

Internet Information Services (IIS) 6.0

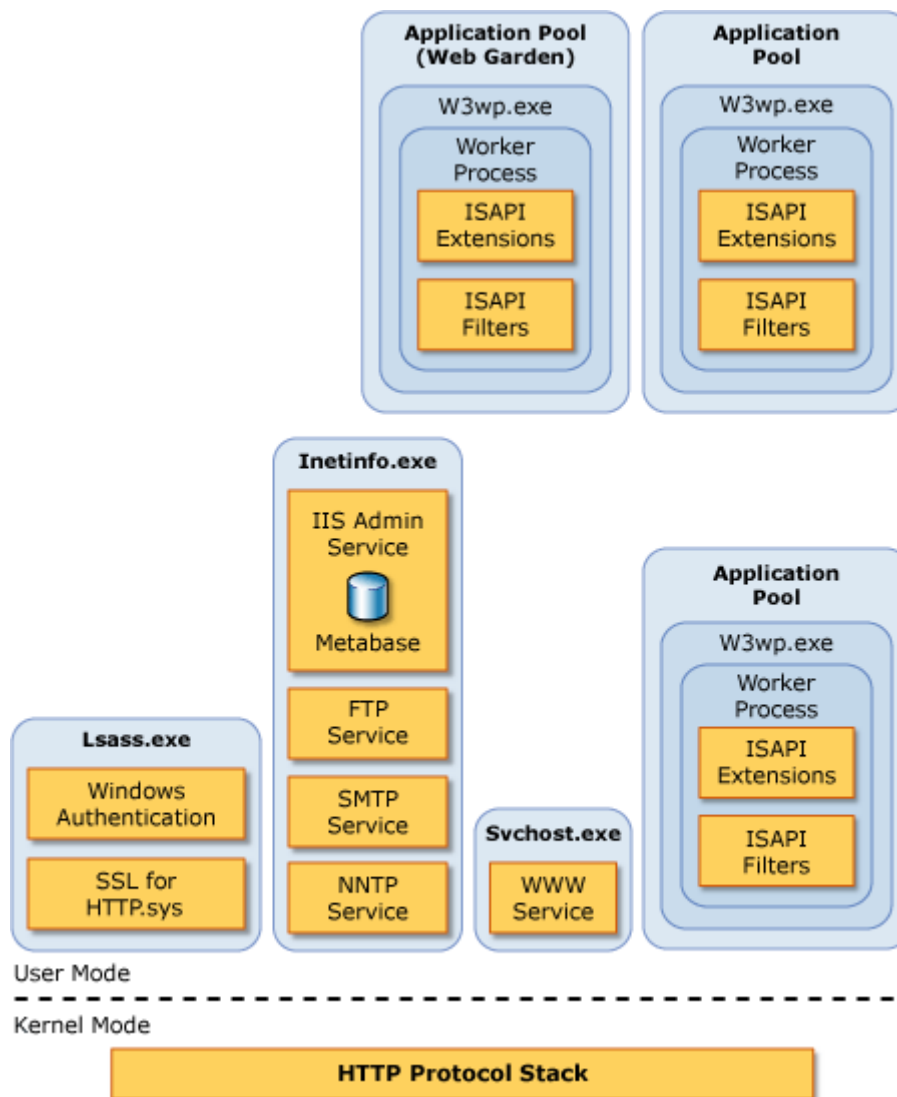
V operačním systému Windows Server 2003 je obsažena i služba IIS v 6.0. Služba IIS poskytuje jak www server tak i některé další služby (FTP, NNTP, ...). Jedná se o novou verzi služby IIS obsažené již v předchozích verzích Microsoft Windows Server. Službu IIS je možné, s určitými omezeními, instalovat i na pracovní stanici se systémem Windows XP. V současné době je k dispozici i beta verze IIS 7.0.

Základní pojmy relevantní k WWW:

- **World Wide Web (www)** – označení pro aplikace využívající protokol HTTP.
- **Hyper Text Transport Protokol (http)** – protokol z rodiny IP, který je využíván pro výměnu dokumentů HTML. Jeho verze 1.1 je definována v RFC 2616. Využívá obvykle port 80 v případě použití SSL - **https** pak port 443.
- **HTTPS** – protokol umožňuje prohlížet www stránky šifrovaně. Používá SSL nebo TLS šifrování.
- **Secure Socket Layer (SSL)** – pracuje na principu asymetrické šifry. Pracuje nad protokolem TCP/IP, šifruje data pro aplikační vrstvu, která využívá protokolu HTTP.
- **Uniform Resource Locator (URL)** – slouží k přesné specifikaci umístění zdrojů informací jako dokument nebo služba na webových serverech.
- **Active Server Pages (ASP)** – platforma nezávislá na programovacím jazyku, která umožňuje vykonání kódu na straně serveru a odeslání výsledku ve formě HTML uživateli.
- **.NET Framework** – rozšíření ASP, označováno jako ASP.NET. V ASP.NET je možné programovat v C#, C++, VBASICU atd. Rozšiřuje možnosti bezstavového protokolu HTTP implementací technik ViewState a SessionState. Aktuální verze: .NET Framework 3.0.
- **HyperText Preprocessor (PHP)** – skriptovací jazyk sloužící k tvorbě dynamických webových stránek.
- **Network Load Balancing (NLB)** – používá se pokud nestačí výkon jednoho serveru pro obsluhu požadavků. Definiuje farmu webových serverů, které vystupují pod jednou IP adresou.
- **Internet Server Application Programming Interface (ISAPI)** – plug-in moduly pro webové servery.

Architektura IIS 6.0

IIS verze 6 přináší novou architekturu, která umožňuje dosáhnout lepšího výkonu webových aplikací. Nazývá se **Application isolation**, díky tomu se aplikace (weby) navzájem neovlivňují a je možné jednotlivým aplikacím přiřadit určité množství systémových prostředků. Existují dva režimy IIS application isolation, oba však pracují nad službou **HTTP Protocol Stack**. Tato služba je zodpovědná za předávání http dotazů z internetu aplikaci.



Architektura IIS 6.0 – Worker Processes Isolation Mode

Služby IIS 6.0

Service Name	Description	Service Short Name	Core Component	Host
World Wide Web Publishing Service (WWW service)	Delivers Web publishing services.	W3SVC	Iisw3adm.dll	Svchost.exe
File Transfer Protocol (FTP)	Allows file uploads and downloads from remote systems.	MSFTPSVC	Ftpsvc.dll	Inetinfo.exe
Simple Mail Transfer Protocol (SMTP)	Sends and receives electronic messages (e-mail).	SMTPSVC	Smtpsvc.dll	Inetinfo.exe
Network News Transfer Protocol (NNTP)	Distributes network news messages.	NNTPSVC	Nntpsvc.dll	Inetinfo.exe
IIS Admin Service	Manages the metabase.	IISADMIN	Iisadmin.dll	Inetinfo.exe

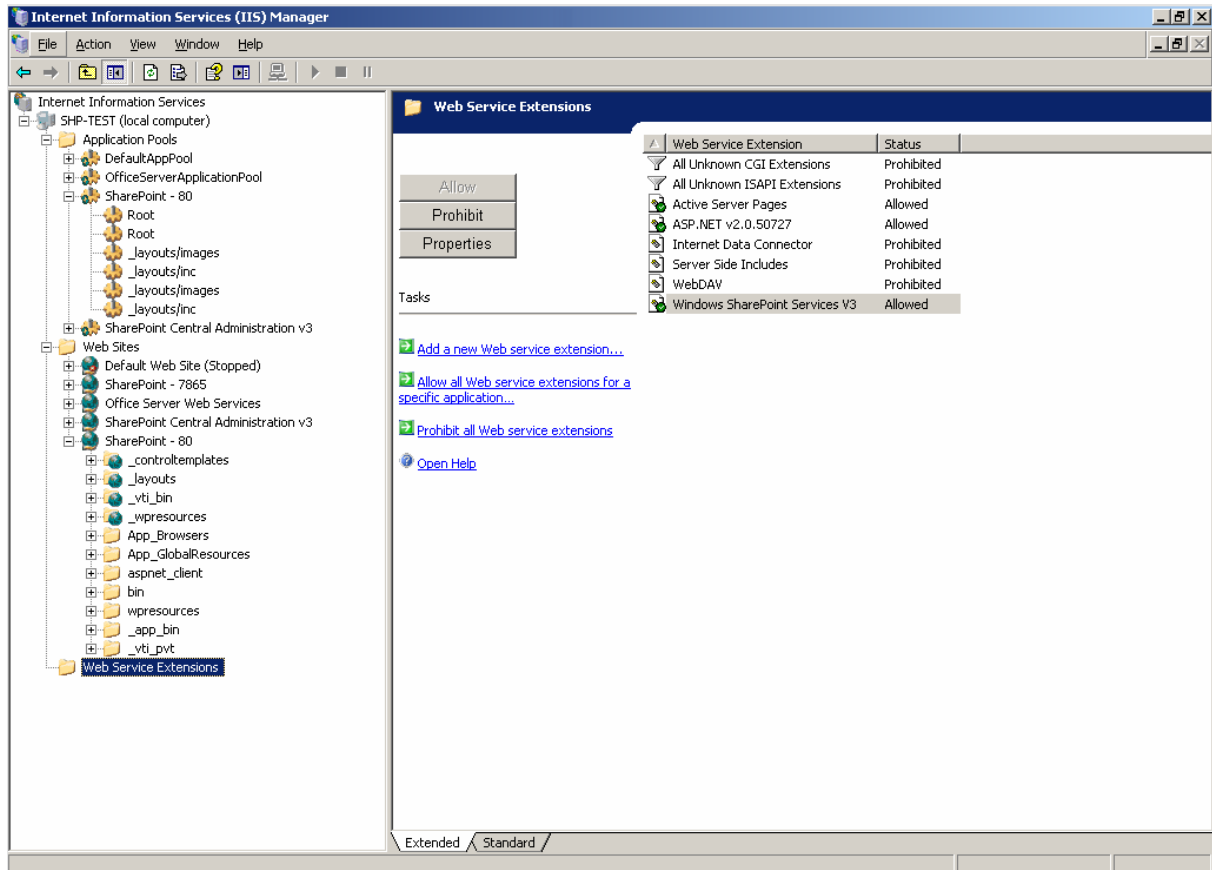
Jednotlivé služby IIS 6.0

Klíčové komponenty IIS 6.0

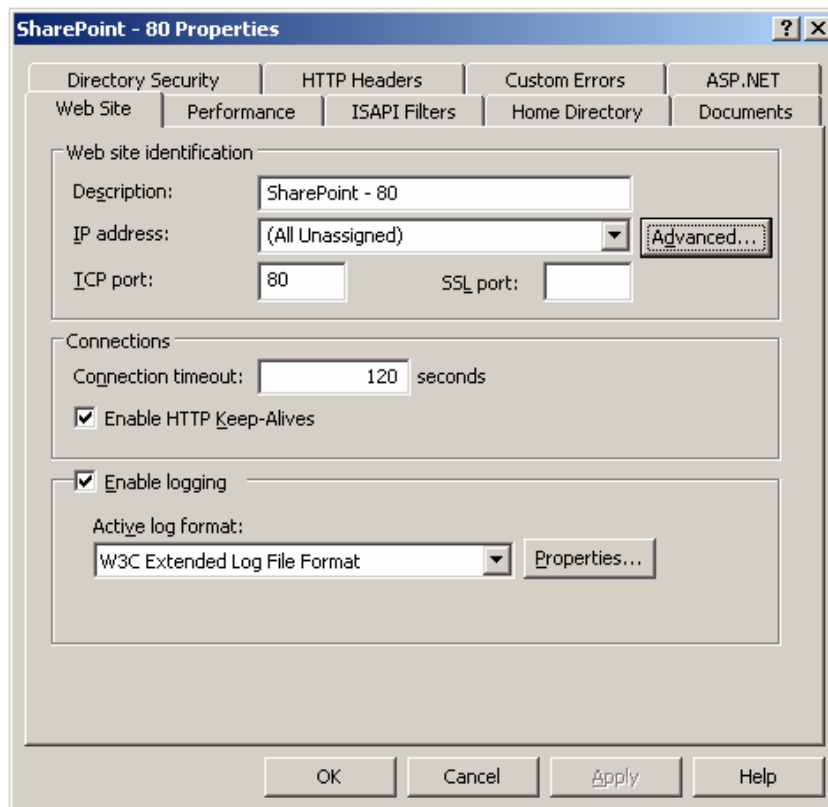
- **HTTP Protocol Stack (http.sys)** – součást operačního systému Windows, je součástí Kernelu. Zajišťuje následující služby:
 - Směrování HTTP dotazů do správné fronty k vyřízení
 - Ukládá si do paměti výsledky dotazů
 - Zajišťuje logování pro www službu
 - Implementuje QoS
- **Worker processes** – jedná se o uživatelský mód, který zpracovává požadavky jako vrátit statickou HTML stránku, volání rozšíření ISAPI nebo CGI. Tato komponenta také spouští ASP.NET aplikaci.
- **WWW Service Administration and Monitoring** – administrace služby IIS, WWW Service řídí Worker processes, určuje kdy je zapotřebí jej spustit, zastavit apod.
- **Inetinfo.exe** – běží v rámci worker process isolation mode. Hostuje IIS metabase a ostatní ne-webové služby (FTP, NNTP,...)
- **IIS Metabase** – uchovává informace o nastavení IIS ve formě XML. Jedná se o soubory:
 - **MetaBase.xml** - konfigurace IIS specifická k dané instalaci
 - **MBSchema.xml** – schéma metabase, výchozí konfigurace IIS

Nastavení IIS 6.0

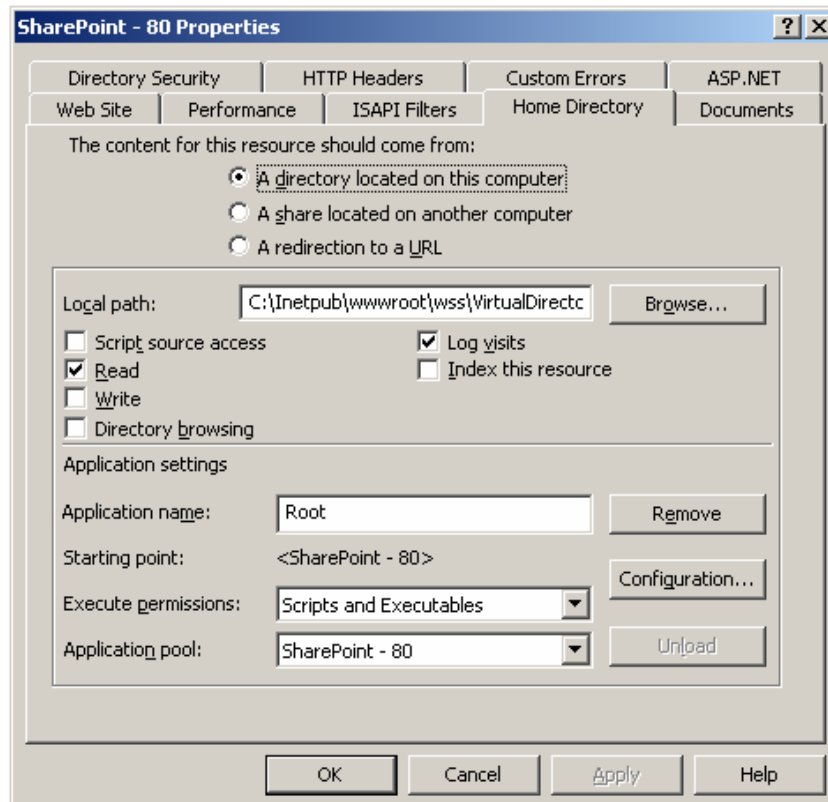
Instalace IIS se provádí přes Přidat nebo Odebrat součásti systému Windows. Můžeme vybrat, které komponenty chceme nainstalovat. Další rozšíření www serveru jako .NET Framework nebo PHP je zapotřebí instalovat zvlášť. Tato rozšíření jsou pak zobrazena jako Web Service Extensions.



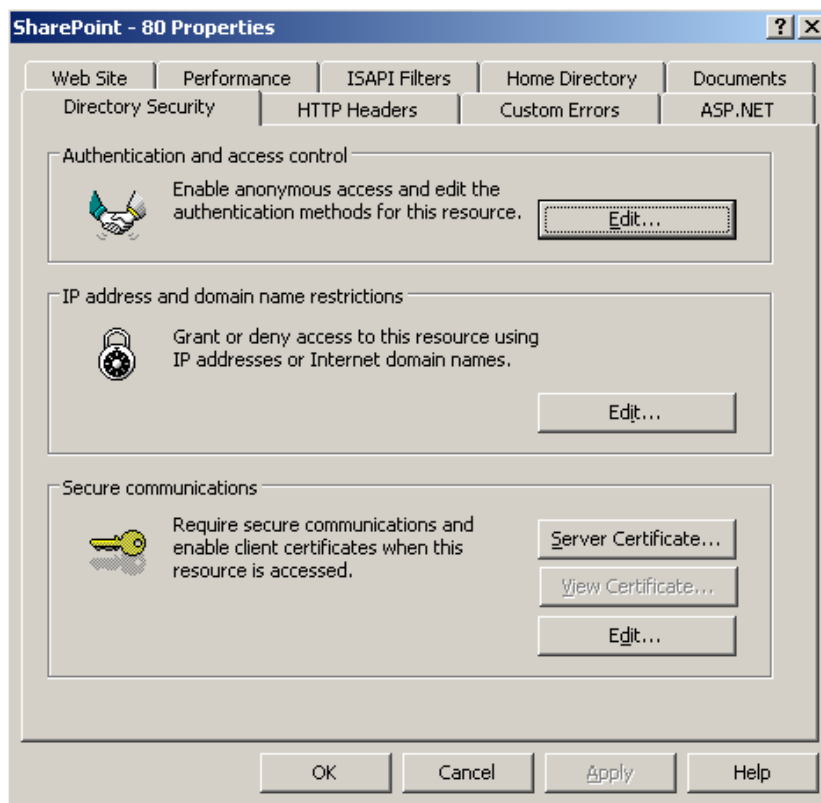
MMC konzole pro správu IIS



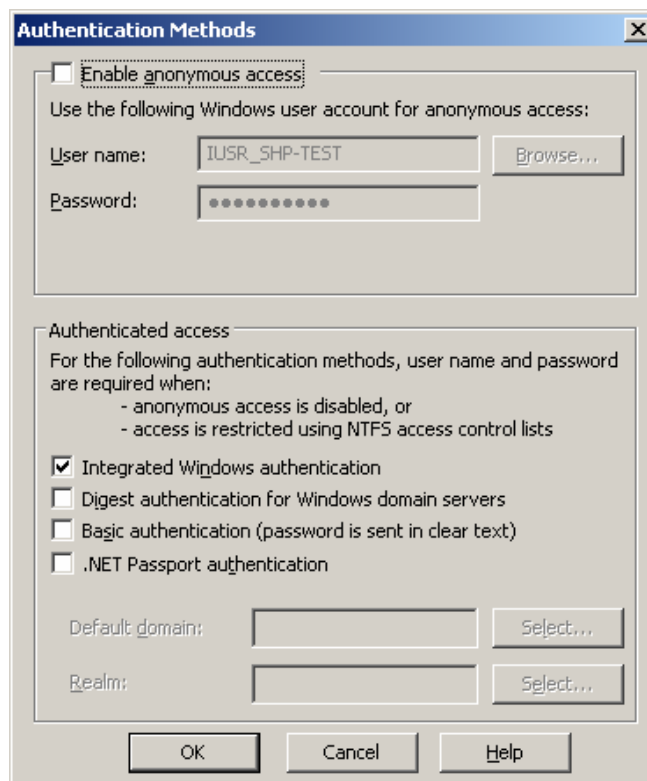
Základní nastavení webové stránky. Zde je důležitý zejména port, na kterém bude daná aplikace naslouchat. Jeden port může být použit pouze pro jednu webovou stránku.



Nastavení výchozího adresáře pro danou webovou stránku.



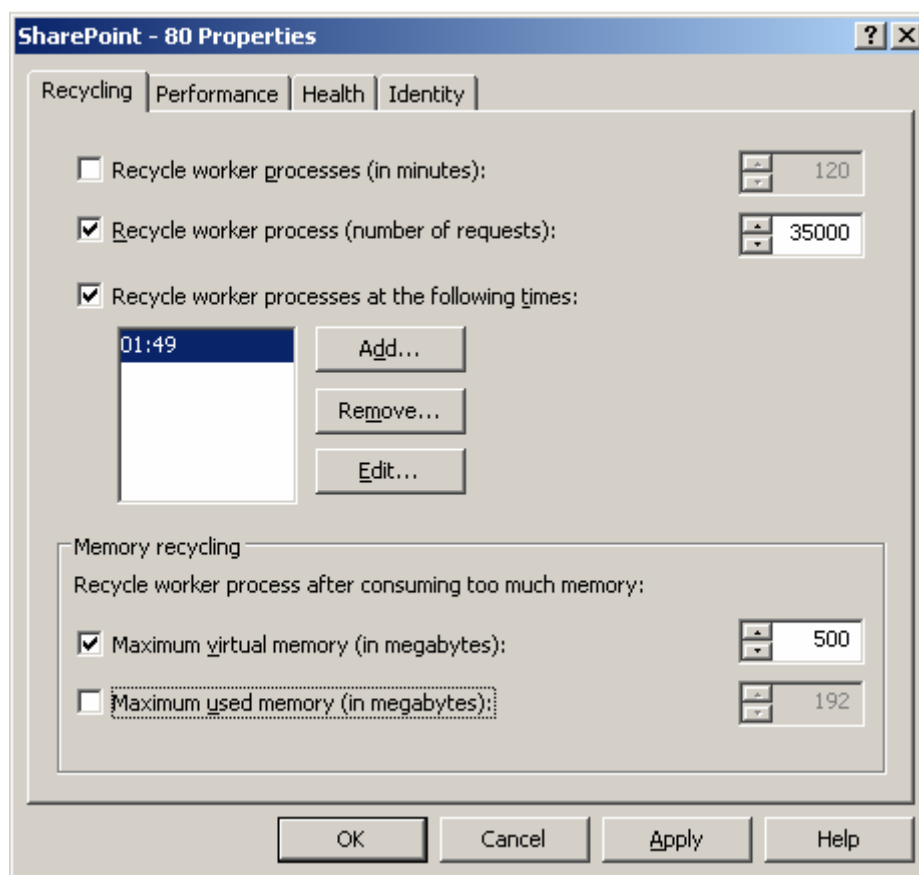
Nastavení zabezpečení webové stránky v IIS 6.0. V případě, že chceme použít SSL musíme instalovat certifikát serveru. Certifikát slouží k ověření totožnosti a k šifrování.



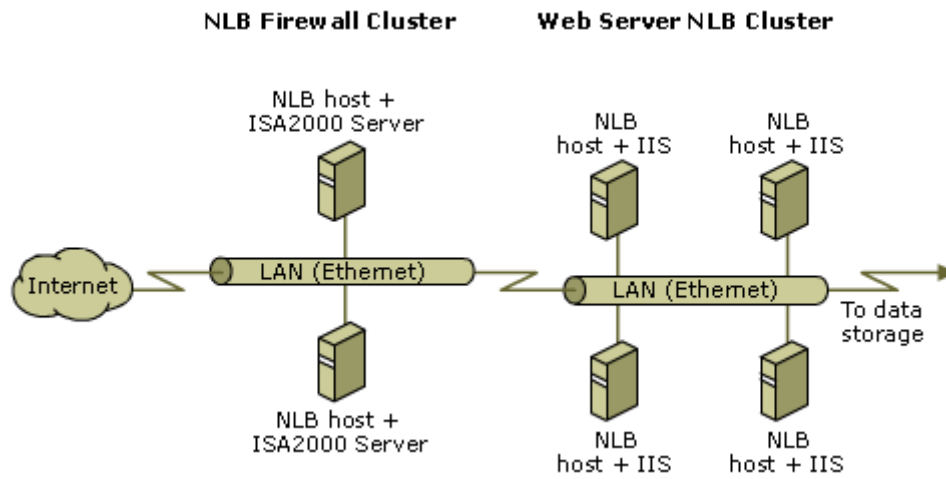
Nastavení autentikace pro přístup k webové stránce. V případě, že není povolen anonymní přístup, IIS se bude řídit oprávněními na základě souborového systému.

Ustavení SSL spojení (SSL handshake)

1. Klient pošle serveru požadavek na SSL spojení, spolu s různými doplňujícími informacemi (verze SSL, nastavení šifrování atd.).
2. Server pošle klientovi odpověď na jeho požadavek, která obsahuje stejný typ informací a hlavně certifikát serveru.
3. Podle přijatého certifikátu si klient ověří autentičnost serveru. Certifikát také obsahuje veřejný klíč serveru.
4. Na základě dosud obdržených informací vygeneruje klient základ šifrovacího klíče, kterým se bude šifrovat následná komunikace. Ten zašifruje veřejným klíčem serveru a pošle mu ho.
5. Server použije svůj soukromý klíč k rozšifrování základu šifrovacího klíče. Z tohoto základu vygenerují jak server, tak klient hlavní šifrovací klíč.
6. Klient a server si navzájem potvrdí, že od teď bude jejich komunikace šifrovaná tímto klíčem. Fáze handshake tímto končí.
7. Je ustaveno zabezpečené spojení šifrované vygenerovaným šifrovacím klíčem.
8. Aplikace od teď dál komunikují přes šifrované spojení. Například POST požadavek na server se do této doby neodešle.



Vlastnosti Application Pool. Zde definujeme nastavení worker process jako přiřazení systémových prostředků nebo účet pod kterým aplikace poběží.



Použití více webových serverů pro balancování výkonu a zajištění vysoké dostupnosti webové aplikace. U webových serverů není vhodné používat klasický cluster využívající SAN pole (active / active nebo active / pasive).