COMBIVIS connect Server-Struktur FAQ Nr.0005

Part	Version	Revision	Datum	Status
de	7.0.023	002	2019-01-01	Released

Inhalt

KEB Automation KG
Südstr. 38, 32683 Barntrup
Deutschland
E-Mail: info@keb.de
Tel +49 5263 401-0
Fax +49 5263 401-116
www.keb.de

Amtsgericht Lemgo HRA 5649
DUNS-Nr. 314108728
USt-IdNr. DE309087075
Sparkasse Paderborn-Detmold
IBAN DE 19 4765 0130 0000 0060 07
BIC WELADE3L

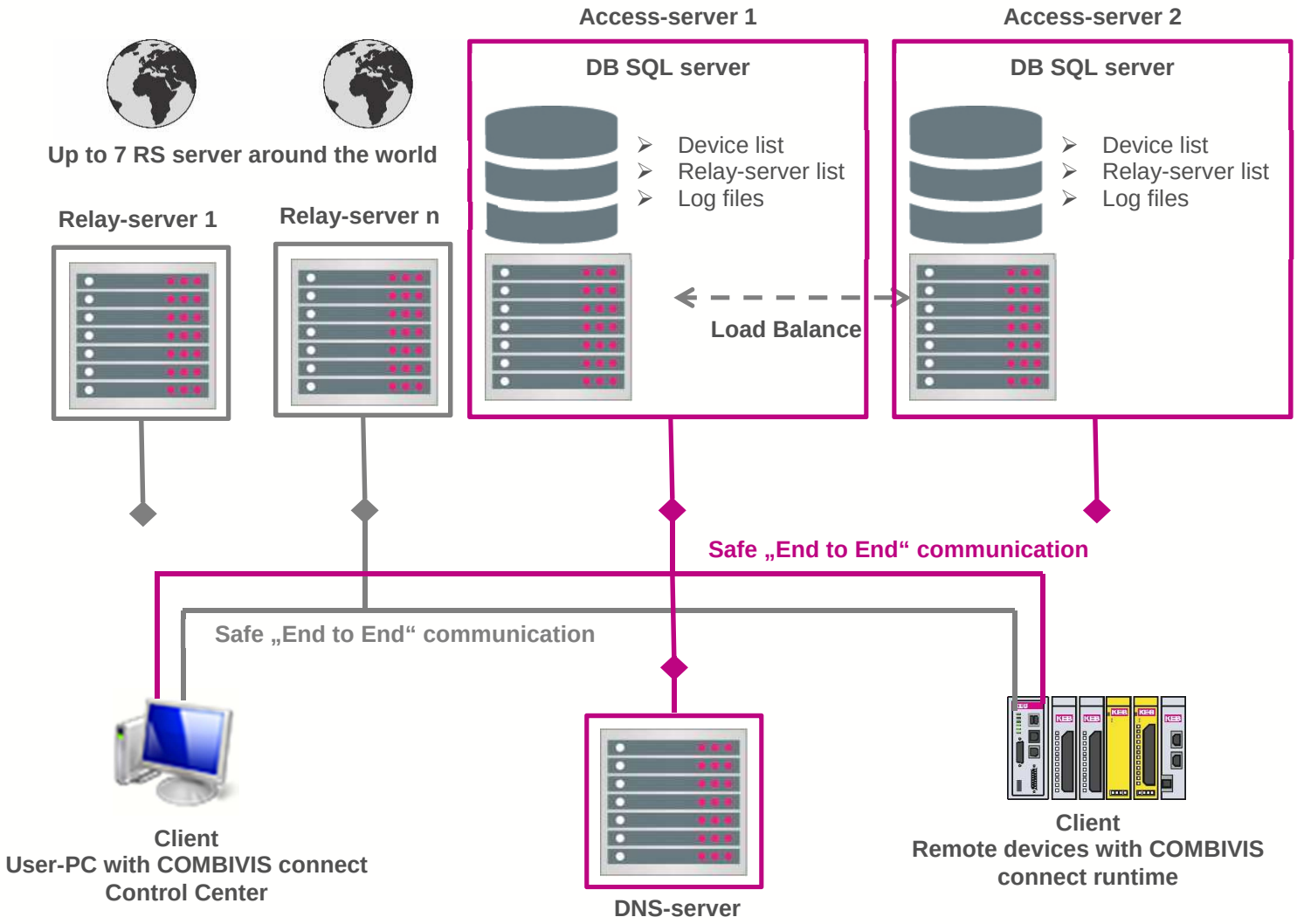
Persönlich haftende Gesellschafter:
Vittorio Tavella
KEB Verwaltungs-GmbH Barntrup
Amtsgericht Lemgo HRB 8965
Geschäftsführer: Curt Bauer CMO
Ralf Lutter COO, Vittorio Tavella CFO
Wolfgang Wiele CTO

Einleitung

Dieses Dokument beschreibt die Struktur der COMBIVIS Connect Server und Ports, welche für die Kommunikation benötigt werden.

Server Struktur

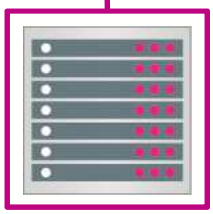
Die COMBIVIS Connect Struktur besteht aus Access-, Relay-, DNS-Server und Clients. Die Clients sind der Benutzer-PC, mit COMBIVIS connect Control Center und dem Remote-Gerät mit der COMBIVIS connect Runtime.
Die Sicherheit der Serverstruktur ist zertifiziert durch das deutsche Bundesamt für Sicherheit in der Informationstechnik (BSI) nach ISA 99 und IEC.



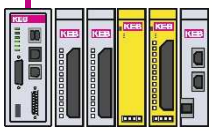
Clients: COMBIVIS connect Control Center und Runtime

Die Softwareumgebung COMBIVIS connect Control Center wird auf dem Benutzer-PC ausgeführt, die COMBIVIS connect Runtime auf dem Remote-Gerät. Von Version 7 an wählen beide Programme den Access-Server selbständig aus.
Beide Clients verwenden die, vom DNS Server bereitgestellten, Alias-Servernamen. Hinter den Alias-Namen sind die zugehörigen IP-Adressen hinterlegt. Dieses Vorgehen erlaubt mehr Flexibilität in Bezug auf zukünftige Updates oder Hinzufügen von IP-Adressen.

Client
User-PC with COMBIVIS connect Control Center



DNS-server

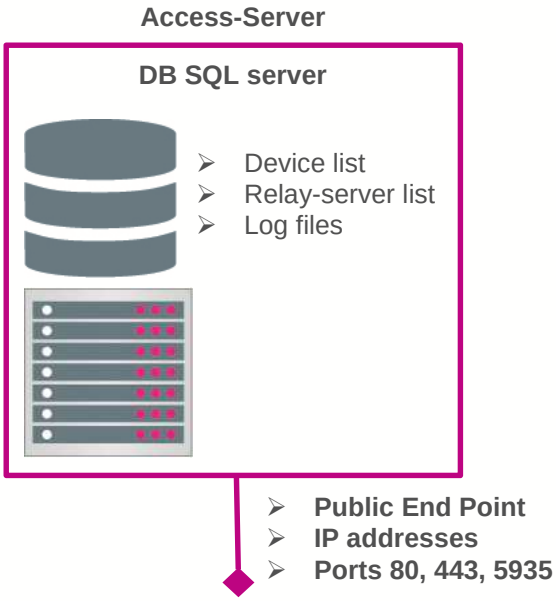


Client
Remote devices with COMBIVIS connect runtime

Alias:
ccas1.keb.de
ccas2.keb.de
combivisconnectrs1.keb.de
.
.
.
Combivisconnectrs7.keb.de

Access-Server

Der Access-Server dient zum Verwalten der Benutzer- und Geräte-Zugriffe. Die Informationen dazu werden in der Device-, Relay-Server- und Log- Datei gespeichert. Nachdem die Geräte/Benutzer verifiziert wurden, wird ein Relay-Server ausgewählt, der die „end-to-end“-Verbindung aufbaut. Dieser Relay-Server wird nach der besten Performance (geringste Latenz) und einem “Load Balance“-Algorithmus ausgewählt. Jeder Server kann die Ports 80 (HTTP), 443 (HTTPS) und 5935 (Custom) verwenden. Der Access-Server benutzt einen dynamischen Namen, der mit einer statischen IP-Adresse verknüpft ist.



Servernamen und -ports

Für einen erfolgreichen Verbindungaufbau zu den Servern ist es notwendig einen der drei folgenden Ports freizuschalten: 80 (HTTP), 443 (HTTPS), 5935 (Custom)

Außerdem werden folgende Servernamen benötigt und müssen somit in den Firewall-Richtlinien freigegeben sein:

Access-server:

- ccas1.keb.de
- ccas2.keb.de

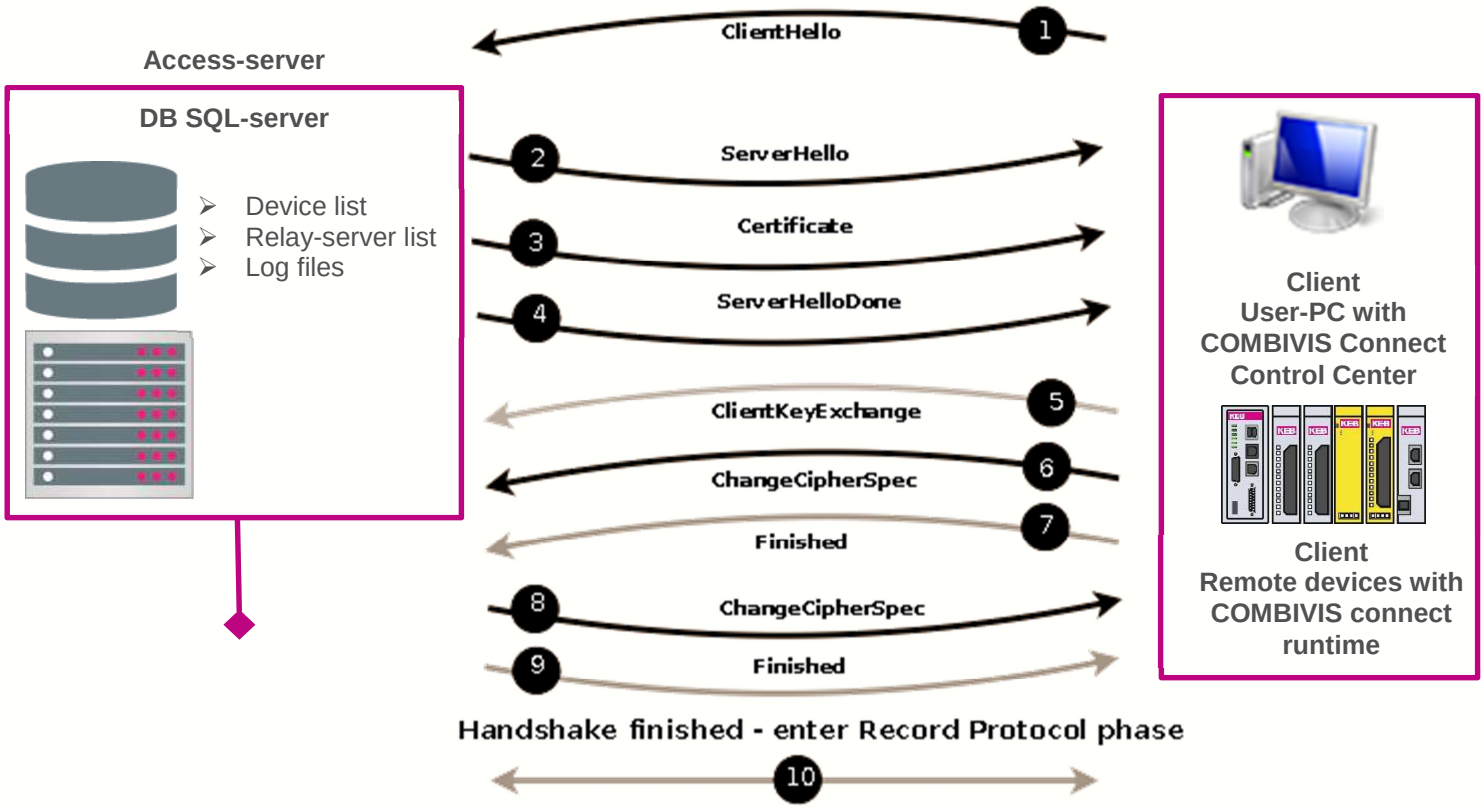
Relay-server:

- combivisconnectrs1.keb.de
- combivisconnectrs2.keb.de
- combivisconnectrs3.keb.de
- combivisconnectrs4.keb.de
- combivisconnectrs5.keb.de
- combivisconnectrs6.keb.de
- combivisconnectrs7.keb.de

Die Firewall muss die Verwaltung von dynamischen Servernamen unterstützen. Dies ermöglicht eine IP-unabhängige Zuweisung von Servern und zukünftige Erweiterungs- / Änderungsmöglichkeiten.

TLS/SSL - Protokollsequenz (Handshake)

Vor dem Austausch von Daten zwischen den beiden Clients initialisiert das TLS(SSL)-Protokoll einen Handshake-Vorgang zwischen Accessserver und Client (siehe handshakediagram). Der Accessserver verifiziert das Zertifikat, Cipher-Spezifikationen und Schlüssel.



Vorgehen nach TLS (SSL)-Handshake

1. Der Accessserver verifiziert die Authentifizierung:
   - COMBIVIS connect control center (Domainname, Benutzerpasswort)
   - COMBIVIS connect Runtime (Zertifikat)
2. Der Accessserver verifiziert die Geräteliste, welche vom Client erreicht werden kann.
3. Mit Hilfe des Access-Servers verwenden beide Clients die beste Route zum RelayServer. Die beste Performance (Latenz) wird sowohl durch die Runtime als auch durch das Control Center berechnet
   - Austausch der Sitzungsschlüssel (Diese werden jede Sitzung neu generiert „Perfect forward secret“ (PFS))
4. Sobald alle Regeln festgelegt wurden, leitet der Relay-Server alle Daten weiter
   - Remote Desktop
   - VPN Tunnel

Disclaimer

KEB Automation KG reserves the right to change/adapt specifications and technical data without prior notification. The safety and warning reference specified in this manual is not exhaustive. Although the manual and the information contained in it is made with care, KEB does not accept responsibility for misprint or other errors or resulting damages. The marks and product names are trademarks or registered trademarks of the respective title owners.

The information contained in the technical documentation, as well as any user-specific advice in verbal or in written form are made to the best of our knowledge and information about the application. However, they are considered for information only without responsibility. This also applies to any violation of industrial property rights of a third-party.

Inspection of our units in view of their suitability for the intended use must be done generally by the user. Inspections are particular necessary, if changes are executed, which serve for the further development or adaption of our products to the applications (hardware, software or download lists). Inspections must be repeated completely, even if only parts of hardware, software or download lists are modified.

Application and use of our units in the target products is outside of our control and therefore lies exclusively in the area of responsibility of the user.

KEB Automation KG
Südstraße 38 • D-32683 Barntrup
fon: +49 5263 401-0 • fax: +49 5263 401-116
net: www.keb.de • mail: info@keb.de