



Apache unter OpenVMS


warum und wie
2C01

Clemens Wermelskirchen
Stanford University

Hans Bachner
Hewlett-Packard



© 2004 Hewlett-Packard Development Company, L.P.
The information contained herein is subject to change without notice



Inhalt

- Apache – Überblick und Entstehung
- HP Secure Web Server
- Optionale Module
- Ausblick
- Installation
- Konfiguration des Servers
- Sicherheit
- Was – wozu – wie?
- Information, Links, Literatur

IT-Symposium 2005 www.decus.de 2

Apache –

Überblick und Entstehung



Apache - Entstehung

- basiert auf NCSA ([U.S.] National Center for Supercomputing Applications) HTTPd Projekt
- Projekt wurde von der U.S. Regierung finanziert, daher war HTTPd in der Public Domain (1994)
- basierend auf NCSA HTTPd 1.3 wurde eine Open Source Entwicklungs-Umgebung aufgesetzt
- erste Beiträge in Form von Patches für den NCSA HTTPd
- 1995 wurde der erste "patchy" Server freigegeben
- "a patchy Server" ⇒ "Apache Server"
- wurde inzwischen völlig neu geschrieben



Apache - Entstehung

- die beteiligten Personen bildeten im Februar 1995 "The Apache Group"
 - inzwischen "Apache Software Foundation"
 - <http://www.apache.org/>
- die Apache Software Foundation betreibt und unterstützt auch zahlreiche andere Projekte
 - SOAP, Xerces (XML), Jakarta, TOMCAT (JSP), ...
- viele Erweiterungen / Verbesserungen sind inzwischen verfügbar
 - Perl, PHP, JServ, JSSI, ...



Apache HTTP Server

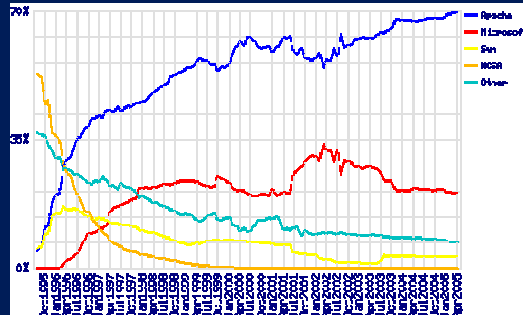
- HTTP/1.1 (RFC2616) compliant
- vielfältig konfigurierbar, erweiterbar
- Anpassungen / Erweiterungen möglich durch Apache module API
- vollständiger Quellcode frei erhältlich
- läuft auf OpenVMS, Windows, UNIX, Mac OS und anderen Betriebssystemen
- Aktive Weiterentwicklung



Apache HTTP Server

- seit März 1996 der meist verwendete Webserver im Internet

- aktuell:
Apache 69.32%
MS IIS 20.45%
(April 2005)



- http://news.netcraft.com/archives/web_server_survey.html

HP Secure Webserver
(SWS)

HP Secure Webserver für OpenVMS (SWS)



- Basis: aktuelle Apache-Baselevels
- Anpassungen für:
 - OpenVMS Security Architektur
 - OpenVMS Cluster Architektur
- SSL Unterstützung (zertifikatsgestützte verschlüsselte Datenübertragung)
- von Verisign unterstützte Plattform
 - <http://www.verisign.com/support/install/>
- verschiedene Skripting-Möglichkeiten (CGI, Java, Perl, PHP)

IT-Symposium 2005

www.decus.de

9

HP Secure Webserver für OpenVMS (SWS)



- SWS Quellcode verfügbar (dzt. nur für 1.3)
- OpenVMS Website (<http://h71000.www7.hp.com/>) läuft mit SWS
- wird von Netcraft (<http://news.netcraft.com>) auch korrekt erkannt („What's that site running?...“):
OS ... OpenVMS
- Beiträge aus der User-Community:
 - ht://Dig
 - Python
 - SWISH-E

IT-Symposium 2005

www.decus.de

10



SWS Releases für OpenVMS

- CSWS V1.0 – Apache V1.3.12 (Okt. 2000)
- ...
- SWS V1.3-1 – Apache V1.3.26 (Feb. 2005)
 - OpenVMS Alpha ab V7.3-1 (mit ACRTL-Patch), V8.2
 - OpenVMS I64 V8.2
- SWS V2.0 – Apache V2.0.47 (Okt. 2003)
 - OpenVMS Alpha ab V7.3-1 (mit ACRTL-Patch); läuft nicht unter V8.2
 - erfordert STREAM_LF Attribut für alle Dateien

IT-Symposium 2005

www.decus.de

11



Apache Module (Stand: SWS V1.3)

- Standard Apache Module
 - mod_access, mod_actions, mod_alias, mod_asis, mod_auth, mod_autoindex, mod_cgi, mod_define, mod_dir, mod_env, mod_imap, mod_include, mod_info, mod_log_config, mod_mime, mod_negotiation, mod_proxy, mod_rewrite, mod_setenvif, mod_so, mod_ssl (DSO), mod_status, mod_unique_id, mod_userdir
- OpenVMS-spezifische Module
 - mod_auth_openvms (DSO), mod_osuscript
- optionale Module
 - mod_jk, mod_jserv, mod_perl, mod_php, mod_DAV
 - als DSO implementiert (Dynamic Shared Object, in OpenVMS: shareable image)
- von Benutzern erstellte Module (ohne Support durch HP)
 - mod_put, mod_python etc.

IT-Symposium 2005

www.decus.de

12



Apache Module

- welche Module sind aktiv?
 - \$ mc apache\$root:[000000]apache_httpd.exe_alpha -l
 - \$ mc apache\$root:[000000]apache_httpd.exe -l
 - ab V1.3-1
- und wie konfiguriert?
 - <http://meinserver/server-info>
- genaue Liste der implementierten Module und Direktiven im „SWS Installation and Configuration Guide“

IT-Symposium 2005

www.decus.de

13



SWS Releases für OpenVMS

- SWS V1.3(-1)
 - suEXEC Unterstützung
 - Implementierung über OpenVMS Rights Identifier anstatt uidmin/gidmin Restriktionen
 - WebDAV
 - Distributed Authoring & Versioning
 - „poor man's Pathworks“
 - OpenSSL 0.9.6b
 - Verbesserungen in MOD_AUTH_OPENVMS
 - „require group“ über Rights Identifier implementiert
 - neue Konfigurations-/Administrations Optionen
 - V1.3-1:
 - Unterstützung für OpenVMS V8.2 Alpha und I64
 - aktuelle Security-Patches

IT-Symposium 2005

www.decus.de

14



SWS Releases für OpenVMS

- SWS V2.0
 - implementiert das „pre-fork“ Modell
 - „multi-threaded“ Modell derzeit nicht
 - hier identisch zu SWS V1.3
 - unterstützt IPv6 (zusätzlich zu IPv4)
 - Voraussetzungen:
 - ODS-5
 - OpenVMS Alpha V7.3-1, V7.3-2
 - TCP/IP 5.3 (oder Multinet, TCPWare)
 - erfordert Stream-LF Format für alle beteiligten Dateien (noch...)

Optionale Module



CSWS_JAVA (Tomcat)

- CSWS_JAVA V2.1
 - basiert auf Tomcat/Catalina V4.1.24
 - implementiert JSP V1.2, Servlet V2.3, Ant (teilweise)
 - Alpha:
 - OpenVMS V7.3-1, V7.3-2, V8.2
 - Java V1.3.1 oder neuer
 - OpenVMS-Patches für Java! siehe Release Notes
 - I64:
 - OpenVMS V8.2
 - Java V1.4.2
 - unterstützt auch Anwendungen für Tomvac V3.x

IT-Symposium 2005

www.decus.de

17



CSWS_PHP

- CSWS_PHP V1.2-1
 - basiert auf PHP 4.3.2
 - Alpha:
 - OpenVMS V7.3-1, V7.3-2, V8.2
 - SWS V1.3 (min), V2.0
 - I64:
 - OpenVMS V8.2
 - SWS V1.3-1
 - mit MySQL Erweiterung
 - mit OpenVMS Erweiterung (Filenam-Konvertierung, getjpi, getsyi, getdvi, ...)
 - SSL-Unterstützung auf Basis OpenSSL 0.9.7D (SSL V1.2 for OpenVMS)

IT-Symposium 2005

www.decus.de

18



Perl für OpenVMS

- Perl für OpenVMS 5.6.1 für OpenVMS Alpha
 - OpenVMS Alpha V7.2-1
 - Perl 5.6.1 ECO 3 (Link in den CSWS_PERL Release Notes!): OpenVMS Alpha V7.2-2
- Perl für OpenVMS 5.6.1-1A1 für OpenVMS I64
 - OpenVMS I64 V8.2
 - basiert auf Perl 5.6.1 ECO 3



CSWS_PERL

- V1.1 (mod_perl 1.25)
 - OpenVMS Alpha V7.3-1 und höher (einschl. V8.2)
 - SWS 1.2 und höher
 - Perl 5.6.1
- V1.1-1 (mod_perl 1.25)
 - OpenVMS I64 V8.2
 - SWS 1.3-1
 - Perl 5.6.1-1A1
- V2.0 (mod_perl 2.0 build 1.99.09)
 - OpenVMS Alpha V7.3-1 und höher (nicht V8.2)
 - SWS 2.0
 - Perl 5.6.1 ECO 3

Ausblick

SWS wie geht's weiter?



- OpenVMS Alpha V7.3-2, V8.2, I64 V8.2
- SWS 2.1
 - basierend auf Apache 2.0.52
 - Stream_LF Restriktion kann optional aufgehoben werden (Performance-Einbuße!)
 - geplantes Erscheinen um die Jahresmitte
- voraussichtlich in der zweiten Jahreshälfte:
 - CSWS_JAVA – basierend auf Tomcat 5.5
 - CSWS_PHP – basierend auf PHP 4.3.10
 - CSWS_PERL – basierend auf mod_perl 2.0 (für SWS 2.*)
 - Perl 5.8.6

Installation

Kits



- Download-Links für SWS und optionale Module auf <http://h71000.www7.hp.com/openvms/products/ips/apache/cswws.html>
 - oder <http://www.hp.com/go/openvms>
Abschnitt „OpenVMS Solutions“
 - Link „E-business and integration“
 - Tab „Technology“
 - Links im Abschnitt „Web servers“
- aktuelle Patches (Sicherheit, funktional) auf http://h71000...com/openvms/products/ips/apache/cswws_patches.html
 - auch für frühere Versionen



Installation

- Kits entpacken, z.B.
`$ RUN CPQ-AXPVMS-CSWS-V0103-1-1.PCSI_SFX_AXPEXE`
- Standard Installation:
`$ PROD INST CSWS /DEST=device:[directory-name]`
 - vorzugsweise auf ODS-5 Platte (erforderlich für SWS 2.0, CSWS_JAVA u.a.)
- Konfiguration:
`$ @SYS$MANAGER:APACHE$CONFIG`
 - legt APACHE\$WWW Account an (optional anderer Account)
 - definiert (systemweite) logische Namen
 - aktiviert optional MOD_SSL, MOD_suEXEC
 - setzt korrekte Owner und Zugriffsrechte unter APACHE\$ROOT

IT-Symposium 2005

www.decus.de

25



Installation testen

- am Terminal:
`$ telnet localhost 80`
`HEAD / HTTP/1.0` (2mal Return drücken)
`HTTP/1.1 200 OK`
`Date: Fri, 01 Apr 2005 19:33:56 GMT`
`Server: Apache/1.3.26 (OpenVMS)`
...
- im Browser:
<http://localhost/> bzw.
<http://<servername>/>

IT-Symposium 2005

www.decus.de

26



Konfiguration

- `apache$root:[conf]httpd.conf` (Textdatei)
 - Konfiguration des Servers und der virtuellen Hosts
 - Laden und Konfiguration zusätzlicher Module
 - Definition von Dokument-Typen und -Handlern
 - Definition der Dokument-Verzeichnisse und Zugriffsbeschränkungen
 - Definition von Logfiles and deren Formaten
 - sinnvoll: eigene Konfigurationsdateien für zusätzliche Module
 - `Include /apache$root/conf/mod_perl.conf`
- Änderungen erfordern einen Neustart
 - `$ @sys$startup:apache$startup graceful`

IT-Symposium 2005

www.decus.de

27



Online Dokumentation

- Beschreibung der Konfigurations-Direktiven in <http://meinserver/manual>
- ausführliche Kommentare in `httpd.conf`
- mehr Details auf <http://httpd.apache.org/docs/> bzw. <http://httpd.apache.org/docs-2.0/>

IT-Symposium 2005

www.decus.de

28



Upgrade

- (shareable) Images hießen bisher xxx.EXE_ALPHA
- ab SWS V1.3-1 fällt der Architektur-Postfix weg:
xxx.EXE
- das gilt auch für DSO-Module
(z.B. mod_ssl.exe_alpha, mod_webdav.exe_alpha,
mod_auth_openvms.exe_alpha)
- beim Upgrade: Konfigurationsdateien entsprechend
anpassen!

Sicherheit



Sicherheit

- Server und Scripts laufen standardmäßig unter einem nicht-privilegierten Account (APACHE\$WWW)
 - auch der Start erfolgt unter diesem Account
 - unter UNIX laufen Teile des Codes unter root
- Funktionen, die Privilegien benötigen, sind als „user-written system services“ implementiert
 - Öffnen von Port 80, auth_openvms, ...
 - Zugriff auf diese Services konfigurierbar limitiert
- SSL erlaubt mächtige Authentifizierung und Verschlüsselung

IT-Symposium 2005

www.decus.de

31



Sicherheit

- ein Webserver öffnet ein System gegenüber dem Netzwerk – das ist auch sein Zweck
- der Schaden durch Sicherheitslücken kann vernachlässigbar, aber auch existenzbedrohend sein
- Sicherheitslücken entstehen durch Softwarefehler (steigende Komplexität – mehr potentielle Fehler) oder durch Konfigurationsfehler
- zusätzliche Module (Java, Perl, PHP) und freigeschaltete Funktionen (CGI) erhöhen das Risiko

IT-Symposium 2005

www.decus.de

32



Sicherheit

- daher:
Funktionen/Module nur aktivieren, wenn sie auch
gebraucht werden!
- OpenVMS bietet aufgrund der integralen
Sicherheits-Architektur optimale Voraussetzungen
 - extrem wenige Lücken, die überhaupt ausgenützt werden
können

Was – wozu – wie?

Ein „Mini-HowTo“

DCL CGI

- Standard ScriptAlias (CGI-Verzeichnis) ist `apache$root:[cgi-bin]`
- enthält zwei Beispiele (.COM, .EXE)
- simples Beispiel:

```
$ set noon
$ write sys$output f$fa0("!AS!!/!", "Content-type: text/plain")
$ show system /interactive
$ exit
```
- wichtig: nach dem Response-Header **zwei** „new line“ Sequenzen erzeugen (hier: `!/` für `f$fa0`, `\n` in Perl oder C, ...), dann erst mit dem Response-Body beginnen

mod_auth_openvms

- verwendet Benutzernamen/Passwort im SYSUAF.DAT zur Authentifizierung
- verwendet group UIC und rights identifiers zur Erkennung von Gruppen-Zugehörigkeit („require group“ Direktive)
- Einschränkung auf bestimmte SYSUAF-Benutzer möglich: Rights Identifier
`APACHE$MOD_AUTH_OPENVMS_ENABLE`
- alternativ: bestimmte SYSUAF-Benutzer ausschließen: Rights Identifier
`APACHE$MOD_AUTH_OPENVMS_DISABLE`



mod_auth_openvms

```
<Directory "/apache$common/htdocs">  
  AuthType Basic  
  AuthName "OpenVMS authentication"  
  AuthOpenVMSUser On  
  require valid-user  
  Options Indexes FollowSymLinks Multiviews  
  AllowOverride None  
  #  
  # Auth* Direktiven können auch in .htaccess files für Verzeichnis-  
  # spezifische Definitionen stehen, wenn „AllowOverride AuthConfig“  
  # angegeben wird  
</Directory>
```



mod_info

- zeigt aktuelle Server-Konfiguration an
- Zugangsbeschränkung definieren!
 - vor allem, wenn der Server öffentlich zugänglich ist
- in httpd.conf:

```
<Location /server-info>  
  SetHandler server-info  
  Order deny,allow  
  Deny from all  
  Allow from .meine-domain.at  
  # Allow from 172.16  
</Location>
```



mod_status

- zeigt aktuellen Server-Zustand an
- Zugangsbeschränkung definieren!
 - vor allem, wenn der Server öffentlich zugänglich ist
- in httpd.conf:

```
<Location /server-status>  
    SetHandler server-status  
    Order deny,allow  
    Deny from all  
    Allow from .meine-domain.at  
    # Allow from 172.16  
</Location>  
ExtendedStatus On           # Off
```

IT-Symposium 2005

www.decus.de

39



mod_dav

- DAV - Distributed Authoring and Versioning
 - (RFC 2518)
- erlaubt (gemeinsamen, auch schreibenden) Zugriff auf Dateien auf einem Server mit DAV-fähigen Anwendungen / Clients
 - http://www.webdav.org/mod_dav
- Ordner erscheinen im Windows Explorer als Web-Ordner
- kann zur Pflege der Webinhalte verwendet werden (einfacher Zugriff auf Webdokumente) oder einfach als gemeinsam genutzte Dateiablage
 - Sicherheitseinstellungen beachten!

IT-Symposium 2005

www.decus.de

40



mod_dav Setup

- Verzeichnis anlegen
 - `$ create /dir /own=apache$www -`
`_ $ apache$common:[projekt]`
- httpd.conf erweitern
 - Module laden
 - `LoadModule dav_module modules/mod_dav.exe`
 - `LoadModule dav_fs_module modules/mod_dav_fs.exe`
 - Locking Database definieren
 - `DAVLockDB /apache$common/projekt/lock.db`
 - Alias definieren
 - `Alias /projekt "/apache$common/projekt"`

IT-Symposium 2005

www.decus.de

41



mod_dav Setup (2)

- httpd.conf erweitern (2)
 - Location definieren
 - `<Location /projekt>`
 - `AuthType Basic`
 - `AuthName "OpenVMS authentication"`
 - `AuthOpenVMSUser On`
 - `require valid-user`
 - `AllowOverride None`
 - `DAV On`
 - `Options Indexes`
 - `Order allow,deny`
 - `#Beispiel – nur Lesezugriff für alle authentifizierten Benutzer`
 - `Allow from all`
 - `<LimitExcept GET HEAD OPTIONS>`
 - `require user webadmin`
 - `</Limit>`
 - `require valid-user`
 - `</Location>`

IT-Symposium 2005

www.decus.de

42



mod_dav

- Zugriff über Internet Explorer:
 - Datei / Öffnen...
 - „Als Webordner öffnen“ anhängen
 - URL des DAV Ordners eingeben
 - in unserem Beispiel: <http://meinserver/projekt>
 - Internet Explorer zeigt den Inhalt des DAV Ordners an
 - Windows Explorer zeigt den DAV Ordner in einem „Webordner“ Ordner an
 - kann wie ein (Netzwerk-) Laufwerk benutzt werden



mod_gzip

- komprimiert Server Response vor der Übertragung zum Browser
- Reduktion des Transfervolumens bei reinen Textseiten zwischen 50% und 80% realistisch
- ist nicht Teil von SWS
- derzeit nur für Apache 1.3.x (mod_deflate für 2.0.x)
- Download von <http://sourceforge.net/projects/mod-gzip/>
- entpacken, übersetzen, shareable Image links
 - Anleitung im SWS Installation and Configuration Guide
- Image nach apache\$commons:[modules] kopieren



mod_gzip Konfiguration

- httpd.conf
 - Include /apache\$root/conf/mod_gzip.conf
- mod_gzip.conf
 - Beispielkonfiguration wird im Downloadpaket mitgeliefert
 - muss gegebenenfalls angepasst/ergänzt werden
 - mod_gzip_minimum_file_size, mod_gzip_maximum_file_size,
 - mod_gzip_maximum_inmem_size
 - gelegentliche Probleme mit PDF-Plugin in Internet Explorer
 - mod_gzip_item_exclude file \.pdf\$
 - mod_gzip_item_exclude mime ^application/pdf\$
 - Erweiterungen für Tomcat / Struts
 - mod_gzip_item_include file \.jsp;
 - mod_gzip_item_include file \.do;

IT-Symposium 2005

www.decus.de

45



mod_gzip und mod_ssl

- mod_ssl klinkt sich offenbar zu früh in die Ausgabe des Webservers ein
 - Symptom - Meldungen im error_log
 - mod_gzip: EMPTY FILE [/tmp/_547372588_99_0.wrk] in sendfile2
 - mod_gzip: Make sure all named directories exist and have the correct permissions.
 - Workaround:
 - virtueller Host für alle SSL-Requests (port 443) ohne mod_gzip
 - leitet per Proxy alles weiter an einen anderen virtuellen Host
 - in diesem erfolgt die eigentliche Verarbeitung einschließlich Komprimierung der Server-Response

IT-Symposium 2005

www.decus.de

46



mod_gzip und mod_ssl (2)

- Konfiguration:
 - httpd.conf

```
ProxyRequests On
Listen 4430
<VirtualHost _default_:4430>
  <Directory />
    order deny,allow
    deny from all
    allow from 127.0.0.1
  </Directory>
</VirtualHost>
```



mod_gzip und mod_ssl (3)

- Konfiguration:
 - mod_ssl.conf

```
<VirtualHost *:443>
ProxyRequests Off
ProxyPass / http://localhost:4430/
ProxyPassReverse / http://localhost:4430/
mod_gzip_on No
SSLEngine on
# restliche SSL-Konfiguration folgt hier
SSLCipherSuite ...
SSLCertificateFile ...
SSLCertificateKeyFile ...
...
</VirtualHost>
```


Links – Literatur – Information

Links



- SWS Website
 - http://h71000.www7.hp.com/openvms/products/ips/_apache/csws.html
- Patches für SWS & Co.
 - http://h71000.www7.hp.com/openvms/products/ips/_apache/csws_patches.html
- Dokumentation für SWS & Co.
 - http://h71000.www7.hp.com/openvms/products/ips/_apache/csws_doc.html
- OpenVMS eBusiness Technologien
 - <http://h71000.www7.hp.com/ebusiness/technology.html>

Links (2)

- Apache Software Foundation
 - <http://www.apache.org/>
- Tomcat (CSWS_JAVA)
 - <http://jakarta.apache.org/tomcat>
- WebDAV
 - http://www.webdav.org/mod_dav
- mod_gzip
 - <http://sourceforge.net/projects/mod-gzip/>

Literatur

- **Apache Server Bible**, Mohammed J. Kabir, 1998, IDG Books
- **Apache Server 2 Bible**, Mohammed J. Kabir, 2. Aufl. 2002, IDG Books
- **Apache Server Unleashed**, Rich Bowen and Ken Coar, 2000, SAMS
- **Apache, The Definitive Guide**, Ben Laurie and Peter Laurie, 3. Aufl. 2002, O'Reilly
- **Apache Administrator Handbook**, Rich Bowen, 2002, Sams
- **OpenVMS with Apache, OSU, and WASD**, Alan Winston, 2003, Digital Press
- **SSL and TLS, Designing and Building Secure Systems**, Eric Rescorla, 2000, Addison-Wesley

- HTTP 1.1 protocol specification, <http://www.ietf.org/rfc/rfc2616.txt>, Updates in RFC 2817
- TLS 1.0 (SSL 3.0) protocol specification, <http://www.ietf.org/rfc/rfc2246.txt>, Updates in RFC 3546
- HTML 4.01 specification, <http://www.w3.org/TR/html4/>



Information

- SWS Support durch HP (im Standard OpenVMS Support inkludiert)
 - einschließlich der von OpenVMS Engineering portierten Zusatzmodule CSWS_JAVA, CSWS_PHP, ...
- Open Source Community
 - Mailinglisten für die meisten Projekte
- Usenet – Newsgroups
 - alt.apache.configuration
 - comp.infosystems.www.servers.*
- Google 😊
- weitere Fragen? Mail an Hans.Bachner@hp.com

IT-Symposium 2005

www.decus.de

53

