.net, DNS:Lyncfe03.Ctxns.net, DNS:Lyncfe04.Ctxns.net, DNS:Pool.CTXNS.net, DNS:dialin.ctxns.net, DNS:meet.ctxns.net, DNS:admin.ctxns.net, DNS:LyncdiscoverInternal.CTXNS.net, DNS:LyncWeb.CTXNS.net, DNS:Lyncdiscover.CTXNS.net

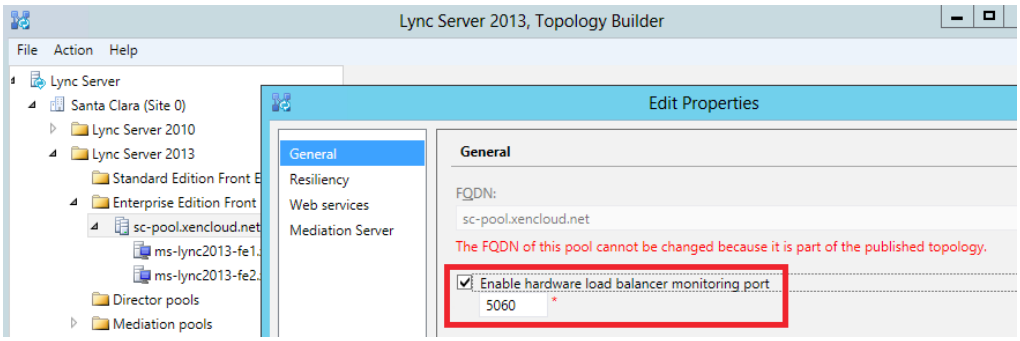
add ssl certKey poolupdate_cert -cert pool-update-r2.pem -key pool-update-r2.ky

bind ssl vserver v_front_end_443 -certkeyName poolupdate_cert
bind ssl vserver v_front_end_444 -certkeyName poolupdate_cert
bind ssl vserver v_front_end_4443 -certkeyName poolupdate_cert
bind ssl vserver v_front_end_5061 -certkeyName poolupdate_cert

---

Monitoring Resources

The Front-End Pool SIP Traffic on port 5061 is encrypted. However, you can optionally enable the unencrypted port 5060 for health monitoring (Note: SIP communication only occurs on the encrypted port, optionally enabling port 5060 is for health monitoring purposes only). This is achieved with the Lync Topology Builder as shown below.



Once the change has been made, publish the topology to enable this port and then create the custom NetScaler monitor. NOTE: Future release of NetScaler software will support Extended Content Verification via SIP-TCP. SIP_TCP monitor is available with 10.5.e thus we assume that and write. Put a note to use SIP-UDP for previous releases.

Create custom monitor for the internal SIP virtual servers (optional)

Load balancing, Reverse Proxy for External traffic

Load Balancing Edge Pool

In this scenario, the NetScaler will serve as the connectivity point to both the internal and external NICs for multiple Edge Servers in an array.

- Access Edge: The Access Edge service provides a single, trusted connection point for both outbound and inbound Session Initiation Protocol (SIP) traffic.
- Web Conferencing Edge: The Web Conferencing Edge service enables external users to join meetings that are hosted on an internal Lync Server 2013 deployment.
- A/V Edge service: The A/V Edge service makes audio, video, application sharing, and file transfer available to external users. Users can add audio and video to meetings that include external participants, and they can communicate using audio and/or video directly with an external user in point-to-point sessions. The A/V Edge service also provides support for desktop sharing and file transfer.
- XMPP Proxy: The XMPP Proxy service accepts and sends extensible messaging and presence protocol (XMPP) messages to and from configured XMPP Federated partners.

HTTPS Reverse Proxy

For Microsoft Lync Server 2013 Edge Server deployments, an HTTPS reverse proxy (i.e. NetScaler) in the perimeter network is required for external clients to access the Lync Server 2013 Web Services (called Web Components in Office Communications Server) on the Director and the user's home pool. The reason for a reverse proxy is because the web services are located in the internal Lync Pool; the Lync Edge does not provide these features.

Some of the features that require external access through a reverse proxy include the following:

- Enabling external users to download meeting content for your meetings.
- Enabling external users to expand distribution groups.
- Enabling remote users to download files from the Address Book service.
- Accessing the Lync Web App client.
- Accessing the Dial-in Conferencing Settings webpage.
- Accessing the Location Information service.
- Enabling external devices to connect to Device Update web service and obtain updates.
- Enabling mobile applications to automatically discover and use the mobility (Mcx) URLs from the Internet.
- Enabling the Lync 2013 client, Lync Windows Store app and Lync 2013 Mobile client to locate the Lync Discover (autodiscover) URLs and use Unified Communications Web API (UCWA).

Mobility

All Mobility Service traffic goes through the reverse proxy, regardless of where the origination point is—internal or external. In the case of a single reverse proxy or a farm of reverse proxies, or a device that is providing the reverse proxy function, an issue can arise when the internal traffic is egressing through an interface and attempting to immediately ingress on the same interface. This often leads to a Security rule violation known as TCP packet spoofing or just spoofing. Hair pinning (the egress and immediate ingress of a packet or series of packets) must be allowed in order for mobility to function. One way to resolve this issue is to use a reverse proxy that is separate from the firewall (the spoofing prevention rule should always be enforced at the firewall, for security purposes). The hairpin can occur at the external interface of the reverse proxy instead of the firewall external interface. You detect the spoofing at the firewall, and relax the rule at the reverse proxy, thereby allowing the hairpin that mobility requires.

Federations & XMPP Partners

Federation, public instant messaging connectivity and Extensible Messaging and Presence Protocol (XMPP) define a different class of external users – Federated users. Users of a federated Lync Server deployment or XMPP deployment have access to a limited set of services and are authenticated by the external deployment. Remote users are members of your Lync Server deployment and have access to all services offered by your deployment.

Public instant messaging connectivity is a special type of federation that allows a Lync Server client to access configured public Instant Messaging partners using the Lync 2013. The current public instant messaging connectivity partners are:

- America Online
- Windows Live
- Yahoo!

Note: An end of life date of June 2014 for AOL and Yahoo! has been announced.

A public instant messaging connectivity configuration allows Lync user's access to public instant messaging connectivity users by:

- IM and Presence
- Visibility of public instant messaging connectivity contacts in Lync client
- Person to person IM conversations with contacts
- Audio and video calls with Windows Live users

Lync Server federation defines an agreement between your Lync Server deployment and other Office Communications Server 2007 R2 or Lync Server deployments. A Lync Server federated configuration allows Lync user's access to federated users by:

- IM and Presence
- Creation of federated contacts in the Lync client

XMPP federation defines an external deployment based on the eXtensible Messaging and Presence Protocol. An XMPP configuration allows Lync user's access to allowed XMPP domain users by:

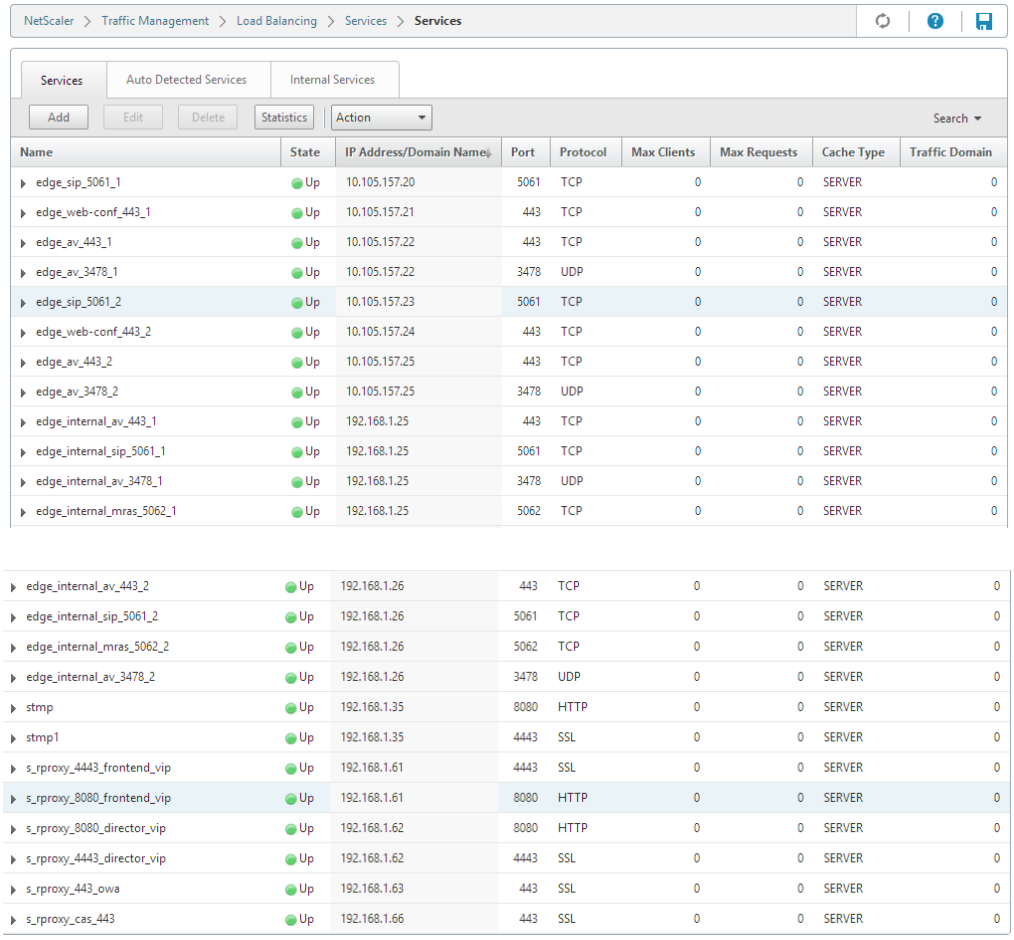
- IM and Presence – person to person only
- Creation of XMPP federated contacts in the Lync client

Table 2: Lab IP Addresses

Role	FQDN	IP	Additional
Lync Edge Internal Server	Edge1.ctxns.net	192.168.1.64	
Lync Edge External Server 1	LyncEdge01.ctxns.net	192.168.1.25	
Lync Edge External Server 1	LyncEdge02.ctxns.net	192.168.1.26	
NetScaler		10.105.157.70	

Follow steps given in internal traffic load balancing section to create monitors, servers and services. You should have following services configured as part of deployment.

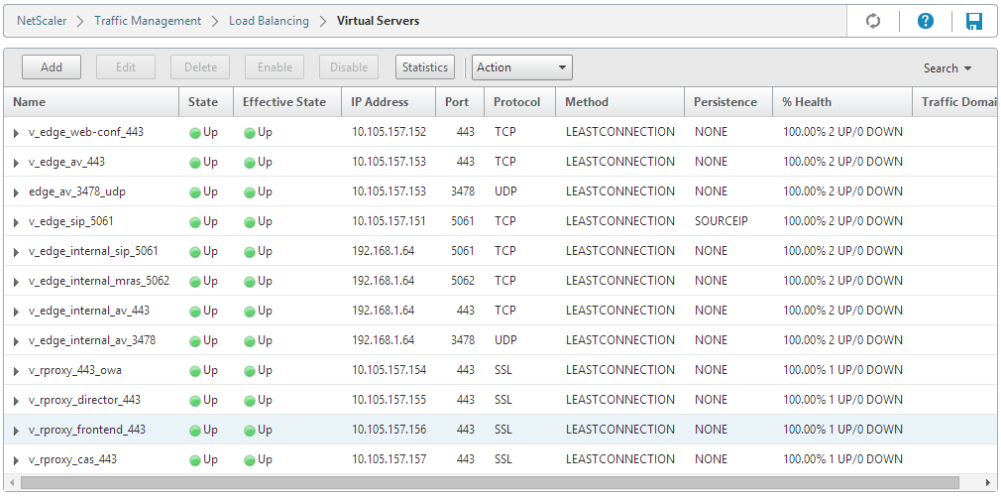
Create Services



Name	State	IP Address/Domain Name	Port	Protocol	Max Clients	Max Requests	Cache Type	Traffic Domain
edge_sip_5061_1	Up	10.105.157.20	5061	TCP	0	0	SERVER	0
edge_web-conf_443_1	Up	10.105.157.21	443	TCP	0	0	SERVER	0
edge_av_443_1	Up	10.105.157.22	443	TCP	0	0	SERVER	0
edge_av_3478_1	Up	10.105.157.22	3478	UDP	0	0	SERVER	0
edge_sip_5061_2	Up	10.105.157.23	5061	TCP	0	0	SERVER	0
edge_web-conf_443_2	Up	10.105.157.24	443	TCP	0	0	SERVER	0
edge_av_443_2	Up	10.105.157.25	443	TCP	0	0	SERVER	0
edge_av_3478_2	Up	10.105.157.25	3478	UDP	0	0	SERVER	0
edge_internal_av_443_1	Up	192.168.1.25	443	TCP	0	0	SERVER	0
edge_internal_sip_5061_1	Up	192.168.1.25	5061	TCP	0	0	SERVER	0
edge_internal_av_3478_1	Up	192.168.1.25	3478	UDP	0	0	SERVER	0
edge_internal_mras_5062_1	Up	192.168.1.25	5062	TCP	0	0	SERVER	0
edge_internal_av_443_2	Up	192.168.1.26	443	TCP	0	0	SERVER	0
edge_internal_sip_5061_2	Up	192.168.1.26	5061	TCP	0	0	SERVER	0
edge_internal_mras_5062_2	Up	192.168.1.26	5062	TCP	0	0	SERVER	0
edge_internal_av_3478_2	Up	192.168.1.26	3478	UDP	0	0	SERVER	0
stmp	Up	192.168.1.35	8080	HTTP	0	0	SERVER	0
stmp1	Up	192.168.1.35	4443	SSL	0	0	SERVER	0
s_rproxy_4443_frontend_vip	Up	192.168.1.61	4443	SSL	0	0	SERVER	0
s_rproxy_8080_frontend_vip	Up	192.168.1.61	8080	HTTP	0	0	SERVER	0
s_rproxy_8080_director_vip	Up	192.168.1.62	8080	HTTP	0	0	SERVER	0
s_rproxy_4443_director_vip	Up	192.168.1.62	4443	SSL	0	0	SERVER	0
s_rproxy_443_owa	Up	192.168.1.63	443	SSL	0	0	SERVER	0
s_rproxy_cas_443	Up	192.168.1.66	443	SSL	0	0	SERVER	0

Follow steps given in internal traffic load balancing section to create required vServers. You should have following vServers configured as part of deployment.

Create virtual servers



Name	State	Effective State	IP Address	Port	Protocol	Method	Persistence	% Health	Traffic Domai
v_edge_web-conf_443	Up	Up	10.105.157.152	443	TCP	LEASTCONNECTION	NONE	100.00% 2 UP/0 DOWN	
v_edge_av_443	Up	Up	10.105.157.153	443	TCP	LEASTCONNECTION	NONE	100.00% 2 UP/0 DOWN	
edge_av_3478_udp	Up	Up	10.105.157.153	3478	UDP	LEASTCONNECTION	NONE	100.00% 2 UP/0 DOWN	
v_edge_sip_5061	Up	Up	10.105.157.151	5061	TCP	LEASTCONNECTION	SOURCEIP	100.00% 2 UP/0 DOWN	
v_edge_internal_sip_5061	Up	Up	192.168.1.64	5061	TCP	LEASTCONNECTION	NONE	100.00% 2 UP/0 DOWN	
v_edge_internal_mras_5062	Up	Up	192.168.1.64	5062	TCP	LEASTCONNECTION	NONE	100.00% 2 UP/0 DOWN	
v_edge_internal_av_443	Up	Up	192.168.1.64	443	TCP	LEASTCONNECTION	NONE	100.00% 2 UP/0 DOWN	
v_edge_internal_av_3478	Up	Up	192.168.1.64	3478	UDP	LEASTCONNECTION	NONE	100.00% 2 UP/0 DOWN	
v_rproxy_443_owa	Up	Up	10.105.157.154	443	SSL	LEASTCONNECTION	NONE	100.00% 1 UP/0 DOWN	
v_rproxy_director_443	Up	Up	10.105.157.155	443	SSL	LEASTCONNECTION	NONE	100.00% 1 UP/0 DOWN	
v_rproxy_frontend_443	Up	Up	10.105.157.156	443	SSL	LEASTCONNECTION	NONE	100.00% 1 UP/0 DOWN	
v_rproxy_cas_443	Up	Up	10.105.157.157	443	SSL	LEASTCONNECTION	NONE	100.00% 1 UP/0 DOWN	

External DNS Considerations

Below is an example of external DNS Configuration used while testing in the lab:

Owa.ctxns.net	10.105.157.154:443	192.168.1.15	Domain Controller & DNS
Lyncdiscover.ctxns.net	10.105.157.155:443	192.168.1.20	Default Instance for Lync 2013
Lyncweb.ctxns.net	10.105.157.156:443	192.168.1.21	Pool Name: Pool.Ctxns.net
LyncWebDir.ctxns.net	10.105.157.155:443	192.168.1.22	Pool Name: Pool.Ctxns.net
Dialin.ctxns.net	10.105.157.155:443	192.168.1.23	Pool Name: Pool.Ctxns.net
Meet.ctxns.net	10.105.157.155:443	192.168.1.32	Pool Name: Pool.Ctxns.net
Mail.ctxns.net	10.105.157.157:443	172.16.99.201	xencloud\user1
Sip.ctxns.net	10.105.157.151:5061	172.16.99.202	xencloud\user2
webconf.ctxns.net	10.105.157.152:443	172.16.99.203	xencloud\user3
av.ctxns.net	10.105.157.153:443	10.105.157.50	

SSL Certificate Considerations

Create the below Server Certificate using a Public Trusted CA with Subject name and Subject alternative name as below

Subject: CN=*.ctxns.net

Subject Alternative Name:

DNS:dialin.ctxns.net,
DNS:meet.ctxns.net,
DNS:Lyncdiscover.ctxns.net,
DNS:Lyncwebdir.ctxns.net,
DNS:admin.ctxns.net,
DNS:sip.ctxns.net,
DNS:webconf.ctxns.net,
DNS:av.ctxns.net,
DNS:owa.ctxns.net,
DNS:Lyncweb.ctxns.net,
DNS:*.ctxns.net

Example::the above cert is generated with rp.pem and its corresponding private key rpkey.pem

Add this cert inside the NS and bind it with below External VIP's

```
add ssl certKey rpcert -cert rp.pem -key rpkey.pem

bind ssl vserver v_rproxy_443_owa -certkeyName rpcert
bind ssl vserver v_rproxy_director_443 -certkeyName rpcert
bind ssl vserver v_rproxy_frontend_443 -certkeyName rpcert
```

Benefits of using a hardware appliance load balancer

Lync 2013 allows load balancing the network traffic that is unique to Lync server such as SIP and media traffic. DNS load balancing support Front End pools, Edge Server pools, Director pools, and stand-alone Mediation Server pools. While DNS load balancing is lean and easy to maintain this simplicity comes at cost of lack of high availability, security and quality of services for end users.

Following are the benefits of using a hardware appliance-based load balancer in Lync 2013 deployment.

1. Persistency of HTTP traffic

Though IM traffic is SIP, data like Address book, Shared content, Web based meeting connectivity, Group expansion, and Device update is HTTP. HTTP traffic is session oriented and thus needs persistency. DNS load balancing does not support persistency and deploying a single application server leads to single point of failure. Hardware appliance based load balancers

- Support HTTP traffic load balancing with persistency
- Provide world class HTTP load balancing, monitoring and persistency module
- Leverage connection multiplexing for optimal utilization of server resources
- State of art optimization features that can be used along with load balancing

2. Quick automatic failure

DNS Load Balancing relies on the client or endpoint to decide the availability of the servers in each pool which is a reactive rather than a proactive mechanism. Query to an FQDN sends list of IPs of all the pool members and if a client hits a failed node it will pick the next node in list resulting. This sort of reactive mechanism result in a delay. In addition, failed nodes needs to be manually removed from list.

- Hardware appliance based load balancers provide ping monitors to check availability. This provides a proactive mechanism that reduce the delay.
- Leverage application aware monitors of NetScaler for intelligent monitoring
- NetScaler Global Server Load Balancing (GSLB) can provide DR solution across data centers

3. Seamless integration for federation cases

OCS 2007 does not support DNS load balancing and neither does public IM services like AOL, Gmail etc. do. DNS load balancing on Edge Servers causes a loss of failover ability and makes inter-enterprise integration difficult. These scenarios will work as long as all Edge Servers in the pool are up and running, but if one Edge Server is unavailable, any requests for these scenarios that are sent to it will fail, instead of routing to another Edge Server

- Hardware appliance based load balancers provide seamless inter-Enterprise integration as it provides transparent load balancing and a high availability solution.

4. Seamless integration for Exchange server UM which does not support DNS load balancing

5. Support for telephony equipment

Call failure rates are high when using DNS load balancing for mediation server role with IPBX that does not understand DNS load balancing.

Conclusion

A leading application delivery solution, Citrix® NetScaler not only meets but exceeds Microsoft's external load balancer recommendations for Lync deployments. Working closely with Microsoft's engineering and test teams, Citrix has designed NetScaler to optimize the delivery of traffic, achieving significant TCO savings while providing increased availability, capacity, performance, security and manageability. Eliminating infrastructure overhead to maximize Lync value is the goal of NetScaler solutions. To learn more about how NetScaler can bring these benefits to Lync installations or address other application delivery requirements, please visit http://www.citrix.com.

Appendix

Product versions used during testing

Microsoft Lync 2013	en_lync_server_2013_x64
Lync Client (MS Office 2013)	en_office_professional_plus_2013_x86
Lync Platform (Server 2012)	en_windows_server_2012_x64
Active Directory (Server 2012)	en_windows_server_2012_x64
SQL Server (SQL Server 2012)	en_sql_server_2012_standard_edition_with_sp1_x64
Citrix NetScaler 10.1	NS10.1: Build 112.15.nc
Citrix XenServer 6.1	6.1: Build 59235p
Firewalls and Delay Router	CentOS 6.4

Lync PowerShell Commands

Export Configuration for Edge Servers	Export-CsConfiguration –FileName <path/filename>
Update Address Book	Update-CsAddressBook
Verify Status of Replication	Get-CsManagementStoreReplicationStatus
Display Access Edge Configuration	Get-CsAccessEdgeConfiguration

Corporate Headquarters
Fort Lauderdale, FL, USA

Silicon Valley Headquarters
Santa Clara, CA, USA

EMEA Headquarters
Schaffhausen, Switzerland

India Development Center
Bangalore, India

Online Division Headquarters
Santa Barbara, CA, USA

Pacific Headquarters
Hong Kong, China

Latin America Headquarters
Coral Gables, FL, USA

UK Development Center
Chalfont, United Kingdom

About Citrix
Citrix (NASDAQ:CTXS) is a leader in mobile workspaces, providing virtualization, mobility management, networking and cloud services to enable new ways to work better. Citrix solutions power business mobility through secure, personal workspaces that provide people with instant access to apps, desktops, data and communications on any device, over any network and cloud. This year Citrix is celebrating 25 years of innovation, making IT simpler and people more productive. With annual revenue in 2013 of $2.9 billion, Citrix solutions are in use at more than 330,000 organizations and by over 100 million users globally. Learn more at www.citrix.com