SSHのポートフォワード機能を使って、インターネット(クラウド)上にあるDBとレプリケーションする

インターネット(クラウド)上のサーバー間でセキュリティを考慮して通信させたい

【シチュエーション】

インターネット(クラウド)上のサーバー間で(バックエンドNW：裏LAN を使わずに)
・ DBのレプリケーションしたい
・ バックアップサーバーへ日々、バックアップを行いたい
などなど、インターネット上に(素で)3306/TCPや873/TCPを使わない為には・・・

【方法】

Tunnelを張る。ぱっと思いつくアプリは
・ OpenVPN
・ stunnel
・ OpenSSH

【(比較的簡単な)OpenSSHを使ってトンネルを張る】

最近はSSHがデフォでインストールされているし、追加インストール無で済む。
しかし、root権限レベルの設定変更は必要だが、googleと設定方法はたくさんHitするし、
比較的、簡単に設定できると思う。
googleなら、「SSH」「ポートフォワーディング」

【設定を行うにあたり】

OpenSSHの本来の使われ方は、対象機器に(Secureに)ログインする為に利用。
ログイン後は、対象機器で色々なコマンドを(権限の範囲で)実行可能。

○ 対象機器の管理者＝SSHログイン利用者
普通に対象機器のアカウント/パスワードを作成すれば良い。

リモート端末上では、MySQL TCP/IP Socket 127.0.0.1:3306 がListen状態の場合、
トンネル ローカル端末(127.0.0.1:33306)→リモート端末(127.0.0.1:3306) フォワード設定

© 2026 netstaff <netstaff@chovits.net> | 2026-11-22 23:13
URL: https://www.chovits.jp/phpmyfaq/content/0cat=1/24/ja/sshのポートフォワード機能を使って、インターネットクラウド上にあるdbとレプリケーションする.html

ちょっと難しいですが、
SSH接続(通信方向： ローカル端末 -> リモート端末
トンネル通信方向： ローカル端末 -> リモート端末
トンネル通信方向で、設定が微妙に異なりますので注意が必要です。

[Windows機でTeratermなら]

① 事前設定
Teratermのメニューバー [設定] -> [SSH転送] -> [追加]
(1) ローカルのポートをチェック。「33306」を入力
(2) リッスンは未入力 (未入力だと127.0.0.1)
(3) リモート側ホスト 「127.0.0.1」を入力
(4) ポート 「3306」を入力
[OK] -> [OK] で、設定完了

② 対象機器にログインする
Teratermのメニューバー [ファイル] -> [新しい接続]
ホスト 「203.0.113.1 ポート 「22」
でSSHログインする

③ ローカル端末のTCP/IPソケット確認
コマンドプロンプトを開いて、「netstat -ant」とかで見ると、
ローカル端末で、33306/TCP ポートがListenされているはず。

④ ポートフォワード(トンネル)で接続
C:\>mysql -h 127.0.0.1 -P 33306 -u foo -p'takoika'
すると、リモート端末(172.16.20.1)で動作しているMySQLへ接続できる。

[Linux端末なら]
$ ssh -L 33306:127.0.0.1:3306 operator001@203.0.113.1
~
LocalPort:リモートIP:リモートポート

※ ポートフォワードするローカル端末側のIP(リッスンIP)は、127.0.0.1 としてください。
もしプライベートIPアドレス 192.168.1.1 を設定しまうと、
Bさんが、Aさんの端末を踏み台にして、172.16.20.1:3306 (MySQL)へ接続できてしまうかもしれません。
→ Windows端末だとWindowsファイアーウォール設定や、MySQLの接続許可ホスト設定など通信拒否されるかもしれませんが。

© 2026 netstaff <netstaff@chovits.net> | 2026-11-22 23:13
URL: https://www.chovits.jp/phpmyfaq/content/0cat=1/24/ja/sshのポートフォワード機能を使って、インターネットクラウド上にあるdbとレプリケーションする.html

*teratermの**SSH転送設定 「リモートサーバーのポート(ラジオボタン)」**とか、**ssh の -R オプション**があるが、*
トンネルの通信を逆方向(リモート端末->ローカル端末)にするものだが、滅多に使わないので忘れて良い。
=> 逆方向も出来たよな～ぐらい覚えておいて、使う必要が出来たら、改めて調べたら良いレベル。
=> 著者は、業務上で-R は使った事がない。

〇 対象機器の管理者ではない、SSHログイン利用者
結局の話、どこまで信用できる？という話になってしまいます。

① SSHのポートフォワードだけやりたい。(コマンド実行しない)

sshdconfigを編集しないといけないので、設定はサーバー管理者が行う事になるだろう。
ログイン不要(/bin/bashは必要ない)なので、sshdconfig に

```
Match User user001
AllowTCPForwarding yes
ChrootDirectory /root/dummylogin/user001
```

とか書いておいて、公開鍵認証するなら、
/root/dummylogin/user001/.ssh/authorizedkeys
設定しておく。

利用者には、ポートフォワード利用時に、sshの "-N" オプションを付けて接続を行ってもらう。

※ ずっと張りっぱなしなら、'autossh' が便利。
万一セッションが切断されたら、autosshが再接続してくれる。

② SSHログインしたい場合

[方法1] rbashを使う。
[方法2] CHROOT環境を構築する。(sshdconfig ChrootDirectoryを使う)

どちらの方法も、一長一短です。
結局のところ、どこまで「SSHログイン者を信用できるか」というレベルになります。
rbashの設定は比較的設定が簡単ですが、正しく設定しないと期待した効果が得られないかもしれません。
chroot環境を構築するのは、手間がかかります。

著者の場合は、設定に手間はかかるけど、chroot環境を作って設定しています。
手間がかかる部分(chroot環境の構築)は、自作スクリプトで簡易化しています。
自作スクリプトは、別の記事で公開予定です。

添付ファイル::

一意的なソリューション ID: #1023
製作者: n/a
最終更新: 2022-10-24 07:44

© 2026 netstaff <netstaff@chovits.net> | 2026-11-22 23:13
URL: https://www.chovits.jp/phpmyfaq/content/0cat=1/24/ja/sshのポートフォワード機能を使って、インターネットクラウド上にあるdbとレプリケーションする.html