# HOWTO - Enable Nginx Reverse Proxy

**Overview** What is the reverse proxy? Why do we need it? How does it work? Installing Nginx Linux Centos 6 / RHEL 6 Install the nginx.repo Centos 6 RHEL 6 Update yum **Install Nginx** Centos 7 / RHEL 7 Create a nginx.repo Centos 7 RHEL 7 Update Yum **Install Nginx Windows** Download Verify Nginx Windows Installation **Configuration** Nginx **BEFORE START** Linux **Windows SSL** Certificates **Certificates and Encodings** X509 File Extensions Encodings (also used as extensions) **Common Extensions** Configuring Nginx Certs SSL Ciphers SSL TLVv1.2 only

Running as a Service Linux Windows HTTP to HTTPs redirection Reverse Proxy Listmanager Disable SSL HTTP and HTTPs ports

Tests Application Rating <u>Test</u> Invalidating the Test Cache

Example Configuration Single file

## Overview

## What is the reverse proxy?

A reverse proxy server is a type of proxy server that typically sits behind the firewall in a private network and directs client requests to the appropriate backend server. A reverse proxy provides an additional level of abstraction and control to ensure the smooth flow of network traffic between clients and servers, including security, availability, performance and traffic shaping.



## Why do we need it?

The LM web server is not able to get an "A" rate on SSL Test Rating and It is caused by LM doesn't support strong/new ciphers for TLS encrypted connections (HTTPS/SSL). This inability to handle secure TLS/SSL connections is caused by an incomplete HTTP/HTTPS server implementation provided by ActiveTCL 1.4/1.5 and OpenSSL 1.0.2u.



## How does it work?

As we can see at "<u>What is the Reverse Proxy</u>" topic, it will work in front of the current LM web server, forcing all HTTP traffic be redirected to HTTPS and using just the LM HTTP implementation to avoid over-heading and improve performance. It will also use all new and well secured TLSv1.2 cyphers to provide an "A" rate on SSL implementation.



It will be implemented by a <u>Nginx</u> instance listening on HTTP (TCP 80) and HTTPS (TCP 443) ports all the internet requests and then mediating all connections to LM HTTP server (TCP 8080 - if they are running on the same server).

Overall Rating		1	E.	Ĩ	Ē	
	Certificate					
	Protocol Support					
A	Key Exchange					
	Cipher Strength					
	0	20	40	60	80	100

Nginx will provide all needed configuration and infrastructure to support an "A" rate.

## **Installing Nginx**

Nginx is an extremely high performance web server which has the ability to handle thousands of requests per second with little hardware requirements. It can be installed on any operating system and it comes as an open source application as well.

### PLEASE USE NGINX VERSION >= 1.16 (WE WILL USE 1.18 for this HOWTO).

Linux

Centos 6 / RHEL 6

Install the nginx.repo

Centos 6
Run these commands:
# wget
http://nginx.org/packages/centos/6/noarch/RPMS/nginx-release-centos-6-0.el
6.ngx.noarch.rpm

# rpm -ivh nginx-release-centos-6-0.el6.ngx.noarch.rpm

RHEL 6
Run these commands:
# wget
http://nginx.org/packages/rhel/6/noarch/RPMS/nginx-release-rhel-6-0.el6.ng
x.noarch.rpm
# rpm -ivh nginx-release-rhel-6-0.el6.ngx.noarch.rpm

Update yum

Run command: \$ yum update

Install Nginx Run command: \$ yum install nginx

## Centos 7 / RHEL 7

Create a nginx.repo Run command: \$ vi /etc/yum.repos.d/nginx.repo

Centos 7 Paste this at /etc/yum.repos.d/nginx.repo:

[nginx] name=nginx repo baseurl=http://nginx.org/packages/mainline/centos/7/\$basearch/ gpgcheck=0 enabled=1

RHEL 7 Paste this at /etc/yum.repos.d/nginx.repo:

[nginx] name=nginx repo baseurl=http://nginx.org/packages/mainline/rhel/7/\$basearch/ gpgcheck=0 enabled=1

Update Yum Run command: \$ yum update
Install Nginx
Run command:
\$ yum install nginx

#### Test opening on your browser:

		Welcome to nginxl - Chromium		0	0 😣
	) Welcome t	onginx! ×			0
←	→ C 🗅 h	ttp://10.21.136.134	•	D	:
	Welco	me to nginx!			
	If you see th working. Fu	is page, the nginx web server is successfully installe ther configuration is required.	d and		
	For online d Commercial	ocumentation and support please refer to <u>nginx.org</u> . support is available at <u>nginx.com</u> .			
	Thank you f	or using nginx.			

## Windows

### Download

Nginx comes pre-compiled for Windows which makes it extremely easy to get started. If it did not come pre-compiled, you would need to have a compiler installed on your computer with a full environment. Fortunately, this is not the case.

Download Nginx Windows here: <u>http://nginx.org/en/download.html</u>

Once you've downloaded Nginx for Windows, you can extract it to your folder of choice, we recommend that you install it somewhere easily accessible such as **C:\nginx**.

### Verify Nginx Windows Installation

In order to make sure that the service is working with no problems, we recommend that you start a command prompt window and type the following, make sure that you update the path if you've installed it in another folder.

C:\nginx\nginx.exe

You should be able to go to http://localhost/ and you should see the "Welcome to Nginx" default page. If you see that page, then we can be sure that Nginx has been installed properly. We will now shut it down and install it as a service, to stop it, you can use this command.

C:\nginx\nginx.exe -s stop

Now, if you were using Nginx as a simple development server, you can use these simple commands to start and stop the server as you need. However, if you will be using it as a production server, you would want to install it as a <u>Windows service</u>.

## Configuration

Nginx

### **BEFORE START**

Linux

No actions required.

#### Windows

Please be sure to use double-backslashes (\\) to define paths into nginx.conf and also be sure you already have an **error\_log** and **pid** directives defined.

```
IT VOLL COO THIC HARD THO HAINY WON CONJOR IC
                                                                           CHCCOCCTI
厵
                                                                           х
                           nginx.conf (C:\nginx\conf) - GVIM
File Edit Tools
              Syntax
                    Buffers
                           Window Help
3808
                               🗟 🔁 🔁 🍰 🏂 🕄
                                                    ግ 🗿 🖸
                                                               ? &
              ම ලි
                     ん・国・
                           ٩Ì
\wedge
#user nobody;
worker_processes 1;
                                                                                 ≣
error_log logs\\error.log;
#error log logs/error.log notice;
#error_log logs/error.log info;
           logs\\nginx.pid;
pid
events {
   worker connections 1024;
http {
    include
                  mime.types;
    default type application/octet-stream;
                       '$remote_addr - $remote_user [$time_local] "$request" '
    #log_format main
                       '$status $body bytes_sent "$http_referer"
                       "$http_user_agent" "$http_x_forwarded_for"';
    Ħ
12 lines yanked into "+
                                                              1,0-1
                                                                             Тор
```

## **SSL** Certificates

#### Certificates and Encodings

At its core an X.509 certificate is a digital document that has been encoded and/or digitally signed according to RFC 5280.

In fact, the term X.509 certificate usually refers to the IETF's PKIX Certificate and CRL Profile of the X.509 v3 certificate standard, as specified in RFC 5280, commonly referred to as PKIX for Public Key Infrastructure (X.509).

#### X509 File Extensions

The first thing we have to understand is what each type of file extension is. There is a lot of confusion about what DER, PEM, CRT, and CER are and many have incorrectly said that they are all interchangeable. While in certain cases some can be interchanged the best practice is to identify how your certificate is encoded and then label it correctly. Correctly labeled certificates will be much easier to manipulat

Encodings (also used as extensions)

- **DER** = The DER extension is used for binary DER encoded certificates. These files may also bear the CER or the CRT extension. Proper English usage would be "I have a DER encoded certificate" not "I have a DER certificate".
- **PEM** = The PEM extension is used for different types of X.509v3 files which contain ASCII (Base64) armored data prefixed with a "---- BEGIN ..." line.

#### Common Extensions

- **CRT** = The CRT extension is used for certificates. The certificates may be encoded as binary DER or as ASCII PEM. The CER and CRT extensions are nearly synonymous. Most common among \*nix systems
- **CER** = alternate form of .crt (Microsoft Convention) You can use MS to convert .crt to .cer (.both DER encoded .cer, or base64[PEM] encoded .cer) The .cer file extension is also recognized by IE as a command to run a MS cryptoAPI command (specifically rundll32.exe cryptext.dll,CryptExtOpenCER) which displays a dialogue for importing and/or viewing certificate contents.
- **KEY** = The KEY extension is used both for public and private PKCS#8 keys. The keys may be encoded as binary DER or as ASCII PEM.

The only time CRT and CER can safely be interchanged is when the encoding type can be identical. (ie PEM encoded CRT = PEM encoded CER)

#### **Configuring Nginx Certs**

At /etc/nginx/nginx.conf, and inside the server { .. } block, use the ssl certificate and ssl certificate key like this example:

```
ssl_certificate /usr/local/lm/tclweb/bin/lyris.net/lyris.net.pem;
ssl_certificate_key
```

/usr/local/lm/tclweb/bin/lyris.net/lyris.net.key;

## SSL Ciphers

At /etc/nginx/nginx.conf, and inside the server { .. } block, use the ssl\_prefer\_server\_ciphers and ssl\_ciphers like this example:

```
# enables server-side protection from BEAST attacks
# http://blog.ivanristic.com/2013/09/is-beast-still-a-threat.html
ssl_prefer_server_ciphers on;
#ssl_protocols TLSv1 TLSv1.1 TLSv1.2 TLSv1.3;
ssl_protocols TLSv1.2 TLSv1.3;
# ciphers chosen for forward secrecy and compatibility
```

#

http://blog.ivanristic.com/2013/08/configuring-apache-nginx-and-opens
sl-for-forward-secrecy.html

#### ssl\_ciphers

'ECDHE-ECDSA-CHACHA20-POLY1305:ECDHE-RSA-CHACHA20-POLY1305:ECDHE-ECDS A-AES128-GCM-SHA256:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES256-GC M-SHA384:ECDHE-RSA-AES256-GCM-SHA384:DHE-RSA-AES128-GCM-SHA256:DHE-RS A-AES256-GCM-SHA384:ECDHE-ECDSA-AES128-SHA256:ECDHE-RSA-AES128-SHA256 :ECDHE-ECDSA-AES128-SHA:ECDHE-RSA-AES256-SHA384:ECDHE-RSA-AES128-SHA: ECDHE-ECDSA-AES256-SHA384:ECDHE-ECDSA-AES256-SHA:ECDHE-RSA-AES128-SHA :DHE-RSA-AES128-SHA256:DHE-RSA-AES128-SHA:DHE-RSA-AES256-SHA :DHE-RSA-AES128-SHA256:DHE-RSA-AES128-SHA:DHE-RSA-AES256-SHA256:DHE-R SA-AES256-SHA:ECDHE-ECDSA-DES-CBC3-SHA:ECDHE-RSA-DES-CBC3-SHA:EDH-RSA -DES-CBC3-SHA:AES128-GCM-SHA256:AES256-GCM-SHA384:AES128-SHA256:AES256 6-SHA256:AES128-SHA:AES256-SHA:DES-CBC3-SHA:!DSS';

For more information about ciphers please check this article.

### SSL TLVv1.2 only

At /etc/nginx/nginx.conf use the ssl\_protocols to enable just TLSv1.2.

#### Example:

```
ssl_protocols TLSv1.2;
```

#### Running as a Service

Linux

Type the following chkconfig command: # chkconfig nginx on

#### Windows

We downloaded from <a href="https://github.com/kohsuke/winsw/releases">https://github.com/kohsuke/winsw/releases</a> the last stable version (2.10.1 - WindSW.NETCore31.x64.exe) and copied it to the Nginx folder (c:\nginx) as nginxscv.exe.

After download, copy, and rename the nginxsvc.exe, you will need to create a service file inside the Nginx (c:\nginx) folder, please be sure to create a file with the name nginxsvc.xml with the following contents:

```
<service>
<id>nginx</id>
```

```
<name>nginx</name>
<description>nginx</description>
<executable>c:\nginx\nginx.exe</executable>
<logpath>c:\nginx\logs</logpath>
<logmode>roll</logmode>
<depend></depend>
<startarguments></startarguments>
<stoparguments>-s stop</stoparguments>
<workingdirectory>c:\nginx</workingdirectory>
</service>
```

You are now ready to install the Windows service, you can proceed to run the following command:

C:\nginx\nginxsvc.exe install

You can now proceed to manage the service from your service manager. The easiest and fastest way to access it is to type the following in your command prompt:

services.msc

You should be all done at this point.

Q,	Services					_ 🗆 X
File Action View Help						
Services (Local) Services (Local)						
nginx	Name	Description	Status	Startup Type	Log On As	^
-	🌼 KtmRm for Distributed Tran	Coordinates		Manual (Trig	Network S	
Start the service	🎑 Link-Layer Topology Discov	Creates a N		Manual	Local Service	
	🔍 Local Session Manager	Core Windo	Running	Automatic	Local Syste	
Description:	🎑 Machine Debug Manager	Supports Io	Running	Automatic	Local Syste	
nginx	🔍 Microsoft iSCSI Initiator Ser	Manages In		Manual	Local Syste	
	🌼 Microsoft Software Shadow	Manages so		Manual	Local Syste	
	🛸 Microsoft Storage Spaces S	Host service		Manual	Network S	
	🎑 Mozilla Maintenance Service	The Mozilla		Manual	Local Syste	
	🎑 Multimedia Class Scheduler	Enables rela		Manual	Local Syste	_
	Net.Tcp Port Sharing Service	Provides abi		Disabled	Local Service	=
	🔍 Netlogon	Maintains a		Manual	Local Syste	
	Network Access Protection	The Networ		Manual	Network S	
	Network Connections	Manages o		Manual	Local Syste	
	🔍 Network Connectivity Assis	Provides Dir		Manual (Trig	Local Syste	
	Network List Service	Identifies th	Running	Manual	Local Service	
	Network Location Awareness	Collects an	Running	Automatic	Network S	
	Retwork Store Interface Ser	This service	Running	Automatic	Local Service	
	🔍 nginx	nginx		Automatic	Local Syste	
	🔍 Optimize drives	Helps the c		Manual	Local Syste	
	Reformance Counter DLL	Enables rem		Manual	Local Service	
	Reformance Logs & Alerts	Performanc		Manual	Local Service	
	Riug and Play	Enables a c	Running	Manual	Local Syste	~
Extended Standard						

You have Nginx as a service and you can set it up to start automatically when it is booted with your operating system!

		ling the service	e with id 'n	ainx'				
<b>9</b>		Services	5					x
File Action View	Help							
♦ ♦	) 🗟 🚺 🖬 🕨 🖬 🕪							
Services (Local)	Services (Local)	,						
	nginx	Name	Description	Status	Startup Type	Log On As		^
	-	🔍 Network Connectivity Assis	Provides Dir		Manual (Trig	Local Syste		
	Stop the service	🔍 Network List Service	Identifies th	Running	Manual	Local Service		
	Restart the service	Network Location Awareness	Collects an	Running	Automatic	Network S		
		🔍 Network Store Interface Ser	This service	Running	Automatic	Local Service		
	Description:	😘 nginx	nginx	Running	Automatic	Local Syste		
	nginx	🔍 Optimize drives	Helps the c		Manual	Local Syste		
		🔍 Performance Counter DLL	Enables rem		Manual	Local Service		
		🔍 Performance Logs & Alerts	Performanc		Manual	Local Service		
		Riug and Play	Enables a c	Running	Manual	Local Syste		~
	Extended Standard /							
1								
	Louis I warm		_				1	

After you click on the "Start" button you will see the status "Running"

and then you can open the browser at <u>http://localhost</u> to check if it is opening the default Nginx page.



If you need to disable the Windows default port 80 (HTTP.sys), please run as "Administrator" at the command line:

```
net stop http /y
sc config http start= disabled
```

For more information please check this article: http://www.devside.net/wamp-server/opening-up-port-80-for-apache-to-use-on-windows

### HTTP to HTTPs redirection

At /etc/nginx/nginx.conf, and inside the location /path { .. } block, use the return <http answer code> <url> like this example:

```
# redirect all http traffic to https
server {
    listen 80 default_server;
    listen [::]:80 default_server;
    server_name my.servername.com;
    return 301 https://$host$request_uri;
}
```

### **Reverse Proxy**

```
At /etc/nginx/nginx.conf, and inside the location /path { ... } block, use the
proxy_pass, proxy_set_header, proxy_cache_valid,
proxy_cache_use_stale_error, and proxy_redirect like this example:
    # ... the rest of your configuration
    location / {
        proxy_set_header Host $host;
        proxy_cache_valid 200 7d;
        proxy_cache_use_stale error timeout invalid_header updating
    http_500 http_502 http_503 http_504;
        proxy_set_header X-Forwarded-Proto https;
        proxy_set_header Host $http_host;
        proxy_set_header Host $http_host;
        proxy_set_header Host $http_host;
        proxy_set_header Host $http_host;
        proxy_pass http://url.to.your.service[:<port>]/;
```

}

## Listmanager

#### Web UI

**Disable SSL** 

- 1. Edit your \${LM HOME}/tclweb/bin/tclhttpd.rc file
- 2. Find this section

```
# SSL Configuration
# SSL REQUEST - should the server ask for certificates from clients?
Config SSL REQUEST
                       1
# SSL REQUIRE - should the server require certificates?
Config SSL REQUIRE
                       1
  3. Switch all to 0 (zero)
# SSL Configuration
# SSL_REQUEST - should the server ask for certificates from clients?
Config SSL REQUEST
                      0
# SSL REQUIRE - should the server require certificates?
Config SSL REQUIRE
                      0
  4. Find this section
\# USE SSL2 - Allow the use of SSL version 2
# (You cannot get this with a "no patents" build of OpenSSL)
Config USE SSL2
                      1
# USE SSL3 - Allow the use of SSL version 3
```

## Config USE SSL3 1 # USE TLS1 - Allow the use of TLS version 1 Config USE TLS1 1 5. Switch them to 0 (zero) # USE SSL2 - Allow the use of SSL version 2 # (You cannot get this with a "no patents" build of OpenSSL) Config USE SSL2 0 # USE SSL3 - Allow the use of SSL version 3 Config USE SSL3 0 # USE TLS1 - Allow the use of TLS version 1 Config USE TLS1 0 6. Save the file 7. Restart LM HTTP and HTTPs ports 8. Edit your \${LM HOME}/tclweb/bin/tclhttpd.rc file 9. Find this section # port - the listening port for the server for HTTP requests. # The standard web port is 80. Config port 80 # https port - the listening port for the server for HTTPS requests. # The standard SSL port is 443. Config https port 443 10. Switch all to 8080 and 8443 # port - the listening port for the server for HTTP requests.

# The standard web port is 80.

#### Config port 8080

# https\_port - the listening port for the server for HTTPS requests. # The standard SSL port is 443.

Config https\_port 8443

### SOAP API

Unfortunately we can't assign a different port for SOAP API service so it always will run on port 82 (HTTP or HTTPS). It force us to use an path assignment for the SOAP service (/\_soap/) like

← → C ☆ 🏽 Im-demo.lyris.net/soap/?wsdl
👖 Apps 🦉 E-mail 📧 TeamCity 🛹 Jira 💥 Wiki 🤍 Confluence 🕠 Trilogy ★ Bookmarks 🕧 Best JSON to YA 📀 Test Analytics 🌀 E-r
This XML file does not appear to have any style information associated with it. The document tree is shown below.
<pre>v<definitions enc="http://schemas.xmlsoap.org/soap/encoding/" name="lmapi" targetnamespace="http://schemas.xmlsoap.org/wsdl/" x<schema="" xmlns:dime="http://schemas.xmlsoap.org/wsdl/" xmlns:dmb="http://schemas.xmlsoap.org/wsdl/soap/" xmlns:nmme="http://schemas.xmlsoap.org/wsdl/mm/" xmlns:nsi="http://schemas.xmlsoap.org/wsdl/soap/" xmlns:soap-="" xmlns:soap-enc="http://schemas.xmlsoap.org/wsdl/soap/" xmlns:soap-env="http://schemas.xmlsoap.org/soap/encoding/" xmlns:tns="http://www.lyris.com/lmapi" xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/" xmlns:xsi="http://www.wlyris.com/lmapi"></definitions></pre>
<pre><enumeration value="p"></enumeration> <i const="0" enum=""> <enumeration value="p"></enumeration> <!-- enum const = 1--> <enumeration value="p"></enumeration></i></pre>
<pre><!-- enum const = 2-->  </pre>
<pre>% simpletype name= listype.num &gt;</pre>
<pre><!-- enum const = 1--> <enumeration value="discussion-moderated"></enumeration> <!-- enum const = 2--> <enumeration value="discussion-unmoderated"></enumeration></pre>
enum const = 3   w <simpletype name="MriVisibilityEnum"></simpletype>
<pre>v<restriction base="xsd:string">   <enumeration value="V"></enumeration>   <!-- enum const = 0-->   <enumeration value="I"></enumeration></restriction></pre>
enum const = 1 <enumeration value="I"></enumeration> enum const = 2
<pre></pre> /simpleType> <pre>v<simpletype name="MemberStatusEnum"> v<restriction base="xsd:string"> </restriction></simpletype></pre> <pre>v<restriction value="normal"></restriction></pre>
enum const = 0 <enumeration value="member"></enumeration> enum const = 1 <enumeration value="confirm"></enumeration>
enum const = 2 <enumeration value="confirm-failed"></enumeration> enum const = 3 <enumeration value="private"></enumeration>
<pre><enumeration value="expired"></enumeration> <enumeration value="expired"></enumeration></pre>

To enable it you just have to add a new entry above the "location / {" block to map it to the LM SOAP API interface.

```
location /_soap {
    proxy_set_header Host $host;
    proxy_cache_valid 200 7d;
    proxy_cache_use_stale error timeout invalid_header updating
http_500 http_502 http_503 http_504;
    proxy_set_header X-Forwarded-Proto https;
    proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
    proxy_redirect off;
    proxy_pass http://url.to.your.service:82/;
}
```

Then it will be available at <a href="https://url.to.your.service/\_soap/?wsdl">https://url.to.your.service/\_soap/?wsdl</a>.

Don't forget to disable your firewall access from the Internet to the LM TCP 82 port (SOAP) and change your scripts to use the new URL based on SSL reverse proxy.

## Tests

## Application

1. Open the Chrome/Firefox



2. Open the Inspector



3. Open the Network Tab



4. Into the URL bar, type the LM URL to be tested using the http:// at the beginning



5. Check into the Network Tab if you got a 301 Redirect to the https:// url

	HIM	L CSS	33	AHR	1 onto		media	w5 0u			
Sta	Me	Domain		File				Cause	Туре	Transferred	Si
	GET	🔒 lm-d	emo	1				document	t	0 B	0 B
	GET	🔒 Im-d	emo	1				document		0 B	0 B
302	GET	A Im-d	emo.ly					document	t html	7,50 KB	
200	GET	⊜ Im-d	emo	/utilitie	es/login/	login/?Do	:Post=	document	t html	7,37 KB	7,1
200	GET	🔒 lm-d	emo	styles	.css			styleshee	t css	21,36 KB	21,
200	GET	🔒 lm-d	emo	rebrar	ndable.c:	ss		styleshee	t css	10,74 KB	10,
200	GET	🔒 Im-d	emo	theme	.CSS			styleshee	t css	17,44 KB	17,
200	GET	🔒 Im-d	emo	logo-l	yris-Im-1	fractal.gif		img	gif	8,55 KB	8,1
Ō	11 red	quests	98,4	3 KB /	101,57	KB transfe	rred	Finish: 2,10	0 min	DOMContent	Loaded
Reque Reque Reque	Heade est URL est meti te addr	ers C : https hod: GET ess: 74.	ookie ://lm T 116.2	s P -demo. 236.10	arams .lyris. 14:443	Respor	nse T	Timings	Stack T	race Sec	urity
Reque Reque Remo Status Versio	Heade est URL est meti te addr s code: on: HTT	ers C : https hod: GET ess: 74. 302 Fo P/1.1	:ookie ://lm [ 116.2 pund	s P -demo. 236.10 ⑦	arams .lyris. 14:443	Respon net/	nse T	Timings	Stack T	race Sector	end
Reque Reque Remo Status Versio	Heade est URL est meti te addr s code: on: HTT ilter hea	ers C : https: hod: GET ess: 74. 302 Fo P/1.1 aders beaders	://lm [ 116.2 pund	s P -demo 236.10 ⑦	arams .lyris. 14:443	Responet/	nse 1	Timings	Stack T	race Sec Edit and Res	end
Reque Reque Remo Status Versic Versic	Heade est URL est meti te addr s code: on: HTT ilter hea sponse	ers C : https hod: GET ess: 74. 302 Fo P/1.1 aders headers	://lm r 116.2 ound (398	s P demo. 236.10 ⑦ B)	arams .lyris. 14:443	Respo net/	nse	Timings	Stack T	race Sect Edit and Res aw headers (	end
Reque Reque Remo Status Versio Versio Versio Re @	Heade est URL est meti- te addr s code: on: HTT ilter hea sponse Conner Conter	ers C : https: hod: GET ess: 74. 302 Fo P/1.1 aders headers ction: ke ht-Length	:ookie ://lm 116.2 ound (398 ep-aliv a: 248	s P demo 236.10 ⑦ B)	arams .lyris. 14:443	Respon	nse	Timings	Stack T	edit and Res	end
Reque Reque Remo Status Versic Versic Re ? Re ? ?	Heade est URL est meti te addr s code: on: HTT ilter hea sponse Connee Connee Conter	ers C : https: hod: GET ess: 74. 302 Fo P/1.1 aders headers ction: ke nt-Length ht-Type: 1	(398 ep-aliv tr 248	s P demo 236.10 ② B) ve	arams .lyris. 14:443	Respon	nse	Timings	Stack T	race Sector	end
Reque Reque Remo Status Versic Versic Re ? Re ? ? ? ? ?	Heade est URL est meti- te addri- s code: on: HTT ilter hea- sponse Conner Conter Date: \$	ers C : https: hod: GET ess: 74. 302 Fo P/1.1 aders headers ction: ke ht-Length ht-Type: : Sat, 22 Fo	(398 ep-alim text/ht eb 202	s P demo 236.10 ⑦ B) ve tml 20 21:3	arams .lyris. 14:443 7:38 GM	Respon	nse T	Timings	Stack T	race Sec Edit and Res aw headers (	end
Reque Reque Remo Status Versic Versic Re ? Re ? ? ? ? ? ? ? ? ? ? ?	Heade est URL est meti- te addr s code: on: HTT ilter hea sponse Conter Conter Date: \$ Locatio	ers C : https: hod: GET ess: 74. 302 Fo P/1.1 aders headers ction: ke ht-Length ht-Type: t Sat, 22 Fo on: /utiliti	cookie ://lm 116.2 bund (398 ep-alim : 248 text/ht eb 202 ies/log	s P demo. 236.10 ? B) ve tml 20.21:3 jin/login	arams .lyris. 14:443 7:38 GM n/?DocP	Respon net/ IT osbe042	nse T	Timings 535f936351	Stack T R afdb4e3	Edit and Res aw headers (	end
Reque Reque Remo Status Versic ? Re ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ?	Heade est URL est metit te addr s code: on: HTT ilter hea sponse Conter Date: \$ Locations Server:	ers C : https: hod: GET ess: 74. 302 Fo P/1.1 aders headers ction: ke nt-Length nt-Type: : Sat, 22 Fi on: /utiliti : nginx	cookie ;//lm r 116.2 ound (398 ep-alin ep-alin r: 248 text/ht eb 202 ies/log	s P demo. 236.10 ② B) ve tml 20.21:3 jin/login	arams .lyris. 14:443 7:38 GM n/?DocP	Respon net/ IT osbe042	nse T	Timings 535f936351	Stack T R afdb4e3!	Edit and Res aw headers (	end

6. Inform your login/password and click on the Login button

User Name:	luis.reis@aurea.com
Password:	
	If you have forgotten your password, <u>click</u> here.

7. Check if the LM loaded without any alert at the URL bar

← → ♂ ଢ		//Im-demo.lyris.net/utilitie	s/login/list_change/		
lyris/LM <sup>*</sup> v.12			Welcome I	uis.reis@aurea.com   Logout	List: 00148984-listcopy Language: English
Expand      Collapse	🔧 Change List				
🏫 Home	Utilities : Login Status : Change List				O 🗷 O
Calendar					
A Members	ALL A B C D E	FGHIJK	L M N O P	QRSTU	V W X Y Z # \$
	List Name	Site Name	Contact	Created	Keywords
Content	00148984-listcopy	main	Admin	2014-10-09 01:05:00	Select
📩 Segments	01513034	amadorsite	Admin	2019-04-05 08:14:25	Select
E Mailings	01581019_child1	amadorsite	Admin	2019-11-01 08:07:50	Select
Mailings	01581019_child2	amadorsite	Admin	2019-11-01 08:09:23	Select
Reports	01581019_child3	amadorsite	Admin	2019-11-01 08:48:45	Select
× Utilities	01581019_parent	amadorsite	Admin	2019-11-01 07:59:55	Select
I ist Settings	01595329	main	Admin	2019-12-20 07:50:11	Select
• Web Forms	101april	blake	Admin	2015-04-21 09:37:00	Select
Automated      ▶	5303	main	Admin	2017-07-05 01:35:53	Select
Messages	abi_discussion	main	Admin	2019-08-26 03:10:31	Select
Administration	abi_import	main	Admin	2019-10-28 02:30:24	Select
Login Status	abimod1	main	Admin	2019-11-26 09:38:34	Select
• Other     ▶	abizar1	main	Admin	2018-04-26 09:52:08	Select
St. Shortoute	abizar2	main	Admin	2020-02-21 02:45:22	Select
✓ Shortcuts	acoustic_covers	jorgejr	Admin	2013-06-25 09:50:00	Select
New List     MailCheanne	adminstestlist	main	Admin	2018-05-16 10:39:37	Select
Septer	albertos	main	Admin	2017-04-14 07:05:50	Select
Dashboard	aldo2	main	Admin	2014-10-07 16:56:00	Select
Deliverability     Dashboard	Show fewer   Show more				Previous
Discussion Forum     List Settings Map     Site Map     Help	Lyris, Inc.   Email Marketing Software				

## Rating

The Secure Sockets Layer (SSL) protocol is a standard for encrypted network communication. We feel that there is surprisingly little attention paid to how SSL is configured, given its widespread usage. SSL is relatively easy to use, but it does have its traps. This guide aims to establish a straightforward assessment methodology, allowing administrators to assess SSL server configuration confidently without the need to become SSL experts.

Complete Guide: <u>SSL Server Rating Guide</u>

### Test

1. Open the SSL Labs website: <u>https://www.ssllabs.com</u>



2. Click at "Test your server"



3. At "Hostname", type your URL



4. Wait for the results

•••	📅 PC/X   🛷 PC/X   🛷 [DE X   ኞ [DE X   🚳 SSL X   🌇 Uni X   🕻 Hov X   🕻 RHEX   🖉 Ngl X   🔞 ngl X   🤇 Reli X   🚳 SSL X   Novagu X   -	F
$\leftrightarrow \rightarrow$	C 🏠 📫 ssilabs.com/ssilest/analyze.html?d=lm-demo.lyris.net&latest 🏠 🖌 🖸 🕲 🖤 📔	💭 E
Apps	★ Bookmarks 🚯 Test Analytics 🔞 E-mail 🚯 AWS Console 🏮 Amazon Web Servi 🧮 Outrage RCA Templ 🧮 Architecture Docu 📑 End to End Scenari »   🛅 Outro	favoritos
	Qualys. SSL Labs Home Projects Qualys Free Trial Contact	
	You are here: Home > Projects > SSL Server Test > Im-demo.lyris.net	
	SSL Report: Im-demo.lyris.net (74.116.236.104)	
	Please wait	
	Retrieving certificate	
	SSL Report v2.1.0	
	Copyright © 2009-2020 Qualys, Inc. All Rights Reserved. Terms and Conditions	
	Try Qualys for free! Experience the award-winning Qualys Cloud Platform and the entire collection of Qualys Cloud Apps, including certificate security solutions.	

5. Check your rate

#### SSL Report: Im-demo.lyris.net (74.116.236.104)

Assessed on: Sun, 30 Aug 2020 00:15:20 UTC | Hide | Clear cache

Scan Another »

Summary							
Overall Rating		Ĩ	(C	Ť	(		
	Certificate						
	Protocol Support						
Ат	Key Exchange						
	Cipher Strength						
	0	20	40	60	80	100	
Visit our <u>documentation page</u> for more	information, configuration guides, and	i books. Kno	own issues	are docur	nented <u>her</u>	<u>e</u> .	
HTTP Strict Transport Sec	urity (HSTS) with long duration deploy	ed on this s	server. <u>MO</u>	<u>RE INFO »</u>			

Invalidating the Test Cache

Just click at the "Clear Cache" link on the top of the page.



## **Example Configuration**

Save these configurations into /etc/nginx/conf.d/default.conf, or at C:\nginx\conf\nginx.conf for Windows hosts - inside the http section, and check if it conflicts with any other existent configuration.

- 1. Please also replace all variables placeholders, like <code>%%NGINX\_HTTP\_PORT%%</code>, to your own values.
- 2. Please also fill the %%NGINX\_SSL\_CERT%% and %%NGINX\_SSL\_KEYS%% pointing to your .CRT/.PEM and .KEY SSL certificates using the FULL PATH notation
  - a. In Linux use the normal notation like /etc/ssl/certificates.crt or /etc/ssl/certificates.key
  - b. In Windows use the normal path location, just replacing slashes (/) by double backslashes (\\) like C: \\Windows instead of C: /Windows.
    - i. It must be done for all custom paths

## Single file

server {

```
listen %%NGINX HTTP PORT%% default server;
    listen [::]:%%NGINX HTTP PORT%% default server;
    server name localhost;
    return 301 https://$host$request uri;
}
server {
    listen %%NGINX HTTPS PORT%% ssl http2;
    listen [::]:%%NGINX_HTTPS_PORT%% ssl http2;
    server name localhost;
    ssl certificate %%NGINX SSL CERT%%;
    ssl certificate key %%NGINX SSL KEYS%%;
    # enable session resumption to improve https performance
    # http://vincent.bernat.im/en/blog/2011-ssl-session-reuse-rfc5077.html
    ssl session cache shared:SSL:50m;
    ssl session timeout 1d;
    ssl session tickets off;
    # Diffie-Hellman parameter for DHE ciphersuites, recommended 4096 bits
    ssl dhparam /etc/nginx/conf.d/dhparam.pem;
    # enables server-side protection from BEAST attacks
    # http://blog.ivanristic.com/2013/09/is-beast-still-a-threat.html
    ssl prefer server ciphers on;
    # disable SSLv3(enabled by default since nginx 0.8.19) since it's less secure then
TLS http://en.wikipedia.org/wiki/Secure Sockets Layer#SSL 3.0
    #ssl protocols TLSv1 TLSv1.1 TLSv1.2 TLSv1.3;
    ssl protocols TLSv1.2 TLSv1.3;
    # ciphers chosen for forward secrecy and compatibility
http://blog.ivanristic.com/2013/08/configuring-apache-nginx-and-openssl-for-forward-se
crecy.html
    ssl ciphers
'ECDHE-ECDSA-CHACHA20-POLY1305:ECDHE-RSA-CHACHA20-POLY1305:ECDHE-ECDSA-AES128-GCM-SHA2
56:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-GCM-SHA3
84:DHE-RSA-AES128-GCM-SHA256:DHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES128-SHA256:ECDHE
-RSA-AES128-SHA256:ECDHE-ECDSA-AES128-SHA:ECDHE-RSA-AES256-SHA384:ECDHE-RSA-AES128-SHA
:ECDHE-ECDSA-AES256-SHA384:ECDHE-ECDSA-AES256-SHA:ECDHE-RSA-AES256-SHA:DHE-RSA-AES128-
SHA256:DHE-RSA-AES128-SHA:DHE-RSA-AES256-SHA256:DHE-RSA-AES256-SHA:ECDHE-ECDSA-DES-CBC
3-SHA: ECDHE-RSA-DES-CBC3-SHA: EDH-RSA-DES-CBC3-SHA: AES128-GCM-SHA256: AES256-GCM-SHA384:
AES128-SHA256:AES256-SHA256:AES128-SHA:AES256-SHA:DES-CBC3-SHA:!DSS';
```

# enable ocsp stapling (mechanism by which a site can convey certificate revocation information to visitors in a privacy-preserving, scalable manner)

```
# http://blog.mozilla.org/security/2013/07/29/ocsp-stapling-in-firefox/
    resolver 8.8.8.8 8.8.4.4;
    ssl stapling on;
    ssl stapling verify on;
    ssl trusted certificate %%NGINX SSL CERT%%;
    # config to enable HSTS(HTTP Strict Transport Security)
https://developer.mozilla.org/en-US/docs/Security/HTTP Strict Transport Security
    # to avoid ssl stripping https://en.wikipedia.org/wiki/SSL stripping#SSL stripping
    # also https://hstspreload.org/
    # comment this out if your backend service doesn't add this header
    # add header Strict-Transport-Security "max-age=31536000; includeSubdomains;
preload";
    # ... the rest of your configuration
    location / {
       proxy_set_header Host $host;
       proxy_cache valid 200 7d;
        proxy_cache_use_stale error timeout invalid_header updating http 500 http 502
http 503 http 504;
       proxy set header X-Forwarded-Proto https;
        proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
        proxy set header Host $http host;
       proxy redirect off;
       proxy pass http://%%LOCAL IP%%:%%HTTP PORT%%;
    }
    location /soap {
       proxy set header Host $host;
       proxy cache valid 200 7d;
       proxy_cache_use_stale error timeout invalid_header updating http_500 http_502
http 503 http 504;
       proxy set header X-Forwarded-Proto https;
        proxy set header X-Forwarded-For $proxy add x forwarded for;
       proxy redirect off;
       proxy_pass https://%%LOCAL_IP%%:%%SOAP_PORT%%/;
    }
}
```