OCSPStapling

OCSP Stapling

OCSP Stapling is one of the many new features introduced with httpd 2.4. It allows client software using SSL to communicate with your server to efficiently check that your server certificate has not been revoked. The primary how-to for OCSP Stapling in httpd is at OCSP Stapling How-To. Read that first.

This guide includes:

- summary of fixes to OCSP Stapling in different releases of httpd
- distribution-specific information about enabling OCSP Stapling

Fixes related to OCSP Stapling in different 2.4.x levels

Note: Some distributors of httpd, including Linux vendors, use a particular httpd 2.4.x version for the life of the related product, and choose to selectively apply fixes to that codebase without fully upgrading httpd to a new version. Any stapling-related fixes which vendors have backported to an older 2.4.x version are not reflected in the following table.

First open source release with fix	Considerations	Description
2.4.13	This helps performance in a multiple-certificate configuration (e.g., multiple SSL virtual host) when there are many certificates or slow responders.	Handshakes are blocked/stalled unnecessarily when the OCSP response for a different certificate is being refreshed from the OCSP responder.
2.4.11	If you don't have the crash, you don't care about this bug.	PR 54357 – crash at startup or restart with stapling enabled in some configurations
2.4.10	The fix only affects certificates with no responder (rare).	Better handling for certificates with no responder

Distribution-specific hints for enabling OCSP Stapling

OCSP Stapling is usually enabled using only global (non vhost-specific) directives. In some cases, vhost-specific directives may be required. For example, you may have a default SSL-enabled vhost which uses a self-signed certificate which is intended to handle only those requests for a server name not supported in your configuration, which will result in stapling-related log messages at startup since stapling can't be performed for that certificate. You could quiet those log messages by adding `SSLUseStapling Off` inside the related vhost.

A number of third-party distributions of httpd have their own conventions for where global and vhost-specific SSL configuration directives are placed. A number of these distributions are covered below. (In the event that you bypass the distribution's configuration layout, the material below will not be useful.)

Open source distribution of httpd with the default layout

The default configuration uses `conf/extra/httpd-ssl.conf` for the global SSL configuration as well as the default SSL-enabled vhost. Place these directives before the `## SSL Virtual Host Context` comment:

```
SSLUseStapling On
SSLStaplingCache shmcb:logs/ssl_stapling(32768)
```

Beginning with httpd 2.4.11, the default configuration will include these directives, commented out. Simply uncomment `SSLUseStapling` and `SSLStaplingCache`. If you install httpd 2.4.11 or later over an existing httpd 2.4.x installation, the new default SSL configuration will be stored in `conf/original/extra/httpd-ssl.conf`; you can carefully compare your existing configuration with the new default to see what improvements you wish to integrate into your existing configuration.

Apache Lounge distribution of httpd for Windows

Note: Apache Lounge is not affiliated with the Apache Software Foundation.

The default configuration files in this distribution match those of the open source httpd distribution. Be aware that paths for run-time files such as `SSLSessionCache` are hard-coded to `C:/Apache24/logs`, which should have already been changed by the administrator based on where httpd is installed. Use the same directory in your `SSLStaplingCache` directive as in your existing `SSLSessionCache` directive.

FreeBSD 9 and 10 Port Package "apache24"

The normal default `httpd-ssl.conf` file is in the directory `/usr/local/etc/apache24/extra`; that contains global SSL settings as well as settings for the default SSL-enabled virtual host. The default configuration uses the directory `/var/run` for the location of cache and other run-time files, so the two minimal lines required to enable OCSP Stapling with this distribution are

```
SSLUseStapling On
SSLStaplingCache shmcb:/var/run/ssl_stapling(32768)
```

These lines can be placed just before the `## SSL Virtual Host Context` comment.

Non-default virtual host configurations will likely be stored in the directory `/usr/local/etc/apache24/Includes`.

openSUSE 13.2

The global mod_ssl configuration is in the file `/etc/apache2/ssl-global.conf`. The platform configurations use the directory `/var/lib/apache2` for the location of cache and other run-time files, so the two minimal lines required to enable OCSP Stapling for this platform are

```
SSLUseStapling On
SSLStaplingCache shmcb:/var/lib/apache2/ssl_stapling(32768)
```

These directives should be placed just before `</IfModule>` directive at the end of `ssl-global.conf`.

In the event that the OCSP Stapling configuration should differ for some virtual hosts, make any changes for the default virtual host in `/etc/apache2/default-vhost-ssl.conf`, and for other SSL-enabled virtual hosts in `/etc/apache2/vhosts.d/my-vhost-ssl.conf`.

Red Hat Enterprise Linux 7, CentOS 7, and Fedora 20

The global mod_ssl configuration is in the file `/etc/httpd/conf.d/ssl.conf`. The platform configurations use the directory `/run/httpd` for the location of cache and other run-time files, so the two minimal lines required to enable OCSP Stapling for this platform are

```
SSLUseStapling On
SSLStaplingCache shmcb:/run/httpd/ssl_stapling(32768)
```

These directives should be placed just before the following text:

```
##
## SSL Virtual Host Context
##
<VirtualHost _default_:443>
```

Any other OCSP Stapling directives required globally would be placed here as well.

In the event that the OCSP Stapling configuration should differ for some virtual hosts, the file to edit will likely differ based on site policy. The platform `.conf` file referred to above also defines a default SSL-enabled virtual host for port 443, so changes to that virtual host would be made there. Any other SSL-enabled virtual hosts would likely be defined in site-specific files within the `/etc/httpd/conf.d directory`.

Ubuntu 14, Debian test (Jessie)

The global mod_ssl configuration is in the file `/etc/apache2/mods-available/ssl.conf` and is symlinked into `/etc/apache2/mods-enabled` once you run `a2enmod` for mod_ssl. The Ubuntu configurations use the variable `APACHE_RUN_DIR` for the location of cache and other run-time files, so the two minimal lines required to enable OCSP Stapling for Ubuntu are

```
SSLUseStapling On
SSLStaplingCache shmcb:${APACHE_RUN_DIR}/ssl_stapling(32768)
```

These directives should be placed just before `</IfModule>` near the end of the file. Any other OCSP Stapling directives required globally would be placed here as well.

In the event that the OCSP Stapling configuration should differ for some virtual hosts, edit the appropriate file in the `/etc/apache2/sites-enabled` directory, and add the required directives inside the SSL-enabled virtual host. The default SSL-enabled virtual host may be in `/etc/sites-enabled/default-ssl.conf`.