Table of Contents

Setting Up an SSH Console	. 1
Configure SSH in FreeNAS	. 1
Specify SSH Public Key For a User	. 3
Setting up PuTTY in Windows	. 5
Public Key Authentication in PuTTY	. 5
Generating the keypair	. 6
Configuring the connection	. 9
Using SSH on a Mac	15
Using SSH on Linux	18

Setting Up an SSH Console

SSH stands for Secure SHell, and is a secure method to connect to a remote computer over a network. There are many advantages to using an SSH console rather than say the shell facility in the FreeNAS GUI.

The SSH console is a window that has a scrolling function which means you can go back and view the output in the console. You can also select large bodies of text and copy and paste them. This can be particularly useful when trying to get help from someone as they need to see what you have done. It is also useful when compiling data (i.e. SMART test data).

An SSH console is also very secure in two ways. Firstly it can be configured to require a Public/Private key and a password before you can log in to the session and the server. Secondly the connection between the server and the client is encrypted. This means any information that goes between the two cannot be read directly.

Configure SSH in FreeNAS

Open your web browser and type in the IP address of the FreeNAS web GUI that you noted down earlier (Fester used 192.168.0.58).

The web GUI will present itself and ask for the login details. Enter the username which is **root** (1) and your password (2) and click the "Log In" button (3).

Welcome to FreeNAS®
Username: root 1 Password: •••• 2 Log In 3

Now you are logged into FreeNAS.

- Now navigate to the "Services" page (1).
- Click on the tiny spanner icon next to "SSH" (2).
- If you do not want the root user to be able to log in using only a password (i.e., if you want to require a public key, or if you don't want the root user to be able to log in remotely at all), uncheck the "Login as Root with password" tick box (3).

- If you want to require public key authentication, uncheck the "Allow password authentication" tick box (4).
- Make sure the remaining tick boxes are unchecked (5).
- Now click the "OK" button (6).

Account	System	Tasks	Network	Storage	Directory	ر Sharing	6 Services	Plugins	Jails	Reporting	T Wizard
Services							1				
AFP		OFF	2								
CIFS		OFF	٩ _								
Domain	Controller	OFF	2	SSH Setting	js	_	_	_	88		
Dynami	c DNS	OFF	2	TCD Dort			22		(i)		
FTP		OFF	4	TCP POIL			22		U		
iSCSI		OFF	2	Login as I	Root with pa	assword:					
LLDP		OFF	4	Allow Pas	sword Auth	entication	• ♦				
NFS		OFF	2	Allow TCI	P Port Forwa	arding:	_				
Rsync		OFF	3	Compress	5 Connection	ns:					
S.M.A.R	.т.	ON	2	ОКС	Adva	anced Mode					
SNMP		OFF	2	$\overline{}$	_	-	_	_	_		
SSH		OFF	() 2								
TFTP		OFF	4								
UPS		OFF	2								
WebDA	v	OFF	2								

Now turn on the SSH service.

2023/06/27 20:35			3/19						Se	Setting Up an SSH Console		
Account	System	0 Tasks	Network	Storage	Directory	(Sharing	Services	Plugins	Jails	Reporting	S Wizard	
Services												
AFP		OFF	4									
CIFS		OFF	4									
Domain	Controller	OFF	4									
Dynami	ic DNS	OFF	4									
FTP		OFF	4									
iSCSI		OFF	4									
LLDP		OFF	4									
NFS		OFF	4									
Rsync		OFF	4									
S.M.A.F	.	ON	4									
SNMP		OFF	4									
SSH		ON	D-s									
TFTP		OFF	4									
UPS		OFF	4									
WebDA	v	OFF	4									

Specify SSH Public Key For a User

If you have required public key authentication in the SSH configuration, you'll need to tell FreeNAS what the public key is for each user who will be connecting via SSH. To do that, Navigate to the "Account" page by clicking on the Account icon (1). Now click on the "Users" button (2).

Account System	O Tasks	Network	Storage	L Directory	le sharing	Services	Plugins) Jails	Reporting	T Wizard	
Account											
Groups Users	2										
Add Group											
Add Group											
Add Group Group ID			Group	Name			Built	-in Group			Permit Sud
Add Group Group ID 0			Group	Name			Built	-in Group			Permit Sud false
Add Group Group ID 0 1			Group wheel daemo	Name			Built true true	-in Group			Permit Sud false false

Now select the "root" user account (1) (it will turn blue when selected) and click on the "Modify User" button (2).

danb35's Wiki - https://www.familybrown.org/dokuwiki/

Account	System 3	Tasks Network	Storage	ory Sharing	Services Plue	gins Jails	Reporting	S Wizard
Account								
Groups	Users							
Add User								
User ID	Usernam	e Primary Grou ID	Home Directory	Shell	Full Name	Built-in User	E-mail	Disable
0	root	0	/root	/bin/csh	root	true		false
1	daemon	1	/root	/usr/sbin /nologin	Owner of many system processes	true		false
2	operator	5	/	/usr/sbin /nologin	System &	true		false
3	bin	7	/	/usr/sbin /nologin	Binaries Commands and Source	true		false
4	tty	65533	1	/usr/sbin /nologin	Tty Sandbox	true		false
5	kmem	2	/	/usr/sbin /nologin	KMem Sandbox	true		false
7	games	13	1	/usr/sbin /nologin	Games pseudo-user	true		false
8	news	8	/	/usr/sbin /nologin	News Subsystem	true		false
9	man	9	/usr/share/man	/usr/sbin /nologin	Mister Man Pages	true		false
14	ftp	14	/nonexistent	/bin/csh		true		false
	achd	22	/var/empty	/usr/shin	Secure Shell	true		false

The modify user window should now pop up. Scroll down till you come across the "SSH Public Key:" entry (1).

Now right click in the blank box next to it and paste in the previously copied public key (2).

Now click the "OK" button (3).

2023/06/27 20:35

Ø	2	Z	6	ø	-			
Tasks	Permit Sudo:						^	V
	Microsoft Account:					_		
e	SSH Public Key: 1					2		
	Home Directory Mode:	Read Write Execute	er Group Ot	her				
	Auxiliary groups:	Available dhcp pflogd audit authpf avahi bin		<	1	•	Ξ	
•	OK Cancel	Diff					-	

Setting up PuTTY in Windows

Modern operating systems ship with an SSH client installed. Unfortunately, Windows is still not a modern operating system in this regard, so a third-party client will need to be used. Popular clients include Bitvise and PuTTY.

Public Key Authentication in PuTTY

Switch on and boot up a personal computer that is part of your private network (if you use it to connect to the internet then this will probably work).

Download PuTTY and PuTTYgen to your personal computer (not the server).

Install PuTTy and PuTTYgen under an administrator's account or right click on their respective installation programs and run as an administrator.

Generating the keypair

When installed run PuTTYgen under an administrator's account or right click on the program and run as an administrator.

When the PuTTYgen window appears check "SSH-2 RSA" is selected (1), if it isn't select it.

Next check the "Number of bits in a generated key:" is set to 2048 (2).

Now click the "Generate" button (3).

PuTTY Key Generator	
File Key Conversions Help	
Key	
No key.	
Actions	
Generate a public/private key pair	3 Generate
Load an existing private key file	Load
Save the generated key	Save public key Save private key
Parameters	
Type of key to generate:	SSH-2DSA
Number of bits in a generated key:	2 2048

Now move your mouse in a random way within the box labelled "Key" (1) in PuTTYgen until the green bar

fills up (2).

PuTTY Key Generator	? ×
File Key Conversions Help	
Key 1	
Please generate some randomness by moving the mou	use over the blank area.
2	
Actions	
Generate a public/private key pair	Generate
This Window Rando Load an existing private key file	Load
Save the generated key Sa	ave public key Save private key
Parameters	
Type of key to generate: SSH-1 (RSA) SSH-2 RSA	◯ SSH-2 DSA
Number of bits in a generated key:	2048

When the green bar is full the key will be generated and a new screen will appear.

In the "Key comment" text box (1) type a comment which will help you identify the key.

Now type in a password for the private key in the "Key passphrase" text box (2), remember it as this will be needed later (Fester just used **test** again).

Retype the password into the "Confirm passphrase" text box (3).

Now save the private key by clicking on the "Save private key" button (4).

An additional window will pop up, navigate to where you would like to save the key, give it a name (5) and click the "Save" button (6). Save it somewhere convenient as this will be needed soon.

Now right click in the "Public key for pasting into OpenSSH authorized_keys file:" window (7) and from

the pop up submenu chose "Select All" (8).

The text within this window should become highlighted. Now right click again in this window as you did a moment ago and from the pop up submenu this time select "Copy".

😴 PuTTY Key Generator	? ×
File Key Conversions Help	
Кеу	
Public key for pasting into OpenSSH authorized_keys file:	
Kovfingerprint	Undo
	Cut
Key comment 1 You can type in a helpful comment here.	Сору
Key passphrase: 2	Paste
Confirm passphrase3 ••••	Delete
Actions	Select All 8
Generate a public/private key pair Genera	te Right to left Reading order
Load an existing private key file	Show Unicode control characters
Save the generated key Save public key Save privat	le key
Parameters 4	
Type of key to generate: SSH-1 (RSA) SSH-2 RSA SSH-2 DSA	
Number of bits in a generated key: 2048	

2023/06/27 20:35

1	PuTTY Key Generator			
	File Key Conversions Help			
1	😴 Save private key as:			٢
			✓ 4→ Search temp	9
	Organize New folder		1	
	Name	Date modified Type	Size	
		No items match your sea	arch.	
				_
	File name: Give it a	good name 5		•
	Save as type: PuTTY Pr	ivate Key Files (*.ppk)		•
	Hide Folders		6 Save Cancel]

Configuring the connection

Now run PuTTY under an administrator's account or right click on it and run as an administrator.

In the "Host Name or (IP address)" box (1) type in the IP address of the FreeNAS web GUI (Fester's was 192.168.0.58).

Check the port number in the "Port" box (2) is set to 22.

The "Connection type:" should be set to SSH (3).

Now in the "Category" window click the small plus symbol "+" next to SSH (4). This should open up this section to reveal subcategories.

Then click on "Auth" (5), not the "+" sign but the actual text itself.

🕵 PuTTY Configuration			? X
Category:			
E Session		Basic options for your PuTTY session	n
Logging		Specify the destination you want to connect to	
Keyboard		Host Name (or IP address) Po	ort
Bell		192.168.0.58 1 22	2
- Window - Appearance		Connection type: Raw Telnet Rlogin SSH	Serial
Behaviour Translation Selection Colours	Ξ	Load, save or delete a stored session 3 Saved Sessions	
Connection Data Proxy Telnet Plogin SSH 4		Default Settings	Load Save Delete
Cipher Auth 5 	•	Close window on exit. Always Never Only on clean	exit
About	Help	Open	Cancel

This should take you to a different screen.

On this screen click the "Browse" (1) button next to the "private key file for authentication:" (2).



This will bring up a window in which you can load in the private key into PuTTY. Navigate to where you stored the private key, click on it and then click the "Open" button.

1	🕵 PuTTY Configu	uration						
ſ	🕵 Select private	e key file					X	
					▼ ⁴ 7	Search Desktop	٩	
	Organize 🔻	New folder					0	
	Name	<u>^</u>	Date modified	Туре	Size		*	
1								
							Ξ	
	SSHCons	oleTest.ppk	22/04/2016 20:35	PuTTY Private Key	2 KB		*	
٦	File name:		SSHConsoleTest.ppk		▼ PuT	✓ PuTTY Private Key Files (*.pp ▼		
						Open 🚽 Canc	el	
							th.	

With the key now loaded in, go back to the "Session" category in the "Category" window (1).

It is possible to save the settings of this session. This is a good idea because otherwise we would need to re-enter all the details each time we wanted to start a session in PuTTY.

In the "Saved Sessions" box (2) type a good name for the session (Fester called it "HDD Validation SSH").

Now click on the "Save" button (3). The saved session should now appear in the window to the left of this (4).

Now click on the "Open" button (5) to start the session (have the password you created in PuTTYgen standing by).



A PuTTY security alert window should now open. It will show the server's RSA2 key fingerprint and will ask if you trust this host before allowing the connection. Click the "Yes" button.



(There is a way to check this by using the RSA2 fingerprint but I can't remember how, if someone lets me know I will try to include it in the guide or you could replace this or any section with your own?)

You will now have access to the PuTTY session as soon as you login. Type the username next to the "Login as:" text (1). In this case it is **root**.

Next you will be asked for the password you created in PuTTYgen. Type it in next to the "Passphrase for key "Test SSH":" text (2) (Fester used **test**).

As you type the password the text will not appear on the screen, this is normal and a security feature.



To leave the SSH console just type **exit** and the session along with the window will close.

That's the SSH console configured in FreeNAS.

Using SSH on a Mac

Mac OS X includes an SSH client, but it must be used from the command line. To use it, you'll need to open a terminal window. Start by clicking the launchpad button in your dock (it looks like a rocket):



Begin typing "Terminal" into the search bar at the top, until you see the Terminal icon below:



Then click on the Terminal icon. You'll see a window like this:



To connect to a server using SSH, you can simply type

ssh user@host

Where "user" and "host" are the username and hostname, respectively, that you want to connect to. For example,

ssh root@freenas

Or you can use an IP address:

ssh root@192.168.0.5

If you have required public key authentication on your FreeNAS server, you'll need to generate a keypair. To do this, type

ssh-keygen -t rsa

...and simply accept the defaults. The result will look like this:

```
Last update: 2017/06/29 11:42
```

```
Dan-MacBook-Pro-7:~ dan$ ssh-keygen -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (/Users/dan/.ssh/id rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /Users/dan/.ssh/id_rsa.
Your public key has been saved in /Users/dan/.ssh/id_rsa.pub.
The key fingerprint is:
SHA256:ZB0ZFqEWWJuCgEWIyFd/Thk5KOuncH8LT06w0CSdRdk dan@Dan-MacBook-Pro-7.local
The key's randomart image is:
----[RSA 2048]----+
+=+ .. +*.B=
=. o o+o E+.
   . . +oB+o
    ..0=+
    ..+ .S.
    .00..0
    00+0 0
   --[SHA2561
Dan-MacBook-Pro-7:~ dan$
```

The system will prompt you for a passphrase; this is optional. If you enter a passphrase, you will need to enter it every time you use this keypair (i.e., every time you use ssh). If you leave the passphrase blank, you won't need to enter it when you connect to a remote server, but neither will a thief who manages to steal your computer. You'll now need to view your public key, to enter it in the FreeNAS configuration. To do that, type

cat .ssh/id_rsa.pub

The result will look like this:

```
ssh-rsa
```

```
AAAAB3NzaC1yc2EAAAADAQABAAABAQCxoFuJ2Px8sIA0zla1FXjnG+af2kRNhj/FcQ5nhOn6F2LepgX
f/4SQFjx5BWaD88H6/06lTaUAqprxKS4m33SKN7poH6RaeIfbJXwjJ/o0Cx0QbugGAeMKjH0Bg4fsHw
vqGLT7o0lcQ0ubmGBZlSx9R9IFNmnDLAru+Z5gjuAwKCXGw2dxVqbq2IwB3jEoA3bbo8gy6Dso5wV75
0EC+dYlB/lQrxW/uscgPjpi1XCFVuWtajyz9jujakR1uHuRRphsp56GXVTovwM3P6h52ADDhr5vkfsk
GKgmETj940x5+MFbmBvC9iIMIeRGLfWIAQY+8NjosQYfieU5U48oDmDb dan@Dan-MacBook-
Pro-7.local
```

Copy this, all on line line, and paste it into your FreeNAS configuration.

Using SSH on Linux

SSH on Linux works just like SSH on a Mac. Follow the instructions above.

From: https://www.familybrown.org/dokuwiki/ - danb35's Wiki

Permanent link: https://www.familybrown.org/dokuwiki/doku.php?id=fester:ssh_setup

Last update: 2017/06/29 11:42

