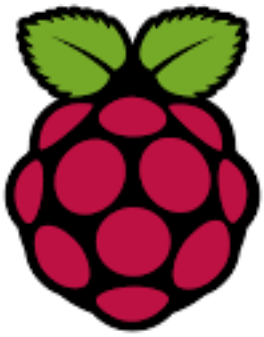
Server FTP Sicuro mediante Raspberry Pi 3b & vsftpd

Resoconto di materiali e presentazione



Vincenzo Puca 297113

14 febbraio 2022

Il progetto da me proposto consiste nella creazione e nell'uso di un server ftp con connessione sicura mediante il prodotto raspberry pi 3b con relativa installazione del applicativo vsftpd, tramite il sistema operativo raspbian, installato a sua volta con scheda micro sd su raspberry.

Il funzionamento è quello di un server ftp con richiesta delle credenziali di accesso, l'accesso stesso sarà reso disponibile soltanto ai dispositivi nella stessa rete locale del server, essendo il server sftp, sarà di tipo sicuro e qualsiasi dato in trasferimento o di log in verrà correttamente crittografato secondo lo standard TLS/SSL. Per raggiungere questo obbiettivo utilizzerò l'applicativo openssl, anch'esso istallato sulla macchina server.

Ogni utente verrà creato al momento dall'installazione di vsftp e, una volta effettuato correttamente il log in , ogni utente potrà vedere in maniera sicura ogni propria cartella utente, inoltre potrà, a piacimento , aggiungere o eliminare cartelle e file, è possibile anche rinominare ogni oggetto a scelta.

Per accedere al server sftp sarà necessario un applicativo di client su macchina esterna, questo può essere installato sia su dispositivi mobile che fissi in maniera completamente automatizzata. Per la prova utilizzerò il software FileZilla da macOS,per la connessione da remoto al server ho utilizzato vnc viewer.

Di seguito sono riportati i link dei produttori e i passaggi da me svolti (con relativa spiegazione per comando) per la realizzazione del progetto.

https://www.raspberrypi.com
https://www.openssl.org
https://security.appspot.com/vsftpd.html
https://www.raspberrypi.com/software/operating-systems
https://www.realvnc.com/en/connect/
https://filezilla-project.org
https://www.apple.com/it/macos/monterey

Comandi Server console:

sudo apt update - per aggiornare i servizi preesistenti

sudo apt install vsftpd - per installare l'applicativo vsftpd

sudo systemctl status vsftpd - per verificare che il servizio sia installato

Creazione di un secondo utente:

sudo adduser usertest2

Quando richiesto inserire la nuova password per l'utente, ora questo sarà correttamente creato (tramite questo comando sarà possibile aggiungere altri utenti a piacere)

Comandi configurazione vsftpd:

sudo nano /etc/vsftpd.conf - per aprire il file di configurazione

All'interno del file .conf appena aperto si procede con la modifica di:

anonymous_enable=NO

local_enable=YES

Queste righe vengono utilizzate per accertarsi che solo gli utenti locali creati sulla macchina possano entrare nella stessa.

write_enable=YES

Utilizzato per permettere le modifiche al filesystem come modificare o rimuovere file.

chroot_local_user=YES

Riga molto importante, se attivata non consente agli utenti di uscire dalla propria area file, non permettendogli così di vedere i file altrui.

user_sub_token=$USER

local_root=/home/$USER/ftp

Comandi usati per permettere di usare questa configurazione all'utente corrente e ad altri utenti futuri tramite l'utilizzo del sub token $USER

Salvare il file di configurazione appena modificato.

Comandi Server console:

sudo systemctl restart vsftpd - per riavviare il servizio ([1])

Il servizio è ora attivo e funzionante, il problema però è che sarà in forma non sicura, ftp raggiungibile dalla porta 21, per cambiare il servizio in sftp andremo ad installare il programma openssl e tramite la creazione di un certificato con aggiunta di una chiave RSA a 2048 bit renderemo il servizio sicuro TSL SLL raggiungibile dalla porta 22.

Comandi Server console:

sudo openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout /etc/ssl/private/vsftpd.pem -out /etc/ssl/private/vsftpd.pem

Con il comando appena digitato imposteremo il certificato a durata di 1 anno tramite il flag -days, con -keyout e -out sullo stesso valore la chiave e il certificato saranno nello stesso file.

Verrà ora richiesto dal programma la compilazione delle informazioni personali per il certificato come il nome dello stato, la provincia, l'indirizzo email e il nome dell'organizzazione.

Una volta terminata la creazione del certificato apriremo nuovamente il file di configurazione vsftpd.

sudo nano /etc/vsftpd.conf

In fondo al file andremo a "decommentare" le seguenti righe:

rsa_cert_file=/etc/ssl/certs/ssl-cert-snakeoil.pem

rsa_private_key_file=/etc/ssl/private/ssl-cert-snakeoil.key

In questo modo vsftpd potrà usare il certificato appena creato, abilitiamo quindi ssl:

ssl_enable=YES

L’aggiunta delle seguenti righe ci permetteranno di non accettare richieste di connessione anonime al server, in modo che siano solo gli utenti creati al momento dell'installazione a poter accedere

allow_anon_ssl=NO

force_local_data_ssl=YES

force_local_logins_ssl=YES

Infine utilizziamo:

require_ssl_reuse=NO

ssl_ciphers=HIGH

Per bloccare il riuso di ssl e per richiedere suite di criptazione più sicura.

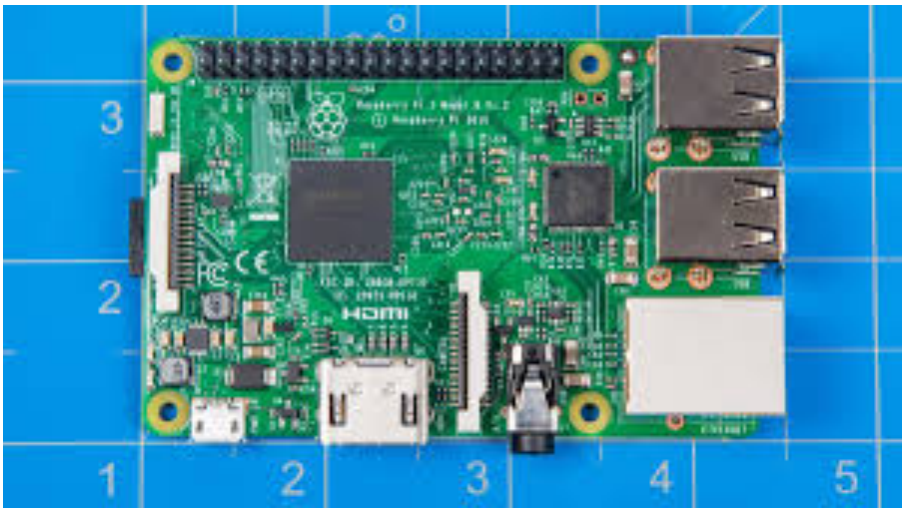
Chiudiamo e salviamo il file.

A questo punto riutilizzeremo ancora una volta nella console server il comando (¹) per riavviare il servizio.

L'attivazione del servizio è ora completa.

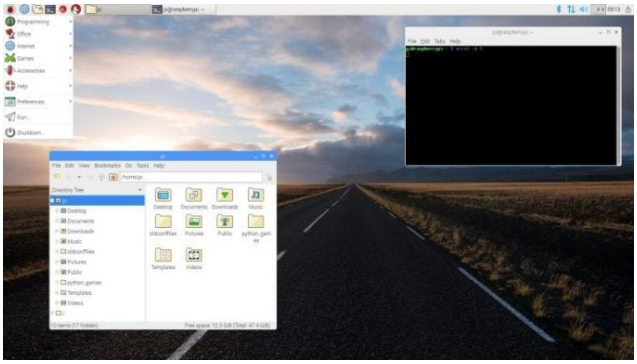
Ora tramite l'uso di FileZilla su client basterà accedere al server tramite le credenziali precedentemente inserite, indirizzo ip locale del server e porta 22 per accedere ai file utente.

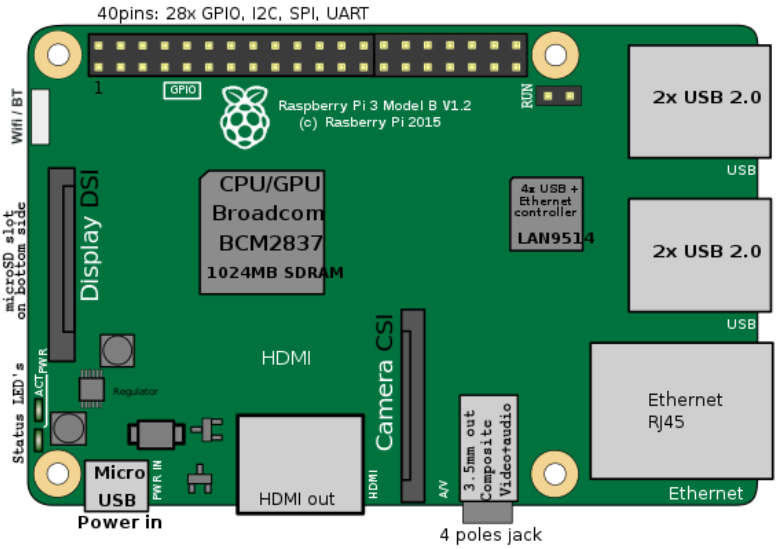
Foto e screenshot:



Raspberry pi 3b

Desktop con riga di comando raspbian su raspberry





Schermata iniziale FileZilla