

## SSH PASSWORDLESS AUTHENTICATION

System1-cserver – 192.168.198.128

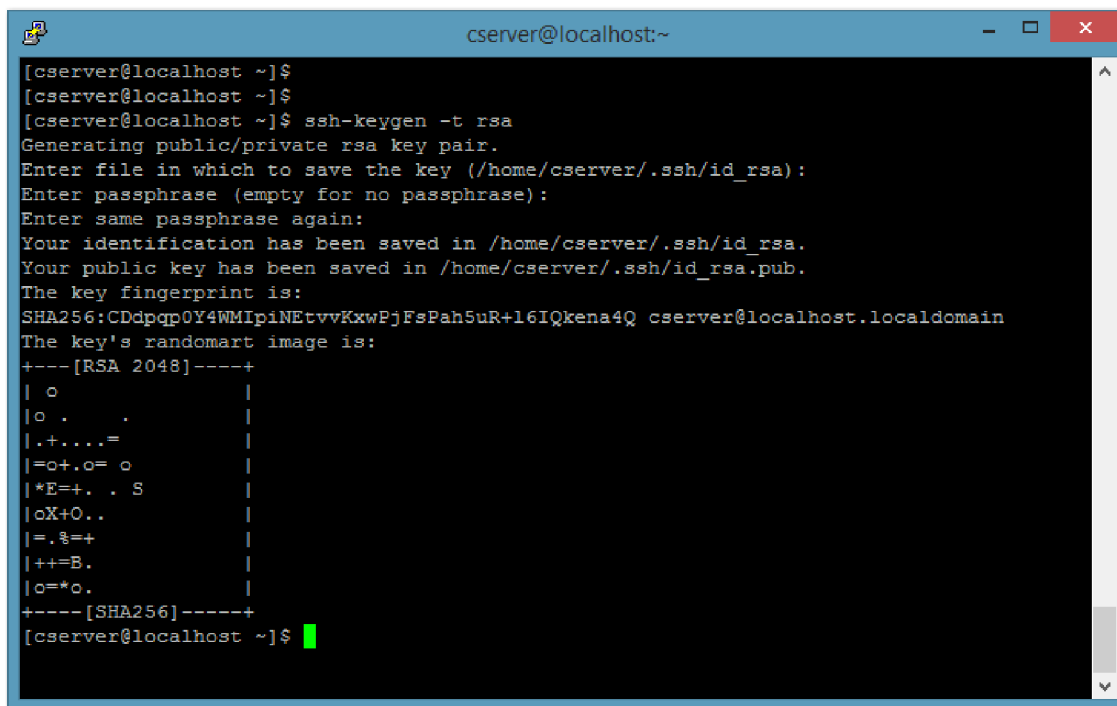
System2-cclient– 192.168.198.130

Trying to establish ssh passwordless authentication between server & client

### On server system

Step1: open terminal and enter

ssh-keygen -t rsa



```
cserver@localhost:~  
[cserver@localhost ~]$  
[cserver@localhost ~]$ ssh-keygen -t rsa  
Generating public/private rsa key pair.  
Enter file in which to save the key (/home/cserver/.ssh/id_rsa):  
Enter passphrase (empty for no passphrase):  
Enter same passphrase again:  
Your identification has been saved in /home/cserver/.ssh/id_rsa.  
Your public key has been saved in /home/cserver/.ssh/id_rsa.pub.  
The key fingerprint is:  
SHA256:CDdpgp0Y4WMIpiNetvvKxwFjFsPah5uR+l6IQkena4Q cserver@localhost.localdomain  
The key's randomart image is:  
+---[RSA 2048]-----+  
| o |  
|o . . |  
|.+.+.+. |  
|=o+.o= o |  
|*E=+. . S |  
|oX+O.. |  
|= .&=+ |  
|++=B. |  
|o=*o. |  
+---[SHA256]-----+  
[cserver@localhost ~]$
```

Note down this command will save id\_rsa file and id\_rsa.pub (public key) file will save in **/home/\$USER/.ssh** path, if we want to change we can change this path.

And we didn't given any passphrase (password)

Step2:

Copy the file with name authorized\_keys and set authorized\_keys file permission 600

```
cserver@localhost:~/ssh
[cserver@localhost .ssh]$ cp id_rsa.pub authorized_keys
[cserver@localhost .ssh]$
[cserver@localhost .ssh]$ ll authorized_keys
-rw-r--r-- 1 cserver cserver 411 Oct 14 12:08 authorized_keys
[cserver@localhost .ssh]$ chmod 600 authorized_keys
[cserver@localhost .ssh]$
[cserver@localhost .ssh]$ ll authorized_keys
-rw----- 1 cserver cserver 411 Oct 14 12:08 authorized_keys
[cserver@localhost .ssh]$
[cserver@localhost .ssh]$
```

Share file with the remote system using any secure connection like scp, ftp...

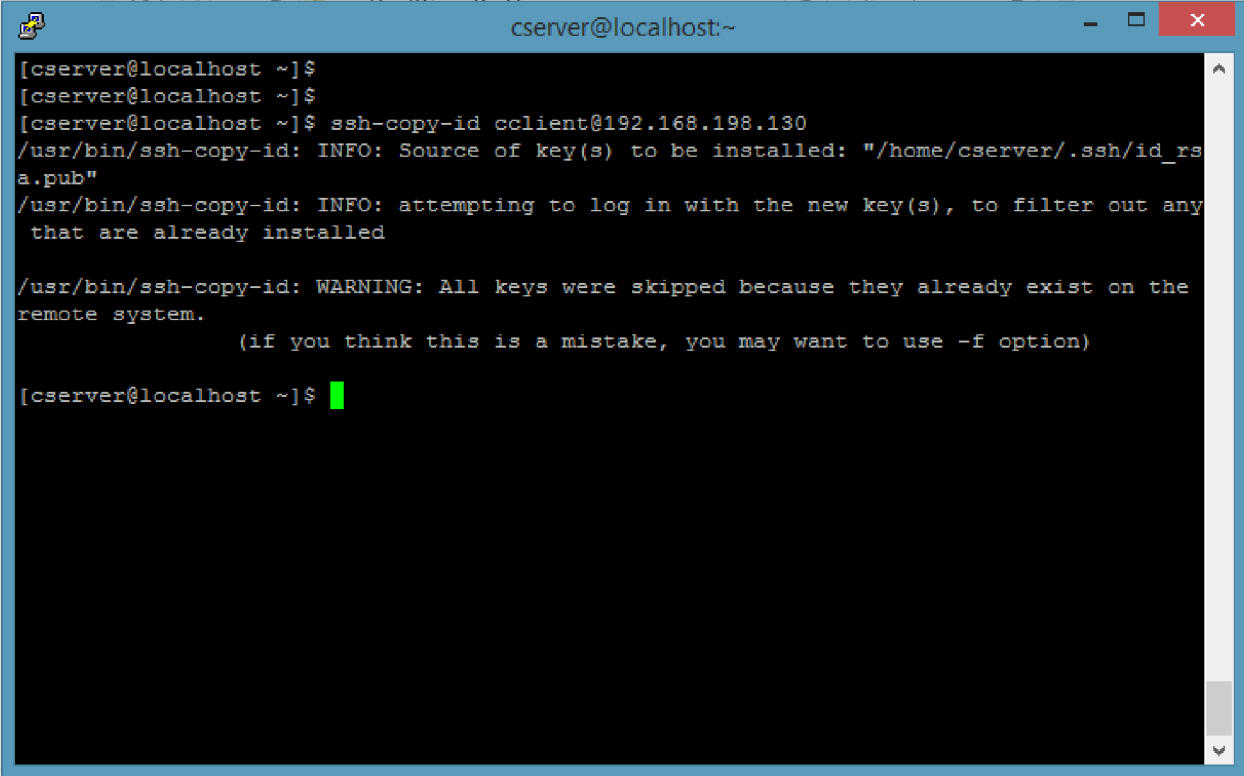
```
scp .ssh/authorized_keys cclient@192.168.198.130:/home/cclient/.ssh
```

```
cserver@localhost:~
[cserver@localhost ~]$ scp .ssh/authorized_keys cclient@192.168.198.130:/home/cclient/.ssh
The authenticity of host '192.168.198.130 (192.168.198.130)' can't be established.
ECDSA key fingerprint is SHA256:T/F4AfUOZ+p5dFgqAXvUfMXXnGVAftwA7iw+mCyHfxI.
ECDSA key fingerprint is MD5:bb:2e:70:21:a6:9b:be:eb:14:17:ae:6b:da:e4:8c:a8.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.198.130' (ECDSA) to the list of known hosts.
cclient@192.168.198.130's password:
authorized_keys                                100% 411 172.1KB/s 00:00
[cserver@localhost ~]$
```

or

use below command

ssh-copy-id [cclient@192.168.198.130](mailto:cclient@192.168.198.130)

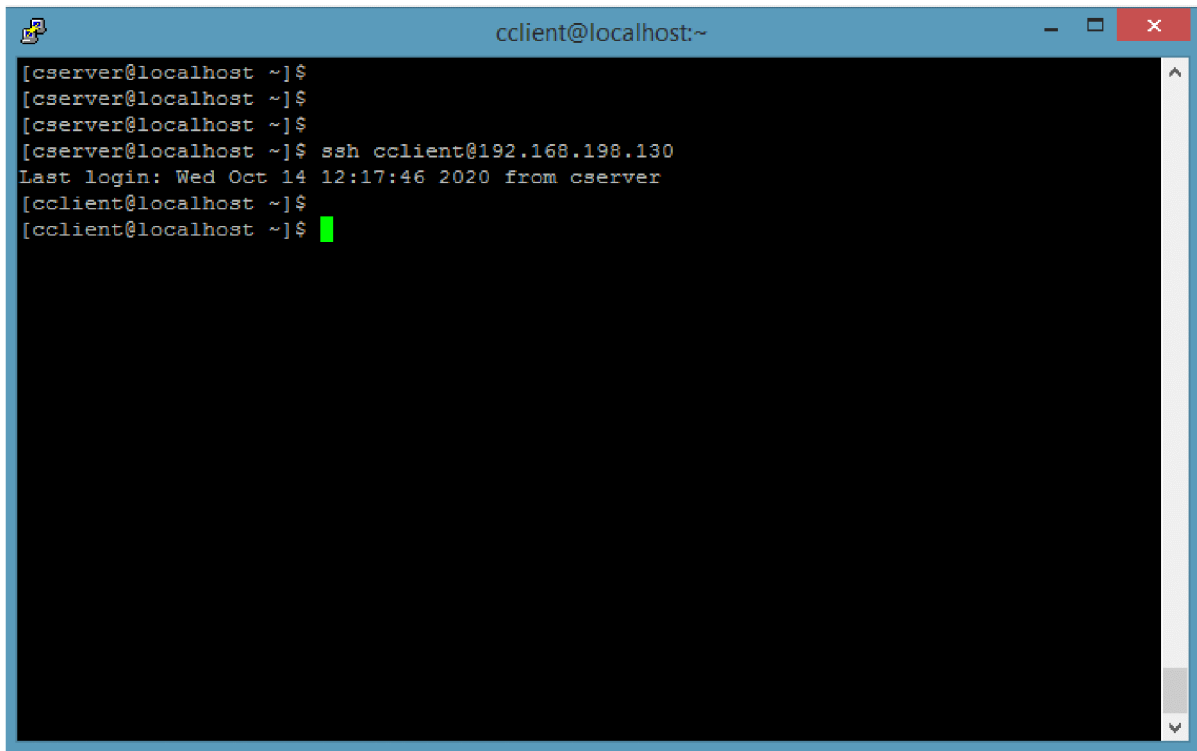
A terminal window titled 'cserver@localhost:~' with standard window controls. The terminal shows the following text:

```
[cserver@localhost ~]$  
[cserver@localhost ~]$  
[cserver@localhost ~]$ ssh-copy-id cclient@192.168.198.130  
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/home/cserver/.ssh/id_rsa.pub"  
/usr/bin/ssh-copy-id: INFO: attempting to log in with the new key(s), to filter out any  
that are already installed  
  
/usr/bin/ssh-copy-id: WARNING: All keys were skipped because they already exist on the  
remote system.  
                (if you think this is a mistake, you may want to use -f option)  
  
[cserver@localhost ~]$
```

Step3:

Now you can connect remote system without using password.

See below figure before connection the host name is **cserver@localhost** and after connection the host name is **cclient@localhost**



A terminal window titled 'cclient@localhost:~' with standard window controls. The terminal shows a sequence of commands and output from a user on 'cserver' connecting to 'ccient' on 'localhost' via SSH. The output includes the last login time and the user's prompt on the client machine.

```
[cserver@localhost ~]$  
[cserver@localhost ~]$  
[cserver@localhost ~]$  
[cserver@localhost ~]$ ssh ccient@192.168.198.130  
Last login: Wed Oct 14 12:17:46 2020 from cserver  
[ccient@localhost ~]$  
[ccient@localhost ~]$
```

Reference:

<https://www.youtube.com/watch?v=NWuDfRDqjRs>