**Webhosting – server Apache 2**

Základem webových služeb v interních sítích a na internetu je webhosting. Webhosting je služba využívající protokolu **HTTP (Hyper Text Tranfer Protocol)** k přenosu informací (texty, obrázky případně další soubory) po síti pracující jako architektura **klient/server**. Protokol HTTP je sám o sobě **nestavovým protokolem**, pro přenos informací po síti využívá protokol **TCP**. Data jsou přenášena jako **čistý text**, binární soubory jsou převáděny do textové podoby pomocí rozšíření **"MIME" (Multipurpose Internet Mail Extension)**. Jako webhosting zpravidla označujeme službu na serveru (v Linuxu démona), který naslouchá na příslušných portech (zpravidla **80, 443**) a odpovídá na požadavky zaslané od klientů. Klientem je v tomto případě webový prohlížeč na vzdáleném PC. Pod Linuxem jsou nejpoužívanějšími službami **Apache, NGINX**, pod Windows je to **IIS**.

**Vezre protokolu**

Protokol http je specifikován v několika verzích – **HTTP/0.9, HTTP/1.0** a v současné době nejrozšířenější **HTTP/1.1**. V roce 2015 byl schválen nový standard pod označením **HTTP/2**, který přináší některé nové vlastnosti jako posílání více požadavků najednou v jednom proudu, lepší podporu šifrování a data přenášená v binární podobě.

**Stavové informace**

Jelikož http protokol je nestavový, používá pro uchovávání stavů malé soubory uložené na PC klienta, kterým říkáme **COOKIES**.

**Šifrování přenášených informací**

Jelikož data putují přes http v čitelné podobě, bylo pro potřeby zabezpečení přenášených informaci vyvinuto několik protokolů přidávající podporu šifrování přenášených dat. Jedná se o protokoly **SSL (Secure Socket Layer)** a **TLS (Transport Layer Securtity)**, které pro svou činnost využívají opět protokolu TCP. Šifrované přenosy jsou označeny jako **HTTPS**.

**SSL** je starší méně bezpečnou variantou, existuje ve verzích **SSL1.0, SSL2.0, SSL3.0**. V současné době není SSL protokol považován za bezpečný, je doporučeno ho na serveru vypnout. Náhradu tvoří bezpečnější **TLS**.

**TLS** je novější protokol poskytující lepší zabezpečení dat, existuje ve verzích **TLS1.0, TLS1.1**, v současné době používaný **TLS1.2** a **TLS1.3**.

**URL (Uniform Resource Locator) / URI (Uniform Resource Identifier**)

Tvoří základ pro adresování zdrojů na webu (klasická webová adresa), skládá se z několika částí:

http: // [www.spsmb.cz](http://www.spsmb.cz) : 8080 /index.php ? parametr=hodnota  
(protokol) (host – adresa) (port) (dokument) (parametry querystring oddělené znakem &)

**Metody**

Pro komunikace klienta se serverem jsou definovány tzv. metody:

* GET – požadavek na zaslání dat (dokumentu) ze serveru
* HEAD – jako GET, ale pouze metadata bez samotného dokumentu
* POST – odeslání dat na server (formuláře), jako součást požadavku. Jde použít i GET, který data předává v URL.
* PUT – nahrání souboru na server, potřeba oprávnění
* DELETE – smazání objektu na serveru, potřeba oprávnění
* TRACE – kopie požadavku zpět klientovi
* OPTIONS – dotaz na metody podporované serverem
* CONNECT – konverze spojení na TCP/IP tunel pro použití zabezpečené (SSL) komunikace přes nezabezpečený HTTP Proxy

**HTTP stavové kódy (nesouvisí se stavem spojení)**

Vrací se v záhlaví odpovědi od serveru, upřesňují stav vyřízení požadavku. Jsou identifikovány trojmístným číslem, reprezentují pět kategorií:

1xx – informační

2xx – úspěšně vyřízený HTTP požadavek (standardně 200)

3xx – HTTP požadavky týkající se přesměrování

4xx – chyby na straně klienta (klasicky 404 – Not Found)

5xx – chyby na straně serveru (většinou 500 – Internal Server Error)

**Apache**

Jeden z nejpoužívanějších webových serveru na Linuxu i na vlastním Internetu, v současné době ve verzi 2.4.

Instalace

apt-get install apache2 libapache2-mod-php5 (podpora PHP módu)

**Části apache serveru:**

/etc/apache2 – konfigurační soubory  
/var/www – kořenový adresář webové služby  
/usr/share – adresáře doc/apache\* - dokumentace

**Konfigurace**

/etc/apache2/apache2.conf – hlavní konfigurace serveru  
/etc/apache2/envvars – nastavení základních proměnných Apache  
/etc/apache2/ssl – certifikáty pro SSL (TLS)  
/etc/apache2/conf-available – dílčí konfigurace  
/etc/apache2/mods-available – použitelné moduly (sada funkcí serveru)  
/etc/apache2/sites-available – konfigurace www stránek, které jsou k dispozici (viz. virtuální adresář)

Poslední tři adresáře mají ještě podružný adresář s koncovkou -enabled, který obsahuje všechny věci, které jsou na serveru povolené.

**Virtuální adresáře**

Jsou to adresáře s vlastním obsahem webu (dokumenty, obrázky apod.), zpravidla je umístěn ve složce /var/www/název\_vistuálního\_adresáře. Související konfigurace je v souboru /etc/apache2/apache2.conf a /etc/apache2/sites-available.

**Zakázání nepotřebných modulů**

Některé moduly nejsou potřeba (seznam dole), z bezpečnostních důvodů je vypneme příkazem **a2dismod***název\_modulu*, mohly by představovat bezpečnostní riziko.   
Povolení můžeme provést pomocí **a2enmod** *název\_modulu*.

mod\_imap, mod\_include, mod\_info, mod\_userdir, mod\_status, mod\_cgi, mod\_autoindex

Upravíme konfigurační soubory /etc/apache2/apache2.conf, /etc/apache2/conf-available a /etc/apache2/sites-available dle vzoru a do /etc/apache2/apache2.conf přidáme tyto řádky (kontrola proti zneužití cookies a iframe, zákaz zobrazení ETag):

Header edit Set-Cookie ^(.\*)$ $1;HttpOnly;Secure

Header always append X-Frame-Options SAMEORIGIN

FileETag None

V souboru /etc/apache2/conf-available/security.conf nastavíme:

* ServerSignature Off
* ServerTokens Prod
* TraceEnable Off

**Aktivujeme konfiguraci a WWW stránky**

**a2enconf** *konfigurační soubor (*pomocí a2disconf ji můžeme deaktivovat)  
**a2ensite** *konfigurační soubor* (pomocí a2dissite ji můžeme deaktivovat)

**Restartujeme Apache2**

systemctl apache2 restart

Následně vyzkoušíme stránku v prohlížeči.

**Nastavení SSL/TLS**

Dle vzoru nakonfigurujeme /etc/apache2/mods-available/ssl.conf:

* nastavíme podporované šifry
* nastavíme podporované protokoly

Dle vzoru nastavíme /etc/apache2/sites-available/default-ssl.conf:

* nastavíme virtuální adresář
* nastavíme cestu k souborům s certifikátem

Vygenerujeme certifikát do /etc/apache2/ssl

openssl req -new -x509 -newkey rsa:4096 -days 365 -nodes -out server.pem -keyout server.key

Práva k souborům certifikátu nastavíme na 600.

Restartujeme server a vyzkoušíme.