Tequila

Configuring the Apache module

Claude Lecommandeur
EPFL - KIS
claude.lecommandeur@epfl.ch

Table of Contents

Overview

The mod_tequila Apache module is designed to protect static data, files and/or directories (whole trees), or even a whole external WWW server.

It is an Apache module, so you configure it in your *httpd.conf* or in *.htaccess* files. The module doesn't require any attribute from the server, instead it asks the server whether a particular filter is satisfied. A filter is a set of conditions acting over the user attributes.

If the filter is satisfied access is granted to the document, and a session is created for future use. The session is attached to the protected document and all its children if it is a directory.

Global commands

TequilaLogLevel value

The more *value* is the more log you get. Value of 0 means no logs (only errors). Maximum value is 99.

TequilaLog *filename*

The name of the log file. Default is /etc/httpd/logs/tequila.log. The Apache server must have write access to this file.

TequilaServer *server_name*

The name of the local Tequila server. Default is tequila.*local_domain*.

TequilaServerURL *server_url*

The URL of the local Tequila server. Default is

http://tequila.*local_domain*/cgi-bin/tequila/auth

TequilaSessionDir *directory*

The name of the sessions directory. Default is /var/www/Tequila/Sessions/. The Apache server must have write access to this directory.

TequilaSessionMax *value*

Sessions duration in seconds. Default is 12 * 3600 (24 hours).

Location specific commands

TequilaResource *name*

The application is a 'resource' in the Tequila vocabulary. That means that all information about it is stored inside the server and that there is strong cross authentication between application and server. Use of resources is described in the managing-server document (I'm actually not sure I did it).

TequilaCheckServerName

The module will check that the server name is correct and matches the name in the certificate presented by the server.

TequilaCAFile *file*

Where is located the Certification Authority that signed the Tequila server certificate. Only used when **TequilaCheckServerName** is active.

TequilaCertFile *file*

Where is located the certificate of the application. Only used when **TequilaResource** is active.

TequilaKeyFile *file*

Where is located the private key of the application. Only used when **TequilaResource** is active.

TequilaService *name*

The name ot the application. It is displayed in the login screen.

TequilaAllowIf *condition*

The condition must be met to give access to the current location. The syntax of the condition is :

attribute=*value*&attribute=*value*&...

The condition will be met if and only if all the user's attributes match the given values.

You can give as many TequilaAllowIf directives as you want for each location. All these directives will be or'ed, that means that if only one condition need to be met for access to be given.

If the equal ('=') is replaced with '=~', pattern matching is done instead of strict equality. In any case the comparison is done ignoring case.

If no value is given, it is equivalent to '=~.*', that means that the attribute must have a non null value.

TequilaAllowNet *subnet-specification*

Incoming clients from the specified subnet are not subject to filters verification, they are given immediate access to the protected file.

TequilaAllows *condition*

Used to lift restriction imposed by the server. The Tequila server has a default set of filters that are applied by default to all users. The reason behind this is to have a set of users that are not seen by default, guests users for example. This command can be used to lift some of these restriction.

Example in http.conf :

```
LoadModule tequila_module modules/mod_tequila.so
AddModule mod_tequila.c

<IfModule mod_tequila.c>
  TequilaLogLevel       2
  TequilaLog            /etc/httpd/logs/tequila.log
  TequilaServer         tequila.epfl.ch
  TequilaSessionDir     /var/www/Tequila/Sessions
  TequilaSessionMax     3600


  <Location /restricted/>
    TequilaAllowIf firstname=Claude&name=Lecommandeur
    TequilaAllowIf org=EPFL
  </Location>
```

This means that the location /restricted/oscar/ will be protected by **Tequila**. Only users of EPFL and Claude Lecommandeur will have access to it. If access is given, files will be given from /var/www/restricted/oscar/. For example :

http://server.epfl.ch/restricted/oscar/Oscar.html will fetch

/var/www/restricted/oscar/Oscar.html

Beware to use only relative links in all html files in /var/www/restricted/oscardoc/ if

you want to have the access rights to be inherited.

```
  <Location /restricted/www/>
    TequilaRewrite http://www.epfl.ch/
    TequilaAllowIf org=EPFL
    TequilaAllowIf org=FOO
  </Location>

</IfModule>
```

In this example, the access is checked for a whole remote site (http://www.epfl.ch/). Only people from EPFL or FOO will be allowed to access. In this case, it is even more difficult to have only relative links in all the documents on the remote server (this is not the case on the server in this example). Ans of course the target server must not be accessible directly, this will defeat the Tequila protection.

Example of .htaccess file :

```
TequilaAllowNet 128.178

TequilaAllowIf  group=aasl&org=EPFL
TequilaAllowIf  username=possoz&org=EPFL
TequilaAllowIf  group=groupware

TequilaAllows   categorie=epfl-guests
```

TequilaRequest *attribute attribute ...*

Asks Tequila to return the value of these attributes. Note that when there is a constraint on an attribute (with TequilaAllowIf), the value of this attribute is automatically returned.

Example in :

```
  <Location /restricted/>
    TequilaAllowIf firstname=Claude
    TequilaRequest name firstname uniqueid
  </Location>
```

TequilaIdentities *one|any*

What the server should do when the user has several identities (attached to several units with the same username). If 'one', the first that matches the constraints is returned, is 'any', the user has to choose herself between all the matching identities.

TequilaRewrite *new_location*

The current location will be rewritten as *new_location* in case of successful authentication (and the filters are satisfied).

TequilaNoSSL

Suppress SSL use in the protocol with server. Default is to use SSL if configured at compile time.