How to Deploy with Microsoft Lync Server 2010 and 2013

https://campus.barracuda.com/doc/19333290/

Product Versions and Prerequisites

This article applies to the Barracuda Load Balancer ADC 5.1 and above, with

- Microsoft® Lync® Server 2010 or 2013 Enterprise Edition
- For Lync Mobility, Apple iPhone and iPad; Android phone; Windows Phone 7; and Nokia mobile devices

For a full list of the prerequisites for this deployment, see Microsoft Lync 2010 and 2013 Server Deployment.

Before You Begin

Print or copy the IP Worksheet and use it to record your configuration. Complete this worksheet as you perform the tasks to deploy the Microsoft Lync Server. The worksheet will help you when you run the Topology Builder.

If you want additional information on deployment requirements and options, the following Microsoft Lync References are available:

- For a list of requirements, see Microsoft Lync 2010 and 2013 Server Deployment.
- For deployment options, see Understanding Microsoft Lync Server Deployment Options.
- For mobility deployment details, see the Microsoft TechNet article Deploying Mobility.

Before Running Lync Topology Builder

Do not run the Lync Topology Builder until instructed to do so by this deployment guide. All of the services on the Barracuda Load Balancer ADC must be configured *before* running the Topology Builder.

Deployment Tasks

Configuring Clustered Barracuda Load Balancer ADCs

If your Barracuda Load Balancer ADCs are clustered, the configuration between the active and passive units is synchronized; you only need to configure the active Barracuda Load Balancer ADC.

To deploy the Barracuda Load Balancer ADC in a Lync 2010 or 2013 environment, complete the following tasks:

Deployment Task	Where
Task 1. Configure Enterprise Pool Services	Do this on the internal-facing Barracuda Load Balancer ADC.
If you did not collocate A/V Services on your Front End Servers, you must also do the following:	
Task 2. (If applicable) Configure Internal A/V Services	Do this on the A/V Pool Barracuda Load Balancer ADC.
If you have an edge deployment, you must also complete the following tasks:	
Task 3. Configure Internal Edge Services	Do this on the internal-facing Barracuda Load Balancer ADC.
Task 4. Configure External Edge Services	Do this on the external-facing Barracuda Load Balancer ADC.
If you have deployed Director servers, you must also complete the following task:	
Task 5. Configure Director Services	Do this on the Director Barracuda Load Balancer ADC.
Complete the following tasks *after* all Services are configured on the Barracuda Load Balancer ADC:	
Task 6. Run Topology Builder	Do this on the server where Topology Builder is installed.
Task 7. Configure SSL Settings	Do this on the internal-facing Barracuda Load Balancer ADC.
Configure Mobility Services and configure the Barracuda Load Balancer ADC as a reverse proxy:	
Task 8. Configure Lync Mobility Services	Do this on the internal-facing Barracuda Load Balancer ADC.
task9	Do this on the external-facing Barracuda Load Balancer ADC.
If you encounter connectivity issues with your deployment, you can use the Remote Connectivity Analyzer:	
Troubleshooting	

Task 1. Configure Enterprise Pool Services

Configure all services needed for an internal Lync deployment. Perform the following steps on the internal-facing Barracuda Load Balancer ADC.

1. Go to the **BASIC > Services** page in the web interface.
2. Add all of the services listed in Table 1, along with their real servers. For each service, click **Add Service** and enter the values in the corresponding fields. To add a real server, click **Add Server** and enter the IP address and port for the server.

   Table 1. Enterprise Pool Services

   Persistence Settings for Lync 2013
   In these settings, source IP persistence is recommended. However, for Lync 2013, you can choose to use cookie persistence instead.

Name	Type	IP Address	Port	Session Timeout	Real Servers
MTLS_Front	TCP Proxy	IP address for the FQDN of the Internal Enterprise Lync Pool e.g., `192.168.1.11/24` for `frontpool.domain.local`	5061	1800	IP addresses of your front-end servers (K and L from the deployment example)
DCOM_WMI_Front	TCP Proxy	IP address for the FQDN of the Internal Enterprise Lync Pool	135	1800	IP addresses of your front-end servers (K and L from the deployment example)
Internal_Conf_Front	TCP Proxy	IP address for the FQDN of the Internal Enterprise Lync Pool	444	1800	IP addresses of your front-end servers (K and L from the deployment example)
HTTPS_Front	HTTPS	IP address for the FQDN of the Internal Enterprise Lync Pool	443	1800	IP addresses of your front-end servers (K and L from the deployment example)

   The Barracuda Load Balancer ADC is preconfigured with default settings that work with most applications. Lync 2010 requires changes to the **Session Timeout** setting for each service configured for Lync on the Barracuda Load Balancer ADC to ensure compliance with Microsoft specifications.
3. For the DCOM_WMI_Front service *only,* enable TCP port monitoring for each real server associated with the service.
   1. Next to each real server entry in the **Configured Servers** table, click **Edit**.
   2. In the **Edit Server** window, scroll to the **Server Monitor** section and specify these settings:
      - **Testing Method** – Select **TCP Port Check**.
      - **Port** – Enter `5061`. Testing port 5061 for this service is recommended because port 135 always passes the TCP port check, even if Lync Services are not responding.
4. For the HTTPS_Front service *only*, configure cookie persistence.
   1. In the service settings, scroll to the Load Balancing section.
   2. Configure these settings:
      - **Persistence Type** – Select **Cookie Insert** or **Cookie Passive**.
      - **Persistence Time** – Enter `1200`.

5. If you have deployed any of the features in Table 2, add the service for the feature.

Table 2. Services for Optional Features

Persistence Settings for Lync 2013
In these settings, source IP persistence is recommended. However, for Lync 2013, you can choose to use cookie persistence instead.

Name	Type	IP Address	Port	Session Timeout	Persistence	Real Servers
Application_Sharing	TCP Proxy	IP address for the FQDN of the Internal Enterprise Lync Pool	5065	1800	**Type**: Source IP **Time** : 1200	IP addresses of your front-end servers (K and L from the deployment example)
Response_Group_Service	TCP Proxy	IP address for the FQDN of the Internal Enterprise Lync Pool	5071	1800	**Type**: Source IP **Time** : 1200	IP Addresses of your front-end servers (K and L from the deployment example)
Conferencing_Attendant	TCP Proxy	IP address for the FQDN of the Internal Enterprise Lync Pool	5072	1800	**Type**: Source IP **Time** : 1200	IP addresses of your front-end servers (K and L from the deployment example)
Conferencing_Announcement	TCP Proxy	IP address for the FQDN of the Internal Enterprise Lync Pool	5073	1800	**Type**: Source IP **Time** : 1200	IP addresses of your front-end servers (K and L from the deployment example)

Task 2. (If Applicable) Configure Internal A/V Services

Complete this step if you did not collocate A/V Services on your front-end servers.

If you have more than 10,000 users in this pool, it is recommended that you separate the A/V Services of your Internal Lync Pool and do not collocate the A/V services on the Front End Pool. If you choose to collocate A/V Services on your Front End Pool, no further changes to the configuration are required.

Separating out the A/V Services into its own pool requires two more Barracuda Load Balancer ADCs operating as a high availability pair. If your deployment has more than 10,000 A/V users, contact Barracuda Networks Technical Support for assistance.

Task 3. Configure Internal Edge Services

To configure all services needed for a load-balanced Lync Edge deployment, perform the following steps on the internal-facing Barracuda Load Balancer ADC.

1. Go to the **BASIC > Services** page in the web Interface.
2. Add all of the services listed in Table 3, along with their real servers. For each service, click **Add Service** and enter the values in the corresponding fields. To add a real server, click **Add Server** and enter the IP address and port for the server.

Table 3. Internal Edge Services

Persistence Settings for Lync 2013
In these settings, source IP persistence is recommended. However, for Lync 2013, you can choose to use cookie persistence instead.

Service Name	Type	IP Address	Port	Session Timeout	Persistence	Real Servers
MTLS_Edge	TCP Proxy	IP address for the FQDN of the Internal Edge Enterprise Lync Pool e.g., 192.168.1.12/24 for `edgepool.domain.local`	5061	1800	**Type**: Source IP **Time**: 1200	Internal IP addresses of your Edge Servers (I and J from the deployment example)
AV_Auth_Edge	TCP Proxy	IP address for the FQDN of the Internal Edge Enterprise Lync Pool	5062	1800	**Type**: Source IP **Time**: 1200	Internal IP addresses of your Edge Servers (I and J from the deployment example)
AV_Edge	HTTPS	IP address for the FQDN of the Internal Edge Enterprise Lync Pool	443	1800	**Type**: Cookie Insert *or* Cookie Passive **Time**: 1200 Specify the **Cookie Name** if needed.	Internal IP addresses of your Edge Servers (I and J from the deployment example)

Replica_Replicator_Edge	HTTPS	IP address for the FQDN of the Internal Edge Enterprise Lync Pool	4443	1800	**Type**: Cookie Insert *or* Cookie Passive **Time**: 1200 Specify the **Cookie Name** if needed.	Internal IP addresses of your Edge Servers (I and J from the deployment example)
Web_Conferencing_Edge	TCP Proxy	IP address for the FQDN of the Internal Edge Enterprise Lync Pool	8057	1800	**Type**: Source IP **Time**: 1200	Internal IP addresses of your Edge Servers (I and J from the deployment example)
RDP_Media_Edge	UDP Proxy	IP address for the FQDN of the Internal Edge Enterprise Lync Pool	3478	1800	**Type**: Source IP **Time**: 1200	Internal IP addresses of your Edge Servers (I and J from the deployment example)

Task 4. Configure External Edge Services

WAN refers to interface(s) configured to access the external network.

LAN refers to interface(s) configured to access the internal network.

Ensure that the real servers are physically connected to a switch that is connected to the LAN-facing port (for two-armed deployment) or the WAN-facing port (for one-armed deployment) of the Barracuda Load Balancer ADC.

To configure all services needed for a load-balanced Edge Deployment of Lync Server, perform the following steps on the external-facing (Internet-facing) Barracuda Load Balancer ADC.

1. Go to the **BASIC > Services** page in the web interface.
2. Add all of the services listed in Table 4, along with their real servers. For each service, click **Add Service** and enter the values in the corresponding fields. To add a real server, click **Add Server** and enter the IP address and port for the server.

Table 4. External Edge Services

Persistence Settings for Lync 2013

In these settings, source IP persistence is recommended. However, for Lync 2013, you can choose to use cookie persistence instead.

Name	Type	IP Address	Port	Session Timeout	Persistence	Real Servers
Access_Edge	One-armed:TCP Proxy Two-armed: Layer 4 - TCP	IP address for the FQDN of Access Edge e.g., IP address for `lync.example.com`	443	1800	**Type**: Source IP **Time**: 1200	IP address of Access Edge NICs on each Edge Server (C and F from the deployment example)
Access_Fed_Edge	One-armed:TCP Proxy Two-armed: Layer 4 - TCP	IP address for the FQDN of Access Edge e.g., IP address for `lync.example.com`	5061	1800	**Type**: Source IP **Time**: 1200	IP address of Access Edge NICs on each Edge Server (C and F from the deployment example)
Web_Conferencing_Edge	One-armed:TCP Proxy Two-armed: Layer 4 - TCP	IP address for the FQDN of WebConf Edge e.g., IP address for `webconf.example.com`	443	1800	**Type**: Source IP **Time**: 1200	IP address of of your Edge Servers (D and G from the deployment example)
AV_Edge	One-armed:TCP Proxy Two-armed: Layer 4 - TCP	IP address for the FQDN of AV Edge e.g., IP address for `av.example.com`	443	1800	**Type**: Source IP **Time**: 1200	IP address of your Edge Servers (E and H from the deployment example)
AV_Media_Edge	One-armed: UDP Proxy Two-armed: Layer 4 - UDP	IP address for the FQDN of AV Edge e.g., IP address for `av.example.com`	3478	1800	default settings	IP address of your Edge Servers (E and H from the deployment example)

Task 5. Configure Director Services

To configure all services needed for a load-balanced Edge Deployment of Lync Server, perform the following steps on the external-facing Barracuda Load Balancer ADC.

Persistence Settings for Lync 2013

In these settings for the Director Services, source IP persistence is recommended. However, for Lync 2013, you can choose to use cookie persistence instead.

1. Go to the **BASIC > Services** page in the web interface.
2. Add the following Directory_MTLS service with its real servers. Click **Add Service** and enter the values in the corresponding fields. To add a real server, click **Add Server** and enter the IP address and port for the server.

Name	Type	IP Address	Port	Session Timeout	Persistence	Real Servers
Directory_MTLS	TCP Proxy	IP address for the FQDN of the Directory Service	5061	1800	**Type**: Source IP **Time**: 1200	IP address of your Directory Servers

3. If you must support Office Communications Server prior to version 2007 R2, add the following Directory_MTLS_Legacy service. If you only have versions of Office Communications Server that are 2007 R2 or later (including Lync), do not add this service.

Name	Type	IP Address	Port	Session Timeout	Persistence	Real Servers
Directory_MTLS_Legacy	TCP Proxy	IP for FQDN of the Directory Service	5060	1800	**Type**: Source IP **Time**: 1200	IP address of your Directory Servers

Task 6. Run Topology Builder

After you configure all services on the Barracuda Load Balancer ADC, run LyncTopology Builder. To complete the required fields, use the configuration information that you recorded in the IP Worksheet.

Task 7. Configure SSL Settings

Install an SSL certificate on the internal-facing Barracuda Load Balancer ADC for the HTTPS services

that were configured previously. The Barracuda Load Balancer ADC uses this certificate to decrypt the SSL traffic directed to the HTTPS services, and it checks for a persistence cookie.

Also, you must configure back-end SSL on the real servers to re-encrypt traffic before sending it to a server in the pool.

Using the Microsoft Management Console (MMC), export a certificate along with its private key, from one of the front-end Lync servers. Ensure the pool name is in the certificate.

Perform the following steps on the internal-facing Barracuda Load Balancer ADC for the HTTPS_Front service.

1. Go to the **BASIC > Certificates** page, and import the certificate.
2. Go to the **BASIC > Services** page and edit the service. In the **Certificates** section of the service settings, select the uploaded certificate.
3. Enable SSL in the settings of the real servers.
    1. Next to each real server entry in the **Configured Servers** table, click **Edit**.
    2. In the **Edit Server** window:
        1. Scroll to the **SSL** section and turn on the **Server uses SSL** setting.
        2. Scroll to the **Certificates** section and select the certificate that you uploaded.
4. If you deployed Edge services on the internal-facing Barracuda Load Balancer ADC, repeat these steps for the Replica_Replicator_Edge and AV_Edge services.

Your installation of the Barracuda Load Balancer ADC and Microsoft Lync Server is now complete. Continue to configure the Barracuda Load Balancer ADC for Lync Mobility.

Task 8. Configure Lync Mobility Services

To configure the services needed for a Lync Mobility deployment, perform the following steps on the internal-facing Barracuda Load Balancer ADC.

Persistence Settings for Lync 2013

In these settings for the Lync Mobility Services, source IP persistence is recommended. However, for Lync 2013, you can choose to use cookie persistence instead.

1. Go to the **BASIC > Services** page in the web interface.
2. Add the following Lync_Mobility_HTTPS service with its real servers. Click **Add Service** and enter the values in the corresponding fields. To add a real server, click **Add Server** and enter the IP address and port for the server.

Name	Type	IP Address	Session Timeout	Certificate	Persistence	Real Servers
Lync_Mobility_HTTPS	HTTPS	IP address for the FQDN of the Internal Enterprise Lync pool Port is 4443	1800	Select the certificate assigned to the Lync front-end server for external web services. For more information on creating and assigning the certificate, see Appendix A. Certificate for Lync Mobility Service.	**Type**: Cookie Insert *or* Cookie Passive **Time**: 1200 Specify the **Cookie Name** if needed.	Internal IP addresses of front-end servers Port is 4443

3. Edit the SSL settings for the real servers of the Lync_Mobility_HTTPS service.
    1. Next to each real server entry in the **Configured Servers** table, click **Edit**.
    2. In the **Edit Server** window, scroll to the **SSL** section.
    3. Set **Server Uses SSL** to **On**.
    4. Expand the settings, and set **Validate Certificate** to **Off**.
4. If you enabled Lync Mobility connections over HTTP, add the following Lync_Mobility_HTTP service.

Name	Type	IP Address	Session Timeout	Persistence	Real Servers
Lync_Mobility_HTTP	HTTP	IP address for the FQDN of the Internal Enterprise Lync pool Port is 8080	1800	default	Internal IP addresses of front-end servers Port is 8080

Task 9. Configure the Barracuda Load Balancer ADC as a Reverse Proxy for Lync Mobility Services

A reverse proxy is required to support Lync Mobility Services, because it lets remote users access the functionality provided by Lync Web Services. To configure the services needed to deploy the Barracuda Load Balancer ADC as a reverse proxy, perform the following steps on the external-facing Barracuda Load Balancer ADC.

Persistence Settings for Lync 2013

In these settings for the Lync Mobiliity Services, source IP persistence is recommended.

However, for Lync 2013, you can choose to use cookie persistence instead.

1. Go to the **BASIC > Services** page.
2. Add the following Lync_RP_HTTPS service with its real servers. Click **Add Service** and enter the values in the corresponding fields. To add a real server, click **Add Server** and enter the IP address and port for the server.

Service Name	Type	IP Address	Session Timeout	Certificate	Persistence	Real Server
Lync_RP_HTTPS	HTTPS	IP address of the FQDN of the External Web Services Port is 443	1800	Select the certificate assigned to the Lync front-end server for external web services. For more information on creating and assigning the certificate, see Appendix A. Certificate for Lync Mobility Service.	**Type**: Cookie Insert or Cookie Passive **Time** : 1200 **Cookie Name** : MS_WSMAN	VIP address of the Lync Mobility HTTPS service Port is 4443

3. Edit the SSL settings for the real servers of the Lync_RP_HTTPS service.
    1. Next to each real server entry in the **Configured Servers** table, click **Edit**.
    2. In the **Edit Server** window, scroll to the **SSL** section.
    3. Set **Server Uses SSL** to **On**.
    4. Expand the settings, and set **Validate Certificate** to **Off**.
4. If you enabled Lync Mobility connections over HTTP, add the following Lync_RP_HTTP service.

Service Name	Type	IP Address	Session Timeout	Persistence	Real Server
Lync_RP_HTTP	HTTP	IP address of the FQDN of the External Web Services Port is 80	1800	default	VIP address of the Lync Mobility HTTP service Port is 8080

Troubleshooting

To troubleshoot connectivity issues by simulating different scenarios, you can use the Remote Connectivity Analyzer at:

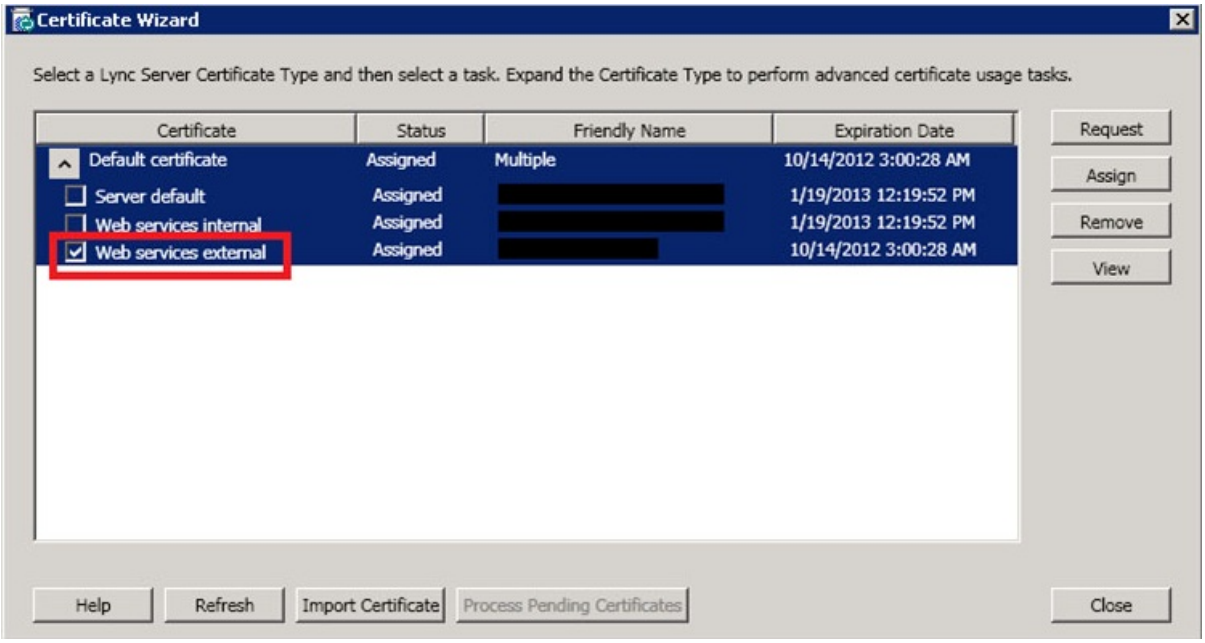
https://testconnectivity.microsoft.com/

Appendix A. Certificate for Lync Mobility Service

Using the Lync Certificate Wizard, you can create the certificate to be assigned to the Lync Mobility Service and to the Reverse Proxy (RP) Service. The certificate's SAN must contain the autodiscover URL and your external web services URL. The Lync_RP_HTTPS service and the Lync_Mobility_HTTPS service that you create on the Barracuda Load Balancer ADC can be assigned the same certificate.

For more information regarding certificate requirements, refer to the Microsoft TechNet article called Certificate Summary - Reverse Proxy.

When you use the Lync Certificate Wizard to request the certificate, select the **Web services external** check box and assign the certificate to the Barracuda Load Balancer ADC:



Next Step

You can configure authentication and access control for your applications. For more information, see Access Control.

Figures

1. CertificateWizard.jpg