
Chrooting on SSH?

by **fzoulchembryl** » Wed Jun 10, 2009 2:28 pm

hi everybody

in first, excuse me for my bad english ! i'll do my best !
i've got a server on ssh at home, and the users can go above the default directory (/mnt)

in my /mnt i've got 2 subdirectory /mnt/RAID5 and mnt/UPLOAD

i would like to chroot all the users to the /mnt and not to up on the roots (/)

is it possible? i just want to chroot all my users in the default directory, now they can move up above the /mnt
/. (<= root of the disk)
|_ /mnt (<= where i want to chroot my users)
|_ / RAID5
|_ /UPLOAD

i don't want them to go on the root of the hard disk and for this i need to chroot my users

http://www.trustonme.net/didactels/318.html

i find something about this, but not compaptible with freebsd.
please help me, it's dangerous to let my ssh server like this users can navigate all the disk!
i think they haven't got the permission in write, but i dont like to know all my users are navigating my hard disk.
thank's to help me !

Re: Chrooting on SSH?

by **danmero** » Thu Jun 11, 2009 12:00 pm

> *fzoulchembryl wrote:*i just want to chroot all my users in the default directory

Shell user(ssh) must be able to traverse root(/) to access(read/execute) some utilities, otherwise he doesn't need shell access.

> *fzoulchembryl wrote:*now they can move up above the /mnt

Yes, they can go above /mnt but they can't read sensitive information like configuration files or temporary configuration files and they can't write just anywhere.

> *fzoulchembryl wrote:*i don't want them to go on the root of the hard disk and for this i need to chroot my users

Take a look at built-in FreeNAS /usr/sbin/chroot and FreeBSD Handbook > Chapter 15 Jails

---

Re: Chrooting on SSH?

by **fzoulchembryl** » Thu Jun 11, 2009 12:46 pm

thanks, i will look into that.
i know they can't change anything but it's not professional ... ...

Re: Chrooting on SSH?

by **alphazo** » Thu Aug 27, 2009 5:08 pm

Hello,

FTP can be configured to run chrooted so users only see their home directories. I would prefer to use SCPonly on top of SSH for its more secure authentication schemes however as the original poster mentioned users can view the entire

filesystem which is beside being "less professional" can lead to confusion on where to find the information. For non-Unix people it is not obvious that data will be found under /mnt. Again I'm not talking about full SSH shell access but the rather limited scponly mode that restricts usage to file transfer so no console mode. Is there a way to configure that in Freenas even manually. I guess that will include copying so of the executable tools inside the jailed environment.

Thank you
Alphazo / 0.7RC2 Khasadar (revision 4882)

[EDIT] There is a chroot version of scponly that does what we need. It is called scponlyc. Can it run under Freenas?

Re: Chrooting on SSH?

by **srogovtsev** » Tue Sep 01, 2009 5:36 pm

> *alphazo wrote:*There is a chroot version of scponly that does what we need. It is called scponlyc. Can it run under Freenas?

Yes it can.

Re: Chrooting on SSH?

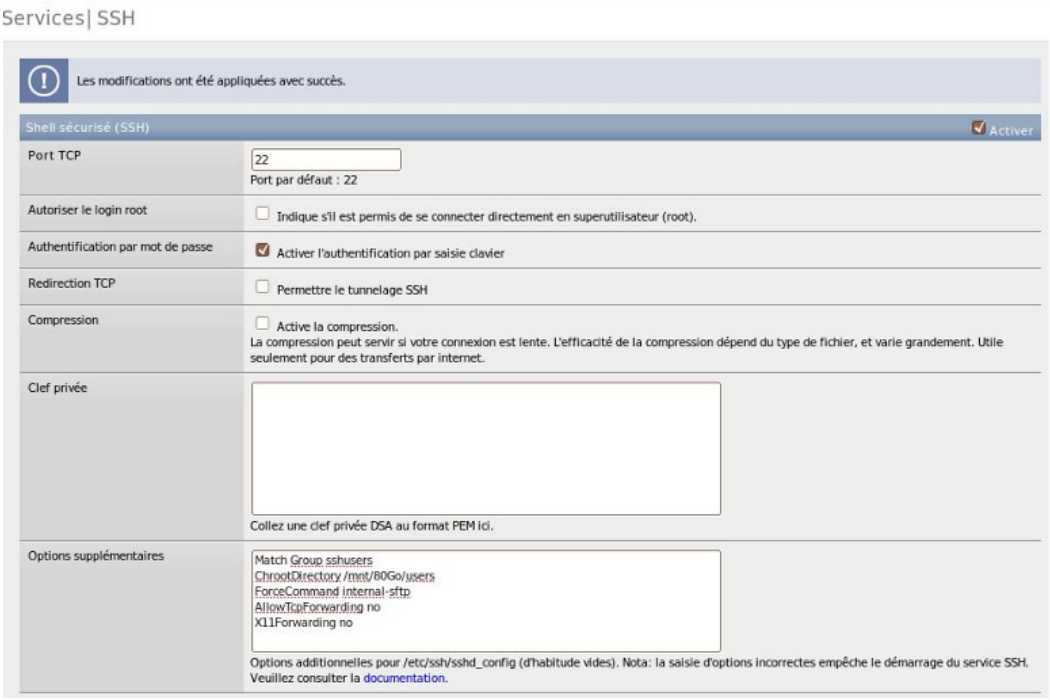
by **jluc6331** » Sat Jan 16, 2010 7:52 pm

Chrooting on SSH is possible with this version of FreeNAS !

First sorry for my poor english.
FreeNAS user since beginning of this year, I use FreeNAS 0.7 (Khasadar)
I would like to chroot my ssh accesses.
Finding some HowTo on the web both in french and in english :
http://www.christopher.compagnon.name/sitewww/freebsd-sftp.html
http://blog.anotherhomepage.org/post/2009/10/04/Transfert-de-fichier-simple-et-s%C3%A9curis%C3%A9-:-sftp-en-chroot
http://undeadly.org/cgi?action=article&sid=20080220110039
I tryed.

Using the WebGUI,
1) I define a new group : sshusers
2) I define a new user :
User1, member of sshusers group, Shell = nologin, home = User1

3) I configure SSH Service, following the various HowTo writting in Supplementary Options



ssh_service.jpg (72.66 KiB) Viewed 490 times

where /mnt is the FreeNAS standard mount point,
/mnt/80Go is the mount point of the disk
/mnt/80Go/users is the users' generic folder where all users will be chrooted

4) into /mnt/80Go/users, I create User1 folder, the home directory of User1 with the following owner and access rights

Code: Select all

```
$ ls -al /mnt/80Go/users
total 24
drwxr-xr-x  6 root     wheel     512 Jan 16 19:32 .
drwxr-xr-x  4 jle      ftp       512 Jan 13 22:18 ..
drwxr-x---  2 User1    sshusers  512 Jan 16 19:32 User1
drwxr-xr-x  3 root     sshusers  512 Jan 16 16:20 home
drwxr-x---  2 root     wheel     512 Jan 16 18:50 mnt
drwxr-xr-x  3 scponly  sshusers  512 Jan 16 18:53 scponly
```

5) Now, using the FreeNAS console, I need to tune the sshd_config file but using an embedded, it is regenerated at each restart of the ssh deamon.
So I modified /etc/rc.d/sshd by replacing the line:
... Subsystem sftp /usr/libexec/sftp-server
with
....Subsystem sftp internal-sftp

6) the last thing I need, is to change owner and access rights of :
/mnt, /mnt/80Go and /mnt/8OGo/users to allow chroot to work properly

Code: Select all

```
#chown -R root:wheel /mnt/80Go/users
#chmod -R 755 /mnt/80Go/users
```

7) and now, it is time to restart the ssh deamon

Code: Select all

```
#/etc/rc.d/sshd restart
```

8) Connecting User1 using ubuntu SSH service, I have a share on /mnt/80Go/users where I can:
+ create files and folders into /mnt/80Go/users/User1 (the home of User1),
+ view the content of /mnt/80Go/users/home and /mnt/80Go/users/scponly
+ do nothing in /mnt/80Go/users/mnt

I have two concerns using an embedded:
the default access rights of /mnt is 777 that I need to correct at each FreeNAS startup.
the regeneration of the /etc/ssh/sshd_config at each FreeNAS startup.

So I will migrate to and full installed version on hard disk to solve these issues unless a way to change some thing is the embedded is possible.

EDIT 17/01/2010: I migrated this morning on a "full install" (same version). All these modifications are now permanent and are working fine. I'm really happy

---

Re: Chrooting on SSH?

by **roguelv** » Thu Feb 11, 2010 4:06 am

Thanks for the guide jluc! I am new to FreeNAS/FreeBSD/Unix/Linux so I have a couple questions as I try to muster my way thru this.

For step 4, where do I go to change those rights?

> 4) into /mnt/80Go/users, I create User1 folder, the home directory of User1 with the following owner and access rights
>
> Code: Select all
>
> ```
> $ ls -al /mnt/80Go/users
> ```

```
total 24
drwxr-xr-x  6 root     wheel     512 Jan 16 19:32 .
drwxr-xr-x  4 jle      ftp       512 Jan 13 22:18 ..
drwxr-x---  2 User1    sshusers  512 Jan 16 19:32 User1
drwxr-xr-x  3 root     sshusers  512 Jan 16 16:20 home
drwxr-x---  2 root     wheel     512 Jan 16 18:50 mnt
drwxr-xr-x  3 scponly  sshusers  512 Jan 16 18:53 scponly
```

Is there a main file that lists all the rights of the groups that are included in FreeNAS? When I go to WebGUI: Access > Users and Groups > Groups, I see alot of groups listed but no idea what they all do or what their permissions are.

And for step 5, I am a bit confused. Should it be "chinternal-sftp" or "internal-sftp"?

> 5) Now, using the FreeNAS console, I need to tune the sshd_config file
> but using an embedded, it is regenerated at each restart of the ssh deamon.
> So I modified /etc/rc.d/sshd by replacing the line
> ... Subsystem sftp /usr/libexec/sftp-server
> by
> ....Subsystem sftp **chinternal**-sftp

And am I deleting "Subsystem sftp /usr/libexec/sftp-server" and replacing it with "Subsystem sftp chinternal-sftp" or just adding a new line with it?

Thanks so much for you time and help!

Re: Chrooting on SSH?

by **jluc6331** » Thu Feb 11, 2010 7:29 am

Hi al,
I'm very pleased to share my configuration. And if it could be useful to somebody, it is nice ....

Hi roguelv,
step 4)
Just use chown and chmod standard Linux command. The man can help you. run these commands as su of course.
quickly :
To change owner and group for a file or directory: > chown new_user:new_group filename
To change the permission for a file or directory: > chmod octal_value filename where the octal_value define the access rights for owner-group-others.
in my special case
> chown User1:sshusers /mnt/80Go/users/User1
> chmod 750 /mnt/80Go/users/User1
but have a look to both man pages to well understand the commands.

step 5)
Sorry, I make a mistake in the new line. (now correct in the original post)
You need to REPLACE the line "Subsystem sftp /usr/libexec/sftp-server" by the new one "Subsystem sftp internal-sftp"

Happy if I help you.
J-Luc

Re: Chrooting on SSH?

by **al562** » Thu Feb 11, 2010 7:37 am

Hi Roguelv,

Welcome to FreeNAS forum.

Please read and follow the Forum Rules & Guidelines and the FAQs (Basic).
By doing so you will:

- Understand what information you should provide when you ask a question or report a problem/bug. By providing all information upfront you will get faster and better answers; that's what you want right?
- Find the answer to your problem in FAQs (Basic), FAQs (Advanced) or use the Advanced search to search the forum.
- Help us understand your problem and allow us to provide an accurate answer/solution without asking additional

questions.
- Help the community by keeping the forum clean, focused and professional.
- Remember to use WebGUI tab> Help|Report Generator when creating new topics/threads, it is available if your FreeNAS version > 0.7

Looks like Jluc6331 is doing a good job helping you out. I will just add some links and a few odds and ends that you may find useful.

> *roguelv wrote:*where do I go to change those rights?

Usually you will resort to a CLI (Command Line Interface); via SSH session, or from shell at the console (#6), or in WebGUI Tab> **Advanced|Command**, or you can use **Advanced|File Manager** (Quixplorer), but only for simple chmod functionality.
If you really want or need to get into the details of users and groups, the following links should help. You should start by reading (and understanding) An Introduction to Unix Permissions and An Introduction to Unix Permissions -- Part Two and review Unix File Permissions, then:
HOWTO: Setup SFTP users / SAMBA users semi properly
Then read all of these, pay attention to links included in them, when you finish you should be an expert :

A. Setting-up shares and permissions
B. trouble accessing files in XP
C. Permissions problem.
D. Locking Users to their Share[Solved].
E. Using FreeBSD's ACLs
F. GETFACL
G. SETFACL

Regards,
Al

Re: Chrooting on SSH?

by **roguelv** » Thu Feb 11, 2010 7:55 am

Thanks so much for the fast responses. I actually just get done reading and comparing
HOWTO: Setup SFTP users / SAMBA users semi properly to this post, before I noticed the replies back to me.

When comparing the method that Jluc6331 uses to the one by brokentilez (in the above link), what are the differences of doing it the 2 different ways?
I noticed that Jluc6331 adds the "Extra Options" in Step 3 to the Services|SSH panel, and then the part in Step 5. May I ask the reasoning for doing that? I will try to find out what all those extra option parameters mean as well, since I have no idea. Do both guides do the same thing, but just in different styles? Or is one way more secure than the other way?

I did read the info on CHOWN, CHMOD, and will start reading the other links you posted as well.

Thanks again for your guys' time!

Re: Chrooting on SSH?

by **jluc6331** » Fri Feb 12, 2010 8:10 am

Hi roguelv,
Some explanation hereunder

> *roguelv wrote:*I noticed that Jluc6331 adds the "Extra Options" in Step 3 to the Services|SSH panel, and then the part in Step 5. May I ask the reasoning for doing that?

/etc/rc.d/sshd is in FreeNAS the script which start the ssh daemon. It generates at each FreeNAS Server start-up the /etc/ssh/sshd_config file which setup the services and these options.
To do that is use both the script it-self and the content of the "Extra options" of the SSH Service setting windows.
This is why both modification are userful to provide the required level of service.

Some explanations are in the links on top of my post. The third one is in english.
About the "Extra options" meaning, please follow the documentation link of the "Extra options" windows.

I hope these lines may help you. I will be more available this week-end if you need additional information.

Re: Chrooting on SSH?

by **al562** » Fri Feb 12, 2010 4:28 pm

> *roguelv wrote:*When comparing the method that Jluc6331 uses to the one by brokentilez (in the above link), what are the differences of doing it the 2 different ways?

The topic by Brokentilez concerns itself primarily with the configuration of the CIFS/SMB service (WIndows) for access to your files. Here Jluc6331 is primarily concerned with configuration of the SSH service (*nix) for access to your files. While either Windows or *nix can use both services, the difference is the origin of the service and extra/different features they may have.

> *roguelv wrote:*Do both guides do the same thing, but just in different styles?

At the basic level of configuring file and folder permissions, pretty much yes.

> *roguelv wrote:*Or is one way more secure than the other way?

SSH is inherently more secure than CIFS/SMB, but this is a very open ended question. The answer really depends on your intended use, network topology, and your need for security. You will have to learn the features and differences between CIFS/SMB and SSH which are beyond the scope of this topic.

Regards,
Al

Re: Chrooting on SSH?

by **roguelv** » Tue Feb 16, 2010 12:58 am

Ok, I thought I followed the guide exactly, but I have some questions/problems:

1. For step 5, I go to WebGUI Advanced > File Editor and browse to "/etc/rc.d/sshd" and load it. Then on line 40 I change subsystem to "Subsystem sftp internal-sftp"
Is that correct? Or should I be browsing to "/var/etc/ssh/sshd_config" and changing line 4?

2. When I try to login on FileZilla with user1 I get the following error in FileZilla:

> Status: Connecting to 192.168.1.250...
> Response: fzSftp started
> Command: open "user1@192.168.1.250" 22
> Command: Pass: ******
> Error: Connection closed by server with exitcode 2147483647
> Error: Could not connect to server

and in my Diagnostics > Log I get the following:

> SSH log:
> Feb 15 16:40:18 freenas sshd[7340]: SSH: Server;Ltype: Version;Remote: 192.168.1.115-59257;Protocol: 2.0;Client: PuTTY_Local:_Jan__3_2010_22:45:10
> Feb 15 16:40:19 freenas sshd[7340]: Accepted password for user1 from 192.168.1.115 port 59257 ssh2
> Feb 15 16:40:19 freenas sshd[7342]: fatal: bad ownership or modes for chroot directory component "/mnt/80Go/"

Now when I access the shell on my FreeNAS machine (by logging into the computer directly) and I "cd /mnt/" then "ls -al" it lists 80Go as:

> drwxrwxrwx 3 root wheel 512 Feb 15 16:08 80Go

I think that's correct...?
Thanks for any insights to this!

Re: Chrooting on SSH?

by **roguelv** » Wed Feb 17, 2010 5:44 am

Ok, I fixed it by switching my permissions on 80Go to:

> drwxr-xr-x 4 root wheel 512 Feb 16 19:52 80Go

My new question is, if there is a way to have each user (ie: user1, user2, etc...) login and be automatically placed into their home directory? I set the home directory in Access > Users when I created each user. But when I log in with Filezilla, I am still going into the "/mnt/FreeNAS/users" directory and then the user has to enter their personal directory manually. I would like for my users to not be able to see other users directories.

And I was still wondering if I did step 5 correctly also:

> For step 5, I go to WebGUI Advanced > File Editor and browse to "/etc/rc.d/sshd" and load it. Then on line 40 I change subsystem to "Subsystem sftp internal-sftp"
> Is that correct? Or should I be browsing to "/var/etc/ssh/sshd_config" and changing line 4?

Thank you guys so much for your time with this.

Re: Chrooting on SSH?

by **al562** » Wed Feb 17, 2010 7:56 am

> *roguelv wrote:*Ok, I fixed it by switching my permissions on 80Go

Dang it, that's the one thing I hadn't tried yet. Good job  !

> *roguelv wrote:*if there is a way to have each user (ie: user1, user2, etc...) login and be automatically placed into their home directory?

This should be possible, you have already given each user a home directory so you should be able to use the %h token in the chrootdirectory command that you put into the "auxiliary commands" box. Click the documentation link below the box to see details.

> *roguelv wrote:*I was still wondering if I did step 5 correctly

Line 40 in /etc/rc.d/sshd is the only place this needs to be done far as I can tell. I think you did it correctly.

Regards,
Al

Re: Chrooting on SSH?

by **roguelv** » Wed Feb 17, 2010 10:50 am

Thanks! I have no idea why I had to change those permissions though, I was just messing around everywhere and that happened to work.

> if there is a way to have each user (ie: user1, user2, etc...) login and be automatically placed into their home directory?
>
> > This should be possible, you have already given each user a home directory so you should be able to use the %h token in the chrootdirectory command that you put into the "auxiliary commands" box. Click the documentation link below the box to see details.

Yeah, I don't understand why it isn't automatically logging me into the home directory I set up in each user account (via WebGUI Access > Users > Home directory).

So right now I'm changing my SSH extra options "ChrootDirectory /mnt/80Go/users" to "ChrootDirectory %h"
I just tried loggin in with FileZilla and got the same errors as before. Sigh...

> Feb 17 02:35:53 freenas sshd[7603]: fatal: bad ownership or modes for chroot directory component "/mnt/80Go/users/user1/"

So I basically have to change the /user1/ directory the same way I'm guessing?
Right now it's:

> drwxr-x--- 2 user1 sshusers 512 Feb 16 23:35 user1

Which is the way I would like for the /user1 directory to be owned and have permissions... *I think?*
sigh

Thanks again!

Re: Chrooting on SSH?

by **jluc6331** » Sat Feb 20, 2010 6:23 am

Sorry roguelv for the delay, I exercise a system disk crash beginning of this week and so lose a lot of things like bookmarks, accounts and passwords.
Just a quick answer, because a lot of work to restore and a trip this week-end

The permissions are important for chroot and must be set recursively as describe in the step5

#chown -R root:wheel /mnt/80Go/users
#chmod -R 755 /mnt/80Go/users

Regarding the home directory, chroot works as follow (if I well understood):
+ It chroots the user in the ChrootDirectory defined in the "Extras command" AND
+ the home directory of this user must be inside THIS directory.
During the loging and chrooting process, it seems that a directory (using the homedirectory name) is created in "/" too. I don't know why.
So what I think is that it is important:
+ where you declare the "ChrootDirectory"in the "Extras Commands" of the SSH service (step3) AND
+ how you configure at step2 the home of the user.

See my first post, it works fine for me and my users are chrooted in "ChrootDirectory", see all the folders under this point, access in read only all these folders and are "rw" on their home.

Hoping it helps you.
J-Luc