Upgrading NCSA httpd

---

httpd 1.3R –> httpd 1.4

The primary focus of release 1.4 of the NCSA httpd server is to improve performance.

Changes from httpd 1.3R

- Two new configuration directives have been added: *StartServers, MaxServers*. Previously, the httpd server forked with each new request To reduce this overhead the NCSA httpd was modified to support a hunt group. A pool of servers (of size _StartServers_) is created initially. As the load increase additional servers are started as needed to the configured maximum (_MaxServers_). These servers remain in the server pool. If additional requests are received, new servers are forked which answer the request, and die in a similar fashion to previous standalone versions of the code. If you don't want to have a pool of servers at all, you can set up StartServers and MaxServers to 0. In this way, httpd's behavior will be similar to previous versions of the code in standalone form.
- Introduced a new mail script: /cgi–bin/mail
  Associated file: /cgi–bin/mail.list
  This PERL script uses the sendmail binary and an authorized list of recipients to generate an email form for the users on your Web server. It should fulfill the mail needs of Web users everywhere currently asking about custom email scripts and mailto: for sending form results: If called directly, it will output a blank form to fill in, and sends the values to itself for mailing.
  If referenced in the ACTION line of a form, it will forward the FORM INPUT to the named recipient.
  Configuration documentation is provided at the top of the script. Official documentation will be available soon.
- Previously each forked child made initialization calls to retrieve information available to the parent. This information is now retrieved by the parent processed once and passed to all child processes.
- Additional performance and memory management improvements internal to the server have been made.
- Several string copies have been modified to prevent buffer overflows. This addresses the problem reported in CERT Advisory CA–95:04. The CERN suggestion of increasing the buffer size was not implemented because we took a different approach. We do not recommend blindly increasing the buffer sizes because this can cause excessive swapping and performance degredation.
- The NCSA httpd 1.4 supports modifiable error messages for the following errors using a new server resource map directive, *ErrorDocument*.

  REDIRECT 302
  BAD_REQUEST 400

AUTH_REQUIRED 401
FORBIDDEN 403
NOT_FOUND 404
SERVER_ERROR 500
NOT_IMPLEMENTED 501

- Two new logs are supported, an agent log and a referral log. The agent log lists the identity of the requesting client. The referral log lists the URL containing the link to the requested document.

  Three new configuration directives have been added: *AgentLog,RefererLog and RefererIgnore*.

---

httpd 1.3 –> httpd 1.3R

Fixed the vulnerablity described in Cert Advisory CA–95:04. For more information, please read the description:
http://hoohoo.ncsa.uiuc.edu/docs/patch_desc.html.

---

httpd 1.2 –> httpd 1.3

httpd 1.3 is a maintenance release designed to fix some of the bugs which were introduced in httpd 1.2.

Changes from httpd 1.2

- Now compiles cleanly under A/UX and Solaris.
- Directory indexing bugs repaired, new options to suppress last modified, size, and description columns (thanks Tanmoy.)
- Wildcard based access control should work this time.
- Fixed core dump related to recursive parsed document include.
- Fixed bug by which httpd would not follow a symbolic link it should have.
- Fixed file typing (no longer case sensitive like in 1.2.)
- Parent directory escaped in indexes.
- IdentityCheck should work again.
- LAST_MODIFIED and #flastmod are now local zone.
- Time related functions work with NeXT now.

- Fixed spelling error in 500 error page.
- Server will log proper timeout message for non−DNS hosts.
- Added x−bit hack for people to use the x−bit of an HTML file to determine if it is parsed or not.
- Added compile defines so people can customize the amount of DNS the server performs (for speed).

---

httpd 1.1 −> httpd 1.2

httpd 1.2 makes some significant changes over httpd 1.1. These changes make its "look and feel" a bit different than 1.1.

New features

- The CGI interface is now revised to version 1.1. See http://hoohoo.ncsa.uiuc.edu/docs/cgi/10to11.html for changes that were made.
- A new logfile format was agreed upon which should simplify the lives of the authors of logfile analyzers. Quickly, the format is:

  ```
  host rfc931 authuser [DD/Mon/YYYY:hh:mm:ss [+/−]HHMM] "request" status bytes
  ```

  Host = hostname

  rfc931 = RFC931 user name if IdentityCheck active, − if not.

  authuser = HTTP/1.0 authenticated user, − if none.

  DD/Mon/YYY:hh:mm:ss [+/−]HHMM: Local time of the request with timezone offset from GMT at end.

  "request" = the request as sent by the client

  status = the HTTP/1.0 status code from this transaction

  bytes = the count of the bytes sent in this transaction, not including the header. If not applicable, this will be a − character.

- CGI scripts are now allowed anywhere. See documentations on tutorials on the new setup (and how it relates to the old setup), and how to disable this feature in places you don’t want it.
- The server side includes interface has been completely rewritten. For more information, please read the documentation on tutorials.

- There is a new access control option to disable symbolic links only if the owner of the pointer is not the same as the owner of that which is pointed to. This means your users can have symbolic links to things they own, but not to dangerous things like /etc.
- A new access control method called mutual−failure has been added. This method is a bit unorthodox, but allows you to allow hosts from one domain while excluding certain hosts (such as public access machines) from that domain.
- Wildcard expressions are now allowed in various areas of server configuration, to allow patterns to be specified. This is most useful in the Directory directive.
- Directory indexing has been revamped. It looks much different, and I've written a short tutorial on how to set it up.
- Access Control Files now allow the indexing directives as well as the DefaultType directive.
- require user now allows quotes for PGP usernames with spaces.
- Server now explicitly kills CGI scripts when the client aborts.
- Server now verifies the DNS hostname it gets from the IP number to prevent PTR spoofs.
- Support for 304 and If−modified−since.

Bug fixes

All of the known bugs in 1.1 have now been fixed. Now it's time to find the ones I introduce with 1.2.

- Fixed problem running scripts in ServerMode inetd under IRIX.
- Fixed bad port problem under OSF/1.
- Inserted missing return statement for the IdentityCheck directive.
- Fixed problem whereby errors would stop being logged after a restart.
- Fixed 256 character limitation on CGI URLs.

---

httpd 1.0 −> httpd 1.1

httpd 1.1 should plug right in if you already have httpd 1.0.

- Introduced experimental PEM/PGP based encrypted user authentication.

- Improved directory indexing.
- Cleaned up error output and fixed horrible output when server−side include error occurred
- Fixed slight bug in buffering code
- Directory indexing for user−supported directories fixed
- Retrieval of user supported directory with no trailing slash issues redirect again
- Now supports RFC931 identd for logging purposes.
- stderr for scripts and server side includes now sent to error_log
- Fixed bug in NCSA POST script code which would cause Location: to be ignored for local files
- Removed misfeature wherein Location: url's were being escaped by the server
- Args to INC SRVURL escaped to avoid unpleasant surprises
- Location: /cgi−bin/foo?arg now works
- HEAD only for CGI scripts now ignores body put out by stupid scripts

---

httpd 1.0a5 −> httpd1.0

httpd 1.0 is fairly similar to httpd 1.0a5.

Changes which directly require configuration changes

- ScriptAlias now used for CGI scripts only, access your NCSA scripts with OldScriptAlias
- Fixed AddType directive
- The NCSA scripts are no longer included, CGI replacements are now included

Other changes

- NCSA POST scripts now have REMOTE_HOST set
- Added AddEncoding directive to srm.conf and .htaccess
- error_log now logs all failed accesses and the reason for failure
- Time headers are now RFC822 compliant
- You can now alias or disable user−supported directories
- Added a require directive to allow you to allow any valid user
- I/O is now buffered into chunks for speed
- Redirect no longer supported from .htaccess files.
- Added −v and −f command line flags

NCSA httpd Development Team
httpd@ncsa.uiuc.edu