HP-UX - How to Configure SFTP Logging in a Chrooted Environment?

Information

How to enable SFTP INFO level logging for chrooted SFTP users?
"For logging to work, `sftp-server` must be able to access `/dev/log`. Use of `sftp-server` in a chroot configuration therefore requires that `syslogd(8)` establish a logging socket inside the chroot directory."

NOTE: See `sftp-internal(8)` and Secure Shell A.05.20 Release Notes.

Detail

The following steps are a workaround to configure logging in a chrooted SFTP environment on the SFTP server. The trick here is to make syslogd accessible from with in the chrooted environment. This example assumes that a SFTP user has already been created and that the SFTP chroot environment has already been setup by previously running the `/opt/ssh/utils/ssh_chroot_setup.sh` script. This example will use the following configured SFTP user account:

```
#grep sftpusr /etc/passwd
sftpusr:QDtdUGHAb/Xf2:1001:20:chrooted SFTP
user:/home/sftpusr:/bin/sh
```

Configure the SFTP chroot directory and send the logging to an unused syslog facility. It is needed to switch from using the `sftp-server` subsystem to `internal-sftp` to facilitate the chrooted environment. See `sshd_config(5)`.

NOTE: If the "`Match user`" statement is not used, all users logging in with ssh, scp and SFTP will be chrooted.

```
# vi /opt/ssh/etc/sshd_config

#Subsystem      sftp    /opt/ssh/libexec/sftp-server
Subsystem      sftp    internal-sftp -flocal7 -linfo

Match user sftpusr
      ChrootDirectory /newroot

# /sbin/init.d/secsh stop ; /sbin/init.d/secsh start
```

Configure syslogd to log to an unused syslog facility. This must be the same facility used in the sshd_config file.

NOTE: This step is commonly forgotten, especially when the system wide file has been updated.

CAUTION: The syslog.conf file must use the <tab> for white spaces. See logger(1) and syslogd(1M).

```
# vi /etc/syslog.conf
local7.info    /var/adm/syslog/local7-info.log

# cp /etc/syslog.conf /newroot/etc/syslog.conf
```

Copy the syslogd binary and it's dependency libraries in to the respective chrooted environment.

NOTE: These libraries may already be in the new chrooted environment.

```
# mkdir -p /newroot/usr/sbin
# cp -p /usr/sbin/syslogd /newroot/usr/sbin
```

Determine which architecture and shared dynamic library files are required for user's 'syslogd' binary.
** These files may vary from those required on user's system.

NOTE: 'ELF-32' implies the path '/usr/lib/hpux32' and 'PA-RISC1.1' implies the path '/usr/lib/'.

```
# chatr /usr/sbin/syslogd
# file /usr/sbin/syslogd
# mkdir /newroot/usr/lib/<arch of syslogd>
# cp -p /usr/lib/<arch>/libdl\.* /newroot/usr/lib/<arch>/
# cp -p /usr/lib/<arch>/libc\.* /newroot/usr/lib/<arch>/
# cp -p /usr/lib/<arch>/dld\.* /newroot/usr/lib/<arch>/
# cp -p /usr/lib/<arch>/uld\.* /newroot/usr/lib/<arch>/
```

Start the syslogd inside of the chroot environment. See chroot(1M) and syslogd(1M).

```
# mkdir -p /newroot/var/adm/syslog
```

The next command will need to be placed in a system startup script to survive a reboot.

```
# chroot /newroot /usr/sbin/syslogd -D -v
```

There should now be two syslogd programs running:

```
# ps -ef|grep syslogd
```

And the following new device file has been generated:

```
# ll /newroot/dev/log
```

Verify the SSH INFO level logging is working by establishing an SFTP connection to the server and monitor the targeted log file (be sure to look at the chrooted log file).

```
# tail -f /newroot/var/adm/syslog/local7-info.log
```

CAUTION: Running stop and start on `/sbin/init.d/syslogd` will zero out the system wide syslog.log file.

NOTE: The `/opt/ssh/utils/sftponly` is an optional shell wrapper which can be substituted to restrict SFTP access only (no ssh access) to the respective users account. To prevent login(1) access (ftp, telnet, rlogin) remove this shell from /etc/shells.

Excerpt from `/opt/ssh/etc/sshd_config`

```
# Chrooted sftp setup
Subsystem sftp internal-sftp -flocal7 -linfo

# Match users
Match User msc01
     ChrootDirectory /ch/msc02
     X11Forwarding no
     AllowTcpForwarding no
     ForceCommand internal-sftp -l VERBOSE -f LOCAL7

Match User msc02
     ChrootDirectory /ch/msc02
     X11Forwarding no
     AllowTcpForwarding no
     ForceCommand internal-sftp -l VERBOSE -f LOCAL7

Match User msc03
     ChrootDirectory /ch/msc03
     X11Forwarding no
     AllowTcpForwarding no
     ForceCommand internal-sftp -l VERBOSE -f LOCAL7
```