CentOS 6 - FTP Server

Vsftpd Over SSL/TLS

2014/08/16

	Configure Vsftpd to use SSL/TLS.
[1]	Create certificates.

```
[root@www ~]#

cd /etc/pki/tls/certs


[root@www certs]#

openssl req -x509 -nodes -newkey rsa:2048 -keyout vsftpd.pem -out vsftpd.pem -days 365


Generating a 2048 bit RSA private key
......++++++
.......++++++
writing new private key to '/etc/pki/tls/certs/vsftpd.pem'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----

Country Name (2 letter code) [AU]:

JP



# country

State or Province Name (full name) [Some-State]:

Hiroshima



# State

Locality Name (eg, city) []:

Hiroshima



# city

Organization Name (eg, company) [Internet Widgits Pty Ltd]:

Server World
```

```
# company
Organizational Unit Name (eg, section) []:
IT Solution

# department
Common Name (eg, YOUR name) []:
www.srv.world

# server's FQDN
Email Address []:
xxx@srv.world

# admin's email
[root@www certs]#
chmod 600 vsftpd.pem
```

[2]	Configure Vsftpd.

```
[root@www ~]#
vi /etc/vsftpd/vsftpd.conf
# add follows to the end
rsa_cert_file=/etc/pki/tls/certs/vsftpd.pem
ssl_enable=YES
ssl_ciphers=HIGH
ssl_tlsv1=YES
ssl_sslv2=NO
ssl_sslv3=NO
force_local_data_ssl=YES
force_local_logins_ssl=YES
[root@www ~]#
/etc/rc.d/init.d/vsftpd restart

Shutting down vsftpd:                [  OK  ]
Starting vsftpd for vsftpd:          [  OK  ]
```

[3]	If IPTables is running, allow FTP port and fixed PASV ports. For "-I INPUT 5" section below, Replace it to your own environment.

```
[root@www ~]#
vi /etc/vsftpd/vsftpd.conf
```

```
# add to the end: fix PASV ports

pasv_enable=YES
pasv_min_port=21000
pasv_max_port=21010

[root@www ~]#

/etc/rc.d/init.d/vsftpd restart


[root@www ~]#

iptables -I INPUT 5 -p tcp -m state --state NEW -m tcp --dport 21 -j ACCEPT


[root@www ~]#

iptables -I INPUT 5 -p tcp -m state --state NEW -m tcp --dport 21000:21010 -j ACCEPT
```

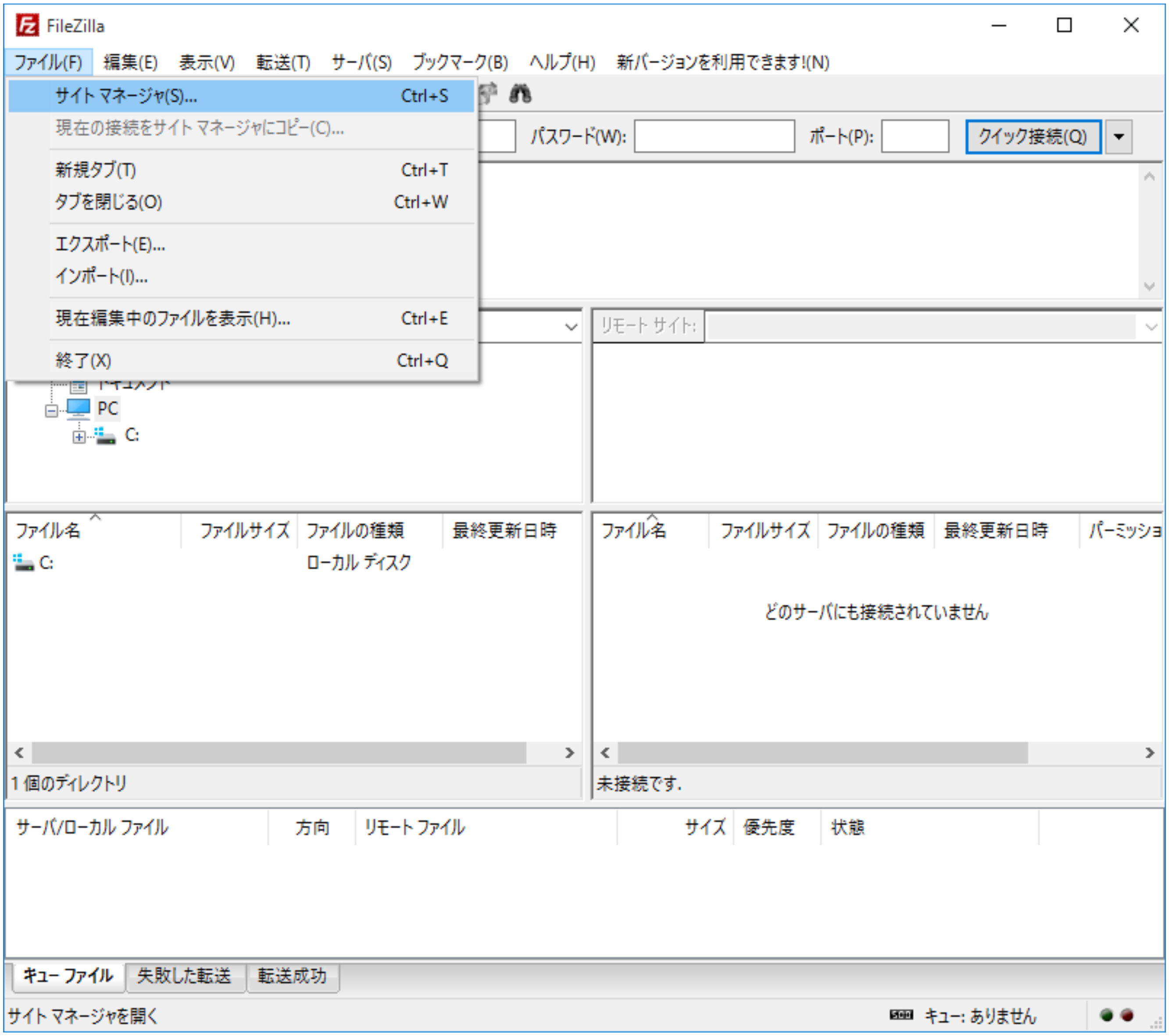
FTP Client : CentOS

	Configure FTP Client to use FTPS connection.
[4]	Install FTP Client and configure like follows.

```
[redhat@dlp ~]$

vi ~/.lftprc

# create new

set ftp:ssl-auth TLS
set ftp:ssl-force true
set ftp:ssl-protect-list yes
set ftp:ssl-protect-data yes
set ftp:ssl-protect-fxp yes
set ssl:verify-certificate no

[redhat@dlp ~]$

lftp -u cent www.srv.world


Password:
lftp cent@www.srv.world:~>
```

FTP Client : Windows

[5]	For example of FileZilla on Windows, Open 'File'-'Site Manager'.


FileZilla
ファイル(F)
編集(E)
表示(V)
転送(T)
サーバ(S)
ブックマーク(B)
ヘルプ(H)
新バージョンを利用できます!(N)
サイト マネージャ(S)... Ctrl+S
現在の接続をサイト マネージャにコピー(C)...
新規タブ(T) Ctrl+T
タブを閉じる(O) Ctrl+W
エクスポート(E)...
インポート(I)...
現在編集中のファイルを表示(H)... Ctrl+E
終了(X) Ctrl+Q
パスワード(W):
ポート(P):
クイック接続(Q)
リモート サイト:
PC
C:
ファイル名
ファイルサイズ
ファイルの種類
最終更新日時
パーミッショ
ローカル ディスク
サーバ/ローカル ファイル
方向
リモート ファイル
サイズ
優先度
状態
キュー ファイル
失敗した転送
転送成功
キュー: ありません

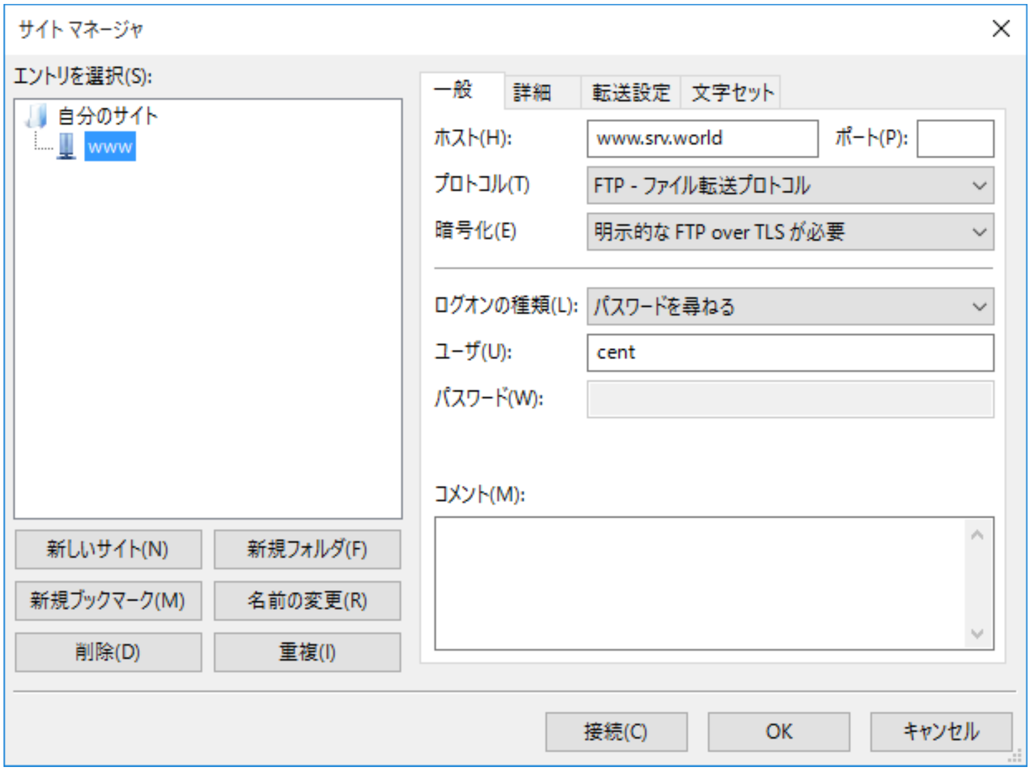
どのサーバにも接続されていません

1 個のディレクトリ

未接続です.

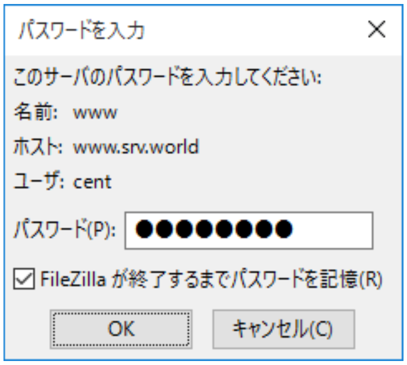
サイト マネージャを開く

[6] Input user info like follows, for encryption field, select "explicit FTP over TLS".


サイト マネージャ
エントリを選択(S):
自分のサイト
www
一般
詳細
転送設定
文字セット
新しいサイト(N)
新規フォルダ(F)
新規ブックマーク(M)
名前の変更(R)
削除(D)
重複(I)
接続(C)
OK
キャンセル

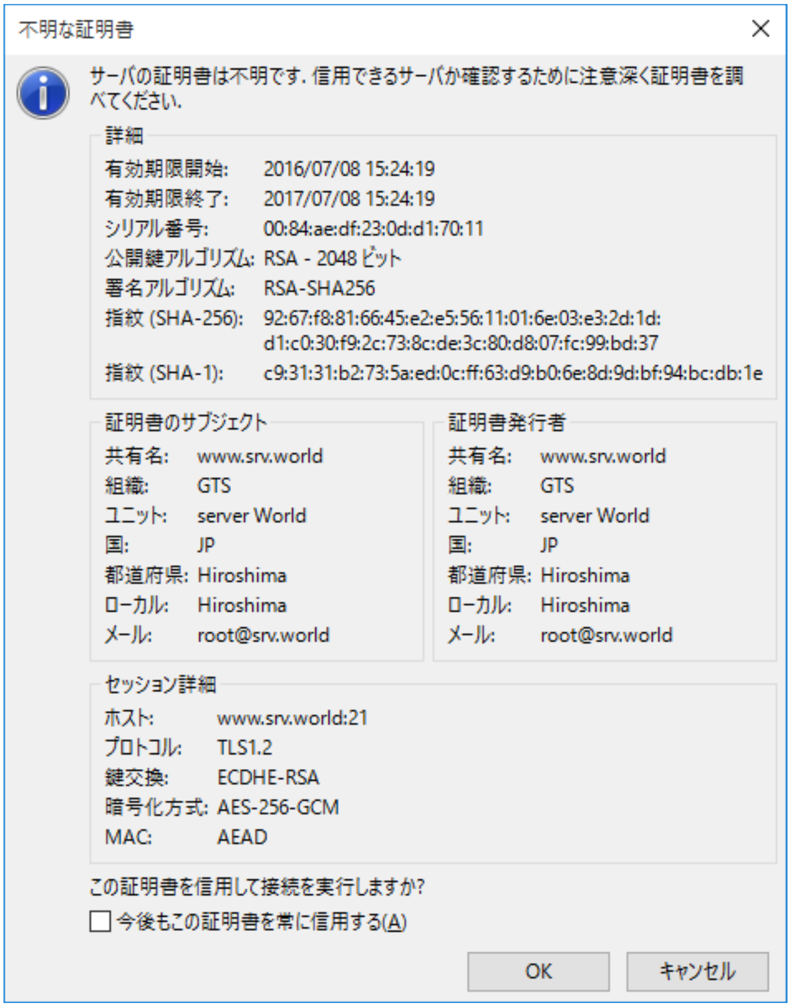
ホスト(H): www.srv.world
ポート(P):
プロトコル(T): FTP - ファイル転送プロトコル
暗号化(E): 明示的な FTP over TLS が必要
ログオンの種類(L): パスワードを尋ねる
ユーザ(U): cent
パスワード(W):
コメント(M):

[7] The user's Password is required. Input it.


パスワードを入力
OK
キャンセル(C)

このサーバのパスワードを入力してください:
名前: www
ホスト: www.srv.world
ユーザ: cent
パスワード(P): ●●●●●●●●
☑ FileZilla が終了するまでパスワードを記憶(R)

[8] The following waring is shown because the certificate is own created, it's no ploblem. Go next.



不明な証明書

サーバの証明書は不明です. 信用できるサーバか確認するために注意深く証明書を調べてください.

詳細

有効期限開始: 2016/07/08 15:24:19
有効期限終了: 2017/07/08 15:24:19
シリアル番号: 00:84:ae:df:23:0d:d1:70:11
公開鍵アルゴリズム: RSA - 2048 ビット
署名アルゴリズム: RSA-SHA256
指紋 (SHA-256): 92:67:f8:81:66:45:e2:e5:56:11:01:6e:03:e3:2d:1d:d1:c0:30:f9:2c:73:8c:de:3c:80:d8:07:fc:99:bd:37
指紋 (SHA-1): c9:31:31:b2:73:5a:ed:0c:ff:63:d9:b0:6e:8d:9d:bf:94:bc:db:1e

証明書のサブジェクト

共有名: www.srv.world
組織: GTS
ユニット: server World
国: JP
都道府県: Hiroshima
ローカル: Hiroshima
メール: root@srv.world

証明書発行者

共有名: www.srv.world
組織: GTS
ユニット: server World
国: JP
都道府県: Hiroshima
ローカル: Hiroshima
メール: root@srv.world

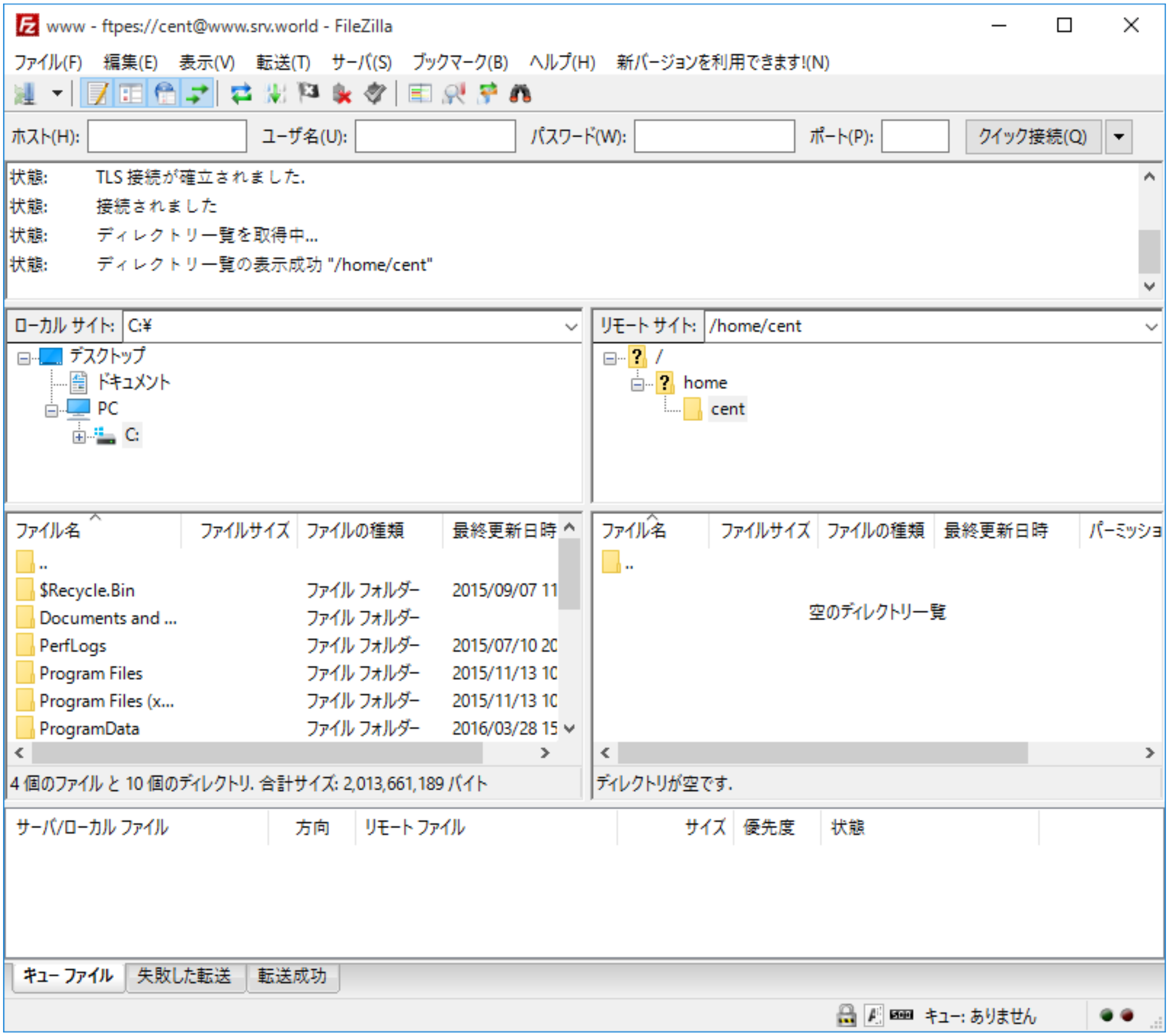
セッション詳細

ホスト: www.srv.world:21
プロトコル: TLS1.2
鍵交換: ECDHE-RSA
暗号化方式: AES-256-GCM
MAC: AEAD

この証明書を信用して接続を実行しますか?

□ 今後もこの証明書を常に信用する(A)

[9] Just connected with FTPS.


www - ftpes://cent@www.srv.world - FileZilla
ファイル(F)
編集(E)
表示(V)
転送(T)
サーバ(S)
ブックマーク(B)
ヘルプ(H)
新バージョンを利用できます!(N)
ホスト(H):
ユーザ名(U):
パスワード(W):
ポート(P):
クイック接続(Q)
サーバ/ローカル ファイル
方向
リモート ファイル
サイズ
優先度
状態
キュー ファイル
失敗した転送
転送成功

状態: TLS 接続が確立されました.
状態: 接続されました
状態: ディレクトリ一覧を取得中...
状態: ディレクトリ一覧の表示成功 "/home/cent"

ローカル サイト: C:¥

- デスクトップ
  - ドキュメント
  - PC
    - C:

ファイル名	ファイルサイズ	ファイルの種類	最終更新日時
..			
$Recycle.Bin		ファイル フォルダー	2015/09/07 11
Documents and ...		ファイル フォルダー	
PerfLogs		ファイル フォルダー	2015/07/10 20
Program Files		ファイル フォルダー	2015/11/13 10
Program Files (x...		ファイル フォルダー	2015/11/13 10
ProgramData		ファイル フォルダー	2016/03/28 15

4 個のファイル と 10 個のディレクトリ. 合計サイズ: 2,013,661,189 バイト

リモート サイト: /home/cent

- /
  - home
    - cent

ファイル名	ファイルサイズ	ファイルの種類	最終更新日時	パーミッショ
..				

空のディレクトリ一覧

ディレクトリが空です.

キュー: ありません

Matched Content