HARTMAN
AUTOMATISERINGS
CONSULTANCY

General Infrastructure

vsftpd FTPS setup

Red Hat Enterprise Linux 5 / CentOS 5

Author: René Hartman

Version: 1.2.2

HARTMAN
AUTOMATISERINGS
CONSULTANCY

DOCUMENT HISTORY

Document Location

Ensure that this document is the current version. Printed documents and locally stored copies may become obsolete due to changes in the master document.

Revision History

Document name:	FTPS_Setup_RHEL5.doc
Version:	1.2.2
Date of 1st version:	14-May-2010
Date of this version:	14-May-2010

Note: in the following table the revision number does not necessarily match with the version number of the document. The version number of the document is merely meant to control the number of saved changes.

Version	**Date**	**Author**	**Status***			**Brief Description, Remarks**
			Cpt	**FA**	**Ap**	
1.0	14-May-2010	René Hartman	**X**			Initial Draft

* Cpt = Concept; FA = For Approval; Ap = Approved

HARTMAN
AUTOMATISERINGS
CONSULTANCY

Reviewers

The following people have reviewed this document

Version	Name	Role	Required date of feedback

Classifications

Status: For approval

HARTMAN
AUTOMATISERINGS
CONSULTANCY

TABLE OF CONTENTS

HARTMAN
AUTOMATISERINGS
CONSULTANCY

1 INTRODUCTION

1.1 Overview

This document provides a detailed description of the installation and configuration of an FTPS Server.

1.2 Document Conventions

Each step in the installation procedure where command line user input is required is first described and then followed by the commands used.

Fonts used:

Information and general guidelines	Tahoma, 10pt
`#/$ Commands`	`Courier New, 8pt`
`Command output`	`Courier New, 8pt`

Commands are preceded by a # symbol indicating that they are executed as the root user or by a $ symbol which means they are executed as a "normal" user.

It is worth noting that when cutting and pasting commands from word documents to a PuTTY session, occasionally a minus '-' symbol is converted to period '.' Watch out for these!

1.3 Prerequisites

1.3.1 Partitions

Some applications require that the `/tmp` partition be executable. For security reasons this directory is sometimes mounted 'noexec'. vsftpd does rely on /tmp, so this presents no issues here.

1.3.2 Software Repository

Tthe vsftpd package is available through the standard repositories as an RPM package, and can be installed using yum.

1.3.3 Specific Users / Groups

group ftp (gid 50) and user ftp (uid 50) will be created during installation of the vsftpd package.

HARTMAN
AUTOMATISERINGS
CONSULTANCY

2 INSTALLATION

The vsftp package can be installed from the OS repository using yum:

```
# yum install vsftpd
```

This is valid for RHEL5 and 4. For RHEL 3, please download and install vsftpd-2.0.1-5.EL4.7.i386.rpm:

```
# rpm -i vsftpd-2.0.1-5.EL4.7.i386.rpm
```

Using `yum install vsftpd` with RHEL3 will install vsftpd-1.2.1-3E.16.i386.rpm which does not support SSL, and thus will not allow secure data transfers. Do not use this version (1.2.1).

When installing vsftpd as outlined above, you'll end up with versions 2.0.1 (RHEL3/4) and 2.0.5 (RHEL5) of vsftpd, both of which use file /etc/vsftpd/vsftpd.conf for their configuration. Version 2.0.1 expects the additional configuration files in /etc, while version 2.0.5 expects those in /etc/vsftpd. For this reason, it's best to keep all config files and lists in /etc/vsftpd and define links to those in /etc for version 2.0.1. File naming differences between versions 2.0.1 and 2.0.5 are straightforward: if v2.0.5 expects file /etc/vsftpd/user_list, the (sym)link for version 2.0.1 will be /etc/vsftpd.user_list, etc.

We'll be using additional configuration files ftpusers and user_list, so when installing version 2.0.1 the following commands need to be executed additionally:

```
# mv /etc/vsftpd.ftpusers /etc/vsftpd/ftpusers
# ln /etc/vsftpd/ftpusers /etc/vsftpd.ftpusers
# mv /etc/vsftpd.user_list /etc/csftpd/user_list
# ln -s /etc/vsftpd/user_list /etc/vsftpd.user_list
```

Please note that pam requires a hard link, while vsftpd accepts symbolic links; i.e: /etc/vsftpd.ftpusers *must* be a hard link to /etc/vsftpd/ftpusers, or else pam will complain:

```
vsftpd[29990]: PAM-listfile: /etc/vsftpd.ftpusers is either world writable or not a normal
file.
```

HARTMAN
AUTOMATISERINGS
CONSULTANCY

2.1 Configuration

2.1.1 SSL

For secure operation, vsftpd requires an SSL certificate. If a self-signed certificate can not be used, an official one needs to be ordered. A self-signed certificate can be generated as follows (this assumes that OpenSSL has been installed earlier; please note that the certificate store itself can also be used to store the certificate instead of the vsfpd dir, as long as vsftpd.conf reflects the proper location):

```
# openssl req -x509 -nodes -days <# of validity days> -subj
'/C=NL/L=Amsterdam/O=<organisation> NL/CN=<fq_hostname>' -newkey rsa:1024 -keyout
/etc/vsftpd/vsftpd.pem -out /etc/vsftpd/vsftpd.pem
```

This certificate can be accepted as a valid one by symlinking it to the certificate store, using script certlink.sh (source listed in Appendix A), which should be placed in the certs directory (location varies with OpenSSL version, can be /usr/share/ssl/certs (RHEL3/4) or /etc/pki/tls/certs (RHEL5):

```
# cd / etc/pki/tls/certs
# ./certlink.sh /etc/vsftpd/vsftpd.pem
```

A symlink similar to `b49c3b1c.0` will be created in the certs directory, pointing to the certificate. The resulting symlink can also be copied to the certs directory of a client host, after which that host will accept that certificate as a valid one (no self-signed warnings or rejections).

HARTMAN
AUTOMATISERINGS
CONSULTANCY

2.1.2 vsftpd

Configuration consists of three files, vsftpd.conf, ftpusers and user_list, which all reside in /etc/vsftpd. For running through xinetd (recommended, and implemented here), a script /etc/xinetd.d/vsftp must be installed as well. When tcpwrappers are enabled in vsftpd.conf, files /etc/hosts.allow and/or /etc/hosts.deny also need to be edited.

File ftpusers is used by pam, needs a hardlink in /etc for versions below 2.0.5, and will be left as provided. It lists users that should never be allowed to sign on using FTP.

File user_list needs a symlink in /etc for versions below 2.0.5 and will only contain the userid(s) for the user(s) that may use ftps. The allow/deny behavior for this file is determined by the userlist options in vsftpd.conf, which by default denies the listed users. As we will be only allowing the listed users, the existing users should be removed and replaced by the intended FTP user(s).

The remainder of the configuration is down to file vsftpd.conf, which should contain only the following uncommented lines:

```
anonymous_enable=NO
local_enable=YES
write_enable=YES
local_umask=022
dirmessage_enable=YES
xferlog_enable=YES
connect_from_port_20=YES
xferlog_file=/var/log/vsftpd
xferlog_std_format=YES
nopriv_user=ftp
chroot_local_user=YES
pam_service_name=vsftpd
userlist_enable=YES
userlist_deny=NO
tcp_wrappers=YES
ssl_enable=YES
rsa_cert_file=/etc/vsftpd/vsftpd.pem
force_local_data_ssl=YES
pasv_min_port=12020
pasv_max_port=12021
```

The last two lines allow for 2 concurrent passive sessions; if more are required, a wider port range can be specified. Be sure to open up the portrange specified in the server's firewall, or else clients will not be able to connect in passive mode, which normally is a requirement in corporate networks.

No other uncommented lines should exist; pay special attention to the listen=YES directive that's enabled by default but should not be when using xinetd.

Should you require support for ASCII conversion during up- or download, please pay special attention to the remarks concerning ASCII mode in the default vsftpd.conf file.

Please note that the `tcp_wrappers=YES` line is optional, but when used, an entry is required in /etc/hosts.allow for each host that's allowed to set up an ftps connection:

```
vsftpd: ip_address_1 ip_address_2 ip_address_3
```

HARTMAN
AUTOMATISERINGS
CONSULTANCY

2.1.3 xinetd

xinetd control requires the following vsftp enabling script in /etc/xinetd.d:

```
service ftp
{
        disable         = no
        socket_type     = stream
        wait            = no
        user            = root
        server          = /usr/sbin/vsftpd
        nice            = 10
}
```

Then restart xinetd:

```
# service xinetd restart
```

Verify that all is well using netstat:

```
# netstat -a|grep ftp
tcp        0      0 *:ftp                   *:*                     LISTEN
```

and/or lftp:

```
# lftp -d user@hostname
```

lftp allows for verification of proper operation. After sign-on, use the ls command to obtain a directory listing. Because debug mode is enabled by specifying the –d option, lftp tells the user nicely what's happening. It may be required to add the line

```
set ftp:ssl-protect-data option
```

to /etc/lftp.conf in order to allow lftp to handle encrypted data.

HARTMAN
AUTOMATISERINGS
CONSULTANCY

3 APPENDIX A

certlink.sh is not a standard script; when not present it can be created by copying this code

```
#!/bin/sh
#
# usage: certlink.sh filename [filename ...]

for CERTFILE in $*; do
  # make sure file exists and is a valid cert
  test -f "$CERTFILE" || continue
  HASH=$(openssl x509 -noout -hash -in "$CERTFILE")
  test -n "$HASH" || continue

  # use lowest available iterator for symlink
  for ITER in 0 1 2 3 4 5 6 7 8 9; do
    test -f "${HASH}.${ITER}" && continue
    ln -s "$CERTFILE" "${HASH}.${ITER}"
    test -L "${HASH}.${ITER}" && break
  done
done
```

into file /etc/pki/tls/certs/certlink.sh and making the file executable:

```
  # chmod 700 certlink.sh
```

Source for certlink.sh originated from the OpenSSL Command-Line HOWTO guide.