HP Secure Web Server for OpenVMS (based on Apache™)
Version 2.2 Release Notes

September 2011

Version 2.2 for OpenVMS Alpha, based on Apache 2.0.63
CPQ-AXPVMS-CSWS-V0202--1.PCSI_SFX_AXPEXE

Version 2.2 for OpenVMS Integrity servers, based on Apache 2.0.63
HP-I64VMS-CSWS-V0202--1.PCSI_SFX_I64EXE

Contents

HP is pleased to provide you with a new HP supported version of *HP Secure Web Server for OpenVMS (based on Apache)*. The Secure Web Server (SWS) includes Secure Sockets Layer (SSL) through mod_ssl and OpenSSL.

Downloading the Kit

The SWS for OpenVMS kit is available for the Alpha and Integrity servers platforms as a compressed self-extracting file.

You can also download the SWS Version 1.3-1, based on Apache 1.3.26, which is an earlier HP supported, customer release version for OpenVMS Alpha and Integrity servers.

Fill and submit the SWS for OpenVMS registration form to download the kit.

For information about expanding and installing the kit, see the *HP Secure Web Server for OpenVMS Installation and Configuration Guide*.

Secure Web Server Documentation

See the Documentation Page for links to the *Installation and Configuration Guide* and the *SSL User Guide* for Version 2.2.

For the SWS Version 1.3-1, documentation and compatible optional kits (CSWS_PERL, CSWS_JAVA, and CSWS_PHP) are also available from the SWS Documentation Page.

Apache Server Documentation

For information about the Apache server, see the Apache HTTP Server documentation.

You can also view the online Apache server documentation at:

http://your.domain/manual

Note: To view some of the Apache server documentation, you must enable MultiViews under `<Directory "/apache$common/htdocs">`.

Bug Fixes in Version 2.2

- Fixed the issue of `modperl` by redirecting the `console` `mode` `stdout` to `/Device/Nul` when the server is starting up, and mirroring the UNIX Multi-Processing Modules (MPM).
- Fixed the issue of `innt_mpm` by recreating the bucket allocator each time the `trans` `pool` is cleared.
- QXCM1000879236: Fixed the issue of case-sensitive comparison in the `configuration` directive.
- QXCM1000903433: Fixed the issue of Lightweight Directory Access Protocol (LDAP) authentication. The modules `mod_auth_kerberos.exe` and `mod_auth_ldap.exe` are not supported in SWS Version 2.1.
- QXCM1000968008: Fixed the issue of `rotatelogs` with `error_log` file.
- QXCM1000976572: Fixed the issue of security audit messages when SWS serve a file located in a user's public directory. This error occurs when the Uniform Resource Locator (URL) accesses a directory through the `UserDir` directive.
- QXCM1001070984: Fixed the issue of Internet Protocol version 6 (IPv6).
- CVE-2009-1891: Fixed the issue of `Denial of Service` or CPU consumption in the `mod_deflate` module.
- CVE-2009-3095: Fixed the issue of access restriction bypass in the `mod_proxy_ftp` module.
- CVE-2009-3555: Fixed the issue of renegotiation handshakes with an existing connection.

Note: The SWS_APACHE Version 2.2 is not vulnerable to the following CVEs: (CVE-2008-2364, CVE-2009-2412, CVE-2009-3560, CVE-2009-3720, CVE-2010-0425, CVE-2010-0434, CVE-2010-1452, CVE-2010-1623).

New Features in Version 2.2

- Based on Apache 2.0.63 from the Apache Software Foundation
- Apache 2.2 is built using the OpenSSL Version 0.9.8h

Changed Features in Version 2.2

- Changes required in `httpd.conf` when upgrading from Version 1.3-1 to Version 2.2

  In SWS Version 2.2, many loadable modules are no longer loaded by default. You must uncomment the modules in `httpd.conf` to load them. See the file `httpd-vms.conf` to load other modules.

  For example, to load the modules, uncomment the following lines in `httpd.conf`:

  ```
  LoadModule osuscript_module modules/mod_osuscript.exe
  LoadModule dav_module modules/mod_dav.exe
  LoadModule dav_fs_module modules/mod_dav_fs.exe
  ```

  The OpenVMS platform supports the following list of modules:

  - AAA
  - Cache
  - Dav
  - Echo
  - Experimental
  - Filters
  - Generators
  - HTTP
  - Loggers
  - Mappers
  - Metadata
  - Proxy
  - SSL

- New directives

  The following **new** directives are included in Version 2.x:

  ```
  AcceptMutex vmsdlm
  VMSServerTag SWS
  VMSServerStartup "/apache$root/000000/apache$startup.com"
  VMSServerShutdown "/apache$root/000000/apache$shutdown.com"
  EnableMMAP on/off
  EnableSendFile on/off
  ```

  Note: In Version 2.2 and Version 2.1, by default, EnableMMAP is set to OFF. In Version 2.0, EnableMMAP was set to ON by default.

- Obsolete directives

  The following are **obsolete** directives in Version 2.x:

  ```
  ServerType
  Port
  ```

- Changed server process naming scheme

  In Version 2.x, SWS uses a new server process naming scheme in which *xxx* is defined by the `VMSServerTag` directive in `httpd.conf`. For example:

  ```
  APACHE$xxx
  APACHE$xxx0000
  APACHE$xxx0001
  ```

  The old naming scheme (in SWS Version 1.3-1 and earlier) *xx* was defined by `SERVER_TAG` in `SYS$MANAGER:APACHE$CONFIG.DAT` via `APACHE$CONFIG.COM`.
  For example:

  ```
  APACHE$xx
  APACHE$xx000
  APACHE$xx001
  ```

- Changed site-specific startup and shutdown procedure definitions

  In Version 2.x, new startup and shutdown procedure definitions are defined by the `VMSServerStartup` and `VMSServerShutdown` directives in `httpd.conf`.

The old definitions (in SWS Version 1.3-1 and earlier) were defined by the `SERVER_STARTUP` and `SERVER_SHUTDOWN` directives in `SYS$MANAGER:APACHE$CONFIG.DAT` via `APACHE$CONFIG.COM`.

Known Problems and Restrictions in Version 2.2

- Do not use SWS Version 2.2 with older SWS optional kits

  Do not use SWS Version 2.2 with the following optional kits. Using these kits together causes a process crash. These kits, in addition to the newer optional kits, are currently available for download from http://h71000.www7.hp.com/openvms/products/ips/apache/csws.html.

  - PERL for OpenVMS 5.6.1 and 5.6.1-1A1
  - CSWS_PERL V2.0, 1.1, and 1.1-1
  - CSWS_PHP V1.2-1 and 1.1
  - CSWS_JAVA V2.1

  SWS Version 2.2 **works properly** with the following **new** optional kits:

  - PERL for OpenVMS 5.8.6
  - CSWS_PERL V2.1
  - CSWS_PHP V1.3 and higher
  - CSWS_JAVA V3.0 and higher

- Installing SWS Version 2.2 on an ODS-2 volume corrupts the previous SWS Version 1.3 installation

  You must install the SWS Version 2.2 kit only on an ODS-5 target volume. If you install this kit on an ODS-2 volume, the installation will fail with the following error:

  ```
  Destination disk is not ODS-5, aborting installation ...
  %PCSI-I-PRCOUTPUT, output from subprocess follows ...
  %SYSTEM-F-ABORT, abort
  ```

  If your existing installation is SWS Version 1.3, then the failed operation will leave it in a corrupt state.

- Language variant filename restriction

  Specify language variants on an OpenVMS system in the same way as you do on a UNIX system, using multiple dots in the filename. For example, the French variant of a filename is *filename.html.fr*.

  In the earlier versions of SWS, you could use an underscore instead of a dot before the language extension (for example, *filename.html_fr*).

- WebDAV database manager type restriction

  WebDAV support requires the VDBM database manager type. VDBM is the default.

  To change the database manager type, set the logical name `APACHE$DAV_DBM_TYPE` so that it is visible to Apache, as `APACHE$COMMON:[000000]LOGIN.COM`.

  Note: SDBM and GDBM are not supported in this release.

- SSLSessionCache DBM file error

  Either of the SDBM or GDBM database manager types, when used, causes the following SSL session cache failure:

```
[Thu Apr 14 16:25:12 2005] [error] (2)no such file or
directory: Cannot create SSLSessionCache DBM file
`/apache$root/000000/logs/ssl_scache'
```

You must use the default VDBM database manager type. To change the database manager type, set the logical name `APACHE$SSL_DBM_TYPE` so that it is visible to Apache, as `APACHE$COMMON:[000000]LOGIN.COM`.

Note: SDBM and GDBM are not supported in this release.

- If suEXEC is enabled in the initial configuration, SWS cannot add a node in a cluster environment

  If you enable suEXEC during the initial configuration of SWS or by using Option 4 (Manage suEXEC users) from the SWS Configuration Menu, then Option 10 of the SWS configuration menu (Add a node to CSWS in a cluster environment) fails.

  As a temporary workaround, use Option 4 to disable suEXEC and use Option 10 to add the node, and then use Option 4 to re-enable suEXEC.

- Problems with `APACHE$MENU.COM` "Create an Apache instance" Option 2

  Option 2 in `APACHE$MENU.COM`, called Create an Apache instance, fails under the following circumstances:

  - Specifying a nonexistent target directory fails with the following error when the directory `[.FOO]` does not exist.

    ```
    Root Location: dev:[APACHE.SPECIFIC.FOO]
    %SYSTEM-W-NOSUCHFILE, no such file \_DKA0:[APACHE.SPECIFIC]FOO.DIR\
    %DCL-W-UNDSYM, undefined symbol - check validity and spelling \INDID\
    %DCL-W-UNDSYM, undefined symbol - check validity and spelling \INDID\
    ```

  - Creating an instance under a name other than `APACHE$WWW` fails with the following error:

    ```
    [Tue Apr 19 11:20:23 2005] [error] (13)permission denied: Unable to
    create input file dev:[directory.[000000]APACHE$xyz.COM
    ```

- Cached files not served

  The proxy cache feature does not serve the cached files in SWS Version 2.2.

- AuthUserFile/AuthGroupFile Override AuthOpenVMSUser/AuthOpenVMSGroup

  If the `mod_auth` directives `AuthUserFile` and `AuthGroupFile` are combined with the `mod_auth_openvms` directives `AuthOpenVMSUser` and `AuthOpenVMSGroup`, the `mod_auth` directives override `mod_auth_openvms`.

  In practice, these sets of directives are not commonly used together.

- `Require user` directive must specify user names in uppercase with `mod_auth_openvms`

  The `Require user` directive must specify user names in uppercase when used with `mod_auth_openvms`.

- ApacheBench tool fails (Integrity servers only)

  On OpenVMS Integrity servers, the ApacheBench tool fails as follows:

  ```
  Test aborted after 10 failures
  apr_connect(): socket is already connected
  (56) %SYSTEM-W-BADESCAPE, syntax
  error in escape sequence
  ```

Documentation Errata

The following section describes the documentation updates and errata for HP Secure Web Server for OpenVMS (based on Apache*)* documentation.

In the *HP Secure Web Server Based on Apache SSL User Guide* the following changes should be made to these sections:

- **Configuration Options**

  To enable SSL:

  1. Generate a self signed certificate, which is valid for 30 days. To do so, use the following certificate tool:

     ```
     $ @APACHE$COMMON:[OPENSSL.COM]OPENSSL_AUTO_CERT.COM
     ```

  2. Uncomment the following directive in the `APACHE$COMMON:[CONF]HTTPD.CONF` file:

     ```
     Include /apache$root/conf/ssl.conf
     ```

- **Disabling SSL**

  To disable SSL, comment the following directive in the `APACHE$COMMON:[CONF]HTTPD.CONF` file:

  ```
  Include /apache$root/conf/ssl.conf
  ```