hpux 如何为ssh和sftp配置chroot环境

Linux系统调优 Linux系统安装 于东阳 2017-09-01 发表

为ssh和sftp配置chroot环境

CHROOT就是Change Root，也就是改变程序执行时所参考的根目录位置。
chroot通过将软件置于一个“jail”(监牢)中，把它与系统其他文件隔离开来。当你要测试一个可能影响你系统或者不安全的软件时，这项技术尤为有用。
从根本上说，chroot是一个特殊的目录，在这个目录中运行的程序无法访问目录外的文件。而从许多方面看，chroot就像在你的系统上安装了另一个系 统。技术上说来，chroot暂时地把根目录（通常是“/”）切换到chroot 目录（比如说“/var/chroot"）。由于根目录是文件系统的顶端，应用程序无法访问高于根目录的目录，所以应用程序与其他的系统文件隔离开了。
需要注意的是，从chroot目录外访问chroot内的文件是可能的。

1 新建一个系统新用户。
root@vm15:/tmp/testyu1 # useradd -m -d /home/tmp/testyu1 -s /usr/bin/sh testyu
root@vm15:/tmp/testyu1 # passwd testyu
Changing password for testyu
New password:
Re-enter new password:
Passwd successfully changed
2 查看系统用户的文件。确认新建的用户是否成功。
root@vm15:/tmp/testyu1 # more /etc/passwd
root:RPwbj.mQMUPBU:0:3::/:/sbin/sh
daemon:*:1:5::/:/sbin/sh
bin:*:2:2::/usr/bin:/sbin/sh
sys:*:3:3::/:
adm:*:4:4::/var/adm:/sbin/sh
uucp:*:5:3::/var/spool/uucppublic:/usr/lbin/uucp/uucico
lp:*:9:7::/var/spool/lp:/sbin/sh
nuucp:*:11:11::/var/spool/uucppublic:/usr/lbin/uucp/uucico
hpdb:*:27:1:ALLBASE:/:/sbin/sh
nobody:*:-2:-2::/:
www:*:30:1::/:
cimsrvr:*:101:101:WBEM Services:/var/opt/wbem:/sbin/sh
smbnull:*:102:102:DO NOT USE OR DELETE - needed by Samba:/var/opt/samba/nologin:/bin/false
opc_op:*:777:177:OVO default operator:/home/opc_op:/sbin/sh
hpsmh:*:103:103:System Management Homepage:/var/opt/hpsmh:/sbin/sh
sfmdb:*:104:20::/home/sfmdb:/sbin/sh
sshd:*:105:104:sshd privsep:/var/empty:/bin/false
iwww:*:106:1::/home/iwww:/sbin/sh
owww:*:107:1::/home/owww:/sbin/sh
tftp:*:108:105:Trivial FTP user:/home/tftp:/usr/bin/false
test:KSJFSZT6Dx6Ok:109:106::/home/test:/usr/bin/sh
test1:x/nsRtObosZV.:110:20::/home/123:/sbin/sh
test2:*:111:20::/home/test2:/sbin/sh
test3:W7tYqkP4Ce8fw:112:20:chrooted user:/home/test3:/bin/sh
test4:IXUEDymG1Flrg:113:20:chrooted user:/user/test2:/bin/sh
test5:*:114:20::/home/tmp/testyu:/sbin/sh
testyu:urPHogTpjMASI:115:20::/home/tmp/testyu1:/usr/bin/sh

3 编辑 /opt/ssh/etc/sshd_config 配置文件，增加新用户和新用户登录目录。
root@vm15:/home # vi /opt/ssh/etc/sshd_config
Example of overriding settings on a per-user basis
Match User test3
ChrootDirectory /newroot
Match User test4
ChrootDirectory /newroot2
Match User testyu
ChrootDirectory /home/tmp/testyu1
#	X11Forwarding no

```
#     AllowTcpForwarding no
#     ForceCommand cvs server
```
4 执行./ssh_chroot_setup.sh 服务。
```
root@vm15:/opt/ssh/utils # ./ssh_chroot_setup.sh

HP SECURE SHELL: CHROOT ENVIRONMENT SETUP - MAIN MENU
        ------------------------------------------------------
        Select one of the option below
        1.Configure a chroot enviroment
        2.Exit

        Enter your choice : 1
Chroot setup
       ---------------
        User name (Maximum eight chars) : testyu

        Chroot setup
       ---------------
        User name (Maximum eight chars) : testyu
        chroot setup checks for user details
        Enter the new root directory for testyu with absolute path (or press return for default(/newroot)):
/home/tmp/testyu1
Select chroot secure shell option
        ----------------------------------
        1 sftp
        2 ssh & sftp & scp
        press return key to skip this step

        Option : 2
        Now configuring the chroot environment for ssh & sftp & scp...finished
        Summary
        --------
        Chroot-ed user : testyu3
        Chroot-ed user&amp;#39;s new root directory : /newroot
        Secure Shell configuration : SSH & SFTP & SCP
```
5 停止 /sbin/init.d/secsh 服务。
```
root@vm15:/opt/ssh/utils # /sbin/init.d/secsh stop
HP-UX Secure Shell stopped
```
6 启动 /sbin/init.d/secsh 服务。
```
root@vm15:/opt/ssh/utils # /sbin/init.d/secsh start
HP-UX Secure Shell started
```
7 确认 /newroot 这个目录是否正常。
```
root@vm15:/opt/ssh/utils # cd /newroot
root@vm15:/newroot # ll
total 16
dr-xr-xr-x   2 bin        bin            96 Aug 10 16:01 bin
dr-xr-xr-x   3 bin        bin            96 Aug 10 16:01 dev
dr-xr-xr-x   2 bin        bin          8192 Aug 10 16:01 etc
dr-xr-xr-x   3 bin        bin            96 Aug 10 16:01 home
dr-xr-xr-x   4 bin        bin            96 Aug 10 16:01 opt
dr-xr-xr-x   2 bin        bin            96 Aug 10 16:01 sbin
drwxrwxrwt   2 root       root           96 Aug 10 16:01 tmp
dr-xr-xr-x   5 bin        bin            96 Aug 10 16:01 usr
dr-xr-xr-x   3 bin        bin            96 Aug 10 16:01 var
```
8 切换到新建的新用户登录系统测试。
```
into newroot home
```