19. Služby WWW, FTP

**1. Obecná charakteristika služeb WWW a FTP**

**Služba WWW**

* **Definice a účel:**

WWW (World Wide Web) je systém propojených dokumentů a multimediálního obsahu, který je zpřístupněn přes internet. Klienti (webové prohlížeče) komunikují se servery pomocí protokolů HTTP (HyperText Transfer Protocol) a HTTPS (HTTP Secure) pro bezpečný přenos dat.

* **Funkce:**
  + Distribuce statického a dynamického obsahu (HTML, CSS, JavaScript, obrázky, videa).
  + Podpora webových aplikací a REST API.
  + Možnost implementace interaktivních a responzivních uživatelských rozhraní.
* **Bezpečnost:**
  + HTTPS šifruje přenos dat.
  + Webové servery implementují autentizaci, autorizaci a další bezpečnostní mechanismy, jako jsou firewally, filtrace požadavků nebo ochrana proti DDoS útokům.

**Služba FTP**

* **Definice a účel:**

FTP (File Transfer Protocol) je protokol určený pro přenos souborů mezi klientem a serverem. Umožňuje nahrávání, stahování a správu souborů na serverech.

* **Základní principy:**
  + FTP pracuje tradičně na portu 21 (pro příkazovou komunikaci) a používá další porty pro datový přenos (20).
  + Může podporovat anonymní přístup nebo autentizaci pomocí uživatelského jména a hesla.
  + Existují bezpečné varianty, jako je FTPS (FTP Secure – s TLS/SSL) nebo SFTP, který je založený na SSH.
* **Použití:**
  + Přenos velkých souborů.
  + Správa webového obsahu (upload nových verzí stránek).
  + Zálohování a synchronizace dat mezi servery.

**2. Konfigurace a správa služby WWW**

**A. V OS Windows**

* **Internet Information Services (IIS):**
  + **Konfigurace:**
    - IIS je nativní webový server pro Windows Server, který umožňuje snadnou správu webových stránek, virtuálních adresářů a aplikačních poolů.
    - Konfigurace se provádí pomocí **IIS Manager** (grafické rozhraní), kde můžete nastavit vlastnosti jednotlivých webů, SSL certifikáty, autentizační metody a povolení modulů.
  + **Správa:**
    - Monitorování výkonu pomocí vestavěných nástrojů (např. Performance Monitor, Event Viewer).
    - Aktualizace konfigurace pomocí PowerShellu (např. pomocí cmdletů jako Get-IISSite nebo New-IISSite).
  + **Další možnosti:**
    - Windows umožňují instalaci alternativních webových serverů, například Apache nebo Nginx, běžících na platformě Windows, a jejich konfigurace se pak řídí příslušnými konfiguračními soubory.

**B. V UNIX-like OS**

* **Obecně:**
  + Adresář pro uložení webových stránek a dalších dokumentů je definován v direktivě DocumentRoot
  + Defaultně odkazuje na /var/www/html
  + Definujeme taky číslo portu, kde web server naslouchá, v direktivě Listen
    - Případně i adresu, pokud chceme, aby naslouchal jen na té adresa (thus jen v tom určitém subnetu)
    - Lze definovat více direktiv Listen
* **Apache HTTP Server a Nginx:**
  + **Apache:**
    - **apt-get install apache2, service apache2 start**
    - Konfigurace probíhá úpravou hlavního souboru (např. **/etc/httpd/conf/httpd.conf** nebo **/etc/apache2/apache2.conf**) a dalších konfiguračních souborů v adresáři /etc/httpd/ či /etc/apache2/.
    - Podpora modulů (mod\_ssl, mod\_rewrite) umožňuje rozšířenou funkčnost, jako je šifrovaná komunikace a URL přebpisování.
  + **Nginx:**
    - Konfigurační soubor (/etc/nginx/nginx.conf) a další soubory v adresáři /etc/nginx/conf.d/ definují chování serveru, reverzní proxy, load balancing a cacheování.
* **Správa a monitorování:**
  + Oba servery lze spravovat pomocí příkazů jako systemctl start|stop|restart apache2 nebo systemctl reload nginx.
  + Logovací mechanismy (access log, error log) slouží k diagnostice a optimalizaci provozu.
  + Webové rozhraní nebo nástroje třetích stran (např. Webmin) mohou usnadnit správu a monitorování.
* **Instalace SSL pro Apache**

1. Instalace — Povolíme SSL pro Apache

a2enmod ssl

1. Vytvoříme adresář pro certifikáty
2. Vygenerujeme certifikát
3. Doplníme do konfigurace virtuálního hosta, který poslouchá na portu 443

SSLEngine on

SSLCertificateFile /etc/httpd/ssl-certs/apache.crt

SSLCertificateKeyFile /etc/httpd/ssl-certs/apache.key

1. Restart service apache2 restart

* **Server s virtuální hosty**
  + Dovolí nám více vícero webů s jinými domény provozovat na jedné IP a portu
  + Každý host má vlastní adresář definovaný v **DocumentRoot** — Direktiva
  + Každý konfigurační soubor pro virtuálního hosta se dává do složky /etc/apache2/sites-availabe/<název webu>.conf
    - Po té, jednotlivé weby můžeme povolovat/zakazoat pomocí a2ensite/a2dissite (jakokdyby ”apache 2 enable site”)

**3. Konfigurace a správa služby FTP**

**A. V OS Windows**

* **FTP Server v rámci IIS:**
  + **Konfigurace:**
    - V rámci IIS můžete nainstalovat FTP Server jako roli, kde vytvoříte FTP web, nastavíte virtuální adresáře a konfigurujete autentizaci (např. základní ověřování, Windows autentizaci).
    - Dále lze nakonfigurovat SSL/TLS (FTPS) pro zabezpečený přenos.
  + **Správa:**
    - Správa probíhá pomocí **IIS Manageru** nebo pomocí PowerShellu.
    - Uživatelům lze přidělovat specifická oprávnění pro čtení nebo zápis na úložišti FTP.
* **Alternativní řešení:**
  + Aplikace jako FileZilla Server poskytují další možnosti správy FTP služby s vlastním grafickým rozhraním.

**B. V UNIX-like OS**

* **Obecně:**
  + Lze konfigurovat:
    - Anonymní přístup
    - Přihlašování k FTP pomocí lokálních uživatelských účtů
    - Omezit ověřené uživatele pro přístup pouze ke svým home složkám
      * soubor chroot\_list\_file je obsahuje line-by-line seznam uživatelských jmen, které mají povolen přístup mimo domovský adresář
    - Omezit šířku psáma pro uživatele v B/s
    - Omezit maximální počet připojení z IP
    - Omezit datové kanály na rozsah portů
    - Nastavit MOTD uvítacího banneru
* **FTP servery (např. vsftpd, ProFTPD, Pure-FTPd):**
  + **Konfigurace vsftpd:**
    - Konfigurační soubor /**etc/vsftpd/vsftpd.conf** obsahuje nastavení jako povolení anonymního přístupu, nastavení pasivního módu, SSL/TLS, omezení přístupu a další.
    - Příkazem systemctl start vsftpd se služba spouští a lze ji spravovat přes standardní mechanismy.
  + **ProFTPD a Pure-FTPd:**
    - Nabízejí flexibilní konfiguraci prostřednictvím vlastních konfiguračních souborů (např. /etc/proftpd/proftpd.conf), podporu virtuálních uživatelů, logging a bezpečnostní politiky.
* **Správa:**
  + Konfigurace a správa probíhá úpravou příslušných konfiguračních souborů a následným restartováním služby.
  + Systémové logy (např. /var/log/vsftpd.log) slouží k monitorování provozu a řešení problémů.
  + Pro zabezpečení lze využít opatření jako omezení přístupu na základě IP adres, nastavení limitů připojení nebo implementaci SSL/TLS.

**Shrnutí**

* **Služba WWW** je základní službou pro distribuci webového obsahu, využívá protokoly HTTP/HTTPS a může být implementována pomocí IIS (Windows) nebo Apache/Nginx (UNIX-like).
* **Služba FTP** umožňuje přenos souborů mezi klientem a serverem a existují možnosti jak pro Windows (IIS FTP Server, FileZilla Server), tak pro UNIX-like systémy (vsftpd, ProFTPD, Pure-FTPd).
* Konfigurace a správa obou služeb se provádí pomocí specializovaných administračních nástrojů a konfiguračních souborů, přičemž je kladen důraz na zabezpečení (SSL/TLS, autentizace) a monitorování provozu.