

NAME

hiawatha - advanced and secure webserver

SYNOPSIS

hiawatha [-c <path>] [-d] [-k] [-h] [-v]
 -c <path>: path to where the configuration files are located.
 -d: don't fork to the background.
 -k: check configuration and exit.
 -h: show help 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.

php-fcgi.conf

See php-fcgi(1) for more information.

.hiawatha

See chapter USER SETTINGS PER DIRECTORY for more information.

SECTIONS

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

```
Section {
    ...
}
```

where the word "Section" must be replaced by "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.

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)

AllowedCiphers = <cipher>[:<cipher>,...]

The crypto ciphers Hiawatha is allowed to use for HTTPS connections. Use the command 'openssl ciphers -v -ssl3' to see a list of available ciphers (see ciphers(1) for more information).

Example: AllowedCiphers = DHE-RSA-AES256-SHA:DHE-DSS-AES256-SHA:AES256-SHA:EDH-RSA-DES-CBC3-SHA:EDH-DSS-DES-CBC3-SHA:DES-CBC3-SHA:DHE-RSA-AES128-SHA:DHE-DSS-AES128-SHA:AES128-SHA:DHE-DSS-RC4-SHA:RC4-SHA:RC4-MD5

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 from the banlist will not be banned.

Example: BanlistMask = allow 192.168.1.2, deny 192.168.0.0/16

BanOnDeniedBody = <ban-time>

Number of seconds to ban an IP in case of a denied request body. See also 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 malformed HTTP request (400 Bad Request). Web-browsers normally don't send malformed HTTP requests. So in case of a 400 errorcode, someone is probably trying something not-so-nice.

Default = 0, example: BanOnGarbage = 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.

Default = -:0, Example: BanOnWrongPassword = 3:120

CacheSize = <size in megabytes>

Size of Hiawatha's internal file cache. Maximum is 50 (megabytes).

Default = 10, example: CacheSize = 15

(requires that Hiawatha was not compiled with --disable-cache)

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 --disable-cache)

CacheMinFilesize = <size in bytes>

Minimum size of a file Hiawatha will store in its internal cache.
Default = 1, example: CacheMaxFilesize = 512

(requires that Hiawatha was not compiled with --disable-cache)

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/php4-cgi.php:php4

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 = /usr/sbin/cgi-wrapper, example: CGIwrapper = /bin/cgi-wrapper

CommandChannel = <portnumber>, <MD5 hash of password>

The port and the password for the CommandChannel. You can use telnet to connect to the CommandChannel (localhost:<portnumber>). Type 'help' in the CommandChannel for more information.
Example: CommandChannel = 81,41d0c72bd73afaa2c207064d81d5a3d9

(requires that Hiawatha was compiled with --enable-command)

ConnectionsPerIP = <number>

Maximum number of simultaneous connections per IP address.
Default = 10, example: ConnectionsPerIP = 5

ConnectionsTotal = <number>

Maximum number of simultaneous connections.
Default = 100, example: ConnectionsTotal = 250

DHparameters = <DH paramater file>

The file that contains the parameters for the Diffie-Hellman key exchange protocol. If you don't know what this is, then you probably don't need it.
Example = DHparameters = dhparam.pem

ExploitLogfile = <filename with full path>

Logfile for all exploit attempts: CSRF, denied bodies, SQL injection and XSS
Default = /var/log/hiawatha/exploit.log, example: ExploitLogfile = /var/log/exploit_attempts.log

GarbageLogfile = <filename with full path>

Logfile for all malformed HTTP requests.
Example: GarbageLogfile = /var/log/hiawatha/garbage.log

HideProxy = <ip-address>[, <ip-address>, ...]

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. This option does not affect the ConnectionsPerIP setting.
Example: HideProxy = 192.168.10.20

Include <filename>|<directory>

Include another configurationfile or configurationfiles 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

KillTimeoutCGI = 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: KillTimeoutCGI = no

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

MimetypeConfig = <configurationfile>

The location of the mimetype configurationfile. If the path is omitted, Hiawatha's configurationfile directory will be used.

Default = mimetype.conf, example: MimetypeConfig = /etc/mime.types

MonitorServer = <ip-address>

Specify the IP address of the monitor server. This enables logging of statistical information.

Example: MonitorServer = 192.168.1.2

MonitorStatsInterval = <seconds>

Define the interval at which Hiawatha will make the statistical information available for the Hiawatha Monitor.

Default = 60, example: MonitorStatsInterval = 30

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 = /var/run/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 and TimeForRequest setting should not be used. If an IP is allowed or not listed, the 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

ServerRoot = <directory>

Rootdirectory for the webserver. Hiawatha will chroot() to this directory after reading the configurationfile and writing the PID file. Cannot be used in combination with UserWebsites. Only use this option when you know what you are doing!

Example: ServerRoot = /var/www

(requires that Hiawatha was compiled with --enable-chroot)

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

SocketSendTimeout = <time>

Sets the SO_SNDTIMEO value for all client connection sockets. Use 0 to disable this feature.

Default = 3, example: SocketSendTimeout = 10

SystemLogfile = <filename with full path>

Logfile for all system- and error messages.

Default = /var/log/hiawatha/system.log, example: SystemLogfile = /var/log/hiawatha.sys

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

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 (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 = /var/lib/hiawatha, 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 connects to (a port opened on an interface).

BindingId = <binding_id>

The binding ID can be used to bind a virtual host to an interface (see RequiredBinding for more information).

Example: BindingId = LAN

EnableAlter = yes|no

Enable the PUT and DELETE HTTP request method for this binding (see AlterList and Upload-Directory 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 address of an 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.

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 100 megabytes.

Default = 1, example: MaxUploadSize = 15

Port = <portnumber>

The portnumber that will be used for the binding. This is a required option.

Example: Port = 80

RequiredCA = <CA certificate file>[, <verify depth>]

Use the CA certificates in this file to authenticate users. Users without a certificate from one of the listed CAs will not be allowed. The default verify depth is 1.

Example: RequiredCA = /etc/ssl/cacert.pem

(requires that Hiawatha was not compiled with --disable-ssl)

SSLcertFile = <SSL private key and certificate file>

Encrypt the connections of the current binding with the SSL private key and certificate in the specified file. Intermediate certificates also go in this file. Make sure the order matches the SSL chain order: host certificate first, CA certificate last.

Example: SSLcertFile = my_domain.pem

(requires that Hiawatha was not compiled with --disable-ssl)

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.

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 section. This is the default host and therefore not virtual. It is wise to have the IP-address of the webserver as the Host-name 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).

Example: AccessList = deny 10.0.0.13, allow 10.0.0.0/24, deny all

AccessLogfile = <filename with full path>

Logfile for the HTTP requests.

Default = /var/log/hiawatha/access.log, example: AccessLogfile = /var/log/hiawatha.acc

Alias = <softlink>:<directory>

An alias is a virtual softlink to a directory. Every request to <websiteroot>/<softlink> will be redirected to <directory>.

Example: Alias = /doc:/usr/share/doc

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 section 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

DenyBody = <regular expression>

If the request body matches the regular expression, return a 403 Forbidden.

Example: DenyBody = ^.*%3Cscript.*%3C%2Fscript%3E.*\$

DenyBot = <name bot>:<path>[, <path>, ...]

Return a 403 Forbidden when a searchbot tries to index <path>. <name bot> must be present in the User-Agent string of the searchbot.

Example: DenyBot = msnbot:/files

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

ErrorHandler = <error code>:<filename>[?key=value&...]

When a 401, 403, 404, 501 or 503 error occurs, this file will be sent to the browser. The Website-Root 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 = /var/log/hiawatha/error.log, example: ErrorLogfile = /var/log/hiawatha.err

ExecuteCGI = yes|no

Allow execution of CGI programs.

Default = no, example: ExecuteCGI = yes

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

ImageReferer = hostname[, hostname, ...];<alternative image>

If the referer of a request for an image is not one of the specified hosts, return the alternative image instead.

Example: ImageReferer = my-domain.com:/var/www/pics/forbidden.gif

LoginMessage = <text>

Message that will be displayed in the login window in case of HTTP authentication (see Password-File for more information). When using Digest HTTP authentication, the LoginMessage should not contain a ':' sign.

Default = Private page, example: LoginMessage = Hugo's MP3 collection

MonitorRequests = yes|no

Make information about every request for this host available for the Hiawatha Monitor.

Default = no, example: MonitorRequests = yes

NoExtensionAs = <extension>

If the requested file has no extension, treat it as if the extension was equal to <extension>.

Example: NoExtension = cgi

PasswordFile = ((basic|digest):<passwordfile>)|none[,<groupfile>]

File which contains the username and password necessary to access this directory. You can create or update this file with htpasswd(1). The format of the lines in the passwordfile for Basic HTTP authentication is:

<username>:<password encrypted with crypt(3)>[:user defined fields: ...]

The file for Digest HTTP authentication can be created or updated with htdigest(1). The realm in the password file is the LoginMessage text. The format of the passwordfile is:

<username>:<realm>:md5(<username>:<realm>:<password>)[:user defined fields: ...]

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> ...]

Example: PasswordFile = basic:/var/www/.passwords,/var/www/.groups

PreventCSRF = yes|no

Prevent Cross-site Request Forgery by ignoring all cookies sent by a browser when following an external link to this website. This setting can cause problems for users who use tools to

hide/remove the Referer HTTP header string while browsing. Please note that this protection is not 100% safe.

Default = no, example: PreventCSRF = yes

PreventSQLi = yes|no

Prevent SQL-injection by detecting injections and denying the request via a 409 response. It is important to understand that the detection of SQL injections is done by best effort. There is no 100% guarantee that no injections are still possible. Note that using this feature can have a negative effect on the performance of your webserver. Use with caution. See also BanOnSQLi.

Default = no, example: PreventSQLi = yes

PreventXSS = yes|no

Prevent cross-site scripting via the URL by replacing a less-than, greater-than, quote or double-quote in the URL with an underscore.

Default = no, example: PreventXSS = yes

RequiredBinding = <binding_id>[, <binding_id>, ...]

Bind a virtual host to one or more interfaces (see chapter BINDING CONFIGURATION for more information). The virtual host can now only be reached via the binded interfaces.

Example: RequiredBinding = LAN

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

RequireSSL = yes|no

Specify that a domain must be visited with a SSL connection. If it is visited via HTTP, Hiawatha will send a redirect (301) with a HTTPS URL.

Default = no, example: RequireSSL = yes

(requires that Hiawatha was not compiled with --disable-ssl)

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

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. The content of a .hiawatha_index in that directory will be included in the XML.

Default = no, example: ShowIndex = /etc/hiawatha/index.xslt

(requires that Hiawatha was not compiled with --disable-xslt)

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 a HTTP error message or invoke the ErrorHandler when a CGI outputs a Status HTTP header line.

Default = yes, example: TriggerOnCGIstatus = no

UserWebsites = yes|no

Activates user websites for this (virtual) host (the /user/ URL's) (see UserDirectory for more information).

Default = no, example: UserWebsites = 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 = PHP5

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 --disable-toolkit)

UseXSLT = yes|no

Activate XSL transformations (see chapter XSLT for more information).

Default = no, example: UseXSLT = yes

(requires that Hiawatha was not compiled with --disable-xslt)

VolatileObject = <filename with full path>

This file will be completely read into the memory before it is send. Because of this, the file can not be greater than 1MB. Use this option for files that change rapidly, such as webcam pictures.

Example: VolatileObject = /var/www/webcam.gif

WebsiteRoot = <directory>

Rootdirectory for this virtual host.

Example: WebsiteRoot = /home/webmaster/website

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 how to override the configuration for specific directories.

Path = <path|sub-path>

The path to the directory. Path is a required field. Note that only the first Directory record that has a matching Path will be used. If Path ends with a slash (/), Hiawatha will seek anywhere in the path of the requested file for a match. If it does not end with a slash, Hiawatha will start matching from the beginning of the path.

Example: Path = /var/www/cgi-bin or Path = /public_html/

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 mime-type. The uploadspeed per connection will be divided by the number of connections.

Example: UploadSpeed = 20,4

UseGZfile = yes|no

If available, upload <requested file>.gz with gzip content encoding instead of the requested file.

Default = no, example: UseGZfile = yes

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

FASTCGI CONFIGURATION

This chapter explains how to use one or more FastCGI servers. Use the 'php-fcgi' tool to start PHP as a FastCGI daemon.

ConnectTo = <ip-address>:<portnumber>|<path>[, <ip-address>:<portnumber>|<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 FastCGI setting in a virtual host.

Example: FastCGIid = PHP5

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 specifying 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 --disable-toolkit.

Call <toolkit_id>

Execute toolkit section <toolkit_id> and continue in the current section.

Example: Call other_rule_set

Match <regular expression> <action>

Perform an action when the URL matches the regular expression, where <action> can be one of the following:

Ban <seconds>

Ban the client for <seconds> seconds.

Call <toolkit_id>

Execute toolkit section <toolkit_id> and continue in the current section.

DenyAccess

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

Exit

Terminate toolkit processing.

Expire <time> seconds|minutes|hours|days|weeks|months [Exit|Return]

Adds an Expires HTTP header with current timestamp + <time>. The default behaviour is to continue after an Expire action.

Goto <toolkit_id>

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

Redirect <url>

Redirect (301) the browser to the specified URL and terminate toolkit processing.

Return

Return from the current UrlToolkit section.

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).

UseFastCGI <fcgi_id>

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

OldBrowser <url>

If the client uses an old browser (MSIE 5/6), show <url> instead of the requested page.

Example: OldBrowser /ie6.html

RequestURI exists|isfile|isdir Return|Exit

If the requested URL exists on disk, don't continue with the URL toolkit.

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

Skip <number>

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

Example: Skip 2

UseSSL

Perform an action when the client is connection via a SSL secured connection.

Call <toolkit_id>

Execute toolkit section <toolkit_id> and continue in the current section.

Exit

Terminate toolkit processing.

Goto <toolkit_id>

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

Return

Return from the current UrlToolkit section.

Skip <lines>

The original URL is stored in the environment variable `SCRIPT_URL`. 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 = my_toolkit
}

UrlToolkit {
    ToolkitId = fix_PHP
    Match ^/index.php4(.*) DenyAccess
    Match ^/index.php5(.*) Rewrite /index.php$1
}

UrlToolkit {
    ToolkitId = my_toolkit
    Call fix_PHP
    RequestURI isfile Return
    Match ^/(.*) Rewrite /index.php?page=$1
}
```

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_'.

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.

AccessList ,
AlterGroup ,
AlterList ,
AlterMode ,
ErrorHandler ,
LoginMessage ,
PasswordFile ,
RequiredGroup ,
RequireSSL ,
Setenv ,
ShowIndex ,
StartFile and
UseGZfile

MIMETYPES

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

<mimetype> <extension> [<extension> ...]

Example: image/jpeg jpg jpeg jpe

EXTRA

gzip Content-Encoding support

Hiawatha has gzip Content-Encoding support in a unique way. Other web servers with gzip Content-Encoding support will compress a file every time this file is requested, over and over again. Compression is only useful for large files. Since most of the large files on a website are JPEG files and JPEG files are hard to compress, most of the compression done by such web servers is a waste of CPU power.

Hiawatha will do this in a more efficient way. When a file, say file.txt, is requested by a browser with gzip support and the UseGZfile option is set to 'yes', Hiawatha will search for a gzipped version of that file: file.txt.gz. If found, Hiawatha will upload this file instead of the original file.

SIGNALS

TERM Shutdown the web server.

HUP Close all open logfiles.

USR1 Unban all IP addresses.

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

FILES

/usr/sbin/hiawatha

/etc/hiawatha/hiawatha.conf

/etc/hiawatha/mime.types

/etc/hiawatha/cgi-wrapper.conf

/etc/hiawatha/php-fcgi.conf

SEE ALSO

cgi-wrapper(1), php-fcgi(1), newroot(1), ssi-cgi(1), wigwam(1)

AUTHOR

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