

# Re: setting up passwordless ssh connections

**Source:** <http://linux.derkeiler.com/Mailing-Lists/Fedora/2005-08/1105.html>

---

**From:** T. Horsnell (*tsh\_at\_mrc-lmb.cam.ac.uk*)

**Date:** 08/07/05

To: For users of Fedora Core releases <fedora-list@redhat.com>

Date: Sun, 7 Aug 2005 19:32:43 +0100 (BST)

>Hi,  
>  
>I am trying to setup passwordless ssh connections  
>  
>so far i have  
>1) created rsa private/public keys  
>2) copied the public key (id\_rsa.pub) to the machine i  
>want to connect to and renamed it authorized\_keys in  
>the .ssh dir  
>  
>when i try to connect it still asks me for the  
>password  
>  
>ssh -v tells me a few things -  
>  
>Next authentication method: publickey  
> \* that's good\*  
>debug1: Trying private key:  
>/home/username/.ssh/identity  
>debug1: read PEM private key done: type RSA  
>  
>\*wonderfull! it is reading the client side private  
>key\*  
>  
>then.....  
>debug1: Authentications that can continue:  
>publickey,gssapi-with-mic,password  
>debug1: Offering public key:  
>/home/username/.ssh/id\_rsa  
>debug1: Authentications that can continue:  
>publickey,gssapi-with-mic,password  
>debug1: Offering public key:  
>/home/username/.ssh/id\_dsa  
>  
>then it goes to password :(  
>

## Fedora: Re: setting up passwordless ssh connections

>it never looks for the authorized\_key file. i have  
>even place id\_rsa in my .ssh dir on the server and  
>even renamed id\_rsa.pub to id\_rsa on the server but  
>nothing helps.  
>  
>so I looked at the server config and changed from the  
>FC defaults to  
>  
>PubkeyAuthentication yes  
>AuthorizedKeysFile .ssh/authorized\_keys  
>  
>interesting enough when sshd was restarted from the  
>init.d script it did not kick any existing users off  
>the server. shouldn't it have broken the connection  
>maybe a need to do a full stop and start for  
>sshd\_config to be re-loaded ?  
>  
>permissions are 0600 on authorized\_keys  
>  
>what am i doing wrong ?

I think the permission 0600 on authorized\_keys is correct.  
Try setting the permissions on \$HOME/.ssh to 700 as well.

To see more what's going on, if you have control of the machine you are trying to log in to, stop sshd and start it manually with `-dd -e` options set: `/usr/sbin/sshd -dd -e` (see man sshd). You should then get a bunch of diagnostics sent to the server terminal when you try to ssh from your client.

Cheers,  
Terry.

>  
>btw what does the `-1` mean in the debug message  
>  
>debug1: identity file /home/username/.ssh/identity  
>type `-1`  
>debug1: identity file /home/username/.ssh/id\_rsa type  
>1  
>debug1: identity file /home/username/.ssh/id\_dsa type  
>2  
>  
>thanx for your help.  
>  
>lazer  
>ssh -v 10.10.10.10  
>OpenSSH\_3.9p1, OpenSSL 0.9.7a Feb 19 2003  
>debug1: Reading configuration data /etc/ssh/ssh\_config  
>debug1: Applying options for \*  
>debug1: Connecting to 10.10.10.10 port 22.

Re: setting up passwordless ssh connections

## Fedora: Re: setting up passwordless ssh connections

```
>debug1: Connection established.
>debug1: identity file /home/username/.ssh/identity
>type -1
>debug1: identity file /home/username/.ssh/id_rsa type
>1
>debug1: identity file /home/username/.ssh/id_dsa type
>2
>debug1: Remote protocol version 2.0, remote software
>version OpenSSH_4.0
>debug1: match: OpenSSH_4.0 pat OpenSSH*
>debug1: Enabling compatibility mode for protocol 2.0
>debug1: Local version string SSH-2.0-OpenSSH_3.9p1
>debug1: SSH2_MSG_KEXINIT sent
>debug1: SSH2_MSG_KEXINIT received
>debug1: kex: server->client aes128-cbc hmac-md5 none
>debug1: kex: client->server aes128-cbc hmac-md5 none
>debug1: SSH2_MSG_KEX_DH_GEX_REQUEST(1024<1024<8192)
>sent
>debug1: expecting SSH2_MSG_KEX_DH_GEX_GROUP
>debug1: SSH2_MSG_KEX_DH_GEX_INIT sent
>debug1: expecting SSH2_MSG_KEX_DH_GEX_REPLY
>debug1: Host '212.25.92.186' is known and matches the
>RSA host key.
>debug1: Found key in /home/username/.ssh/known_hosts:1
>debug1: ssh_rsa_verify: signature correct
>debug1: SSH2_MSG_NEWKEYS sent
>debug1: expecting SSH2_MSG_NEWKEYS
>debug1: SSH2_MSG_NEWKEYS received
>debug1: SSH2_MSG_SERVICE_REQUEST sent
>debug1: SSH2_MSG_SERVICE_ACCEPT received
>debug1: Authentications that can continue:
>publickey,gssapi-with-mic,password
>debug1: Next authentication method: gssapi-with-mic
>debug1: Authentications that can continue:
>publickey,gssapi-with-mic,password
>debug1: Authentications that can continue:
>publickey,gssapi-with-mic,password
>debug1: Next authentication method: publickey
>debug1: Offering public key:
>/home/username/.ssh/id_rsa
>debug1: Authentications that can continue:
>publickey,gssapi-with-mic,password
>debug1: Trying private key:
>/home/username/.ssh/identity
>debug1: read PEM private key done: type RSA
>debug1: Authentications that can continue:
>publickey,gssapi-with-mic,password
>debug1: Offering public key:
>/home/username/.ssh/id_rsa
>debug1: Authentications that can continue:
>publickey,gssapi-with-mic,password
```

