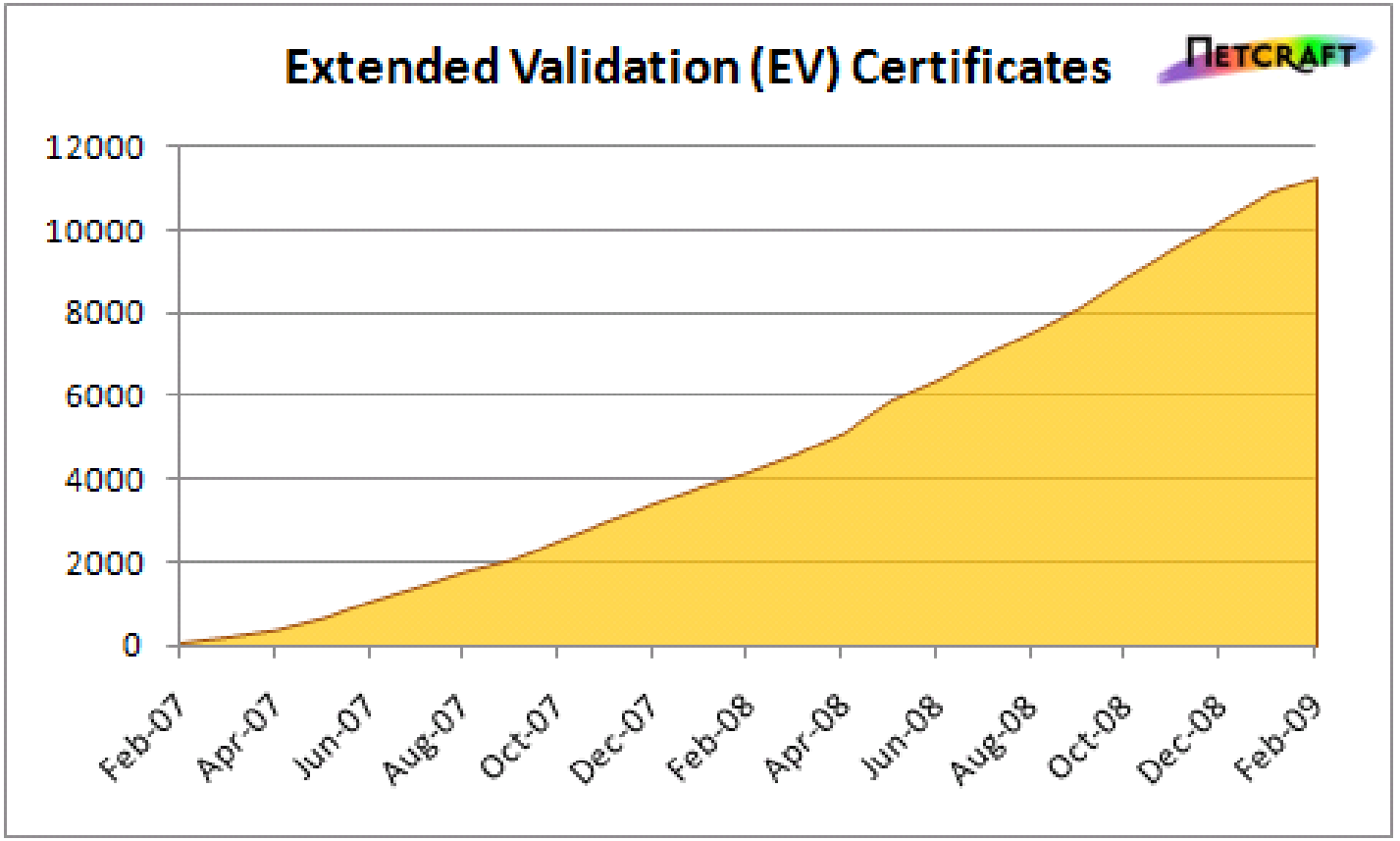
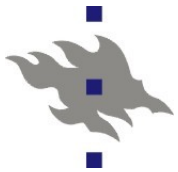
Netcraft: EVC-tilasto

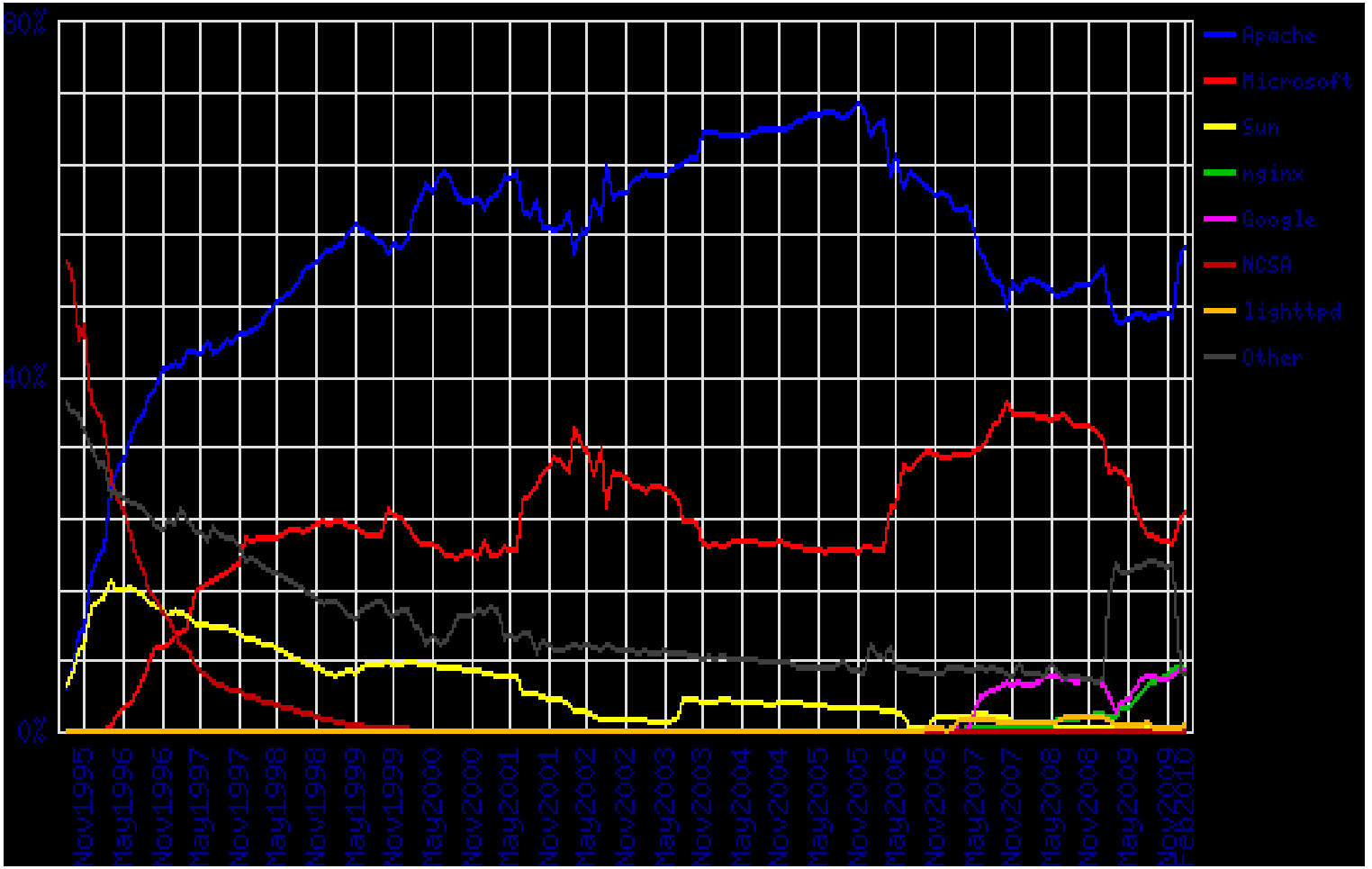




Apache

- Apache on edelleen maailman käytetyin http-palvelin
  - IIS:n ”markkinaosuus” tosin on kasvanut
- Apache on Linuxin rinnalla menestynein OS-ohjelma
- Apache on “ilmainen”
  - Maailmalla on paljon harrastelijoiden apache-asennuksia tai vain unohtuneita palvelimia, joita kukaan ei enää ylläpidä
- Apachella on pitkä historia takanaan
  - Apache projekti perustettiin 1995 jatkamaan NCSA httpd:n kehitystä
- Apache on ”valmis”.
  - Jo apache-1.3 toteutti kaikki http/1.1:n ominaisuudet
- Apache ei ole sovellusalusta
  - Apache tarjoaa vain http-palvelun, ei ohjelmointiympäristöä www-sovellusten toteuttamiseen

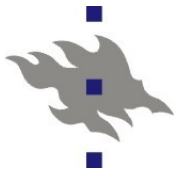
Netcraft: WWW-palvelimet



Päivän harjoitustehtävä

- Miten konfiguroidaan Apachella laitoksen ”intranet”-viritys? Ei tarvitse kokeilla tai oikeasti asentaa apachea, hyvä arvaus apachen konfiguraatiotiedostoon lisättävistä riveistä riittää.

1. Tutustu Apache 2.x:n manuaaliin osoitteessa http://httpd.apache.org/docs/2.2/
2. Miten asetat Apachella seuraavat pääsyrajoitukset hakemistopolun */home/*/intranet* alta tarjoiltaville tiedostoille:
   a. Vaaditaan SSL/TLS-kryptattu yhteys
   b. Vaaditaan autentikointi http basic-autentikoinnilla, eli validi käyttäjätunnus ja salasana. Käyttäjät ja salasanat löytyvät tiedostosta /etc/wwwusers



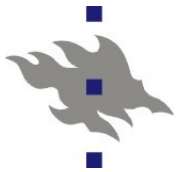
Jatkoa päivän harjoitustehtävään

3. Oletetaan että kaikkien käyttäjien kotihakemistopolut ovat muotoa */home/<luser>/*
   Miten konfiguroit Apachen palauttamaan muotoa *http://serveri/i/luser/foo.html* olevasta URL:ista tiedoston */home/luser/intranet/foo.html* ?

- Tehtävä 2 vaatii laitoksen www-serverillä 7 rivin verran apachen konfigurointia.
- Tehtävä 3 vaatii laitoksen www-serverillä 2 rivin verran apachen konfigurointia

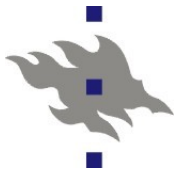
Miksi Apache?

- Riittävän tehokas
- Täydellinen http-tuki
  - Tuki myös ominaisuuksille, joita kukaan ei käytä
- Skaalautuva
  - Apache hyötyy moniprosessoriarkkitehtuureista
  - Apachen proxy-tuella mahdollista myös kuormanjako ja generoitujen sivujen talletus välimuistiin
- Modulaarisuus
  - Varsinaiset www-sovellusympäristöt ovat apache-projektin ulkopuolisia ja usein toteutettu apachen moduleilla
    - php, python, perl, ruby
  - Jopa jonkinlainen asp-tuki ja asp.net tuki löytyy
- SSL/TLS-tuki
  - aina tämä ei ole ollut helposti saatavilla
- Apache on hyvin dokumentoitu
  - http://httpd.apache.org/docs



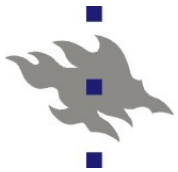
Apachen ominaisuudet

- Tiedostojen jakaminen (staattinen sisältö)
  - URL-avaruuden kuvaus tiedostopoluiksi
- DNS-nimellä ja IP-osoitteella tapahtuva palvelun valinta (virtualhosts)
- URL- ja tiedostokohtainen konfigurointi
  - *.htaccess*-tiedostot yksittäisten alihakemistojen konfigurointiin
  - Käyttäjille sallitut konfiguraatiovaihtoehdot
  - Metatiedot: mime-tyypit ja merkistöt
  - CGI-skriptin suoritus tiedoston tyypin perusteella
  - Tiedoston käsittely apachen modulilla (esim. Php-ohjelman suoritus)
- Monipuolinen lokien konfigurointi



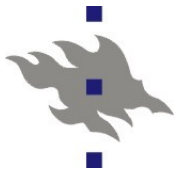
Lisää Apachen ominaisuuksia

- Autentikointi IP-osoitteen perusteella
- Salasana-autentikointi
- Automaattiset hakemistolistaukset
- Http-välimuisti (proxy)
- WebDAV – sivujen etäpäivitys
- Kompressointi
- Suodattimet: sivujen edelleenkäsittely ulkoisilla ohjelmilla tai sisäänrakennetuilla apache-moduleilla
- Http-otsakkeiden muokkaus
- Palvelimen tilan monitorointi



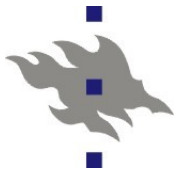
Vielä lisää apachen ominaisuuksia

- Sisältöneuvottelu (content-negotiation): merkistöjen, tiedostotyyppien ja kielen valinta selaimen toivomusten perusteella
- mod_rewrite: yleistyökalu URL:ien kuvaamiseen tiedostojärjestelmään
- Ympäristömuuttujien asetus cgi-skripteille
- SSL/TLS-tuki
- CGI-skriptien suoritus CGI-skriptin omistajan oikeuksin
- Apachen ulkopuoliset modulit
  - PHP-tulkki mod_php
  - Perl-tulkki mod_perl
  - Python-tulkki mod_python
- Ruby on Rails
  - Cgi-skriptien kautta



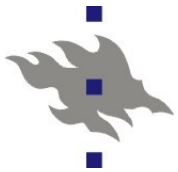
Apache-2.2

- Julkaistiin 1.12.2005
- Parempi proxy-tuki, erityisesti www-välimuistina toimimiselle
- Konfigurointia yksinkertaistettu
  - Mukana konfigurointiesimerkkejä erilaisiin yleisiin tarpeisiin
- Suodatinten (filters) dynaaminen konfigurointi
- SQL-tietokantatuki lisätty apachen ytimeen
  - Tietokantoja käyttävien modulien ei tarvitse enää toteuttaa tietokantayhteyksien luontia itse
  - Modulit voivat jakaa luotuja tietokantayhteyksiä
- Tuki TLS-yhteyden neuvottelulle http-portissa
  - Nimipohjaiset virtuaalipalvelimet myös SSL/TLS-yhteyksille (RFC 2817)



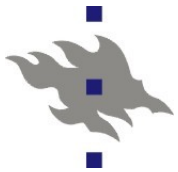
Politiikkapäätöksiä

- Rivikäyttäjien omille sivuille suunnattu palvelin ja keskitetysti ylläpidetty sovelluspalvelin tarvitsevat kovin erilaiset konfiguraatiot
- Yhdellä WWW-hotellipalvelimella voi olla tuhansia käyttäjiä
  - Miten estetään heitä aiheuttamasta vahinkoa itselleen, toisilleen ja palvelimelle?
- Sallitaanko käyttäjien asentaa omia dynaamista sisältöä tuottavia ohjelmistoja?
- Mitä eri www-sovellusalustoja halutaan tarjota?
- Käyttäjien omien ohjelmien eristäminen toisistaan eri käyttäjätunnusten taakse on mahdollista, mutta työlästä ja raskaampaa kuin yhden ainoan jaetun tunnuksen käyttö
- Virtuaalikoneet ovat uusi ratkaisu ongelmaan



Apachen asennuksesta

- 'yum install httpd php mod_python mod_perl'
  - Apache www-palvelimen kääntäminen ja asentaminen on melko helppoa
  - Ulkoisten apache modulien ja niiden tarvitsemien muiden kirjastojen ja ohjelmistojen asennus valitettavasti ei ole!
  - ts. distribuution tarjoaman valmiin apache-asennuksen käyttäminen säästää paljon aikaa
  - Distribuution oma apache-konfiguraatio voi erota paljon pakasta vedetyn apachen konfiguraatiosta
- 'yum install mod_ssl'
  - Asennetaan tai generoidaan ssl-sertifikaatti
- Editoidaan apachen konfigurointitiedosto kuntoon politiikkapäätösten mukaan
  - Helposti sanottu..
- /etc/rc.d/init.d/apache start



Apachen lokit

- Fedoran oletusasennuksessa */var/log/httpd* -hakemistossa
- *access_log*
  - hakujen loki
- *error_log*
  - Virheloki
  - Tänne lokitetaan sivun käsittelyssä, apachen konfiguraatiossa tai skriptien suorituksessa tapahtuneet virheet
  - **Täältä etsitään vihjeitä, jos asiat eivät toimi!**
  - Hakuloki (access_log) ja virhelogi (error_log) ovat erikseen
- *ssl_access_log*, *ssl_error_log*
  - Vastaavat lokit SSL-kryptatuille sivuhauille
- *suexec_log*
  - Käyttäjän oikeuksin suoritettujen cgi-skriptien loki

Apachen konfiguraatio

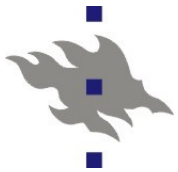
- */etc/httpd* – Apachen konfiguraatiohakemisto
- */etc/httpd/conf/httpd.conf* – varsinainen konfiguraatiotiedosto
- /etc/httpd/conf.d – Hakemisto johon paketoidut apache-modulit pudottavat modulien konfiguraatiotiedostot
- */etc/pki/tls/private/localhost.key*
  /etc/pki/tls/certs/localhost.crt
  - mod_ssl salainen avain ja sertifikaatti
  - Fedorassa sertifikaatit ja avaimet /etc/pki hakemistossa
- */var/www*
  - DocumentRoot ja cgi-bin hakemistot
- */var/log/httpd*
  - Palvelimen lokit

PHP:n asennus

- PHP:n asennus (FC3:ssa) 'yum install php':

Dependencies Resolved
Transaction Listing:
  Install: php.i386 0:4.3.10-3.2

Performing the following to resolve dependencies:
  Install: flac.i386 0:1.1.0-7
  Install: libidn.i386 0:0.5.6-1
  Install: libidn-devel.i386 0:0.5.6-1
  Install: php-pear.i386 0:4.3.10-3.2
  Install: speex.i386 0:1.0.4-4
  Update: curl.i386 0:7.12.3-2
  Update: curl-devel.i386 0:7.12.3-2
  Update: libao.i386 0:0.8.5-2
  Update: libao-devel.i386 0:0.8.5-2
  Update: libogg.i386 2:1.1.2-1
  Update: libogg-devel.i386 2:1.1.2-1
  Update: libvorbis.i386 1:1.1.0-1
  Update: libvorbis-devel.i386 1:1.1.0-1
  Update: vorbis-tools.i386 1:1.0.1-4



Fedoran apache-paketit

- Apache-moduleja:
  - *mod_dav_svn* – subversion versionhallinta http:n yli
  - *mod_ssl* – SSL tuki apacheen (openssl-kirjastolla)
  - *mod_jk* – Apache moduli tomcat:illa toteutettujen web-sovellusten liittämiseen osaksi Apachen URL-avaruutta
  - *mod_perl, mod_python, php, mod_mono*
    - Moduleja www-sovellusten kehitykseen eri kielillä
    - *mod_mono*: asp.net toteutus
- PHP on jaettu myös moduleihin
  - Tämän vuoksi PHP-riippuvuudet FC4:stä eteenpäin hieman järkevämmät
  - *php-cli* – komentorivin PHP-tulkki
  - *php_ldap* – Tuki LDAP-protokollalle
  - *php_mysql, php_pgsql* – tietokantatuki
  - *php_gd* – Grafiikan generointi php:lla

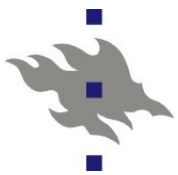
Apache-2.x rinnakkaisuus

- Apachen 1.x versioissa rinnakkain tapahtuvien http-pyyntöjen käsittely tapahtui vain rinnakkaisilla prosesseilla
- Apache 2.x versioihin lisättiin tuki säikeille
  - Joillain apache-alustoilla prosessit ovat raskaita (win32)
- MPM-modulit ovat erilaisia rinnakkaisuustuen toteutuksia
  - Linuxissa prosessit ovat kevyitä: säietuki ei juurikaan lisää tehokkuutta
  - Säietuesta voi olla haittaa: apachen ulkopuoliset modulit tai niiden käyttämät kirjastot eivät välttämättä ole säieturvallisia
  - Linuxissa siis kannattaa käyttää mpm_prefork-moduulia
  - FC6:n httpd paketissa tulee kaksi eri apache-binääriä, toinen prosessituella, toinen säietuella (*httpd.worker*)

Konfiguraatiosyntaksia

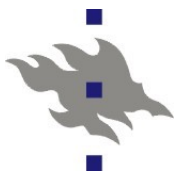
```
<Directory "/var/www/cgi-bin">
    AllowOverride None
    Options None
    Order allow,deny
    Allow from all
</Directory>
```

- Konfiguraatiodirektiivit noudattavat syntaksia 'direktiivi *argumentti1 argumentti2*'
- '*#*'-merkillä alkavat rivit ovat kommentteja
- Direktiiveillä on konteksti, jossa ne vaikuttavat
  - Konteksti voi olla palvelimen globaali kofiguraatio, tiettyä muotoa oleva URL, hakemisto, virtualhost, jne
  - Jotkin direktiivit ovat käytettävissä vain tietyissä konteksteissa



URL:ien kuvaus tiedostoiksi

- *DocumentRoot* – hakemisto josta Apache palvelee tiedostoja
  - *DocumentRoot "/home/www/htdocs"*
- *mod_userdir* - käyttäjien www-sivujen polku
  - Perinteinen *public_html* -hakemisto käyttäjän kotihakemistossa:
    UserDir public_html
  - WWW-sivut erillisessä hakemistohierarkiassa:
    UserDir /var/html
    UserDir /var/www//docs*
  - On mahdollista antaa useita vaihtoehtoisia sijainteja käyttäjän omille sivuille:
    UserDir public_html /hakemisto/jossain http://redirect.here/
  - '~'-merkkiä ei voi vaihtaa toiseksi muuttamatta apachen lähdekoodia(?)



URL:ien kuvaus tiedostoiksi

- mod_alias – URL:ien kuvaus tiedostojärjestelmään ja uulleenohjaukset
- Palveltavan hakemiston tai tiedoston lisäys palvelimelle: *Alias <URL-polku> <Tiedostopolku>*

  Alias /icons/ ”/usr/local/apache/icons”

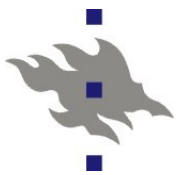
  Alias /hallinto /group/hallinto

  - Tiedostojen ei tarvitse olla *DocumentRoot* hakemiston alla
- Myös säännölliset lausekkeet käytettävissä

  AliasMatch ”^/u/tkt_legg/(.)” \ ”/home/fs/leggio/public_html/$1”*
- URL:ien kuvaus CGI-skripteiksi

  ScriptAlias /cgi-bin/ /www/cgi-bin

  ScriptAliasMatch ^/cgi-bin(.) /www/cgi-bin$1*



Yksinkertaiset uudelleenohjaukset

- mod_alias tarjoaa yksinkertaiset uudelleenohjaukset:
  - *Redirect <http-status> <polku palvelimella> <uusi URL>*
  - Esim:

*Redirect permanent /Jani.Jaakkola *
http://www.cs.helsinki.fi/u/jjaakkol
RedirectMatch (.)\.gif$ http://www.anotherserver.com$1.jpg*

- Uudelleenohjausdirektiivit sovelletaan ensin, Alias-direktiivit vasta uudelleenohjausten jälkeen
- *mod_rewrite* tarjoaa ilmaisuvoimaisempia vaihtoehtoja uudelleenohjauksiin

Ehdollinen konfigurointi

- <*IfModule*>-direktiivillä voidaan ottaa käyttöön ryhmä direktiivejä, jos jokin annettu apache.moduli on käytössä
  - Esim. SSL/TLS-direktiivejä käytetään vain, jos *mod_ssl* on käytössä
- <IfDefine>-direktiivillä voidaan ryhmä direktiivejä ottaa käyttöön, jos jokin annettu ehto on voimassa
  - Apachea käynnistettäessä voidaan komentorivin *-D* optiolla valita vaihtoehtoisia konfiguraatioita

Direktiivien ryhmittely

- Direktiivit hakemistoja, tiedostoja ja URL:eja varten
- *<Directory /folder>*
- *<DirectoryMatch regex>*
  - direktiivit vaikuttavat vain fyysisessä hakemistossa */folder* oleviin tiedostoihin
  - *.htaccess*-tiedostot ovat hakemistoon itseensä säilöttyjä *<Directory>*-ryhmiä (tietyin rajoituksin)
- *<Files *.png>*
- *<FilesMatch regex>*
  - Direktiivit vaikuttavat vain annetun nimisiin tiedostoihin
- *<Location /url/>*
- *<LocationMatch regex>*
  - Annettuun URL:iin sovellettavat direktiivit
- *<Virtualhost host>*
  - Virtuaalipalvelimeen sovellettavat direktiivit

Direktiivien soveltaminen

- Yksi http-haku saattaa sopia moneen direktiiviryhmään
- Ryhmille on määritelty sovellusjärjestys:
  - Ensin <*Directory*> -ryhmät ja hakemiston *.htaccess*-tiedostosta löytyvät komennot hakemistonimen pituuden mukaan lyhyimmästä nimestä pisimpään
  - <*DirectoryMatch regex*> -säännölliseen lausekkeen sopivat
  - <*Files*> ja <*FilesMatch*> samaan aikaan
  - <*Location*> ja <*LocationMatch*> samaan aikaan
  - <*Virtualhost*> -ryhmän sisällä olevat direktiivit suoritetaan <*Virtualhost*> -ryhmän ulkopuolella olevien direktiivien jälkeen, jotta <Virtualhost> -ryhmällä voi ohittaa oletusasetukset
  - Muuten siinä siinä järjestyksessä missä ryhmät löytyvät konfiguraatiotiedostosta

Virtualhost

- DNS-nimen pohjautuva konfiguraation valinta
  - Yhdellä IP-osoitteella ajetaan eri konfiguraatioita eri DNS-nimille tuleviin pyyntöihin
  - *NameVirtualHost* ja *ServerName*
- IP-osoitteeseen pohjautuva konfiguraation valinta
  - <*VirtualHost ip-osoite:portti*>
  - Edellyttää että palvelinkoneella on useampi IP-osoitteita
  - Mahdollistaa myös useamman eri sertifikaatin käytön samalla palvelimella (myös ilman TLS-protokollan apua)

Options -direktiivi

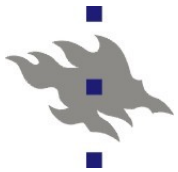
- Valitaan mitkä apachen ominaisuudet ovat käytettävissä direktiivin kontekstissa:
  - *ExecCGI* – sallitaanko CGI-skriptien suorittaminen
  - *All* – kaikki paitsi *MultiViews*. Tämä on oletusarvo
  - *FollowSymLinks* – seuraanko symbolisia linkkejä
  - *Includes* – onko apachen www-sivujen esikäsittelijä käytössä (SSI, Server Side Includes)
  - *IncludesNOEXEC* – onko CGI-skriptien suorittaminen SSI-esikäsittelijän kautta sallittu
  - *Indexes* – generoiko apache hakemistolistauksia hakemistoista, joista puutuu *index.html* -tiedosto
  - *SymLinksIfOwnerMatch* – apache seuraa vain symlinkkejä, joiden omistaja on sama kuin kohdetiedoston omistaja
  - Myös syntaksit: *Options +Foo* ja *Options -foo*

AllowOverride -direktiivi

- Valitaan *.htaccess* -tiedostoilla konfiguroitavat ominaisuudet
  - *AllowOveride none* – ei käytetä .htaccess-tiedostoja lainkaan
  - *AuthConfig* – käyttäjätunnuksilla autentikoinnin konfigurointi sallittu
  - *FileInfo* – metainformaation konfigurointi sallittu (mm. Mime-tyypit)
  - *Limit* – IP-pohjaisten pääsyoikeuksien konfigurointi sallittu
  - *Options* – sallii O*ptions* -komennon käyttämisen
    - Tämä voi olla vaarallinen: tällä sallitaan CGI-skriptien käytössä olon konfigurointi *.htacces* -tiedostoilla

Pääsyrajoitukset

- mod_access tarjoaa yksinkertaiset IP-osoitepohjaiset pääsyrajoitukset
  Allow from all|host|env=env-variable
  Deny from all|host|env=env-variable
- Käytettävissä DNS-nimet, ipv4-osoitteet ja ipv6-osoitteet
- *Order* -direktiivillä valitaan onko pääsy oletusarvoisesti sallittu ja missä järjestyksessä *Allow* ja *Deny säännöt* suoritetaan
- *Order Deny,Allow*
  - Pääsy oletusarvoisesti sallittu, *Allow* -säännöllä presedenssi
- *Order Allow,Deny*
  - Pääsy oletusarvoisesti kielletty, Deny -säännöllä presedenssi



<Directory> esimerkki

```
<Directory /home/*/public_html>
   AllowOverride FileInfo AuthConfig Limit Indexes
   Options MultiViews Indexes SymLinksIfOwnerMatch -ExecCGI Includes
   <Limit GET POST OPTIONS PROPFIND>
      Order allow,deny
      Allow from all
   </Limit>
   <Limit PUT DELETE PATCH PROPPATCH MKCOL COPY MOVE LOCK UNLOCK>
      Order deny,allow
      Deny from all
   </Limit>
</Directory>
```

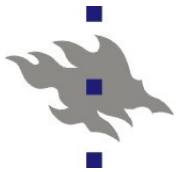
- *Options*
  - Mitkä apachen ominaisuudet hakemistossa ovat käytössä
- *AllowOverride*
  - Mitkä konfiguraatiotiedoston säädöt voidaan vaihtaa '*.htaccess*'-tiedostolla
- Pääsyrajoitukset

Käyttäjätunnukset

- mod_auth - tuki yksinkertaiselle salasana-autentikoinnille
- Salasanat kulkevat verkossa selväkielisinä ellei ssl-kryptaus ole käytössä
  - Vaihtoehtoisesti *mod_auth_digest* modulilla voi toteuttaa challenge-response autentikoinnin
    - Vaatii salasanat omassa salasanaformaatissa
- *AllowOverride AuthConfig* sallii autentikoinnin konfiguroinnin *.htaccess* -tiedostojen avulla
- Tarvitaan salasanatiedosto, joka sattuu olemaan syntaksiltaan samanlainen kuin */etc/shadow*
- Apachen mukana tulee pieni komentoriviohjelma *htpasswd* jolla voi editoida salasanatiedostoja
- Salasanatiedoston voi laittaa dbm-tietokannan taakse
- *AuthGroupFile <tiedosto>* direktiivillä voi salasanatiedostoista löytyviä käyttäjiä jakaa ryhmiin
- *mod_auth_pam:* pam-autentikointi
- *mod_auth_ldap:* LDAP-serveriä vastaan tehty autentikointi

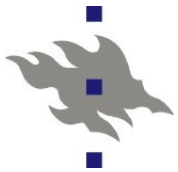
Lisää käyttäjätunnuksista

- Politiikkapäätös: Jos apachen pääsee käsiksi linux-asennuksen salasanatiedostoon, se voi myös vahingossa vuotaa sen ulos verkkoon
  - Vaihtoehtoisesti voi konfiguroida apachen käyttämään esim. PAM-autentikointia tai LDAP-autentikointia, jolloin apachelle ei tarvitse antaa pääsyoikeuksia salasanatiedostoihin
- *AuthUserFile <salasanatiedosto>*
  - Salasanatiedoston sijainti. Salasanatiedosto on syytä pitää paikassa, josta Apache ei suostu jakamaan sitä verkkoon
  - Edes symlinkeillä!
- *Require user userid userid2*
  - Vaaditaan jokin listatuista käyttäjätunnuksista
- *Require group group group2*
  - Vaaditaan käyttäjän kuuluvan johonkin listatuista ryhmistä
- *Require valid-user*
  - Vaaditaan vain salasanatiedostosta löytyvä validi salasana



Apachen SSL-tuki

- SSL-protokollan RSA/DSA-neuvottelu on raskas CPU-aikaa kuluttava prosessi
  - Yhteyden kryptaus valmiiksi neuvotellulla avaimella on paljon kevyempi operaatio
  - Apache osaa säilyttää valmiiksi neuvoteltuja salaisia avaimia välimuistissa
  - *mod_ssl:n* SSL/TLS-toteutus ei siis ole täysin tilaton
- *mod_ssl* -paketin mukana tulee valmis SSL-virtuaaliserveri konfiguraatio
- *mod_ssl* asennusskriptit generoivat valmiin itse-allekirjoitetun sertifikaatin
- SSL-protokolla sallisi kompressoinnin, mutta käytännössä sitä ei missään käytetä

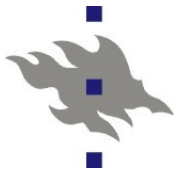


mod_ssl -konfigurointi

- *SSLOptions* – lähinnä CGI-skripteille hyödyllisten SSL-ominaisuuksien konfigurointi
  - *StdEnvVars* – SSL-neuvottelun konteksti skripteille
  - FakeBasicAuth – Asiakassertifikaatti näyttää skriptille onnistuneelta http basic autentikaatiolta
- *SSLPassPhraseDialog* – serverin sertifikaatin dekryptauksen konfigurointi
- *SSLRequire* – yleiskäyttöinen työkalu vaadittujen SSL-ominaisuuksien valintaan
- *SSLRequireSSL* – sallii pääsyn ainoastaan jos SSL-yhteys on onnistuneesti neuvoteltu
- *SSLVerifyClient* – vaatii asiakkaalta sertifikaatin

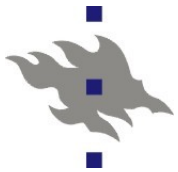
CGI-skriptit

- CGI-skriptit ovat Apachesta erillisiä ohjelmia, jotka suoritetaan vastauksen generoimiseksi http-pyyntöön
  - Yksinkertaisin tapa generoida dynaamista sisältöä
  - CGI-skriptit ovat aina tietoturvariskejä
- Politiikkapäätöksiä CGI-skriptien tapauksessa:
  - Sallitaanko omien CGI-skriptien kirjoitus rivikäyttäjälle
  - Käytetäänkö suexec-mekanismia
  - Vaihtoehtona FastCGI-palvelinprosessit
- *ScriptAlias*
  - Apachen ylläpitäjän hakemisto CGI-skripteille
- *AddHandler cgi-script .php .pl*
  - Hakemistokohtaisesti valittaan mitkä tiedostot suoritetaan cgi-skripteinä
  - *AddHandler* toimii vain jos *Option ExecCGI* on käytössä
  - *AddHandler* toimii myös *.htaccess* -tiedostoissa



Sovellukset käyttäjän oikeuksin

- Apachen *suexec* ominaisuus mahdollistaa CGI-skriptin suorituksen skriptin omistajan oikeuksin
  - *Apache-asennuksessa on tällöin suexec* -niminen setuid-root binääri, jonka avulla apache voi vaihtaa suorittavan prosessin käyttäjätunnuksen, mikäli joukko tietoturvavaatimuksia toteutuu
  - suexec:in asennus on tehty tahallaan hankalaksi
- Suexec on käytössä jos ja vain jos
  - CGI-skripti tuli mod_userdir apache-modulilta (ts. tavallisesti public_html-hakemisto)
  - *SuExecUserGroup user group – CGI-skriptejä suorittavan käyttäjän valinta virtuaalipalvelimella*
- Suphp -paketti tarjoaa vastaavan virityksen jolla php-skriptit voi suorittaa käyttäjän oikeuksin
  - PHP safe mode on vaihtoehto



SSI - Server Side Includes

- SSI toteutettu apache-modulissa *mod_include*
- SSI on joukko html-tiedostoihin tageina upotettavia komentoja, jotka apache suorittaa
- SSI on kevyehkö menetelmä yhdistellä useasta lähteestä kokonaisia www-sivuja
- *Options +Includes* – otetaan SSI-käyttöön
- *AddOutputFilter INCLUDES .shtml* – tehdään SSI-prosessointi kaikissa .shtml-päätteisissä tiedostoissa
- *XBitHack on* – jos html-tiedostossa on x-bitti päällä tehdään SSI-prosessointi
- *XbitHack full* – SSI-käsitellyn tiedoston aikaleimaan vaikuttaa ainoastaan lähdetiedoston aikaleima

SSI-komennot

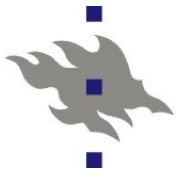
- Syntaksi:

  <!--#element attribute=value attribute=value ... -->
- Tiedostojen inkluusio:

  <!--#include virtual="/footer.html" -->
  - Myös cgi-skriptien inkluusio, mikäli polun takana itse asiassa oli cgi-skripti
- Tavallisen komennon suorittaminen:

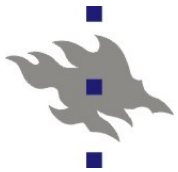
  <!--#exec cmd="date" -->

  <!--#exec cgi=/cgi-bin/foo.pl -->
  - *#exec cgi* tapauksessa oletetaan että cgi-skripti generoi http-otsakkeet
- Myös muuttujien ja ympäristömuuttujien asetukset ja ehdollinen suoritus
- Kontekstitiedon liittäminen: milloin muutettu, tiedoston koko



Proxy-tuki

- Proxy apache vastaa saamaansa www-pyyntöön tekemällä itse haun jollekin toiselle palvelimelle
  - Proxy apache osaa myös FTP- ja TCP-asiakasyhteydet
- Apachea voi käyttää perinteisenä www-proxyna
  - WWW-proxya konfiguroitaessa täytyy **aina** ottaa käyttöön jonkinlainen autentikointi: spämmerit, kräkkerit ja muut ikävät ihmiset löytävät avoimet proxyt väistämättä
  - *mod_cache, mod_mem_cache, mod_disk_cache* toteuttavat välimuistin proxyn kautta haetuille sivuille
- Reverse-proxy
  - Ohjaa annettuun URL:iin tulleet http-pyynnöt toiselle palvelimelle, ts. Edustapalvelimelta taustapalvelimelle
  - Kuorman tasaus
  - Apachen ulkopuolisten http-palvelinten liittäminen osaksi virtuaalista apache URL-avaruutta
  - esim. tomcat-konfiguraatio db.cs.helsinki.fi -palvelimella



Proxyn konfigurointi

Perinteinen proxy

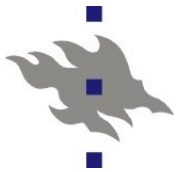
```
ProxyRequests On
ProxyVia On

<Proxy *>
Order deny,allow
Deny from all
Allow from internal.example.com
</Proxy>
```

Reverse proxy

```
 ProxyRequests Off

<Proxy *>
Order deny,allow
Allow from all
</Proxy>

ProxyPass /foo http://foo.example.com/bar
ProxyPassReverse /foo http://foo.example.com/bar
```

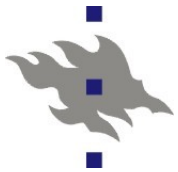
Välimuistin konfigurointi

```
#
# Sample Cache Configuration
#
LoadModule cache_module modules/mod_cache.so

<IfModule mod_cache.c>
#LoadModule disk_cache_module modules/mod_disk_cache.so
# If you want to use mod_disk_cache instead of mod_mem_cache,
# uncomment the line above and comment out the LoadModule line below.
<IfModule mod_disk_cache.c>
CacheRoot c:/cacheroot
CacheEnable disk /
CacheDirLevels 5
CacheDirLength 3
</IfModule>

LoadModule mem_cache_module modules/mod_mem_cache.so
<IfModule mod_mem_cache.c>
CacheEnable mem /
MCacheSize 4096
MCacheMaxObjectCount 100
MCacheMinObjectSize 1
MCacheMaxObjectSize 2048
</IfModule>
# When acting as a proxy, don't cache the list of security updates
CacheDisable http://security.update.server/update-list/
</IfModule>
```



WebDAV

- Web-based Distributed Authoring and Versioning
  - Tiedostojen etäpäivitys käyttäjille
  - RFC 2518 (http PUT, DELETE, jne)
    - Tiedostojärjestelmä http:n yli
  - Myös samanaikaisuuden hallinta
  - Dreamweaver ja MS Office tukevat
- Apache modulit:
  - *mod_dav* – toteuttaa WebDAV-protokollan
  - *mod_dav_fs* – WebDav tiedostojärjestelmässä
- Konfiguraatiossa direktiivi *Dav On*
  - Toimii hakemistoissa, joihin apache-palvelimella on kirjoitusoikeus
  - Apache ei tue talletettavan tiedoston omistajan asettamista
    - Tiedoston omistajaksi tulee Apache-prosessin käyttäjätunnus



Satunnaisia kikkoja

- Kompressointi lennossa:

  <Directory "/your-server-root/manual">

  AddOutputFilterByType DEFLATE text/html

  </Directory>

- Merkistön valinta:

  AddCharset EUC-JP .euc

- Tiedostojen mime-tyyppi:

  AddType text/vnd.wap.wml .wml

- Serverin tilatieto:

  <Location /server-info>

  SetHandler server-info

  </Location>

Squid www-proxy

- Www-proxylla voidaan pitää organisaatiossa usein käytettyjä sivuja välimuistissa keskitetysti
  - Cache-osumat voivat vähentää latenssia
  - Säästetään www-liikenteessä, tyypillisesti n. 20-30%
- Proxy voi toimia palomuurina pahan ulkomaailman ja intranetin välissä – intranetistä ei välttämättä ole suoraa reittiä ulkomaailmaan lainkaan
- http-porttikäytäviä muihin protokolliin (esim. Ftp)
- Squid tukee pakkoproxy-konfiguraatiota
  - Pakkoproxy sieppaa kaiken http-liikenteen proxylle käsiteltäväksi suoraan verkosta
- Organisaatiolle keskitetty paikka monitoroida www-liikennettä
- Konfiguroitavat pääsyrajoitukset
- Squid tuntee myös proxy-hierarkiat ja kollegat
  - ICP – Internet Cache Protocol