

Whitepaper

Produkt: combit address manager / Relationship Manager Client-Verbindungsprobleme beheben

Inhalt

Einleitung	3
SQL Server Konfiguration	4
Konfiguration der Remote Verbindungen	4
Konfiguration der SQL Server-Dienste	6
Konfiguration der SQL Server-Netzwerkkonfiguration	6
Windows Firewall für SQL Server konfigurieren Wichtig: Dynamische TCP-Ports	7 7
Einrichtung eines statischen TCP-Ports	8
Einrichtung der Windows-Firewall Regeln	9

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.

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 ein	e Verbir	ndung z	ur ents	precher	nden S	QL S	Server	Instan	z her
-										~

Verbindung mit Server herstellen					
SQL Serve	er 2012				
Serve <u>r</u> typ:	Datenbankmodul 🗸				
Servema <u>m</u> e:	COMBIT V				
A <u>u</u> thentifizierung:	SQL Server-Authentifizierung V				
<u>A</u> nmeldename:	sa 🗸 🗸				
<u>K</u> ennwort:	*******				
	Kennwort speichem				
Verbinden	Abbrechen Hilfe Optionen >>				

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



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.

8	Servereigenschaften - COMBIT
Seite auswählen Allgemein Arbeitsspeicher Prozessoren Sicherheit Verbindungen Datenbankeinstellungen Erweitert Berechtigungen	Skript ▼ Image: Hilfe Verbindungen Maximale Anzahl von gleichzeitigen Verbindungen (0 = unbegrenzt): 0 ↓ 0 ↓ Abfragekontrolle verwenden, um Abfragen mit langer Ausführungszeit zu verhindem 0 ↓ Stangardverbindungsoptionen: implizite Transaktionen Schließen des Cursors nach Commit ANSI-Auffüllung ANSI-Auffüllung
Verbindung Server: COMBIT Verbindung: sa ♥ Verbindungseigenschaften. anzeigen	ANST NULLS Abbruch bei arithmetischem Fehler Remoteserververbindungen Imeout für Remoteabfragen mit diesem Server zulässen Imeout für Remoteabfragen (Sekunden, 0 = kein Timeout): 600 Imeout für Remoteabfragen (Sekunden, 0 = kein Timeout): 600 Imeout für Remoteabfragen (Sekunden, 0 = kein Timeout): 600 Imeout für Remoteabfragen (Sekunden, 0 = kein Timeout): 600 Imeout für Remoteabfragen (Sekunden, 0 = kein Timeout): 600 Imeout für Remoteabfragen (Sekunden, 0 = kein Timeout): 600 Imeout für Remoteabfragen (Sekunden, 0 = kein Timeout): 600 Imeout für Remoteabfragen (Sekunden, 0 = kein Timeout): 600 Imeout für Remoteabfragen (Sekunden, 0 = kein Timeout): 600 Imeout für Remoteabfragen (Sekunden, 0 = kein Timeout): 600 Imeout für Remoteabfragen (Sekunden, 0 = kein Timeout): 600 Imeout für Remoteabfragen (Sekunden, 0 = kein Timeout): 600 Imeout für Remoteabfragen (Sekunden, 0 = kein Timeout): 600 600 600 600 </th
	OK Abbrechen

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

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.

	Sql Server Configuration Ma	nager			x
Datei Aktion Ansicht ?					
🗢 🔿 🖄 🖬 📓 🧹					
🛞 SQL Server-Konfiguration anager (Lokal)	Name	Status	Startmodus	Anmelden als	Pri
SQL Server-Dienste	SQL Server (COMBIT)	Wird ausgeführt	Automatisch	NT Service\MSSQL	12
. SQL Server-Netzwerkkonfiguration (32 Br	SQL Full-text Filter Daemon Launcher (COMBIT)	Wird ausgeführt	Manuell	NT Service\MSSQL	10
▶ ₽ SQL Native Client 11.0-Konfiguration (32-	SQL Server Reporting Services (COMBIT)	Wird ausgeführt	Automatisch	NT Service\ReportS	13
▶ <u>↓</u> SQL Server-Netzwerkkonfiguration	SQL Server-Agent (COMBIT)	Beendet	Andere (Boot, Syste	NT AUTHORITY\NE	0
▶ 🖳 SQL Native Client 11.0-Konfiguration	to SQL Server-Browser	Wird ausgeführt	Automatisch	NT AUTHORITY\LO	14

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.



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.

*	SqI S	erver Configuration	Manager	L	<u> </u>	ĸ
Datei Aktion Ansicht ?						
🗢 🏟 🖄 🖾 🔒	_		_			
 SQL Server-Konfigurations-Manager (Lokal) SQL Server-Dienste SQL Server-Netzwerkkonfiguration (32 Bir SQL Native Client 11.0-Konfiguration SQL Server-Netzwerkkonfiguration Protokolle für 'COMBIT' SQL Native Client 11.0-Konfiguration 	Protokollname Shared Memory TCP/IP	Status Aktiviert Deaktiviert Aktiviert	Eigenschaft Protokoll IP-Adressen IP-Adresse TCP-Port IP4 Aktiv Aktiviert Dynamische TCP-Ports IP-Adresse TCP-Port IP5 Aktiv Aktiviert Dynamische TCP-Ports IP-Adresse TCP-Port IPAII Dynamische TCP-Ports TCP-Port Aktiv Gibt an, ob die ausgewählte IP-Adresse	ten von TCP/IP ::1 Ja Nein 0 127.0.0.1 Ja Nein 0 fe80::5efe:192.168.10.18 0 dresse aktiv ist.	? ×	
			OK Abb	Übernehmen	Hilfe	
< III >						
	L					

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.

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 **IPAII** 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**.

	IP-Adresse	::1	^
	ICP-Port		
	IP4 Aktiv	la	
	Aktiviert	Nein	
	Dynamische TCP-Ports	0	
	IP-Adresse	127.0.0.1	
	TCP-Port		
Ξ	IP5		
	Aktiv	Ja	
	Aktiviert	Nein	
	Dynamische TCP-Ports	0	
	IP-Adresse	fe80::5efe:192.168.10.185%13	≡
	TCP-Port		
5	IPAII Dynamische TCP-Ports		
L	TCP-Port	49505	~
IP	All		

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**

a	Sql Server Configura	ation Manager			x	
Datei Aktion Ansicht ?						
SQL Server-Konfigurations-Manager (Lokal)	Name 🔍	Status	Startmodus	Anmelden als	Pri	
SQL Server-Dienste	SQL Server (COMBIT)	Mind and a second state	Automatisch	NT Service\MSSQL	12	
SQL Server-Netzverkkonfiguration (32 Bi	n SQL Full-text Filter Daemon Launche	Starten	Manuell	NT Service\MSSQL	10	
SQL Native Client 1.0-Konfiguration (32)	SQL Server Reporting Services (COMI	Beenden	Automatisch	NT Service\ReportS	13.	
⊿ <u>↓</u> SQL Server-Netzweikkonfiguration	SQL Server-Agent (COMBIT)	Anhalten	Andere (Boot, Syste	NT AUTHORITY\NE	0	
🔤 📴 Protokolle für 'C MBIT'	SQL Server-Browser	Fortsetzen	Automatisch	NT AUTHORITY\LO	14	
▷ _豊. SQL Native Client 11.1-Konfiguration		Neu starten				
\		Eigenschaften				
		Hilfe				

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...**

2	Zugelassene Apps						x
€ 🗇 ▾ ↑	🔗 « Windows-Firewall 🕨 Zugelassene Apps	~	Ċ	Systemsteueru	ing duro	hsuchen	Q
l	Kommunikation von Apps durch die Windows-Firewa	ll zulasse	n				
1	Klicken Sie zum Hinzufügen, Ändern oder Entfernen zugelassener Apps	und Ports a	uf "Einst	ellungen ände	ern".		
	Welche Risiken bestehen, wenn die Kommunikation einer App zugelas: wird?	sen	🛞 Ei <u>n</u> ste	ellungen ände	ern		
	Zugelassene Apps und Features:						
	Name	Domäne	Privat	Öffentlich	~		
	Schlüsselverwaltungsdienst						
	Secure Socket Tunneling-Protokoll						
	☑ Sichere WWW-Dienste (HTTPS)		☑				
	SNMP-Trap						
	SQL-Browser						
	✓ SQLServer		✓				
	Überwachung für virtuelle Computer						
	✓ Verbindungsbrokerdienst	✓	✓				
	Verwaltung virtueller TPM-Smartcards						
	Web Access f ür Remotedesktop		\checkmark	\checkmark			
	✓ Windows-Bereitstellungsdienste	\checkmark	✓	\checkmark			
	□ Windows-Firewallremoteverwaltung				\checkmark		
		D	e <u>t</u> ails	<u>E</u> ntferner	ו		
L			Andere	e App zulasser	۱		
			ОК	Abbrech	en		

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...**

	Port bearbeiten X						
Verwenden Sie o Firewall zu öffne merken können. finden Sie in der verwenden möd	diese Einstellungen, um einen Port durch die Windows- n. Wählen Sie einen sinnvollen Namen aus, den Sie sich Informationen zu der Portnummer und zu dem Protokoll Dokumentation der App bzw. des Diensts, den Sie hten.						
<u>N</u> ame:	SQL-Browser						
Portnummer:	1434						
Protokoll:	О <u>I</u> СР						
	● <u>udp</u>						
Welche Risiken be	estehen beim Öffnen sines Ports?						
Sie können auswählen, für welche vetzwerktypen der Port geöffnet ist.							
Netz <u>w</u> erk	OK Abbrechen						

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**.

Netzwerktypen auswählen
Lassen Sie die Kommunikation dieser App oder dieses Ports durch die Windows-Firewall für den ausgewählten Netzwerktyp zu:
Domäne: Netzwerke am Arbeitsplatz, die zu einer Domäne gehören
Privat: Heim- oder Arbeitsplatznetzwerke mit Personen und Geräten, die bekannt und vertrauenswürdig sind
Öffentlich: Netzwerke an öffentlichen Orten, beispielsweise Flughäfen oder Cafés
<u>O</u> K Abbrechen

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...**

	Port bearbeiten					
Verwenden Sie diese Einstellungen, um einen Port durch die Windows- Firewall zu öffnen. Wählen Sie einen sinnvollen Namen aus, den Sie sich merken können. Informationen zu der Portnummer und zu dem Protokoll finden Sie in der Dokumentation der App bzw. des Diensts, den Sie verwenden möchten.						
<u>N</u> ame:	5QLServer					
Portnummer:	49505					
Protokoll:	• <u>I</u> CP					
Welche Risiken be	stehen beim Öffnen ein zs Ports?					
Sie können auswählen, für welche Nerzwerktypen der Port geöffnet ist.						
Netz <u>w</u> erkt	ypen OK Abbrechen					

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.

- 11 -