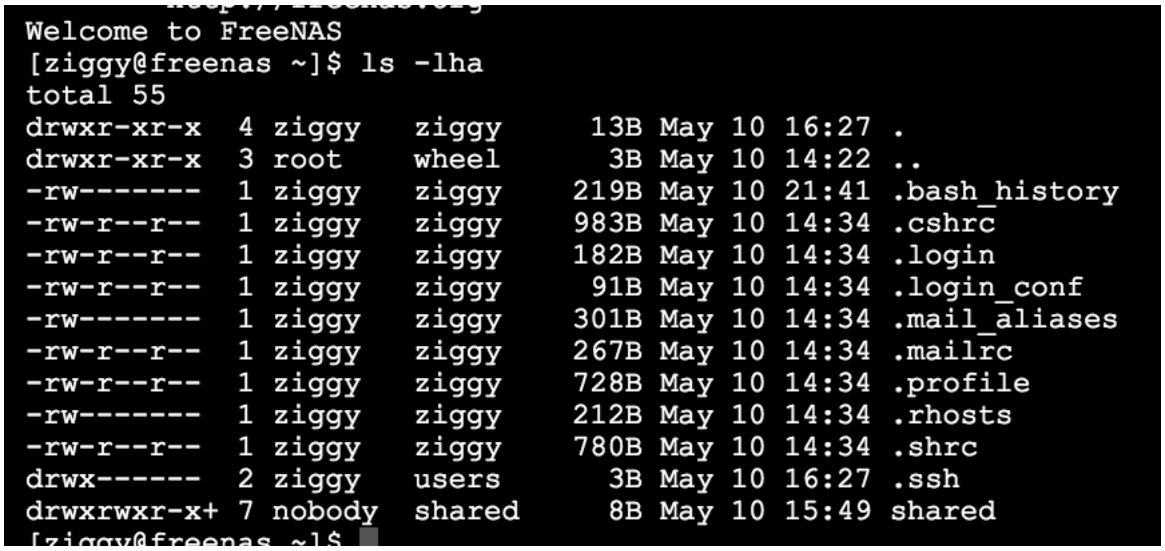
Just tried your syntax from within the LAN and I'm getting "Permission denied (publickey)" so it's still evidently a permissions issue. Hoping we can get to the bottom of this.

You should check all the permissions AFTER you set up the keys, because the key and parent folder permissions are critical.

Yes, I did. That wasn't clear in my previous post, but I checked before and after. I'm attempting to login via ssh for the user 'ziggy'. If you look at the screenshot below for the user ziggy on the Freenas server - and this is where my unix/linux experience begins to breakdown - the first line is, I think, the 'home' directory for that user. Is this correct? Your troubleshooting sections says that:

1. ".. on the server, the user's home directory should not have write permission for group or other." I believe, if this is the home directory that 'drwxr-xr-x' is correct.

SCREENSHOT 1:



2. "On both server and client, the .ssh directory and files in it must be owned by the user."

In screenshot 1 you'll see that the .ssh directory is owned by the user ziggy. It's in a 'users' group to facilitate access to an smb share, but I don't think this should make any difference? In screenshot 2 an 'ls' command shows that the files in the .ssh directory are owned by ziggy, and especially the 'authorized_keys' file:

SCREENSHOT 2:

```
[ziggy@freenas ~/.ssh]$ ls -lha
total 10
drwx------  2 ziggy  users     3B May 10 16:27 .
drwxr-xr-x  4 ziggy  ziggy    13B May 10 16:27 ..
-rw-r--r--  1 ziggy  users    84B May 10 16:27 authorized_keys
```

As regards the client (Mac) machine, the .ssh directory and files within it are owned by the user I'm logged in as on the Mac:

SCREENSHOT 3:

```
[Zigbook@Ziggys-MacBook-Pro:~/.ssh$ ls -lha
total 32
drwx------   6 Zigbook  staff   204B 10 May 16:07 ./
drwxr-xr-x@ 32 Zigbook  staff   1.1K 19 Apr 23:03 ../
-rw-------   1 Zigbook  staff   1.7K 10 May 16:07 id_rsa
-rw-r--r--   1 Zigbook  staff   414B 10 May 16:07 id_rsa.pub
-rw-r--r--   1 Zigbook  staff   365B 10 May 16:01 known_hosts
-rw-r--r--   1 Zigbook  staff   364B 10 May 15:55 known_hosts_old
```

I am assuming I don't have to create a user 'ziggy' on the Mac? The directory and files simply need to be owned by the user I'm logged in as and within which I launch the Terminal and ssh command?

3. "On both server and client, the .ssh directory should have permissions 700."
From both screenshots I believe both server and client are configured correctly for permissions.

4. "The authorized_keys file should have permissions 644."
From screenshot 2 I believe this is also right.

5. "The private key (id_rsa) should have permissions 600."
From screenshot 3 I believe this is also right.

So you generated the key - did you install the public key on the server? Had you turned off password login? What command did you try to login with?

It doesn't matter if you connect locally or remotely; the keys work both ways.

Yes, see screenshot 2 above. This is installed within the user ziggy's directories.
However, I checked your query re disabling password login and to my surprise I discovered I hadn't. Initially the box was greyed out. I eventually figured out that the 'permit sudo' and 'disable password' were mutually exclusive, so I unticked permit sudo and then I could tick disable password. However, I'm still getting "Permission denied (publickey)".

NOTE: I see from the freenas documentation that regarding disable password that “when checked, [this] disables password logins and authentication to SMB shares.” This may undo one of the functions I’m looking for in remote access - as in I want to be able to access an SMB share containing music, photos etc that I manage via a windows machine - but I’ll cross that bridge when I come to it and may have to consider other options for administering that resource.