NAME

hiawatha - advanced and secure webserver

SYNOPSIS

hiawatha [options]

Options: -c <path>: path to where the configrationfiles are located.

-d: don't fork to the background.

-h: show help and exit.

-k: check configuration and exit.

-m: show enabled modules and exit.

-v: show version and compile information and exit.

DESCRIPTION

Hiawatha is a secure webserver for Unix. It has been written with 'being secure' and 'easy to use' as its main goals. Hiawatha has lots of features that no other webserver has. Although most of them started as an experiment, many of them turned out to be quite effective.

Hiawatha has been tested and runs perfectly on Linux, BSD, MacOS X and Cygwin.

CONFIGURATION FILES

Hiawatha has the following configuration files:

cgi-wrapper.conf

See cgi-wrapper(1) for more information.

hiawatha.conf

See chapters SERVER CONFIGURATION, BINDING CONFIGURATION, VIRTUAL HOST CONFIGURATION, DIRECTORY CONFIGURATION, FASTCGI CONFIGURATION, URL TOOLKIT and XSLT for more information.

mimetype.conf

See chapter MIMETYPES for more information.

.hiawatha

See chapter USER SETTINGS PER DIRECTORY for more information.

RECORDS

The binding, directory, FastCGI, virtual host and URL toolkit configuration must be placed inside a record. A record is defined as follows:

```
Record {
        ...
}
```

where the word "Record" must be replaced with "Binding", "Directory", "FastCGIserver", "VirtualHost" or "UrlToolkit".

SERVER CONFIGURATION

The global configuration of the Hiawatha webserver.

set variable = value

With 'set', you can declare a variable. Make sure the name of the variable doesn't conflict with any of the configuration options. The variables are case-sensitive and cannot be redeclared. The variable CONFIG_DIR will be set by Hiawatha to the directory where hiawatha.conf is located.

Example: set local_net = 192.168.1.0/24
AccessList = allow local_net, deny 0.0.0.0/0 (see AccessList for more information about this option)

AnonymizeIP = yes|no
Anonymize IP addresses before writing them to the access and error logfiles.
Default = no Example: AnonymizeIP = yes

BanlistMask = (allow|deny) <ip-address>[/netmask][, (allow|deny) <ip-address>[/netmask], ...]
Prevent IPs from getting banned in case of bad behaviour. By default, all IPs can be banned. IPs that are 'denied' in the banlist will not be banned.
Example: BanlistMask = deny 127.0.0.1, deny 192.168.0.1

BanOnDeniedBody = <ban-time>
Number of seconds to ban an IP in case of a denied request body. See als DenyBody.
Default = 0 Example: BanOnDeniedBody = 120

BanOnFlooding = <number>/<time>:<ban-time>
When a client sends more than <number> requests in <time> seconds, the IP will be banned for <ban-time> seconds.
Default = -/-:0 Example: BanOnFlooding = 10/1:15

BanOnGarbage = <ban-time>
Number of seconds to ban an IP in case of a misformed HTTP request (400 Bad Request). Web-browsers normally don't send misformed HTTP requests. So in case of a 400 errorcode, someone is probably trying something not-so-nice.
Default = 0 Example: BanOnGarbage = 60

BanOnInvalidURL = <ban-time>
Number of seconds to ban an IP in case of an invalid URL.
Default = 0 Example: BanOnInvalidURL = 60

BanOnMaxPerIP = <ban-time>
How many seconds a client will be banned when the maximum number of simultaneous connections has been crossed. See also ConnectionsPerIP.
Default = 2 Example: BanOnMaxPerIP = 5

BanOnMaxReqSize = <ban-time>
Number of seconds to ban an IP in case of a too large HTTP request (413 Request Entity Too Large). See also MaxRequestSize.
Default = 0 Example: BanOnMaxReqSize = 10

BanOnSQLi = <ban-time>
Number of seconds to ban an IP in case of a detected SQL-injection attempt. See also PreventSQLi.
Default = 0 Example: BanOnSQLi = 60

BanOnTimeout = <ban-time>
Number of seconds to ban an IP in case of a timeout before the first request has been send. See also TimeForRequest.
Default = 0 Example: BanOnTimeout = 30

BanOnWrongPassword = <number>:<ban-time>
Number of seconds to ban an IP in case of <number> wrong passwords for HTTP authentication within a minute.
Default = -:0, Example: BanOnWrongPassword = 3:120

BlockExtensions = <extension>[,<extension>, ...]
Prevent the uploading of files with these extensions.
Example: BlockExtensions = pem, key, exe

CAcertificates = <file|directory>
Load CA root certificates which Hiawatha uses for validation when acting as a client, which it does for the reverse proxy and the websockets. If not set, TLS connections that Hiawatha makes are not secure.
Example: CAcertificates = /etc/ssl/certs/ca-certificates.crt

CacheRProxyExtensions = <extension>[, <extension>, ...]
Enable the internal cache for reverse proxy requests for these extensions.
Example: CacheRProxyExtensions = css, gif, html, jpg, js, png, txt

(requires that Hiawatha was not compiled with -DENABLE_CACHE=off or -DENABLE_RPROXY=off)

CacheSize = <size in megabytes>
Size of Hiawatha's internal file cache. Maximum is 1024 (megabytes).
Default = 10 Example: CacheSize = 25

(requires that Hiawatha was not compiled with -DENABLE_CACHE=off)

CacheMaxFilesize = <size in kilobytes>
Maximum size of a file Hiawatha will store in its internal cache.
Default = 256 Example: CacheMaxFilesize = 128

(requires that Hiawatha was not compiled with -DENABLE_CACHE=off)

CGIextension = <extension>[, <extension>, ...]
Default extension of a CGI program.
Example: CGIextension = cgi

CGIhandler = <CGI handler>:<extension>[, <extension>, ...]
Specify the handler for a CGI extension. A handler is an executable which will run the CGI script.
Example: CGIhandler = /usr/bin/php5-cgi:php,php5

CGIwrapper = <CGI wrapper>
Specify the wrapper for CGI processes. A secure CGI wrapper is included in the Hiawatha package (see cgi-wrapper(1) for more information).
Default = /cygdrive/c/Program Files/Hiawatha/program/cgi-wrapper Example: CGIwrapper = /bin/cgi-wrapper

ChallengeClient = <threshold>, (httpheader|javascript), <ban-time>[, <secret>]
Challenge the client to verify that it's a real web browser and not an HTTP bot. When the total amount of connections reaches <threshold>, Hiawatha sends a response to the first request in a connection which will make the client resend the request, but now with a cookie. The cookie can be set via an HTTP Set-Cookie header or a Javascript. Further requests are only accepted when the client sends this cookie. Otherwise, the client is banned for <ban-time> seconds. This feature can be used to reduce the effects of a DDoS attack. The <secret> can be a random string of up to 20 characters (the rest is ignored) and is used to generate the cookie. When not set, Hiawatha will generate a random secret.
Example: ChallengeClient = 200, httpheader, 60

ConnectionsPerIP = <number>
Maximum number of simultaneous connections per IP address. See also RequestLimitMask.
Default = 15 Example: ConnectionsPerIP = 50

ConnectionsTotal = <number>
Maximum number of simultaneous connections.
Default = 150 Example: ConnectionsTotal = 1000

DHsize = 2048|4096|8192
Set the size of the Diffie-Hellman keys.
Default = 2048 Example: DHsize = 4096

ExploitLogfile = <filename with full path>
Logfile for all exploit attempts: CSRF, denied bodies, SQL injection and XSS
Default = /cygdrive/c/Program Files/Hiawatha/logfiles/exploit.log Example: ExploitLogfile = /var/log/exploit_attempts.log

GarbageLogfile = <filename with full path>
Logfile for all misformed HTTP requests.
Example: GarbageLogfile = /cygdrive/c/Program Files/Hiawatha/logfiles/garbage.log

GZipExtensions = <extension>[, <extension>, ...]
Add extensions to the list of extensions of the files Hiawatha will compress before uploading. Files with the text/* or image/svg+xml mimetype will also be compressed.
Default = cer,crt,doc,pem,ppt,ttf,xls,xml,xsl,xslt Example: GZipExtensions = json

HideProxy = <ip-address>[/netmask][, <ip-address>[/netmask], ...]
A request sent from the supplied IP address will be searched for a X-Forwarded-For header. When found, the last IP address in that field will be used as the client IP address. Make sure you only allow trusted reverse proxies in this IP list.
Example: HideProxy = 192.168.10.20

Include <filename>|<directory>
Include another configuration file or configuration files in a directory.
Example: Include /etc/hiawatha/hosts.conf

KickOnBan = yes|no
Close all other connections that originate from the same IP in case of a ban.
Default = no Example: KickOnBan = yes

KillTimedoutCGI = yes|no
If a CGI process times out (see TimeForCGI for more information), Hiawatha will send a TERM signal to the CGI process, wait 1 second and then send a KILL signal to the CGI process. This option has no effect on FastCGI jobs.
Default = yes Example: KillTimedoutCGI = no

ListenBacklog = <value>
The backlog value for the listen() system call. This value defines the size of the waiting queue for incoming connections.
Default = 16 Example: ListenBacklog = 128

LogfileMask = (allow|deny) <ip-address>[/netmask][, (allow|deny) <ip-address>[/netmask], ...]
List of IPs from which HTTP requests will be logged. If an IP does not match an entry in the list, the request will be logged.
Example: LogfileMask = deny 10.0.0.0/24

LogFormat = hiawatha|common|extended
Define the format of the logfile: hiawatha = Hiawatha's default format, common = Common Log Format, extended = Extended Common Log Format.
Default = hiawatha Example: LogFormat = extended

LogTimeouts = yes|no
Log connection timeouts in the system logfile.
Default = yes Example: LogTimeouts = no

MaxServerLoad = <value>
When the server has a load higher than <value>, Hiawatha will drop incoming connections. This options is only available under Linux.
Example: MaxServerLoad = 0.7

MaxUrlLength = <value>
The maximum length of the path of an URL that the webserver accepts as being valid. Otherwise, a 414 error code is returned. The value 'none' disables this check.
Default = 1000 Example: MaxUrlLength = 500

MimetypeConfig = <configuration file>
The location of the mimetype configuration file. It the path is omitted, Hiawatha's configuration file directory will be used.
Default = mimetype.conf Example: MimetypeConfig = /etc/mime.types

MinTLSversion = 1.0|1.1|1.2
Specify the minimum TLS version Hiawatha accepts for HTTPS connections.
Default = 1.1, Example: MinTLSversion = 1.2

(requires that Hiawatha was not compiled with -DENABLE_TLS=off)

MonitorServer = <ip-address>
Specify the IP address of the Hiawatha Monitor server. This enables logging of statistical information. Use a X-Hiawatha-Monitor CGI header to log an event. Use the value 'failed_login' to log a failed login or 'exploit_attempt' to log an exploit attempt.
Example: MonitorServer = 192.168.1.2

(requires that Hiawatha was compiled with -DENABLE_MONITOR=on)

PIDfile = <filename>
The name of the file in which Hiawatha will write its process-ID. Don't change unless you know what you are doing (the CGI-wrapper and the MacOS X preference pane need the PID-file at its default location).
Default = /cygdrive/c/Program Files/Hiawatha/work/hiawatha.pid Example: PIDfile = /data/hiawatha.pid

Platform = cygwin|windows
If set to 'windows', Hiawatha will convert the Unix-style path to CGI programs to a Windows-style path.
Default = windows Example: Platform = cygwin

This option is only available in the Windows (Cygwin) version of Hiawatha.

RebanDuringBan = yes|no
Reset the ban-time when a client tries to reconnect during a ban.
Default = no Example: RebanDuringBan = yes

ReconnectDelay = <time>
The number of seconds Hiawatha will remember the IP address of the connection and pretend the client is still connected. In combination with ConnectionsPerIP, this can be used to prevent flooding. Note that the BanOnMaxPerIP ban-timer will be used, not the BanOnFlooding ban-timer. Causes some load on the server.
Default = 0 Example: ReconnectDelay = 3

RequestLimitMask = (allow|deny) <ip-address>[/netmask][, (allow|deny) <ip-address>[/netmask], ...]
Define for which clients the ConnectionsPerIP, MaxRequestSize, TimeForRequest and PreventSQLi settings should not be used. If an IP is allowed or not listed, the mentioned settings will be used.
Example: RequestLimitMask = deny 192.168.0.1

ServerId = <userid>|<userid>:<groupid>[, <groupid>, ...]
The userid and groupid(s) the server will change to. If only a userid is specified, the groupid(s) will be looked up in /etc/passwd and /etc/group. The userid en groupid of user root are not allowed here. The userid or groupid can also be a name.
Default = 65534:65534 Example: ServerId = www-data

ServerString = <text>
The text behind 'Server:' in the HTTP header of a response. Use 'none' to completely remove the Server string from the HTTP header.
Default = Hiawatha v<version> Example: ServerString = myWebserver

SetResourceLimits = yes|no
Let Hiawatha set the resource limits for number of threads and file descriptors.
Default = yes Example: SetResourceLimits = no

SocketSendTimeout = <time>
Sets the SO_SNDTIMEO value for all client connection sockets. Use 0 to disable this feature.
Default = 3 Example: SocketSendTimeout = 10

Syslog = [system][, exploit][, garbage][, access][, error][, all][;<syslog identifier>]
Log information to syslog.
Example: Syslog = system, access, error

SystemLogfile = <filename with full path>
Logfile for all system- and errormessages.
Default = /cygdrive/c/Program Files/Hiawatha/logfiles/system.log Example: SystemLogfile = /var/log/hiawatha.sys

ThreadKillRate = <amount>
At startup, Hiawatha starts the amount of threads as specified by ThreadPoolSize. When more threads are required, Hiawatha spawns them on the fly. When those extra threads are no longer needed, max <amount> threads are killed per 10 seconds.
Default = 1 Example: ThreadKillRate = 10

ThreadPoolSize = <size>
Initial size of the thread pool.
Default = 25 Example: ThreadPoolSize = 50

Throttle = (<main-mimetype>/[<sub-mimetype>]|.<extension>):<speed in kB/s>
Control the upload speed of certain files.
Example: Throttle = audio/mpeg:30
Throttle = .mp:50

Tomahawk = <port number>, <MD5 hash of password>
The port and the password for Tomahawk. You can use telnet to connect to Tomahawk (localhost:<port number>). Once connected to Tomahawk, type 'help' for more information.
Example: Tomahawk = 81,41d0c72bd73afaa2c207064d81d5a3d9

(requires that Hiawatha was compiled with -DENABLE_TOMAHAWK=on)

TunnelSSH = <ip-address>[, <ip-address>, ...][; <authentication code>]
This option allows you to connect to the SSH daemon on your server when port 22 is blocked by a firewall. The parameter of this option is the IP address from where you want to connect to your server. In PuTTY and WinSCP, use the HTTP proxy type and enable the 'Consider proxying local host connections' option. Use 'localhost' as the hostname and your server's hostname as the proxy hostname. Optionally, you can set an authentication code, which is base64(<username>:<password>). The username and password are for in the PuTTY proxy page. When set, you can connect from any IP address you want.
Example: TunnelSSH = 123.45.67.89

UserDirectory = <directory>
The name of the web directory in a user's home directory (see UserWebsites for more information).
Default = public_html Example: UserDirectory = website

WaitForCGI = yes|no
Lets Hiawatha wait for CGI processes to finish after receiving the last output byte (via waitpid() call) or not (SIGCHLD set to SIG_IGN).
Default = yes Example: WaitForCGI = no

WorkDirectory = <path>
The directory where Hiawatha can temporarily store files for uploading and the Monitor. Note that Hiawatha will change the ownership and access rights of this directory for security reasons. So, don't use existing direcories like /tmp.
Default = /cygdrive/c/Program Files/Hiawatha/work Example: WorkDirectory = /tmp/hiawatha

WrapUserCGI = yes|no
Always use the CGI-wrapper when handling CGI scripts in user websites (see UserWebsites for more information). The userid of the owner of the website will be used.
Default = no Example: WrapUserCGI = yes

BINDING CONFIGURATION

A binding is where a client can connect to (a port on a network interface).

BindingId = <binding_id>
The binding ID can be used to hook a virtual host to a binding (see RequiredBinding for more information).
Example: BindingId = LAN

EnableAccf = yes|no
Enable the HTTP accept filter. This is only available on FreeBSD. This requires the accf_http kernel module to be loaded.
Default = no Example: EnableAccf = yes

EnableAlter = yes|no
Enable the PUT and DELETE HTTP request method for this binding (see AlterList and UploadDirectory for more information).
Default = no Example: EnableAlter = yes

EnableTRACE = yes|no
Enable the TRACE HTTP request method for this binding.
Default = no Example: EnableTRACE = yes

Interface = <IP address>
The IP address of the interface that must be binded.
Default = 0.0.0.0 (IPv4) Example: Interface = 192.168.0.1

MaxKeepAlive = <number>
Maximum number of stay-alives after the first request. After that, the connection will be closed. Of course, the browser can reconnect. But this gives other users a chance to connect in case of a 'crowded' webserver.
Default = 50 Example: MaxKeepAlive = 100

MaxRequestSize = <size>
The maximum size of a request in kilobytes the webserver is allowed to receive. This does not include PUT requests. See also RequestLimitMask.
Default = 64 Example: MaxRequestSize = 256

MaxUploadSize = <size>
The maximum size of a PUT request entity in megabytes the webserver is allowed to receive. The maximum size is 2047 megabytes.
Default = 1 Example: MaxUploadSize = 15

Port = <port number>
The port number that will be used for the binding. This is a required option.
Example: Port = 80

RequiredCA = <CA certificate file>[, <CA CRL file>

Use the CA certificates in this file to authenticate users. Users without a certificate from one of the listed CAs will not be allowed.
Example: RequiredCA = /etc/ssl/cacert.pem, /etc/ssl/cacrl.pem

(requires that Hiawatha was not compiled with -DENABLE_TLS=off)

TLScertFile = <TLS private key and certificate file>

Encrypt the connections of the current binding with the TLS private key and certificate in the specified file. Intermediate certificates also go in this file. Make sure the order matches the TLS chain order: host certificate first, CA certificate last. Use the tool 'lefh' (Let's Encrypt For Hiawatha) to obtain and maintain Let's Encrypt certificates.
Example: TLScertFile = my_domain.pem

(requires that Hiawatha was not compiled with -DENABLE_TLS=off)

TimeForRequest = [<time1>,]<time2>

Maximum time in seconds for a client to send its HTTP request. time1 is for the first request, time2 is for the following requests (Keep-Alive time). If time2 is omitted, time1 is used for all requests. See also RequestLimitMask.
Default = 5, 30 Example: TimeForRequest = 2, 45

VIRTUAL HOST CONFIGURATION

The (virtual) hosts the webserver will be serving. The first host must NOT be placed inside a record. This is the default host and therefor not virtual. It is wise to have the IP-address of the webserver as the Hostname of the default host and give it a blank page. Automated vulnerable-website scanners will not find your possible vulnerable website if you do so.

AccessList = (allow|deny|pwd) <ip-address>[/netmask][, (allow|deny|pwd) <ip-address>[/netmask], ...]

Define which IPs have access to the website. If an IP does not match an entry in the list, access is granted. 'all' is an alias for 0.0.0.0/0. The IP address of the machine that connects and the IP address specified in the X-Forwarded-For header field (deny only) will be used to find a match. 'allow' gives access, 'deny' denies access and 'pwd' gives access if a valid password has been given (see PasswordFile for more information).
Hiawatha will ignore this setting for files in /.well-known/acme-challenge/, which are used for authentication in the Let's Encrypt certificate request process.
Example: AccessList = deny 10.0.0.13, allow 10.0.0.0/24, deny all

AccessLogfile = <filename with full path>[,daily|monthly|weekly]|none

Logfile for the HTTP requests. Hiawatha can rotate them on a daily, weekly or monthly basis. Use 'none' to disable the access log.
Default = /cygdrive/c/Program Files/Hiawatha/logfiles/access.log Example: AccessLogfile = /var/log/hiawatha.acc, weekly

Alias = <softlink>:<directory>

An alias is a virtual softlink to a directory. Every request to <websiteroot>/<softlink> will be rerouted to <directory>.
Example: Alias = /doc:/usr/share/doc

AllowDotFiles = <yes|no>

Allow files that start with a dot (hidden files for Unix) to be downloaded by a client. Requests for .hiawatha files are always blocked. A requests URI that start with /.well-known/ is always accepted, as defined in RFC 5785.
Default = no Example: AllowDotFiles = yes

AlterGroup = <groupname>[, <groupname>, ...]
The <groupname> is the name of the group a user must be a member of to use the PUT and DELETE HTTP method (see PasswordFile and AlterList for more information).
Example: AlterGroup = publishers

AlterList = (allow|deny|pwd) <ip-address>[/netmask][, (allow|deny|pwd) <ip-address>[/netmask], ...]
Define which IPs are allowed to use the PUT and DELETE HTTP request method. If an IP does not match an entry in the list, usage is denied. 'all' is an alias for 0.0.0.0/0. The IP address of the machine that connects and the IP address specified in the X-Forwarded-For header field (deny only) will be used to find a match. Look out for the uploading of CGI scripts! Use "ExecuteCGI = no" in a Directory record to disable CGI execution (see EnableAlter, AlterGroup and AlterMode for more information).
Example: AlterList = deny 10.0.0.13, allow 10.0.0.0/24, deny all

AlterMode = <filemode>
The files that are created via PUT will have the file permissions set to <filemode> (see AlterList for more information).
Default = 640 Example: AlterMode = 664

BanByCGI = yes|no[, <max value>]
Allow a CGI application to ban a client via a 'X-Hiawatha-Ban: <value>' CGI header. The value is the maximum amount of seconds a CGI application is allowed to ban a client.
Default = no Example: BanByCGI = yes

CustomHeaderClient = <key>: <value>
Set a custom HTTP header for every response sent to the client.
Example: CustomHeaderClient = Access-Control-Allow-Origin: *

CustomHeaderBackend = <key>: <value>
Set a custom HTTP header for every request forwarded to the backend while acting as a reverse proxy.
Example: CustomHeaderBackend = X-Custom-Header: some_value

(requires that Hiawatha was not compiled with -DENABLE_RPROXY=off)

DenyBody = <regular expression>
If the request body matches the case insensitive POSIX regular expression, return a 403 Forbidden.
Example: DenyBody = ^.*%3Cscript.*%3C%2Fscript%3E.*$

EnablePathInfo = yes|no
Accepts URLs like /index.php/parameter if /index.php exists and the extension .php has been configured as a CGI program. '/parameter' will be placed in the environment variable PATH_INFO.
Default = no Example: EnablePathInfo = yes

EnforceFirstHostname = yes|no
If the hostname used in the URL is not the same as the first one in the list of the Hostname setting, then Hiawatha will send a 301 redirect with that hostname. This option is ignored if the first hostname starts with a wildcard.
Default = no Example EnforceFirstHostname = yes

ErrorHandler = <error code>:<filename>[?key=value&...]
When a 401, 403, 404, 501 or 503 error occures, this file will be send to the browser. The WebsiteRoot and the ErrorHandler together must form the complete path to the file. The generated errorcode can be found via the environment variable HTTP_GENERATED_ERROR. To override the returned HTTP code in a CGI script, use the HTTP Header "Status", for example "Status: 404".
Example: ErrorHandler = 404:/error.php?code=404

ErrorLogfile = <filename with full path>
Logfile for the messages that have been written to stdout by CGI processes.
Default = /cygdrive/c/Program Files/Hiawatha/logfiles/error.log Example: ErrorLogfile = /var/log/hiawatha.err

ErrorXSLTfile = <XSLT file with full path>
In case of an error, use the specified XSLT file to generate the error message. Upon any error, Hiawatha will fall back to the hardcoded error message. An example of the generated XML that will be used can be found in extra/error.xml inside the source package.
Example: ErrorXSLTfile = /etc/hiawatha/error.xslt

(requires that Hiawatha was not compiled with -DENABLE_XSLT=off)

ExecuteCGI = yes|no
Allow execution of CGI programs.
Default = no Example: ExecuteCGI = yes

FileHashes = <file containing file hashes>
Points Hiawatha to a file containing SHA256 hashes for every file in the webroot directory. Before serving a file, Hiawatha checks the file hash of that file. If it doesn't match, access is denied. This protects against file changes or uploading of malware. FastCGI scripts are also checked if the FastCGI server can be reached via a UNIX socket. The file hashes file can be created via the -s option of the wigwam(1) tool.
Example: FileHashes = /etc/hiawatha/hashes/my_website.txt

FollowSymlinks = yes|no
Allow Hiawatha to follow symlinks to files and directories. Symlinks that stay inside the webroot or are owned by root are always followed. Note that this does not apply to CGI's which are executed via FastCGI, because Hiawatha is not able to look for symlinks on remote FastCGI servers.
Default = no Example: FollowSymlinks = yes

Hostname = <hostname>, [<hostname>, ...]
Name(s) of the host that Hiawatha will be serving. May start with a wildcard, except the first hostname (a valid name is required in case of a 301 error). Hostname is a required field.
Example: Hostname = www.my-domain.com, *.my-domain.com, www.some-alias.com

HTTPAuthToCGI = yes|no
Place the HTTP Authorization header in the CGI's HTTP_AUTHORIZATION environment variable.
Default = no Example: HTTPAuthToCGI = yes

LoginMessage = <text>
Message that will be displayed in the login window in case of HTTP authentication (see PasswordFile for more information). When using Digest HTTP authentication, the LoginMessage should not contain a ':' sign.
Default = Private page Example: LoginMessage = My personal files

NoExtensionAs = <extension>
If the requested file has no extension, treat it as if the extension was equal to <extension>.
Example: NoExtensionAs = cgi

PasswordFile = ((Basic|Digest):<passwordfile>)|none[, <groupfile>]
When this option is set, HTTP authentication is enabled. Use the full path to the password file when that password file should also be used for sub-directories. Entries for the password file can be created via the wigwam(1) tool. The realm for Digest HTTP authentication must be equal to the text set via LoginMessage.
The <groupfile> contains the groupnames followed by the names of the users that are a member of that group. The format of the lines in the groupfile is:

<groupname>:<username>[<username> ...]

Hiawatha will ignore this setting for files in /.well-known/acme-challenge/, which are used for

authentication in the Let's Encrypt certificate request process.
Example: PasswordFile = basic:/var/www/.passwords,/var/www/.groups

PreventCSRF = no|detect|prevent|block
Prevent Cross-Site Request Forgery attacks. The 'detect' option only detects and logs a CSRF attack, 'prevent' discards the POST data and cookies and 'block' returns a 443 error. This setting can cause problems for users who use tools to hide/remove the Referer HTTP header string while browsing.

Don't use this as a generic security feature. Only use it to prevent a specific vulnerablility in an application that can't be taken offline while you wait for a patch.
Default = no Example: PreventCSRF = block

PreventSQLi = no|detect|prevent|block
Prevent SQL-injection attacks. The 'detect' option only detects and logs an SQL injection attack, 'prevent' returns a 404 error and 'block' returns a 441 error. It is important to understand that the detection of SQL injections is done by best effort. There is no 100% guarantee that all SQL injections are blocked. Note that using this feature can have a negative effect on the performance of your webserver and can make the exploit logfile grow very large. See also BanOnSQLi and RequestLimitMask.

Don't use this as a generic security feature. Only use it to prevent a specific vulnerablility in an application that can't be taken offline while you wait for a patch.
Default = no Example: PreventSQLi = detect

PreventXSS = no|detect|prevent|block
Prevent Cross-Site Scripting attacks. The 'detect' option only detects and logs a XSS attack, 'prevent' disables the <script> tag in the input and 'block' returns a 442 error.

Don't use this as a generic security feature. Only use it to prevent a specific vulnerablility in an application that can't be taken offline while you wait for a patch.
Default = no Example: PreventXSS = prevent

PublicKeyPins = <public key file>[, max_age=<value>[d]]
Hiawatha will load public keys from the <public key file>, which will be used to calculate the pin-sha256 values for the Public-Key-Pins HTTP header (HPKP). The <public key file> can contain certificates, certificate signing requests and public keys, all in PEM format. The optional max_age value is in seconds or in days when it ends with a 'd'. The default value for max_age is '30d'.
Example: PublicKeyPins = /etc/hiawatha/letsencrypt.pem, 60d

(requires that Hiawatha was not compiled with -DENABLE_TLS=off)

RequiredBinding = <binding_id>[, <binding_id>, ...]
By default, a virtual host can be visited via all bindings. Via this opion, you can specify via which bindings a virtual host can be visited (see chapter BINDING CONFIGURATION for more information).
Example: RequiredBinding = LAN

RandomHeader = <length>
Adds an X-Random HTTP header to the response for HTTPS connections. The header contains a random string. The length of that string is a random value between 1 and <length>. This header helps to prevent attackers from guessing what file was requested based on the response length. <length> must be between 10 and 1000.
Example: RandomHeader = 250

RequiredCA = <CA certificate file>[, <CA CRL file>
Use the CA certificates in this file to authenticate users. Users without a certificate from one of the listed CAs will not be allowed.

RequiredGroup = <groupname>[, <groupname>, ...]
The <groupname> is the name of the group a user must be a member of to have access (see PasswordFile for more information).
Example: RequiredGroup = webadmins,staff

RequireTLS = yes|no[, <HSTS time>[d]][; includeSubDomains][; preload]
Specify that a domain must be visited with a TLS connection. If it is visited via HTTP, Hiawatha will send a redirect (301) with an HTTPS URL. The <HSTS time> is the max-age value of the Strict-Transport-Security HTTP header in seconds or in days when it ends with a 'd'.
Hiawatha will ignore this setting for files in /.well-known/acme-challenge/, which are used for authentication in the Let's Encrypt certificate request process.
Default = no Example: RequireTLS = yes, 2678400

(requires that Hiawatha was not compiled with -DENABLE_TLS=off)

ReverseProxy = [!]<pattern> [<skip directories>] http[s]://<hostname>[:<port>][/<path>]|<unixsocket> [<timeout>] [keep-alive]
Forward the request with URLs that match the POSIX regular expression <pattern> to another webserver, where <path> is placed before the original URL. When <hostname> is an IP address, the value of the Host HTTP header is unchanged. Otherwise, it is replaced with the value of <hostname>. The optional <skip directories> is a number that indicates how many directories in the original URL should be skipped when sending it to the final webserver. The connection is closed after <timeout> seconds, which is set to 5 seconds by default. By default, Hiawatha doesn't use keep-alive connections to the final webserver. You can enable this by adding 'keep-alive' to the configuration line. When specifying multiple reverse proxies for one (virtual) host, Hiawatha prefers reverse proxies with a scheme (HTTP/HTTPS) matching the one of the client connection. See also CAcertificates.
Example: ReverseProxy = ^/icons/ 1 http://resources.lan/images

(requires that Hiawatha was not compiled with -DENABLE_RPROXY=off)

RunOnAlter = <path to program>
Run a program after a client has sent a PUT or a DELETE request. Information about the request is placed in environment variables, just like CGI
Example: RunOnAlter = /usr/local/sbin/alter-script

Setenv <key> = <value>
Define environment settings for CGI programs.
Example: Setenv PHPRC = /var/www/conf

ScriptAlias = <softlink>:<script>
A script alias is a virtual softlink to a CGI script. Every request to <websiteroot>/<softlink> will be rerouted to <script>.
Example: ScriptAlias = /script.cgi:/usr/lib/script.cgi

ShowIndex = yes|no|<XSLT file with full path>|xml
Return a directory listing in HTML format for a directory request when the startfile does not exist. If you want to change the index layout completely, specify the path of a XSLT file. If the XSLT file is not found or 'xml' is used, Hiawatha will output the XML of the directory index. An example of the XML output can be found in extra/index.xml inside the source package.
Default = no Example: ShowIndex = /etc/hiawatha/index.xslt

(requires that Hiawatha was not compiled with -DENABLE_XSLT=off)

SkipCacheCookie = <cookie name>[, <cookie name>, ...]
Skip the internal cache for requests for GGI scripts that contain one of the mentioned cookies.
Example: SkipCacheCookie = banshee_login_id

TLScertFile = <TLS private key and certificate file>
Use this option inside a virtualhost block if you want to make use of the SNI capabilities of Hiawatha. See the TLScertFile option in the BINDING CONFIGURATION chapter for more information.

StartFile = <filename>
The file which will be send to the browser when a directory is requested.
Default = index.html Example: StartFile = start.php

TimeForCGI = <time>
Maximum time in seconds for a CGI-process to finish its job.
Default = 5 Example: TimeForCGI = 15

TriggerOnCGIstatus = yes|no
Print an HTTP error message or invoke the ErrorHandler when a CGI outputs a Status HTTP header line.
Default = no Example: TriggerOnCGIstatus = yes

UseDirectory = <directory_id>[, <directory_id>, ...]
The Directory records to use for this virtual host. See chapter DIRECTORY CONFIGURATION for more information.
Example: UseDirectory = my_dir

UseLocalConfig = yes|no
Tell Hiawatha to use or ignore .hiawatha files.
Default = no Example: UseLocalConfig = yes

UseFastCGI = <fcgi_server_id>[, <fcgi_server_id>, ...]
The FastCGI server to use for this virtual host. The first FastCGI server record that matches (including extension), will be used. See chapter FASTCGI CONFIGURATION for more information. This option sets ExecuteCGI to 'yes' for this host.
Example: UseFastCGI = PHP7

UserWebsites = yes|no
Activates user websites for this (virtual) host (the /~user/ URL's) (see UserDirectory for more information).
Default = no Example: UserWebsites = yes

UseToolkit = <toolkit_id>[, <toolkit_id>, ...]
Perform special operations, like rewriting via regular expressions, on the URL. See chapter URL TOOLKIT for more information.
Example: UseToolkit = my_toolkit

(requires that Hiawatha was not compiled with -DENABLE_TOOLKIT=off)

UseXSLT = yes|no
Activate XSL transformations (see chapter XSLT for more information).
Default = no Example: UseXSLT = yes

(requires that Hiawatha was not compiled with -DENABLE_XSLT=off)

WebDAVapp = <yes|no>
Enables support for WebDAV applications.
Default: WebDAVapp = no Example: WebDAVapp = yes

WebsiteRoot = <directory>
Root directory for this virtual host. It's not allowed to use the root of a disk as the website root directory.
Example: WebsiteRoot = /home/webmaster/website

WebSocket = ws[s]://<IP address>:<port> <request uri>[,...] [connection timeout]
This setting will make Hiawatha forward the connection to a websocket for every request where the URL starts with <request uri>. A wildcard request URI will forward every request for this host. The connection timeout is in minutes and the default is 10. See also CAcertificates.
Example: WebSocket = ws://127.0.0.1:5000 /chat 30

WrapCGI = <wrap_id>
Specify a CGI-wrapper id for this virtual host (see cgi-wrapper(1) for more information).
Example: WrapCGI = test

DIRECTORY CONFIGURATION

This chapter explains which options can be set for a specific directory. These options will override (virtual) host settings.

DirectoryId = <directory_id>
A unique ID for a directory record. Use this Id with the UseDirectory setting in a virtual host.
Example: DirectoryId = my_dir

ExpirePeriod <time> seconds|minutes|hours|days|weeks|months[, public|private]
Adds an Expires HTTP header with current timestamp + <time>. The public/private (default is private) option defines the value of the Cache-Control header.
Example: ExpirePeriod = 2 weeks, public

Extensions = <extension>[, <extension>, ...]
When set, settings that affect files will only be used when the extension of the requested file matches with the supplied list.
Example: Extensions = png, jpg, gif

Path = <path>[, <path>, ...]
The path to the subdirectory, which may be virtual (not existing on disk). This is a required setting.
Example: Path = /files

RunOnDownload = <path to program>
Run a program when a client requests a static resource. This does not include CGI programs. Information about the request is placed in environment variables, just like CGI.
Example: RunOnDownload = /var/www/log_download

UploadSpeed = <speed>, <maximum number of connections>
Set the uploadspeed in kB/s for all the files in the directory regardless of the extension or mimetype. The uploadspeed per connection will be divided by the number of connections.
Example: UploadSpeed = 20,4

AccessList ,
AlterGroup ,
AlterList ,
AlterMode ,
ExecuteCGI ,
WrapCGI ,
FollowSymlinks ,
PasswordFile ,
RequiredGroup ,
Setenv ,
ShowIndex ,
StartFile and
TimeForCGI

FASTCGI CONFIGURATION

This chapter explains how to use one or more FastCGI servers.

ConnectTo = <ip-address>:<port number>|<path>[, <ip-address>:<port number>|<path>, ...]

The IP-address and TCP port or UNIX socket Hiawatha must connect to to reach the FastCGI server.
Example: ConnectTo = 127.0.0.1:2004 (IPv4)
ConnectTo = [::1]:2004 / ::1.2004 (IPv6)
ConnectTo = /tmp/hiawatha.sock (UNIX socket)

Extension = <extension>[, <extension>, ...]

The extension of the script the FastCGI server is able to interpret. If no extension is specified, all requests will be sent to the FastCGI server.
Example: Extension = php

FastCGIid = <fcgi_server_id>

Give each FastCGI server an unique Id. Use this Id with the UseFastCGI setting in a virtual host.
Example: FastCGIid = PHP7

ServerRoot = <path>

If the FastCGI server is running in a chroot, use this setting to specify that chroot directory.
Example: ServerRoot = /var/www/chroot

SessionTimeout = <time in minutes>

The maximum duration of a CGI session for this FastCGI server. Will only be used when specifing multiple ConnectTo's.
Default = 15 Example: SessionTimeout = 30

URL TOOLKIT

How to use the URL toolkit is explained in this chapter. To use URL toolkits, Hiawatha should not have been compiled with -DENABLE_TOOLKIT=off. The main toolkit commands are:

Do <action>

Perform an action, where <action> can be one of the following:
Ban, Call, DenyAccess, Exit, Goto, OmitRequestLog, Return, Skip or Use.
Example: Do Call other_rule_set

Header <key> [!]<pattern> <action>

Perform an action when the HTTP header <key> matches the POSIX regular expresion <pattern>, where <action> can be one of the following:
Ban, Call, DenyAccess, Exit, Goto, OmitRequestLog, Return, Skip or Use.
A negative pattern (leading exclamation mark) can't be used with the redirect action. The <key> can be * to test every HTTP header. Note that the wildcard means 'any header', not 'every header'.

Match [!]<pattern> <action>

Perform an action when the URL matches the POSIX regular expression <pattern>, where <action> can be one of the following:
Ban, Call, DenyAccess, Exit, Goto, Redirect, Return, Rewrite, Skip or UseFastCGI.
Use MatchCI to perform case insensitive URL matching. A negative pattern (leading exclamation mark) can't be used with the redirect and rewrite action.

Method [!]<request method> <action>

Perform an action when the request method equals <request method>, where <action> can be one of the following:
Call, DenyAccess, Exit, Goto, Return, Skip or Use
Example: Method POST Return

RequestURI exists|isfile|isdir|notfound <action>

Perform an action based on the presence of the requested file, where <action> can be one of the following:

Call, Return, Exit or Skip.
Example: RequestURI isfile Return

ToolkitId = <toolkit_id>
The toolkit ID can be used to bind toolkit rules to a virtual host. See also UseToolkit.
Example: ToolkitId = my_toolkit

TotalConnections <value> <action>
Perform an action if the total amount of connections is equal to or higher than <value>, where <action> can be one of the following:
Call, Goto, OmitRequestLog, Redirect or Skip
Example: TotalConnections 1000 Call CheckUserAgent

UseTLS <action>
Perform an action when the client is connection via a TLS secured connection, where <action> can be one of the following:
Call, Exit, Goto, Return or Skip.

An exclamation mark in front of a pattern (negative pattern matching) makes Hiawatha perform the action when the pattern does not match. The <action> statements mentioned above are described here:

Ban <seconds>
Ban the client for <seconds> seconds.

Call <toolkit_id>
Execute toolkit record <toolkit_id> and continue in the current record afterwards.

DenyAccess
Deny access to the requested file (results in a 403 error) and terminate toolkit processing.

Exit
Terminate toolkit processing.

Goto <toolkit_id>
Execute <toolkit_id> and terminate the current URL rewriting process.

OmitRequestLog
Don't log the current request in the file specified by AccessLogfile.

Redirect [301..308] <url>
Redirect the browser to the specified URL and terminate toolkit processing. The default status code is 301.

Return
Return from the current UrlToolkit record.

Rewrite <replacement> [<max_loop>] [Continue|Return]
Rewrite the current URL using <replacement>. Examples:
"Match ^/pics/(.*) Rewrite /images/$1" will change "/pics/logo.gif" into "/images/logo.gif".
"Match a Rewrite b 3" will change "/aaaaa.html" into "/bbbaa.html". Default value of <max_loop> is 1, maximum is 20.
Rewrite will terminate toolkit processing, unless Continue or Return has been given.

Skip <number>
Skip the next following <number> lines (ToolkitId excluded).

Use <url>
Replace the current URL with <url> and terminate toolkit processing.

UseFastCGI <fcgi_id>
Use FastCGI server with id <fcgi_id> and terminate toolkit processing.

The original URL is stored in the environment variable REQUEST_URI. Before using URL toolkit rules, use the tool 'wigwam' to verify the result of your rules (see wigwam(1) for more information).

Example:

```
VirtualHost {
        ...
        UseToolkit = clean_url
}

UrlToolkit {
        ToolkitId = clean_url
        Match ^/(css|images|js)(/|$) Return
        RequestURI exists Return
        Match ^/.*\?(.*) Rewrite /index.php?$1
        Match ^/.* Rewrite /index.php
}
```

XSLT

If a XML file is requested, Hiawatha can do a XSL transformation when a XSLT sheet is present. For the requested XML file (<name>.xml), '<name>.xslt', 'index.xslt' in the current directory or 'index.xslt' in the WebsiteRoot needs to be present. Otherwise, the XML file itself will be uploaded. The environment variables which are available during CGI execution are available as XSLT parameters. URL variables start with 'GET_', POST variables start with 'POST_' and cookies start with 'COOKIE_'.

CGI OUTPUT CACHE

Hiawatha can cache the output of CGI applications. When and for how long is determined by the application itself. It can use the following CGI headers to control the caching of its output. This feature requires that Hiawatha was not compiled with -DENABLE_CACHE=off.

X-Hiawatha-Cache: <seconds>

The output can be cached for <seconds> seconds. The minimum value is 2, the maximum value is 3600 (one hour).
Example: X-Hiawatha-Cache: 600

X-Hiawatha-Cache-Remove: <url>

The output of <url> should be removed from the cache. Use this when you update a cached page in your CMS. Use 'all' as the URL to clear the cache for the current website.
Example: X-Hiawatha-Cache-Remove: /about

USER SETTINGS PER DIRECTORY

A user can override the settings listed below for a certain directory. This can be done by placing one or more of those settings in a .hiawatha file in that directory. Hiawatha will not look for a .hiawatha file in the root directory of the disk.

AccessList ,
AlterGroup ,
AlterList ,
AlterMode ,
ErrorHandler ,
LoginMessage ,
PasswordFile ,
RequiredGroup ,
ShowIndex ,
StartFile and
UseToolkit (only valid in the root directory of a website)

MIMETYPES

Specify the mimetypes of files in /etc/hiawatha/mimetypes.conf.

<mimetype> <extension> [<extension> ...]
Example: image/jpeg jpg jpeg jpe

SIGNALS

TERM Shutdown the webserver.

HUP Close all open logfiles.

USR1 Unban all IP addresses.

USR2 Clear the internal cache (requires that Hiawatha was not compiled with -DENABLE_CACHE=off).

FILES

/usr/sbin/hiawatha
/etc/hiawatha/hiawatha.conf
/etc/hiawatha/mime.types
/etc/hiawatha/cgi-wrapper.conf

SEE ALSO

cgi-wrapper(1), ssi-cgi(1), wigwam(1)

AUTHOR

Hugo Leisink <hugo@hiawatha-webserver.org> - *https://www.hiawatha-webserver.org/*