KAPITOLA 2

# Správa služeb a klientů SQL Serveru

**V této kapitole:**



Při řízení přístupu k databázovému serveru není nic důležitějšího než správné nastavení služeb, komponent a vlastností sítě. Každá instalace SQL Serveru má specificky nastavené služby, komponenty a síť, a toto nastavení následně určuje úroveň zabezpečení při přístupu k serveru, tj.:

- Kdo může k serveru přistupovat a jakým způsobem.
- K jakým vzdáleným zdrojům se mohou komponenty SQL Serveru připojovat (nebo přijímat připojení) a jakým způsobem.
- Jaké služby SQL Serveru se spouštějí při startu serveru automaticky a jaké se musejí v případě potřeby spouštět ručně.

Pomocí omezení typu, kdo, co a jak se k serveru může připojovat či kam a jak se může připojovat samotný server, je možné zúžit exponovaná místa serveru a tím zvýšit i úroveň zabezpečení serveru i celkový výkon, protože poběží pouze nezbytné služby a komponenty.

SQL Server využívá konfiguraci typu server-klient. Na straně klienta se pro přístup k SQL Serveru používají prvky OLE DB, ODBC, JDBC atd. Na serveru se přístup klientů k SQL Serveru řídí pomocí parametrů SQL Native Client Configuration. Přístup SQL Serveru k lokálním i vzdáleným zdrojům určují služby a síťová konfigurace SQL Serveru. Klientský přístup, služby SQL Serveru a konfigurace sítě se nastavují prostřednictvím nástroje SQL Server Configuration Manager.

# Správa přístupu ke komponentám SQL Serveru

Pro zvýšení úrovně zabezpečení databázového serveru je nutné povolit pouze funkce, které klienti a aplikace potřebují. Tento krok omezuje možnost zneužití serveru útočníky a uzavírá vstupní body pro potenciální útok.

Tabulka 2.1 obsahuje podrobné informace o funkcích, které lze v SQL Serveru konfigurovat u komponent Database Engine, Analysis Services a Reporting Services. V SQL Serveru 2012 je možné tyto funkce konfigurovat pomocí zásad pro správu, o nichž hovoří kapitola 3, „Správa na základě zásad".

Implicitně jsou všechny tyto funkce vypnuty.

**Tabulka 2.1:** Komponenty pro správu přístupu k povrchu SQL Serveru a jejich vlastnosti

| Komponenta/složka | Popis/použití |
|---|---|
| **DATABASE ENGINE** | |
| AdHocRemoteQueriesEnabled | Funkce OPENROWSET a OPENDATASOURCE mohou používat jednorázová připojení pro práci se vzdálenými zdroji bez toho, aby vzdálené zdroje explicitně konfiguroval administrátor. Jestliže aplikace či skripty dané funkce používají, je potřeba OPENROWSET a OPENDATASOURCE povolit. V opačném případě by tyto funkce měly být vypnuté. |
| ClrIntegrationEnabled | Pomocí integrace modulu CLR (common language runtime) je možné vytvářet uložené procedury, triggery, uživatelské typy a uživatelské funkce v jazycích Microsoft Visual Basic, C# a všech dalších jazycích, které podporuje Microsoft .NET Framework. Jestliže aplikace či skripty jazyky z rodiny .NET Framework používají, je nutné tuto funkci povolit, v opačném případě by tato funkce měla být vypnutá. |
| DatabaseMailEnabled | Komponenta Database Mail nahrazuje komponentu SQL Mail a je preferovanou metodou posílání poštovních zpráv z SQL Serveru. Database Mail používá protokol SMTP (Simple Mail Transfer Protocol). Tuto funkci je třeba povolit v případě, že SQL Server obsahuje databázi zpráv (mail host database, vytvořenou pomocí skriptu %ProgramFiles%\Microsoft SQL Server\MSSQL.1\MSSQL\Install\Install_DBMail_Upgrade.sql) a příslušné profily komponenty Database Email a aplikace a skripty využívají uloženou proceduru sp_send_dbmail pro zasílání poštovních zpráv z SQL Serveru. Jinak by měla být tato funkce vypnuta. |
| OleAutomationEnabled | OLE Automation umožňuje používat v dávkách, uložených procedurách a triggerech jazyka Transact-SQL (T-SQL) odkazy na SQL DMO a na vlastní objekty OLE Automation. Funkci je nutné povolit v případě, kdy se využívá technologie OLE Automation, například u rozšířených (extended) uložených procedur sp_OACreate, sp_OADestroy, sp_OAGetErrorInfo, sp_OAGetProperty, sp_OAMethod, sp_OASetProperty a sp_OAStop. V opačném případě by tato funkce měla být vypnutá. |

| Komponenta/složka | Popis/použití |
|---|---|
| RemoteDacEnabled | Při práci s nástrojem SQLCMD v příkazovém řádku a s parametrem -A mohou administrátoři provádět správu SQL Serveru prostřednictvím vyhrazeného spojení z příkazového řádku, lokálně i vzdáleně. Implicitně jsou povolena pouze lokální vyhrazená spojení. Funkce slouží k autorizaci vyhrazených vzdálených spojení. Jinak by měla být vypnuta. |
| ServiceBrokerEndpointActive | Service Broker poskytuje fronty a zprávy pro databázový stroj. Aplikace mohou Service Broker používat pro komunikaci mezi jednotlivými instancemi SQL Serveru. Jestliže aplikace používá Service Broker a jsou nakonfigurovány potřebné koncové body http, je možné nastavit stav jednotlivých koncových bodů na Started, Stopped nebo Disabled. |
| SoapEndpointsEnabled | S nativními webovými službami lze přistupovat k SQL Serveru prostřednictvím protokolu http a zpráv protokolu SOAP (Simple Object Access Protocol). Zprávy SOAP obsahují textové příkazy ve formátu XML. Probíhá-li výměna dat prostřednictvím SOAP a jsou nakonfigurovány potřebné koncové body http, lze nastavit jednotlivé body do stavu Started, Stopped nebo Disabled. Nativní webové služby využívají komponenty Reporting Services, Service Broker a Database Mirroring, ale nastavují se každá zvlášť. |
| SqlMailEnabled | SQL Mail lze použít ve spolupráci se staršími aplikacemi pro posílání poštovních zpráv z SQL Serveru protokolem SMTP. Funkce slouží starším aplikacím a skriptům pro posílání poštovních zpráv z SQL Serveru prostřednictvím uložené procedury xp_sendmail. Pokud se tato funkcionalita nevyužívá, měla by být vypnuta. |
| XPCmdShellEnabled | Uložená procedura xp_cmdshell spouští zadané příkazy prostřednictvím příkazového řádku operačního systému a vrací výsledky v podobě řádků textu. Funkci je nutné povolit v případě, kdy aplikace a skripty spouštějí příkazy v operačním systému. Ve výchozím nastavení mohou proceduru xp_cmdshell používat pouze členové standardní serverové role sysadmin. Oprávnění ke spouštění lze přiřadit i dalším uživatelům. U uživatelů v roli sysadmin se xp_cmdshell spouští v bezpečnostním režimu, v němž běží služba SQL Serveru. U dalších uživatelů přebírá xp_cmdshell zástupný účet příkazového řádku (specifikovaný pomocí xp_cmdshell_proxy_account). Jestliže zástupný účet není dostupný, volání procedury xp_cmdshell skončí chybou. |

| Komponenta/složka | Popis/použití |
|---|---|
| **ANALYSIS SERVICES** | |
| AdHocDataMiningQueriesEnabled | Funkce Data Mining Extensions OPENROWSET vytvoří připojení k datovému zdroji s využitím názvu poskytovatele a připojovacího řetězce. To umožní využívat jednorázová připojení ke vzdáleným datovým zdrojům, aniž by administrátor musel speciálně konfigurovat připojené nebo vzdálené servery. Tato vlastnost musí být povolena, jestliže aplikace či skripty používají funkci OPENROWSET při dolování dat. Jinak by tato vlastnost měla být zakázána, aby aplikace a skripty nemohly při používání funkce OPENROWSET předávat název poskytovatele a připojovací řetězec. |
| AnonymousConnectionsEnabled | Díky anonymním připojením mohou neověření anonymní uživatelé navazovat spojení s komponentou Analytical Services. Funkci je třeba povolit, jestliže aplikace a skripty potřebují přístup pro neověřené uživatele. V opačném případě je vhodné funkci vypnout. |
| LinkedObjectsLinksFromOtherInstancesEnabled | Prostřednictvím komponenty Analytical Services lze používat propojené objekty k propojení dimenzí a skupin měr mezi servery. Funkci je třeba zapnout, mají-li se k dané instanci připojovat jiné SQL Servery. V opačném případě je vhodné funkci vypnout. |
| LinkedObjectsLinksToOtherInstancesEnabled | Prostřednictvím komponenty Analytical Services lze používat propojené objekty k propojení dimenzí a skupin měr mezi servery. Připojení do jiných instancí je potřeba povolit, má-li se komponenta Analytical Services propojovat do jiných serverů. V opačném případě je vhodné ji vypnout. |
| ListenOnlyOnLocalConnections | Komponenta Analytical Services může pracovat se vzdálenými i s lokálními zdroji. Když se komponentě Analytical Services povolí práce se vzdálenými zdroji, komponenta na příslušném TCP/IP portu povolí připojení od instancí lokálních i vzdálených serverů. Když se komponentě Analytical Services práce se vzdálenými zdroji zakáže, stejně jako v prvním případě otevře port TCP/IP na severu, ale naslouchá pouze připojením od instancí lokálních serverů. Funkci je vhodné zapnout, má-li komponenta Analytical Services pracovat pouze s lokálními zdroji. V opačném případě je nutné ji vypnout. |
| UserDefinedFunctionsEnabled | Komponenta Analytical Services je integrována s technologií .NET Framework a může načítat sestavení (assemblies) obsahující uživatelsky definované funkce. Tyto funkce lze vytvářet pomocí CLR nebo prostřednictvím technologie COM. Objekty a funkce CLR využívají integrovaný model zabezpečení. Objekty typu COM tento model nepoužívají, a jsou proto ze své podstaty méně bezpečné. Funkci je třeba povolit, jestliže aplikace a skripty vyžadují uživatelsky definované funkce typu COM. V opačném případě je vhodné funkci vypnout, aby byly povoleny pouze funkce CLR. |

| Komponenta/složka | Popis/použití |
|---|---|
| **REPORTING SERVICES** | |
| **ScheduledEventsAndReportDeliveryEnabled** | **Prostřednictvím komponenty Reporting Services lze vytvářet jednorázové sestavy na vyžádání i naplánované opakovaně vytvářené sestavy. Obvykle se po nainstalování služeb sestav povolí oba typy sestav. Jestliže se naplánované sestavy nepoužívají, lze tento druh generování a doručování sestav prostřednictvím této funkce vypnout.** |
| **WebServiceRequestsAndHTTPAccessEnabled** | **Jednotlivé složky komponenty Reporting Services posílají zprávy ve formátu SOAP pomocí protokolu HTTP a využívají protokol HTTP pro zpracování požadavků při přístupu pomocí URL. Tuto funkcionalitu zajišťuje webová služba Report Server a umožňuje pracovat s komponentou Reporting Services prostřednictvím nástrojů Report Manager, Report Designer a SQL Server Management Studio. Server obvykle po nainstalování služeb sestav zpracovává požadavky zadané přes HTTP i webovou službu. Funkci je třeba povolit, jestliže klientské aplikace používají webovou službu Report Server nebo pokud se sestavy zpracovávají pomocí nástrojů Report Manager, Report Designer nebo SQL Server Management Studio. V opačném případě je vhodné funkci vypnout.** |

# Správa sítě a nativní klientské konfigurace SQL Serveru

Instalace SQL Serveru lze nakonfigurovat tak, aby umožňovaly místní i vzdálená připojení. SQL Server umí používat několik typů protokolů, například Shared Memory, Named Pipes nebo TCP/IP. Tyto protokoly mají samostatná nastavení jak na straně serveru, tak klienta. Tato nastavení je možné konfigurovat pomocí nástroje SQL Server Configuration Manager.

SQL Server Configuration Manager je součástí speciální verze programu Microsoft Management Console a je rovněž dostupný jako modul snap-in, který lze přidat do vlastních konzolí. SQL Server Configuration Manager lze spustit jednou z následujících metod:

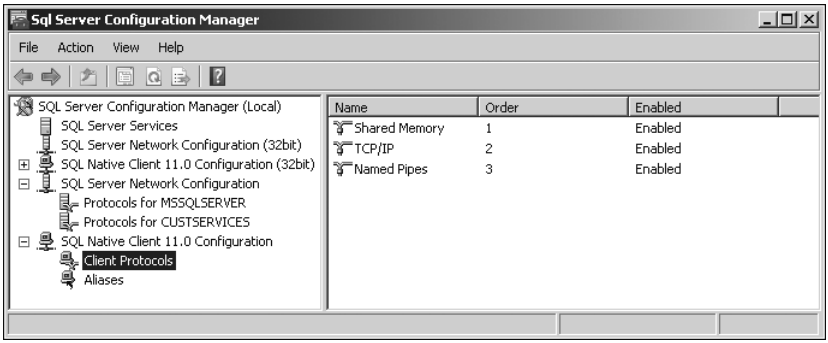
- Přihlaste se lokálně či vzdáleně k operačnímu systému databázového serveru a pak výběrem položek Start, Všechny programy, Microsoft SQL Server 2012, Configuration Tools a volbou SQL Server Configuration Manager spusťte SQL Server Configuration Manager. Nástroj můžete rovněž spustit klepnutím na Start, vložením textu **sqlservermanager11.msc** do vyhledávacího pole a stisknutím klávesy Enter.
- V nástroji SQL Server Management Studio otevřete klávesovou kombinací Ctrl+Alt+G okno Registered Servers. V panelu nástrojů okna Registered Servers vyberte příslušnou skupinu. Klepněte pravým tlačítkem myši na název serveru

a z nabídky vyberte položku SQL Server Configuration Manager. Není-li váš server v pohledu zaregistrován, je nutné jej přidat, což popisuje pasáž „Správa serverů“ v kapitole 1, „Správa SQL Serverů“.

Po spuštění nástroje SQL Server Configuration Manager se zobrazí hlavní okno, viz obrázek 2.1. SQL Server Configuration Manager umožňuje provádět několik základních úkolů:

- Spravovat služby související s instancemi SQL Serveru
- Nastavovat síťové protokoly používané instancemi SQL Serveru
- Spravovat nastavení síťových připojení

**Poznámka:** Na 64bitových počítačích existuje pro správu sítě a nastavení klienta více položek. Položky s příponou (32bit) slouží k 32bitovému nastavení a zbylé uzly k 64bitovému nastavení.




**Obrázek 2.1:** Klienti používají síťové protokoly ve stanoveném pořadí

Síť se konfiguruje samostatně pro každou instanci serveru pod položkou SQL Server Network Configuration. Klientská konfigurace se vytváří pro každého klienta pod položkou SQL Native Client Configuration.

Jestliže je povoleno a nastaveno více klientských protokolů, používají klienti protokoly ve stanoveném pořadí. Výchozí pořadí má tuto podobu:

1. Shared Memory
2. TCP/IP
3. Named Pipes

**Poznámka:** Jakýkoliv systém s nainstalovanou komponentou SQL Server Native Client slouží jako klient SQL Serveru. Mohou mezi ně patřit systémy, na nichž běží Windows 7, i Windows Server 2008 a Windows Server 2008 R2.

## Správa konfigurace připojení

V SQL Serveru lze povolit lokální, vzdálená i vyhrazená připojení. Lokální připojení používají aplikace běžící na počítači, na němž rovněž běží SQL Server. Vzdálená připojení využívají klienti, kteří se k serveru připojují, aplikace běžící na jiných serverech a jiné servery, na nichž běží SQL Server. Vyhrazená, dedikovaná spojení představují speciální diagnostickou metodu, kterou využívají administrátoři SQL Serveru při údržbě SQL Serveru v situaci, kdy běžné připojení není možné (a ovládají se jako funkce daná konfigurací serveru, nikoli jako typ připojení, který lze povolit).

**Poznámka:** Výchozí nastavení připojení závisí na nastavení účtů služeb, nainstalovaných komponentách a na dalších vlastnostech instalace, například na tom, jestli byl proveden upgrade na poslední verzi nebo jde o novou instalaci. Nová instalace obvykle umožní pouze lokální připojení. Při nainstalování dalších komponent, například Reporting Services, obvykle dojde k povolení místních i vzdálených připojení.

Povolení lokálních připojení přináší očividné bezpečnostní výhody, ale ne vždy je možné SQL Server provozovat v tomto režimu. Častokrát (spíše ve většině případů) je nutné povolit příchozí připojení ze vzdálených klientů a serverů a v takovém případě mohou povolené protokoly připojení ovlivnit množství spotřebovávaných zdrojů i relativní bezpečnost serveru. SQL Server 2012 může pro vzdálená připojení používat protokoly TCP/IP a Named Pipes nebo oba společně.

TCP/IP je hojně používaná sada protokolů, která obsahuje Transmission Control Protocol (TCP) a Internet Protocol (IP). SQL Server naslouchá a komunikuje prostřednictvím dynamických portů, statických portů nebo obou typů, v závislosti na nastavení. SQL Server podporuje jak protokol IP verze 4 (IPv4), tak i verze 6 (IPv6). IP adresy, které SQL Server používá pro síťovou komunikaci, rovněž závisejí na nastavení. TCP/IP implementuje standardy pro směrování provozu, což zajišťuje, že datové pakety dorazí na místo určení, i standardy zabezpečení komunikace, které chrání citlivé informace. Díky tomu je protokol TCP/IP ideální způsob komunikace v lokálních sítích (LAN) i veřejných sítích (WAN).

Named Pipes (pojmenované roury) je protokol určený pro místní sítě LAN. V protokolu Named Pipes používá jeden proces část paměti pro předávání informací jinému procesu a výstup z jednoho procesu se stává vstupem do jiného procesu. Druhý proces může být lokální, tedy běžet na stejném serveru jako první proces, nebo může být vzdálený a běžet na jiném počítači než první proces. Lokální pojmenované roury sice běží v privilegovaném režimu a jsou velmi rychlé, ale vzdálené pojmenované roury neběží příliš dobře na pomalejších sítích, protože obvykle generují velké datové přenosy po síti.

Vzhledem k tomu, že protokoly TCP/IP a Named Pipes vyžadují otevření specifických, odlišných portů na firewallu, je možné na serveru nakonfigurovat používání pouze jednoho z těchto protokolů a snížit potenciální prostor pro útoky. Před změnou povole-

ného typu spojení je však potřeba zajistit, že všichni klienti a aplikace používají správnou síťovou knihovnu.

V protokolu TCP/IP může SQL Server komunikovat prostřednictvím protokolu IP a knihovny TCP/IP Sockets Net-Library. Výchozí naslouchací port pro standardní instanci je port TCP 1433. Výchozí naslouchací port pro pojmenované instance se určuje dynamicky nebo ručně prostřednictvím nástroje SQL Server Configuration Manager. Port TCP 1434 slouží pro klientská připojení. Při použití pojmenovaných rour používá SQL Server 2012 síťovou knihovnu Named Pipes Net-Library a komunikuje prostřednictvím standardní síťové adresy: \\.\pipe\sql\query pro výchozí instanci a \\.\pipe\MSSQL$*nazevinstance*\sql\query pro pojmenovanou instanci. Pojmenované roury vyžadují otevřít na firewallu určitý rozsah portů pro komunikaci. Při použití pojmenovaných rour server naslouchá na portu TCP 445.

SQL Server 2012 rovněž podporuje protokol Shared Memory pro lokální připojení. Protokoly VIA, NWLink, IPX/SPX a AppleTalk už nejsou podporovány.

## Nastavení síťového protokolu Shared Memory

Protokol Shared Memory slouží pouze pro lokální připojení. Je-li protokol povolen, může se prostřednictvím něho připojit k serveru libovolný lokální klient. Nemají-li lokální klienti protokol Shared Memory používat, lze jej vypnout. Protokol Shared Memory se zapíná a vypíná následujícím způsobem:

1. Spusťte SQL Server Configuration Manager. Otevřete položku SQL Server Network Configuration a pro SQL Server, s nímž chcete pracovat, vyberte položku Protocols For.
2. Klepněte pravým tlačítkem myši na protokol Shared Memory a pak proveďte jednu z následujících voleb:
   - Volbou Enable povolte používání protokolu.
   - Volbou Disable zakažte používání protokolu.

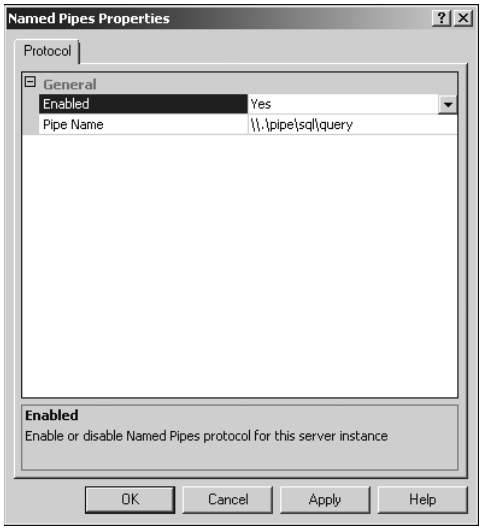
## Nastavení síťového protokolu Named Pipes

Protokol Named Pipes se používá především pro připojení aplikací napsaných pro starší verze systému Microsoft Windows. Při povolení protokolu Named Pipes použije SQL Server síťovou knihovnu Named Pipes Net-Library a komunikuje prostřednictvím standardní síťové adresy: \\.\pipe\sql\query pro výchozí instanci a \\.\pipe\MSSQL$*nazevinstance*\sql\query pro pojmenovanou instanci. Kromě povolení či zákazu protokolu Named Pipes lze nastavovat vlastnosti protokolu a měnit způsob jeho používání.

Síťovou konfiguraci protokolu Named Pipes lze nastavovat následujícím způsobem:

1. Spusťte SQL Server Configuration Manager. Otevřete položku SQL Server Network Configuration a pro SQL Server, s nímž chcete pracovat, zvolte položku Protocols For.

2. Klepněte pravým tlačítkem myši na protokol Named Pipes a z kontextové nabídky vyberte položku Properties.
3. Jak ukazuje obrázek 2.2, lze provádět následující změny:
   - V nabídce Enabled lze protokol povolit nebo zakázat. Chcete-li protokol povolit, zvolte možnost Yes, chcete-li jej zakázat, nastavte možnost No.
   - V poli Pipe Name lze změnit název výchozí roury. (Nezapomeňte upravit také konfiguraci na klientech.)
4. Klepněte na OK.




**Obrázek 2.2:** Nastavení pojmenovaných rour pro SQL Server

## Nastavení síťového protokolu TCP/IP

Protokol TCP/IP je preferovaným protokolem pro připojení k SQL Serveru. Při práci s protokolem TCP/IP naslouchá SQL Server požadavkům na konkrétním portu TCP a na konkrétní IP adrese. Standardně SQL Server naslouchá na portu TCP 1433 na všech IP adresách, jež jsou nakonfigurovány v síťových kartách. Z bezpečnostních důvodů může být někdy vhodné nastavit pro SQL Server protokol TCP/IP jinak. V takovém případě existuje několik možností:

- SQL Server lze nastavit tak, aby naslouchal na všech nakonfigurovaných IP adresách, a používat stejné nastavení portu pro TCP pro všechny dotčené IP adresy.
- SQL Server lze nastavit tak, aby naslouchal jen na konkrétně povolených IP adresách, a pak nakonfigurovat pro každou IP adresu samostatný naslouchací port TCP.

V obou přístupech lze nastavit naslouchací porty TCP ručně nebo dynamicky. Ručně přiřazený naslouchací port je statický a změní se jen při přiřazení nové hodnoty.

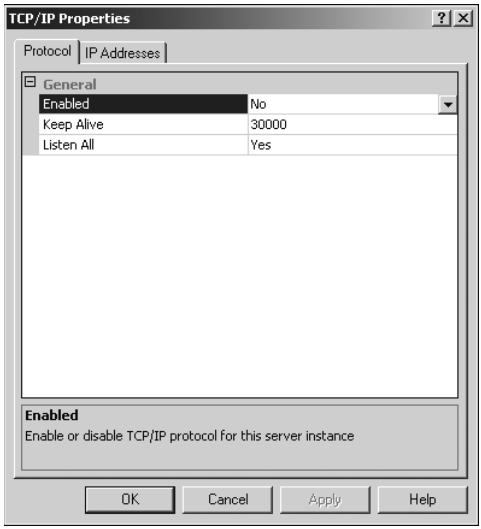
U dynamicky přiřazovaných portů přiřadí daná instance SQL Serveru naslouchací port TCP dynamicky pokaždé při spuštění dané služby. Protože naslouchací port TCP se přiřazuje dynamicky při startu, klientská aplikace potřebuje pomocnou službu, která určí příchozí naslouchací port, a v tu chvíli vstupuje do hry služba SQL Server Browser. Jestliže instance SQL Serveru používají dynamicky přiřazené porty TCP, služba SQL Server Browser ověřuje příchozí připojení a přesměrovává je na aktuální port příslušné instance SQL Serveru.

**Upozornění:** Dynamicky přiřazované porty není vhodné používat v situaci, kdy se klienti připojují přes firewall. Klienti by pak měli problémy pokaždé, když se dynamicky přiřazený port změní, protože by pro správnou funkčnost bylo nutné ještě upravit konfiguraci firewallu.

### *Zakázání, povolení a nastavení TCP/IP*

Protokol TCP/IP lze zakázat, povolit nebo nastavit následujícím postupem:

1. Spusťte SQL Server Configuration Manager. Otevřete položku SQL Server Network Configuration a pak zvolte pro příslušnou instanci SQL Serveru položku Protocols For.
2. Klepněte pravým tlačítkem myši na možnost TCP/IP a z kontextové nabídky vyberte položku Properties. Zobrazí se dialogové okno TCP/IP Properties.
3. Na kartě Protocol můžete v nabídce Enabled protokol zakázat nebo povolit. Chcete-li povolit používání protokolu, zvolte možnost Yes, pro zakázání protokolu zvolte No. Jestliže jste právě protokol TCP/IP zakázali, klepněte na OK a zbývající kroky přeskočte.
4. Na kartě Protocol (viz obrázek 2.3) lze nastavovat parametry, jimiž se řídí způsob, jak daná instance SQL Serveru udržuje nečinná spojení TCP/IP. Slouží k tomu dva parametry:
   - **Listen All** – určuje, zdali SQL Server naslouchá na všech IP adresách, které jsou nastaveny na síťových kartách. Jestliže tento parametr nastavíte na Yes, nastavení vlastností v poli IPAll na kartě IP Adresses bude platit pro všechny aktivní IP adresy. Nastavíte-li parametr na No, musíte nastavit každou IP adresu samostatně, v odpovídajících polích vlastností na kartě IP Adresses.
   - **Keep Alive** – určuje, jak často se SQL Server snaží ověřit, že je počítač na druhém konci vzdáleného připojení stále dostupný. Ve výchozím nastavení ověřuje SQL Server vzdálené připojení po 30 000 milisekundách (30 sekundách) nečinnosti. Ve většině případů vyhoví hodnota mezi 30 a 60 sekundami. V závislosti na vytíženosti serveru a významu klientské aktivity je možné ověřovat a udržovat spojení častěji a zajistit, že nedojde k ukončení spojení. Lze použít nižší hodnoty, třeba 15 000 či 20 000 milisekund (15 až 20 sekund), což zajistí častější prověření nečinných připojení.




**Obrázek 2.3:** Nastavení protokolu TCP/IP pro příslušnou instanci serveru

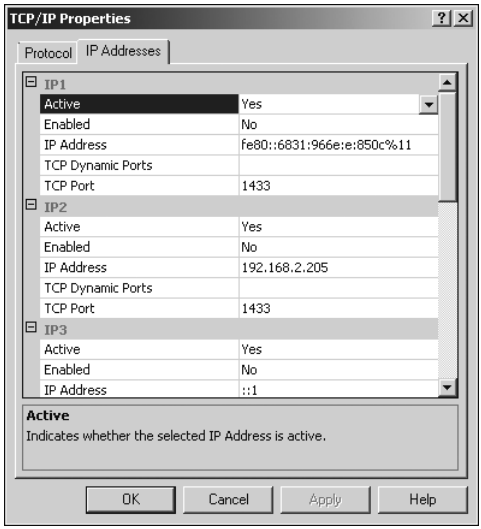
5. Klepněte na tlačítko OK.

### *Statické síťové nastavení TCP/IP*

Instanci SQL Serveru lze nastavit na používání statické síťové konfigurace TCP/IP následujícím způsobem:

1. Spusťte SQL Server Configuration Manager. Otevřete položku SQL Server Network Configuration a pak zvolte pro příslušnou instanci SQL Serveru položku Protocols For.
2. Klepněte pravým tlačítkem myši na možnost TCP/IP a z kontextové nabídky vyberte položku Properties. Na kartě IP Adresses v dialogu TCP/IP Properties by měly být zobrazeny záznamy pro adresy IPv4 a IPv6 nastavené pro server, viz obrázek 2.4. Jednotlivé IP adresy, seřazené podle čísla (například IP1, IP2, IP3 atd.), se používají v situaci, kdy SQL Server naslouchá na konkrétních IP adresách. Možnost IPAll se používá, jestliže SQL Server naslouchá na všech IP adresách serveru.

**Poznámka:** IP adresy 127.0.0.1 a ::1 jsou místní adresy pro IPv4 a IPv6. Tyto adresy slouží k naslouchání připojení od lokálních klientů.




**Obrázek 2.4:** Nastavení potřebných IP adres a naslouchání

3. Chcete-li, aby SQL Server naslouchal na všech nastavených IP adresách serveru, je potřeba provést následující kroky:
   a. Na kartě Protocol nastavte volbu Listen All na Yes.
   b. Na kartě IP Adresses nastavte jeden naslouchací port TCP pro všechny IP adresy (položka IPAll). Výchozí hodnota je 1433. Chcete-li změnit naslouchací port TCP, vložte potřebnou hodnotu do příslušného pole.
4. Chcete-li povolit naslouchání pouze na konkrétních IP adresách a portech TCP, postupujte následovně:
   a. Na kartě Protocol nastavte volbu Listen All na No.
   b. Na kartě IP Adresses zadejte IP adresy, na nichž má SQL Server aktivně naslouchat – nastavením položky Active u dané IP adresy na Yes a položky Enabled na Yes. Pak zadejte pro každou IP adresu do příslušného pole naslouchací port TCP.
   c. Na kartě IP Adresses zadejte IP adresy, na nichž SQL Server nemá aktivně naslouchat – nastavením položky Active u dané IP adresy na No a položky Enabled na No.
5. Klepněte na tlačítko OK.

**Tip:** SQL Server může na jedné IP adrese naslouchat na více portech TCP. Stačí porty vypsat oddělené čárkami, například 1433,1533,1534. Mezi čárkou a hodnotou nesmí být mezera. Pole TCP Port je omezeno na maximální délku 2 047 znaků.

### *Dynamické síťové nastavení TCP/IP*

Instanci SQL Serveru lze také nastavit na dynamické používání sítě TCP/IP, a to následujícím způsobem:

1. Spusťte SQL Server Configuration Manager. Otevřete položku SQL Server Network Configuration a pak vyberte pro příslušnou instanci SQL Serveru položku Protocols For.
2. Klepněte pravým tlačítkem myši na možnost TCP/IP a z kontextové nabídky zvolte položku Properties. Na kartě IP Adresses v dialogu TCP/IP Properties by měly být zobrazeny záznamy pro adresy IPv4 a IPv6 nastavené pro server, viz obrázek 2.4. Jednotlivé IP adresy, seřazené podle čísla (například IP1, IP2, IP3 atd.), se používají v situaci, kdy SQL Server naslouchá na konkrétních IP adresách. Možnost IPAll se používá, jestliže SQL Server naslouchá na všech IP adresách serveru.

**Poznámka:** IP adresy 127.0.0.1 a ::1 jsou místní adresy pro IPv4 a IPv6. Tyto adresy slouží k naslouchání připojení od lokálních klientů.

3. Chcete-li, aby SQL Server naslouchal na všech nastavených IP adresách serveru na jednom a tomtéž dynamickém portu, je potřeba udělat následující:
   a. Na kartě Protocol nastavte volbu Listen All na Yes.
   b. Na kartě IP Adresses odrolujte dolů a do pole TCP Dynamic Ports vložte hodnotu **0** (nula).
4. Chcete-li povolit naslouchání pouze na konkrétních IP adresách, postupujte následovně:
   a. Na kartě Protocol nastavte volbu Listen All na No.
   b. Na kartě IP Adresses zadejte IP adresy, na nichž má SQL Server aktivně naslouchat – nastavením položky Active u dané IP adresy na Yes a položky Enabled na Yes. Pak zadejte do příslušného pole TCP Dynamic Ports hodnotu **0** (nula).
   c. Na kartě IP Adresses zadejte IP adresy, na nichž SQL Server nemá aktivně naslouchat – nastavením položky Active u dané IP adresy na No a položky Enabled na No.
5. Klepněte na tlačítko OK.

## Nastavení zabezpečení pro nativního klienta

Klienti standardně nepoužívají Secure Socket Layer (SSL) ani se nepokoušejí ověřovat serverové certifikáty. Šifrování protokolu nebo ověřování serverových certifikátů lze vynutit následujícím způsobem:

1. Spusťte SQL Server Configuration Manager. Otevřete položky SQL Server Network Configuration a SQL Native Client Configuration.

2. Klepněte pravým tlačítkem myši na SQL Native Client Configuration a vyberte položku Properties.
3. U možnosti Force Protocol Encryption zvolte Yes, chcete-li vynutit šifrování protokolu pomocí SSL. V opačném případě zvolte možnost No. V takovém případě se bude používat nešifrované připojení.
4. U možnosti Trust Server Certificate zvolte Yes, mají-li klienti ověřovat serverové certifikáty. V opačném případě zvolte možnost No. V takovém případě se validace serverových certifikátů neuplatní.

## Nastavení pořadí protokolů nativního klienta

Shared Memory je vždy preferovaný protokol pro lokální připojení. Je-li povoleno, používá se před ostatními povolenými protokoly.

Protokol Shared Memory lze zakázat a pořadí protokolů lze změnit následujícím způsobem:

1. Spusťte SQL Server Configuration Manager. Otevřete položku SQL Native Client Configuration a pak klepněte na položku Client Protocols.
2. Klepněte pravým tlačítkem myši na kterýkoliv z vypsaných protokolů a zvolte položku Order. Zobrazí se dialog Client Protocols Properties.
3. V dialogu Client Protocols Properties, který vidíte na obrázku 2.5, můžete provést následující:
   - Změnit pořadí jednotlivých povolených protokolů. Nejprve klepněte na název protokolu, který chcete přemístit, a pak pomocí šipek napravo od seznamu Enabled Protocols umístěte protokol do požadovaného místa v seznamu.
   - Zakázat či povolit protokoly. Chcete-li zakázat povolený protokol, označte jej a pak klepněte na šipku směřující doleva, čímž jej přesunete do seznamu Disabled Protocols. Chcete-li povolit zakázaný protokol, označte jej a pak klepněte na šipku směřující doprava, čímž jej přesunete do seznamu Enabled Protocols.
   - Povolit či zakázat protokol Shared Memory. Chcete-li povolit protokol Shared Memory pro připojení lokálních klientů, zaškrtněte možnost Enable Shared Memory Protocol. Chcete-li protokol Shared Memory zakázat, volbu Enable Shared Memory Protocol zrušte.
4. Klepněte na tlačítko OK.