combit GmbH
Untere Laube 30
78462 Konstanz

Whitepaper

Produkt: combit address manager / Relationship Manager

Client-Verbindungsprobleme beheben

© Copyright combit GmbH, Alle Rechte vorbehalten.

Inhalt

© Copyright combit GmbH, Alle Rechte vorbehalten.

Einleitung

In Abhängigkeit Ihrer Windows bzw. SQL Server Konfiguration müssen unter Umständen einer oder mehrere der nachfolgenden Punkte überprüft werden, um Verbindungen von einem Client PC auf den Server zu ermöglichen.

© Copyright combit GmbH, Alle Rechte vorbehalten.

SQL Server Konfiguration

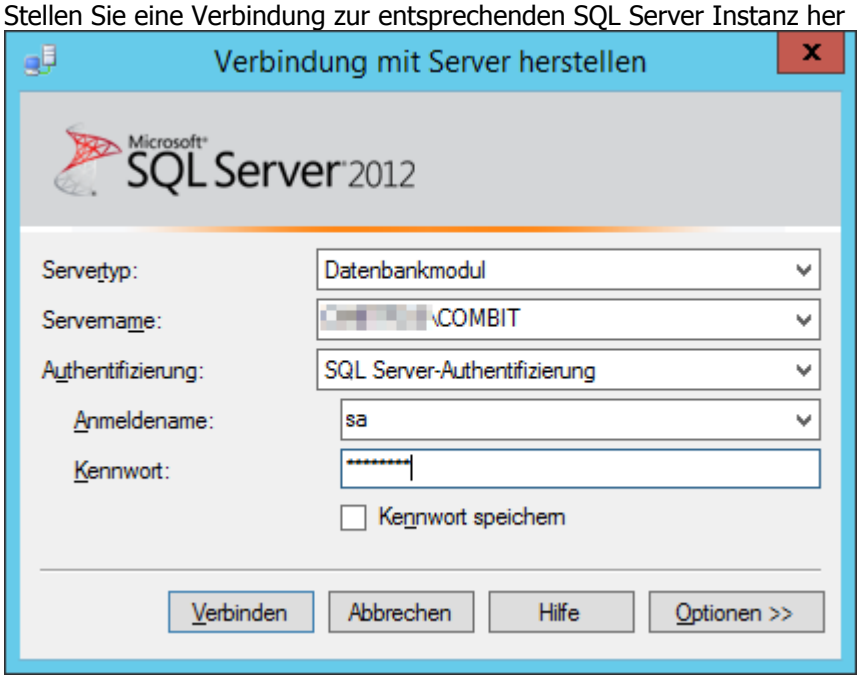
Standardmäßig ermöglicht der SQL Server nur lokale Clientverbindungen. Beim Start des address managers / Relationship Managers auf dem Client erhalten Sie ohne die entsprechende Konfiguration folgende Meldung: **SQL Server ist nicht vorhanden, oder der Zugriff wurde verweigert**.

Damit der address manager / Relationship Manager auf dem Client sich mit dem SQL Server bzw. der Datenbank verbinden kann, prüfen Sie bitte die nachfolgenden Punkte.

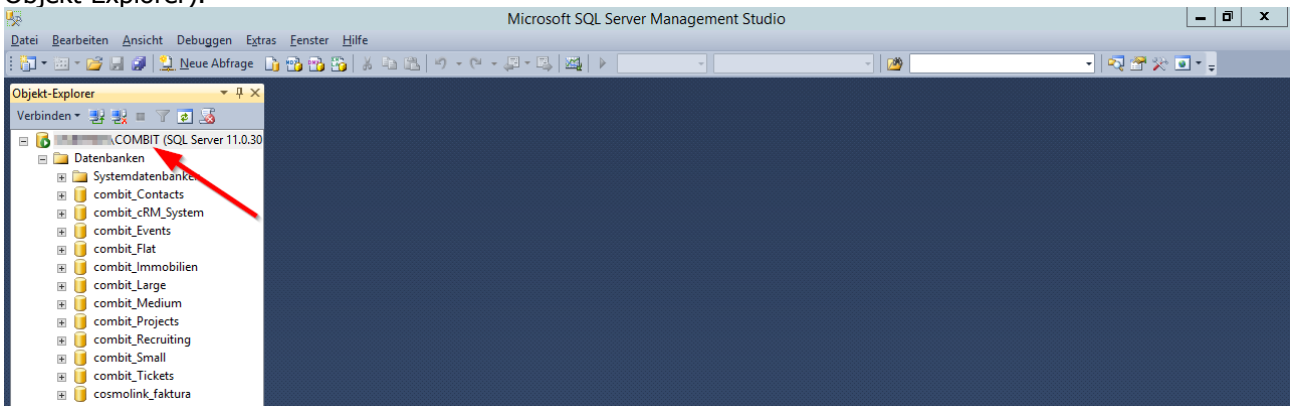
Konfiguration der Remote Verbindungen

Starten Sie aus der SQL Server Programmgruppe im Startmenü das Programm **SQL Server Management Studio**.

Stellen Sie eine Verbindung zur entsprechenden SQL Server Instanz her

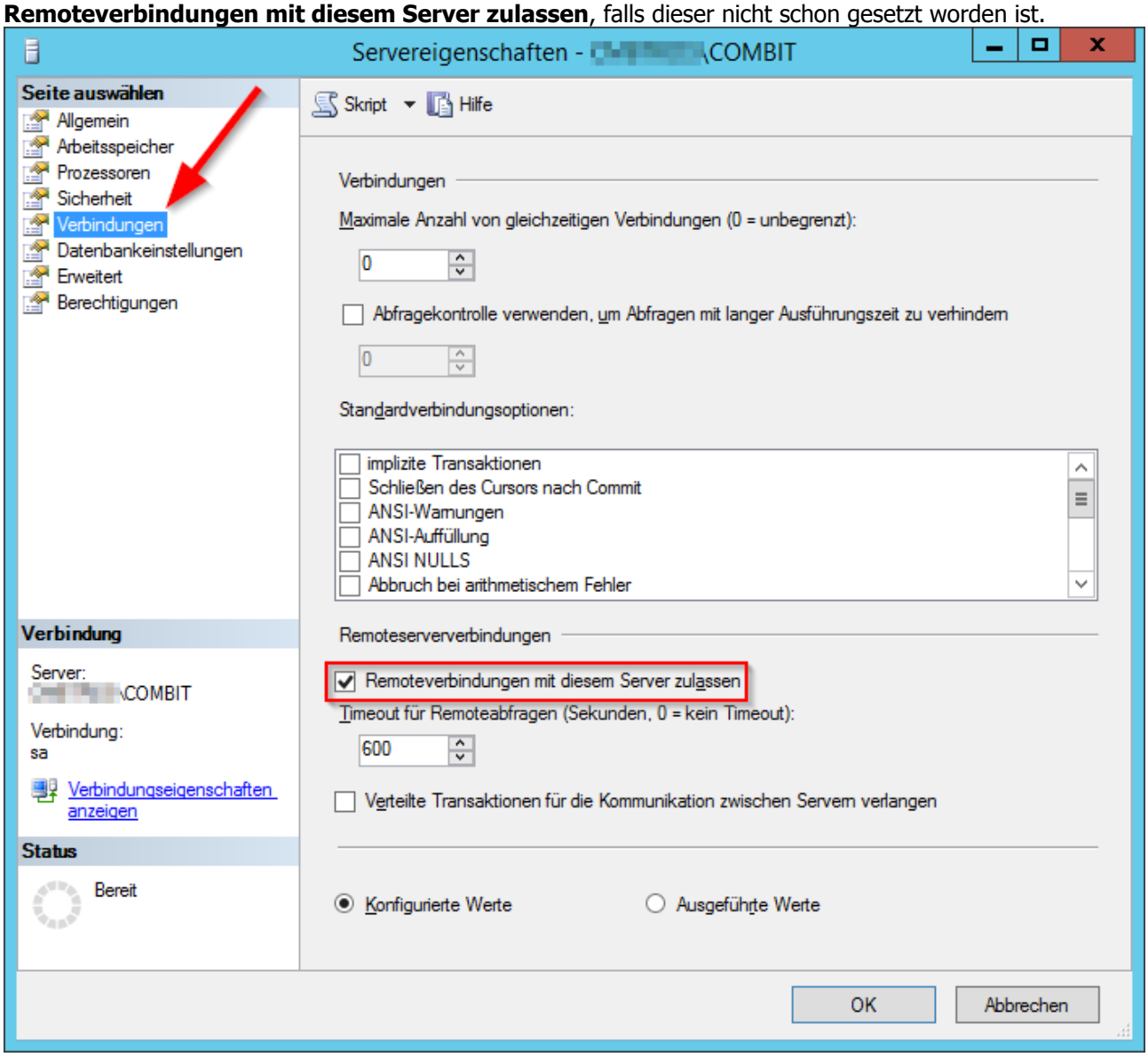


Öffnen Sie die **Eigenschaften** des Servers über einen **Rechtsklick** auf die Instanz (der oberste Eintrag im Objekt-Explorer).



© Copyright combit GmbH, Alle Rechte vorbehalten.

Wählen Sie im folgenden Fenster die Seite **Verbindungen** aus und setzen Sie den Haken bei **Remoteverbindungen mit diesem Server zulassen**, falls dieser nicht schon gesetzt worden ist.



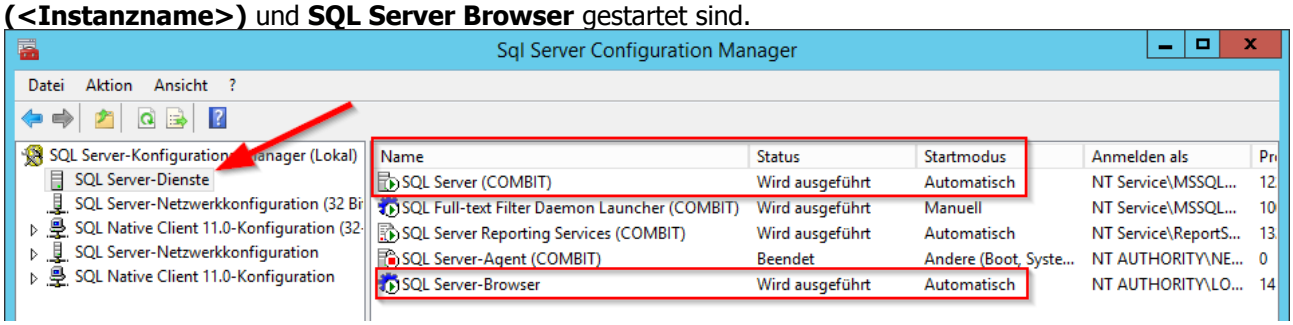
Verlassen Sie anschließend den Dialog mit **OK**.

© Copyright combit GmbH, Alle Rechte vorbehalten.

Konfiguration der SQL Server-Dienste

Starten Sie aus der SQL Server Programmgruppe im Startmenü das Programm **SQL Server-Konfigurations-Manager**.

Navigieren Sie dort zum Punkt **SQL Server-Dienste**. Stellen Sie sicher, dass die Dienste **SQL Server (<Instanzname>)** und **SQL Server Browser** gestartet sind.



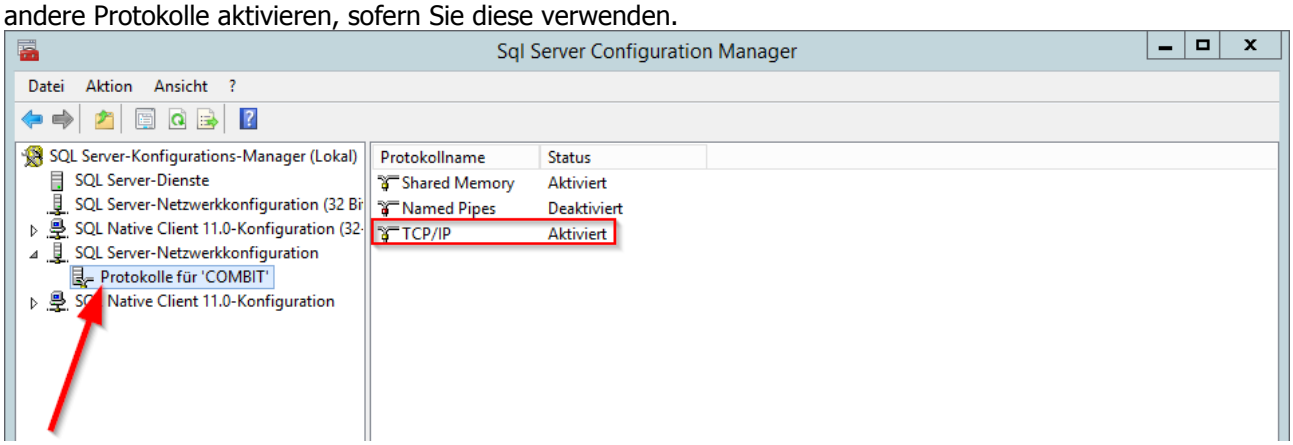
Starten Sie diese ggf. über das Rechtsklick-Kontextmenü. Der **Startmodus** sollte in den **Eigenschaften** unter **Dienst** auf **Automatisch** gestellt werden.

Konfiguration der SQL Server-Netzwerkkonfiguration

Starten Sie aus der SQL Server Programmgruppe im Startmenü das Programm **SQL Server-Konfigurations-Manager**.

Navigieren Sie dort zum Punkt **SQL Server-Netzwerkkonfiguration > Protokolle für '<Instanzname>'**. Falls mehrere SQL Server Instanzen auf Ihrem Server existieren, wählen Sie hier die Instanz aus, in der die combit Datenbanken enthalten sind.

Aktivieren Sie nun das TCP/IP Protokoll über das dazugehörige Rechtsklick-Kontextmenü. Ggf. müssen Sie andere Protokolle aktivieren, sofern Sie diese verwenden.



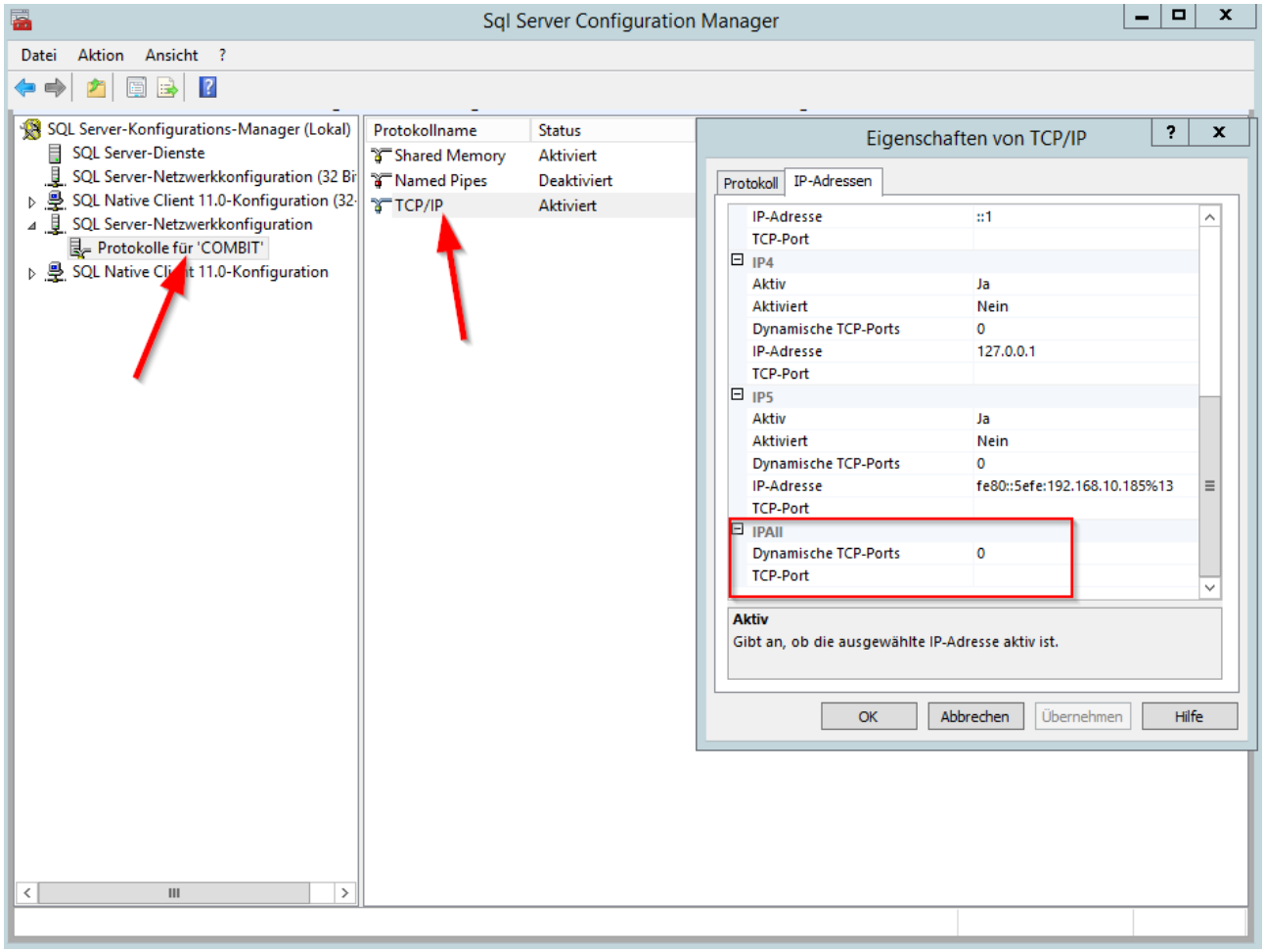
© Copyright combit GmbH, Alle Rechte vorbehalten.

Windows Firewall für SQL Server konfigurieren

Die Microsoft Windows-Firewall verhindert unautorisierte Zugriffe auf den Computer. Dies kann dazu führen, dass möglicherweise auch Verbindungsversuche von cRM Clients auf die auf diesem Computer laufende Microsoft SQL Server Instanz blockiert werden. Der Effekt kann eine lange Wartezeit oder sogar eine "Timeout"-Fehlermeldung beim Starten des cRM sein.

Um den Zugriff von den Clients auf den SQL Server mit aktivierter Windows-Firewall zu ermöglichen, müssen Sie in der Windows-Firewall auf dem Server die entsprechenden Regeln für die Dienste "SQL Server" und "SQL-Browser" eintragen.

Wichtig: Dynamische TCP-Ports
Bitte beachten Sie dabei insbesondere, dass der Microsoft SQL Server bei einer benannten Instanz standardmäßig einen dynamischen TCP-Port (zu sehen über den SQL Server Konfigurations-Manager) verwendet.

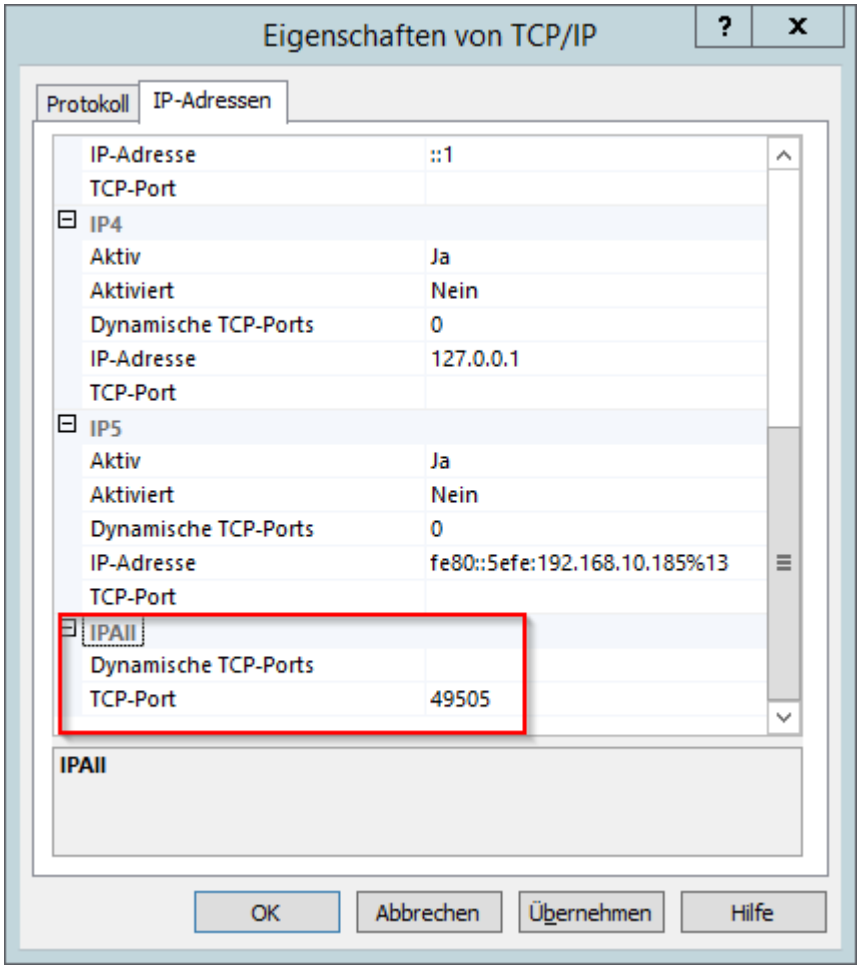


Es ist daher nicht möglich, für diesen dynamischen TCP-Port eine Regel zu definieren. Sollten Sie bereits einen statischen TCP-Port verwenden, überspringen Sie den folgenden Abschnitt und fahren mit der Einrichtung der Windows-Firewall Regeln fort.

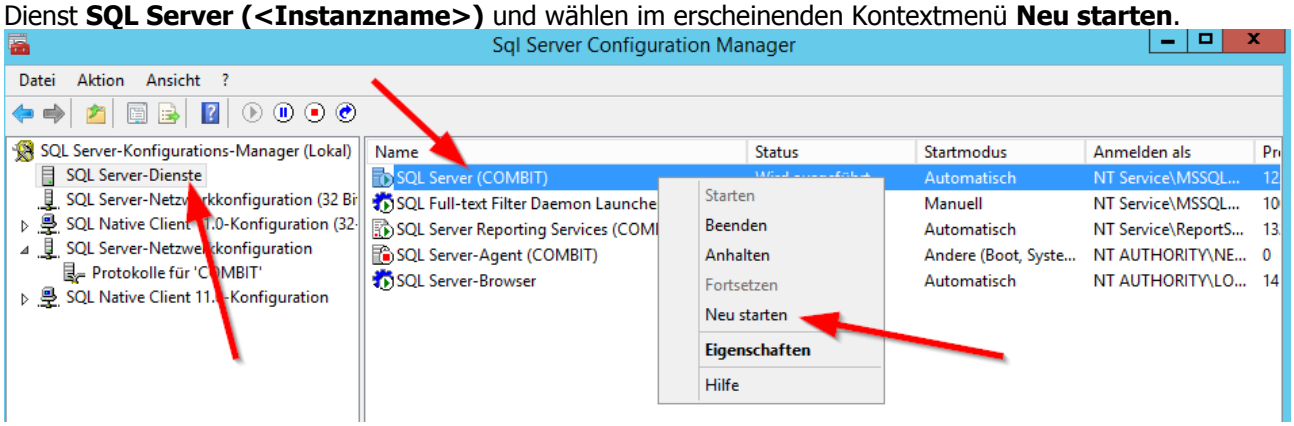
© Copyright combit GmbH, Alle Rechte vorbehalten.

Einrichtung eines statischen TCP-Ports

Die Lösung ist die Einrichtung eines statischen TCP-Ports für die betreffende SQL Server Instanz. Der Port sollte aus dem Bereich von 49152-65535 sein. Dazu müssen Sie in den **Eigenschaften von TCP/IP** unter **IPAll** bei **Dynamische TCP-Ports** den Wert **0 löschen**. Als **TCP-Port** tragen Sie Ihren eigenen definierten Port ein. In unserem Beispiel ist das der Port **49505**.



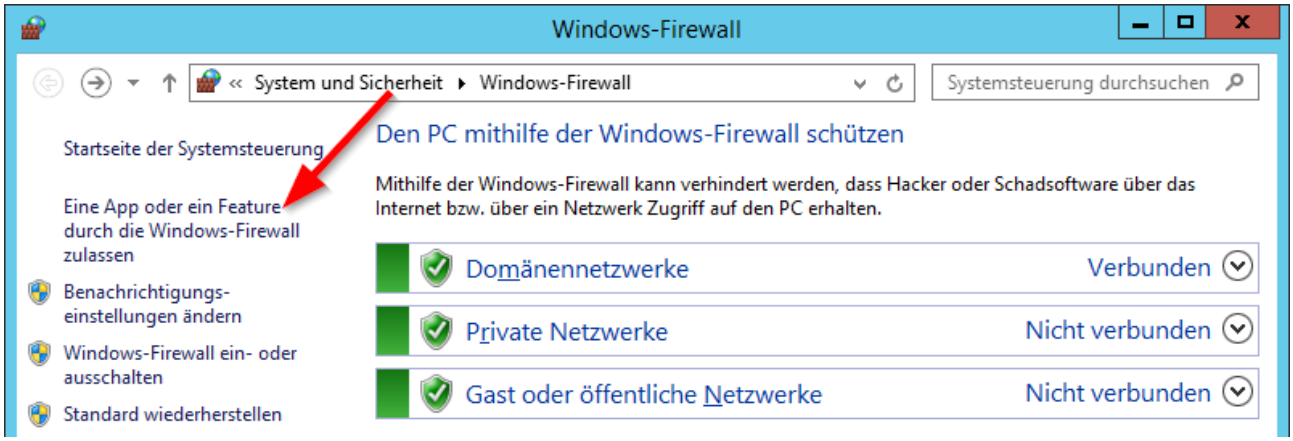
Wenn Sie diese Änderung vorgenommen haben, müssen Sie anschließend im SQL Server-Konfigurations-Manager zum Menüpunkt **SQL Server-Dienste** navigieren. Klicken Sie mit der rechten Maustaste auf den Dienst **SQL Server (<Instanzname>)** und wählen im erscheinenden Kontextmenü **Neu starten**.



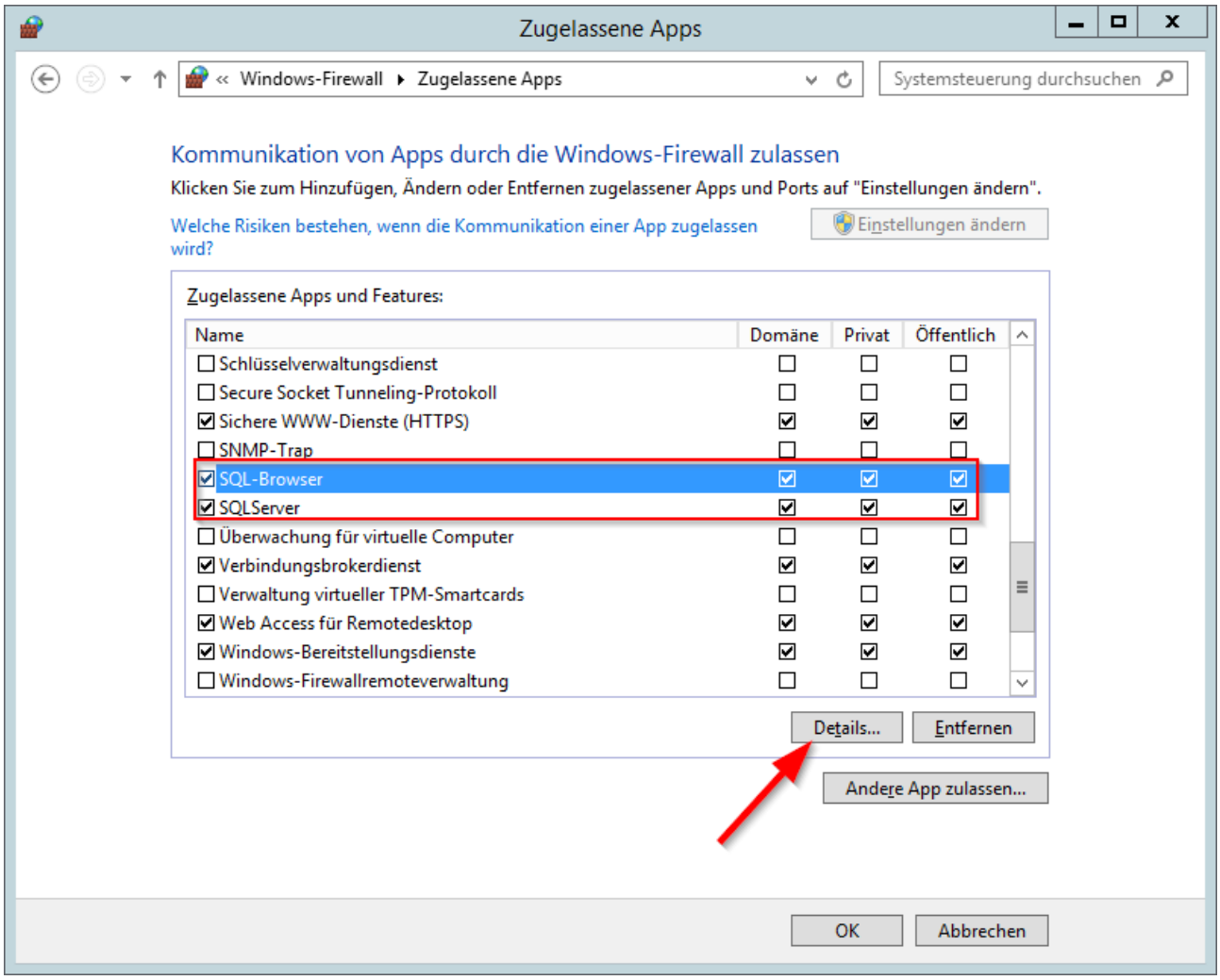
© Copyright combit GmbH, Alle Rechte vorbehalten.

Einrichtung der Windows-Firewall Regeln

Anschließend muss in der Windows-Firewall jeweils eine Regel für den im vorherigen Schritt definierten statischen TCP-Port im SQLServer sowie für den SQL-Browser eingetragen werden. Öffnen Sie hierzu über die **Systemsteuerung** die **Windows-Firewall**. Im folgenden Fenster klicken Sie auf den Menüpunkt **Eine App oder ein Feature durch die Windows-Firewall zulassen**.

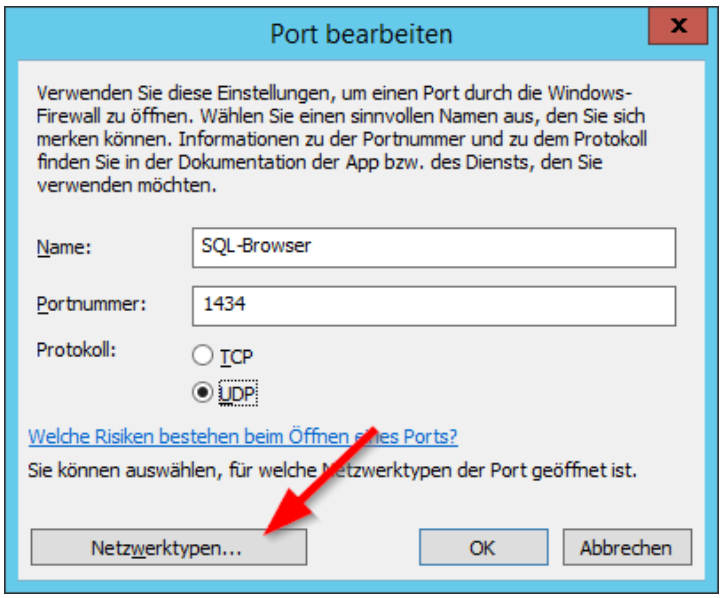


Suchen Sie in der Liste die Features **SQL-Browser** und **SQLServer**. Wählen Sie als erstes den Eintrag **SQL-Browser** aus und drücken Sie anschließend auf **Details...**

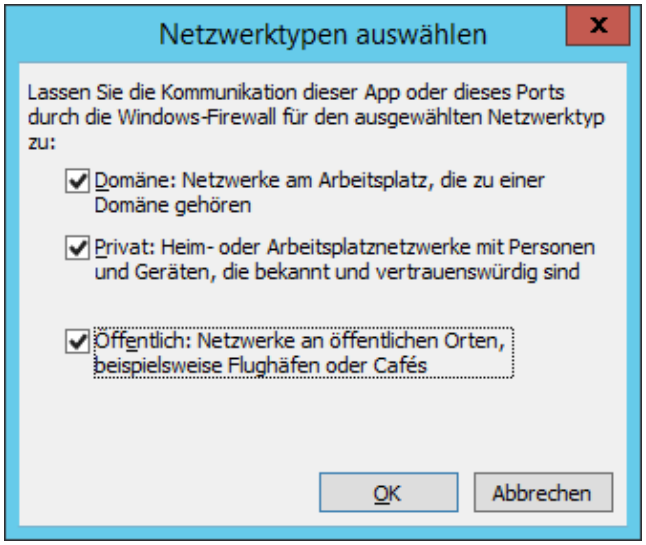


© Copyright combit GmbH, Alle Rechte vorbehalten.

Stellen Sie sicher, dass im folgenden Fenster unter dem Feature **SQL-Browser** die **Portnummer 1434** und als **Protokoll UDP** eingetragen ist. Klicken Sie danach auf **Netzwerktypen...**



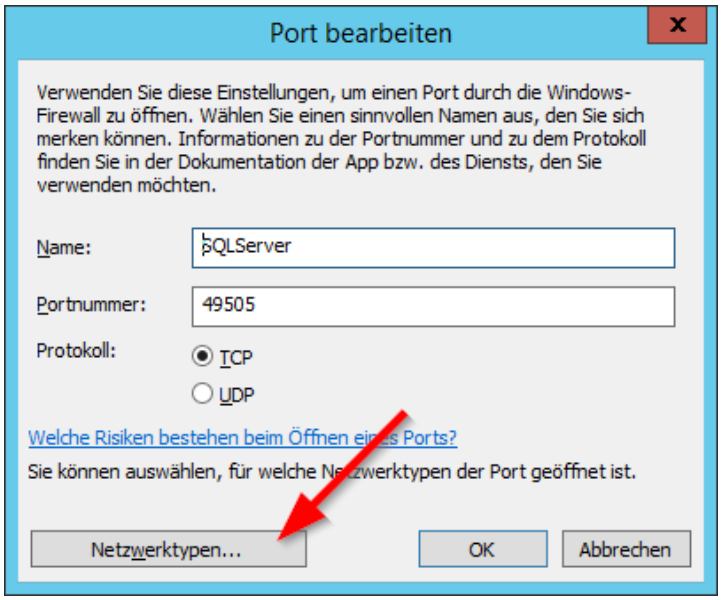
Diese Regeln sollten dann in allen Netzwerkprofilen, über die die Client-Server-Verbindung genutzt werden soll (Domäne, Privat, Öffentlich), eingetragen werden. Wählen Sie alle 3 Netzwerktypen aus und klicken Sie anschließend auf **OK**.



© Copyright combit GmbH, Alle Rechte vorbehalten.

Suchen Sie als nächstes in der Liste der Features den Eintrag **SQLServer**. Wählen Sie diesen aus und drücken Sie anschließend auf **Details...**

Stellen Sie sicher, dass im folgenden Fenster unter dem Feature **SQLServer** die **Portnummer 49505** und als **Protokoll TCP** eingetragen ist. Klicken Sie danach auf **Netzwerktypen...**



Diese Regeln sollten dann in allen Netzwerkprofilen, über die die Client-Server-Verbindung genutzt werden soll (Domäne, Privat, Öffentlich), eingetragen werden. Wählen Sie, wie im Fenster zuvor, alle 3 Netzwerktypen aus und klicken Sie anschließend auf **OK**.

Alternativ können Sie hierzu auch folgende Zeilen kopieren und in einer Batch-Datei (.bat) abspeichern und anschließend ausführen. Die folgenden Befehle aktivieren in Ihrer Firewall für die Dienste **SQLServer** und **SQL-Browser** die jeweiligen Ports. Für den Port 49505 aus dem Beispiel tragen Sie Ihren eigenen definierten Port ein.

```
@echo Aktivieren des Ports für die SQL Server-Standardinstanz
netsh advfirewall firewall add rule name="SQLServer" dir=in action=allow
protocol=TCP localport=49505 enable=yes

@echo Aktivieren des Ports für den SQL Server-Browserdienst
netsh advfirewall firewall add rule name="SQL-Browser" dir=in action=allow
protocol=UDP localport=1434 enable=yes
```

Hinweis: combit macht keine Angaben zu einer bestimmten Eignung obiger Informationen. Irrtümer und Fehler bleiben ausdrücklich vorbehalten, die Angaben erfolgen ohne Gewähr und enthalten keine Zusicherung. Die Informationen können z.T. auch ein Versuch sein, Ihnen bei einer Aufgabenstellung zu helfen, selbst wenn das Produkt eigentlich nicht für diesen speziellen Zweck vorgesehen wurde.

© Copyright combit GmbH, Alle Rechte vorbehalten.