

Verschlüsselte Verbindung zum Firebird-Server

27.07.2024 06:43:52

FAQ-Artikel-Ausdruck

Kategorie:	RRZE: Datenbanken::Firebird	Bewertungen:	0
Status:	öffentlich (Alle)	Ergebnis:	0.00 %
Sprache:	de	Letzte Aktualisierung:	09:11:47 - 24.06.2009

Symptom (öffentlich)

Problem (öffentlich)

Verschlüsselte Verbindung zum Firebird-Server

Lösung (öffentlich)

Um das Übertragen von Klartextpasswörern im Netz zu vermeiden, ist es nötig, die Kommunikation zwischen Clients und Datenbankservern über verschlüsselte Verbindungen ablaufen zu lassen.

Hierzu wird ein verschlüsselter Tunnel zwischen dem Clientrechner und dem Datenbank-Server erstellt. Das einzige was sich dabei für den Datenbank-Client gegenüber einer Verbindung ohne Tunnel ändert, ist, dass die TCP Verbindung nicht zum Server sondern zum eigenen Rechner aufgebaut wird. Dort verbindet sich der Datenbank-Client auf den offenen Port des Tunnelendpunktes und der Rest der Verbindung zur Datenbank erfolgt völlig transparent wie gewohnt.

Folgende Anweisungen funktionieren nicht mit allen aktuellen Servern. Verwenden Sie stattdessen bitte die VPN-Lösungen des RRZE ("<http://www.rrze.uni-erlangen.de/dienste/internet-zugang/vpn/>").

Um ihnen die Einrichtung eines verschlüsselten Tunnels von ihrem lokalen PC zum Datenbankserver zu ermöglichen, wird im folgenden beschrieben wie Sie einen Tunnel mit dem Tool "Zebedee" einrichten.

Verschlüsselte Verbindung mittels "Zebedee":

Zebedee ist ein kleines Kommandozeilentool, welches für Linux/Unix und Windows verfügbar ist.

Sie können damit einen verschlüsselten Tunnel zum Firebird Port des RRZE-Datenbankservers herstellen. Dabei öffnet Zebedee auf ihrem Rechner einen TCP Port über den die Anbindung ihres Datenbank-Clients erfolgt.

Voraussetzung ist, dass am Datenbankserver selbst auch Zebedee läuft. Diese Voraussetzung ist bei allen Firebird Datenbankservern des RRZE gegeben. Um die Verbindung mit Zebedee herzustellen ist ausser der Software keine weitere Einrichtung nötig.
Zebedee Einrichtung unter Windows:

Sie haben zwei Möglichkeiten Zebedee zu installieren:

Installation mittels des vorkonfigurierten RRZE-Zebedee-Package: (dringend empfohlen!)

* Laden Sie den Installer ("http://www.rrze.uni-erlangen.de/infrastruktur/datenbanken/firebird/zebedee/windows/zebedee_rrze_1.0.exe") auf ihren Rechner und führen Sie die Datei aus.

* Anmerkung:
Die Installation kann sowohl als Administrator als auch als gewöhnlicher User durchgeführt werden. Falls Sie Administrator sind, wird während der Installation die Möglichkeit angeboten, Zebedee als Service zu installieren was soviel wie ein automatisches Starten des Dienstes beim Booten bedeutet. Sie können dann jederzeit ohne weiteren Aufwand mit ihrem Datenbank-Client auf die Firebird Datenbank über ihren Tunnel zugreifen, ohne dass Sie diesen erst anlegen müssen.
Die Installation enthält auch vorkonfigurierte Shortcuts für das Startmenü mit denen Sie auch später den Service installieren und Deinstallieren können.

Installation mittels des auf der Zebedee-Homepage angebotenen Pakets:

* Holen Sie sich das Zebedee Installationspaket von der offiziellen Zebedee Homepage ("<http://www.winton.org.uk/zebedee/>") und installieren Sie dieses auf ihrem Rechner.

* Einen Tunnel zum Datenbankserver richten sie dann folgendermassen ein:
zebedee.exe 3050:firebird.rrze.uni-erlangen.de:3050

o Die Bedeutung sämtlicher Kommandozeilenparameter erfahren Sie entweder aus der mitgelieferten Dokumentation im HTML Format oder von dem Manual auf der Zebedee Homepage ("<http://www.winton.org.uk/zebedee/manual.html>").

o Hier konkret ist die erste "3050" der Port, welcher auf ihrem Rechner auf Anfragen ihres Datenbankclients lauscht und "firebird.rrze.uni-erlangen.de:3050" der Remote-Rechner mit dem

Firebird-Server auf Port 3050.

Sie wundern sich vielleicht, dass man nicht den Port angeben muss auf dem Zebedee auf der Gegenseite (also am Datenbankserver) lauscht. Der Grund dafür ist, dass wir den Zebedee default Port 11965 verwenden über den Zebedee von sich aus bescheid weiss. Den Port 11965 müssen Sie aber in ihrer Firewall freigeben, falls Sie hinter einer solchen arbeiten.

Installation von Zebedee als Service

Wenn Sie Zebedee als Windows Service installieren, wird der Tunnel zum Firebird Server automatisch beim Booten ihres Rechners aufgebaut. Hierfür benötigen Sie Administrator Rechte!

Sie müssen hierfür eine Konfigurationsdatei mit den Einstellungen für den Tunnel anlegen oder können auch die im Zebedee-RRZE-Installer enthaltene Konfigurationsdatei verwenden

("http://www.rrze.uni-erlangen.de/infrastruktur/datenbanken/firebird/zebedee/common/zebedee-client.conf").

Haben Sie - wie oben beschrieben - Zebedee mit Hilfe des RRZE Installations-Package installiert können Sie den Service bequem über die Startmenüeinträge steuern.

* Installiert wird der Service mittels `zebedee.exe -n "Zebedee Client Service" -Sinstall=`

* Starten/Stoppen des Service: `net [start|stop] "Zebedee Client Service"`

* Entfernen des Service mittels `zebedee.exe -n "Zebedee Client Service"`

-Sremove

Zugriff auf die Datenbank über den Tunnel:

Verbinden Sie ihre Datenbank-Clients einfach auf den Rechner wo Zebedee läuft (unter Verwendung des Standard Firebird-Ports 3050).

Zebedee Einrichtung unter Unix/Linux

Zebedee gibts für Unix/Linux nur als Source, den man erst selbst zu einem Binary kompilieren muß. Hierfür benötigen Sie den GNU C-Compiler. Sollten Sie wieder Erwarten Probleme beim Erstellen des Binaries haben, wenden Sie sich bitte an den Unix/Linux Betreuer ihres Instituts und bitten diesen um Hilfestellung.

So installieren Sie Zebedee unter Unix/Linux:

Um ihnen die Sache zu erleichtern bieten wir auch vorcompilierte Binaries

für Linux (für libc6 übersetzt,

"http://www.rrze.uni-erlangen.de/infrastruktur/datenbanken/firebird/zebedee/unix/linux/zebedee")

und Solaris (Version 7,

"http://www.rrze.uni-erlangen.de/infrastruktur/datenbanken/firebird/zebedee/unix/solaris/zebedee")

an. Sollte das entsprechende Executable bei ihnen lauffähig sein sparen Sie sich die Arbeit des Compilens.

Compilieren der Quelldateien:

* Holen Sie sich die Sourcen von der Zebedee Download Seite

("http://www.winton.org.uk/zebedee/download.html").

Sie benötigen die Sourcepakete von Zebedee, blowfish, zlib und bzip2.

Es steht zwar geschrieben, dass Sie bzip2 nicht unbedingt benötigen,

jedoch vereinfacht sich das ganze dadurch erheblich.

* Speichern Sie alle vier Packages in das gleiche Verzeichnis ab.

* Entpacken Sie die jeweiligen Archive:

`gunzip`

`tar xvf`

* Compilieren Sie zuerst blowfish, gzip und bzip2. Wie das geht steht in der Datei "BUILDING.txt" im Zebedee Packet.

* Anschließend übersetzen Sie noch Zebedee gemäß den Anweisungen in "BUILDING.txt".

Eventuell müssen Sie das Makefile noch anpassen. Sollte im Normalfall allerdings nicht nötig sein.

* Wenn alles ohne Fehler geklappt hat sollte in ihrem Zebedee Source-Verzeichnis jetzt ein Binary namens "zebedee" liegen.

Installation des Binaries

Das Binary (zebedee) kopieren Sie entweder in ihr Home (z.B. nach \$HOME/bin) oder in das Verzeichnis ihrer sonstigen selbst übersetzten Pakete.

Erstellen eines verschlüsselten Tunnels zum Datenbankserver des RRZE:

Zebedee ist ein Kommandozeilen Tool, welchem man eine Vielzahl von Parametern übergeben kann.

Die Liste der Parameter erhalten Sie mit `./zebedee --help`. Die ausführliche Beschreibung sämtlicher Kommandozeilenparameter finden Sie in der Dokumentation im Sourceverzeichnis oder im Externer auf der Zebedee Homepage ("http://www.winton.org.uk/zebedee/download.html").

Um einen Tunnel zum Firebird Server des RRZE zu erstellen benötigen Sie jedoch nur folgenden Befehl: `zebedee 3050:firebird.rrze.uni-erlangen.de:3050`

* Die erste 3050 beschreibt den Port des Tunnelendpunktes, auf dem Zebedee lauscht und auf Verbindungen ihrer Datenbank-Clients wartet.

* `firebird.rrze.uni-erlangen.de:3050` ist der host:port zu dem der Tunnel "führt".

* Sie wundern sich vielleicht, dass man nicht den Port angeben muss auf

dem Zebedee auf der Gegenseite (also am Datenbankserver) lauscht. Der Grund dafür ist, dass wir den Zebedee default Port 11965 verwenden über den Zebedee von sich aus bescheid weiss.

Installation von Zebedee als Service, der beim Booten gestartet wird. Sollten Sie den Bedarf haben, dass Zebedee automatisch nach dem Hochfahren ihres Rechners den Tunnel zum Firebird Server aufbaut, müssen Sie das Starten von Zebedee in ein Init Script einbinden und/oder das Vorhandensein des Dienstes per Cronjob regelmäßig überprüfen. Hierfür bieten wir Ihnen zwei vorgefertigte Shellscripts an: Eines, das Sie in den Init-Prozess ihres Systems integrieren können und eines zum periodischen Überprüfen, über der Zebedee Dienst läuft, welches Sie über ihren Cron Scheduler starten können. Beachten Sie, daß Zebedee um auf dem Firebird Port 3050 lauschen zu können keine Root Rechte benötigt. Es genügt also völlig wenn Sie den Service unter einem unprivilegiertem Account laufen lassen.

Wir möchten darauf hinweisen, dass wir aufgrund der sehr unterschiedlichen Beschaffenheit von Unix/Linux Systemen für die Einrichtung von Zebedee als Service unter Unix/Linux keinen Support leisten. Wenden Sie sich bitte an den Unix/Linux Administrator ihres Instituts wenn sie Hilfe benötigen.

Hilfestellung zur Einrichtung von Zebedee als Systemdienst unter Unix/Linux:

- * Holen Sie sich die Skriptvorlagen (["http://www.rrze.uni-erlangen.de/infrastruktur/datenbanken/firebird/zebedee/unix/scripts/zebedee_unix_scripts.tar.gz"](http://www.rrze.uni-erlangen.de/infrastruktur/datenbanken/firebird/zebedee/unix/scripts/zebedee_unix_scripts.tar.gz)).
- * Entpacken Sie das Archiv.
- * Kopieren Sie zebedee-daemon.conf z.B. nach /etc.
- * Kopieren Sie zebedee-init in das Verzeichnis wo ihre Init-Skripten liegen und passen Sie die Runlevels ihres Init-Prozesses an.
- * Kopieren Sie zebedee-process-checker z.B. nach /usr/local/bin und tragen Sie ihn in die Crontab des in zebedee-daemon.conf spezifizierten Users ein.
- * Passen Sie zebedee-daemon.conf ihrer lokalen Installation an.
- * Überprüfen Sie die beiden anderen Dateien ob alles passt.
- * Überprüfen Sie ob sich der Service starten und stoppen läßt.
- * Überprüfen Sie ob der Cronjob seinen Dienst tut.

Nun sollte alles funktionieren ;-).

Zur Zeit ist ein Zugriff mit ZeBeDee auf den Server dbphoenix nicht möglich. Wir arbeiten an der Problemlösung.