ftp://205.147.98.133
Installation instructions

Info: ftp://205.147.98.133
Author: Manoj Nishad <manoj.n@manikarananalytics.in>
Date: 2017-02-28, revised _____

Introduction

This document explains how VSFTPD is set up and user authentication is done. The instructions are aimed at any competent Linux system administrator.

Server

The application is hosted at E2E Networks in their NOIDA data centre. It runs on a virtual server (plan VPS-HDD-2B). The server configuration is summarised below:

CPU	Intel(R) Xeon(R) CPU E5-2650 v2 @ 2.60GHz
RAM	26GB
Disk	440GB
OS	CentOS release 6.8 (Final)
IP	205.147.98.133
Traffic	1000GB/month

.

Installation

Make sure you have sudo privilege or use root to perform any installation.

Install vsftpd (very secure FTP daemon) package.

yum install vsftpd -y

Check the version of **vsftpd**

vsftpd -v
vsftpd: version 2.2.2

Edit vsftpd configuration file **/etc/vsftpd/vsftpd.conf**.

 # vi /etc/vsftpd/vsftpd.conf
[...]
Set to "NO"
anonymous_enable=NO

Uncomment
xferlog_file=/var/log/xferlog

Uncomment – increased value
idle_session_timeout=1800
data_connection_timeout=1800

Add at the end of this file
use_localtime=YES
dual_log_enable=YES
log_ftp_protocol=YES
chroot_local_user=YES
pasv_enable=YES
local_root=/home/wind/
max_per_ip=25
max_clients=50

Allow the port that used by vsftpd, Bydefault port number is 20 for ftp-data, and port 21 for ftp connection.

 # iptables -A INPUT -m state --state NEW -m tcp -p tcp --dport 21 -j ACCEPT

 # /etc/init.d/iptables save
 # /etc/init.d/iptables restart

Start the vsftpd service and make it to start automatically on every reboot:

 # service vsftpd start
 # chkconfig vsftpd on

Create FTP users

By default, root user is not allowed to login to ftp server for security purpose. So let us create a testing user called **“test”** with password **“centos”**:
Note: Always keep strong password.

 # useradd test
 # passwd test

Now, remove login shell for user test so that test user can't login in shell.

 # vim /etc/passwd
Go to row where user test located, change their shell. This is an optional to enahnce security.

Old
test:x:556:556::/home/test:/bin/bash
New
test:x:556:556::/home/test:/sbin/nologin

Set selinux to home directory

 # setsebool -P /home/wind

Add module to kernal, Enabling passive mode

 # modprobe ip_conntrack_ftp

Restart the service

 # /etc/init.d/vsftpd restart

creating folder in /home/wind/WIND
Previously all the folders are withine wind, now all folders has shifted to WIND.

mkdir foldername

3. setting permission

chmod 750 foldername

 # creating ACL for each user.

setfacl -m u:username:rx foldername (rx is the permission r=read, x=execute, w=write)

****keep in mind that all folder should have read and execute permission for user=mpl.****

VSFTP is installed and ready to use!!

Thank you :)