**[Interview Questions on Linux Servers with Answers](http://www.golinuxhub.com/2014/01/interview-questions-on-linux-servers.html)**

POSTED BY DEEPAK PRASAD TUESDAY, JANUARY 28, 2014 [NO COMMENTS](http://www.golinuxhub.com/2014/01/interview-questions-on-linux-servers.html#comment-form)

**How can you create a password less connection between multiple Linux machine?**

* To create a password less authentication we need to use [RSA](javascript:void(0);) or DSA key authentication.
* RSA and DSA are used as an algorithm for public-key encryption
* RSA [keys](javascript:void(0);) have minimum key length of 768 bits and the default length is 2048 bit.The key length of DSA is limited to 1024 bit so one can generate stronger RSA keys than DSA keys.
* Create a pair of public and private key with a blank password when prompted.
* Copy the public key to the remote client to which you want to login without password
* Save the public key inside ~/.[ssh](javascript:void(0);)/authorized\_keys file
* Everytime you copy the key to this file, the key is appended in the file.
* Now try to login

**For more details on the commands used and description follow the below link**

[How to create a password less authentication for ssh in Linux?](http://www.golinuxhub.com/2014/01/how-to-create-password-less-ssh.html)

### [How to create password less ssh connection for multiple non-root users](http://www.golinuxhub.com/2014/01/how-to-create-password-less-ssh.html)

POSTED BY DEEPAK PRASAD SUNDAY, JANUARY 12, 2014 [9 COMMENTS](http://www.golinuxhub.com/2014/01/how-to-create-password-less-ssh.html#comment-form)

I had done [password](javascript:void(0);) less shh authentication between multiple Linux box a couple of time but this time I had to do the same for normal [user](javascript:void(0);). I thought it would be same and actually it is the same but still there are few things which we might miss out and also it becomes a bit complicated and confusing as I did so for them I thought I should give some tips.  
  
**Question**  
You have to create a password less [ssh](javascript:void(0);) connection between 3 Linux box for non root user i.e a normal user user1.  
  
**Pre-requisites**  
User user1 should exist on all the 3 Linux box  
  
**Server details**  
server1.example  
IP 192.168.1.6  
  
server2.example  
IP 192.168.1.11  
  
server3.example  
IP 192.168.1.12

### Making password less connection from server1

**On server 1**  
Login as user1[**user1**@**server1** ~]$ ssh-keygen -t rsa  
Generating public/private rsa key pair.  
Enter file in which to save the key (/home/user1/.ssh/id\_rsa):  
Created directory '/home/user1/.ssh'.  
Enter passphrase (empty for no passphrase): [Press ENTER for EMPTY password]  
Enter same passphrase again: [Press ENTER for EMPTY password]  
Your identification has been saved in /home/user1/.ssh/id\_rsa.  
Your public key has been saved in /home/user1/.ssh/id\_rsa.pub.  
The key fingerprint is:  
81:bf:d5:03:3f:a1:a4:81:27:b5:61:e4:e6:17:b9:a0 user1@server1.example  
The key's randomart image is:  
+--[ RSA 2048]----+  
|       .=        |  
|       \* o .     |  
|      + O = .    |  
|       B \* B .   |  
|      E S = =    |  
|         +   o   |  
|        .        |  
|                 |  
|                 |  
+-----------------+  
With the above command we have created a pair of public and private key using RSA type authentication.  
  
Click the link to know more about [RSA and DSA type of authentication](http://www.golinuxhub.com/2012/08/rsa-and-dsa-authentication.html)  
  
Now to create a password less ssh connection we need to copy id\_rsa.pub to the [remote server](javascript:void(0);) i.e **server2** and **server3**  
[**user1@server1** ~]$ ssh-copy-id user1@server2  
The authenticity of host 'server2 (192.168.1.11)' can't be established.  
RSA key fingerprint is de:75:8a:ff:26:1b:b5:82:61:36:9c:44:d2:57:3c:9e.  
Are you sure you want to continue connecting (yes/no)? yes  
Warning: Permanently added 'server2,192.168.1.11' (RSA) to the list of known hosts.  
user1@server2's password: [Give password for user1]  
Now try logging into the machine, with "ssh 'user1@server2'", and check in:  
  
  .ssh/authorized\_keys  
  
to make sure we haven't added extra keys that you weren't expecting.  
[**user1@server1** ~]$ ssh-copy-id user1@server3  
The authenticity of host 'server3 (192.168.1.12)' can't be established.  
RSA key fingerprint is 98:61:fb:91:8b:10:29:e1:b2:db:fd:52:6d:79:d7:1a.  
Are you sure you want to continue connecting (yes/no)? yes  
Warning: Permanently added 'server3,192.168.1.12' (RSA) to the list of known hosts.  
user1@server3's password: [Give password for user1]  
Now try logging into the machine, with "ssh 'user1@server3'", and check in:  
  
  .ssh/authorized\_keys  
  
to make sure we haven't added extra keys that you weren't expecting.**NOTE**: Make sure the permission on authorized\_keys is **600**  
Using the above steps we have successfully created a password less authentication from

server 1 ------> server 2  
server 1 ------> server 3

### Making password less connection from Server 2

**On server 2**  
Login as user1[**user1@server2**~]$ ssh-keygen -t rsa  
Generating public/private rsa key pair.  
Enter file in which to save the key (/home/user1/.ssh/id\_rsa):  
Enter passphrase (empty for no passphrase): [Press ENTER for EMPTY password]  
Enter same passphrase again: [Press ENTER for EMPTY password]  
Your identification has been saved in /home/user1/.ssh/id\_rsa.  
Your public key has been saved in /home/user1/.ssh/id\_rsa.pub.  
The key fingerprint is:  
8f:0d:bc:8c:fc:d1:38:1a:b3:be:7a:8d:fc:8d:0d:1e user1@server2.example  
The key's randomart image is:  
+--[ RSA 2048]----+  
|                 |  
|                 |  
|                 |  
|       .         |  
|        S        |  
|     . o O       |  
|     .=oE +      |  
|      +B.O       |  
|    .+=o= o      |  
+-----------------+

Now to create a password less ssh connection we need to copy id\_rsa.pub to the remote server i.e **server 1** and **server 3**  
[**user1@server2**~]$ ssh-copy-id user1@server1  
The authenticity of host 'server1 (192.168.1.6)' can't be established.  
RSA key fingerprint is b8:36:c1:38:01:db:cc:89:b1:a9:b8:f7:f7:a8:17:ef.  
Are you sure you want to continue connecting (yes/no)? yes  
Warning: Permanently added 'server1,192.168.1.6' (RSA) to the list of known hosts.  
user1@server1's password: [Give password for user1]  
Now try logging into the machine, with "ssh 'user1@server1'", and check in:  
  
  .ssh/authorized\_keys  
  
to make sure we haven't added extra keys that you weren't expecting.  
[**user1@server2**~]$ ssh-copy-id user1@server3  
The authenticity of host 'server3 (192.168.1.12)' can't be established.  
RSA key fingerprint is 98:61:fb:91:8b:10:29:e1:b2:db:fd:52:6d:79:d7:1a.  
Are you sure you want to continue connecting (yes/no)? yes  
Warning: Permanently added 'server3,192.168.1.12' (RSA) to the list of known hosts.  
user1@server3's password: [Give password for user1]  
Now try logging into the machine, with "ssh 'user1@server3'", and check in:  
  
  .ssh/authorized\_keys  
  
to make sure we haven't added extra keys that you weren't expecting.  
Using the above steps we have successfully created a password less authentication from

server 2 ------> server 1  
server 2 ------> server 3

**Making password less connection from Server 3**

**On server 3**

Login as user1

[**user1@server3** ~]$ ssh-keygen -t rsa  
Generating public/private rsa key pair.  
Enter file in which to save the key (/home/user1/.ssh/id\_rsa):  
Enter passphrase (empty for no passphrase): [Press ENTER for EMPTY password]  
Enter same passphrase again: [Press ENTER for EMPTY password]  
Your identification has been saved in /home/user1/.ssh/id\_rsa.  
Your public key has been saved in /home/user1/.ssh/id\_rsa.pub.  
The key fingerprint is:  
5b:99:c5:84:02:fd:ea:95:b7:51:2e:e3:28:f3:9d:9d user1@server3.example  
Now to create a password less ssh connection we need to copy id\_rsa.pub to the remote server i.e **server 1** and **server 2**  
[**user1@server3** ~]$ ssh-copy-id user1@server1  
The authenticity of host 'server1 (192.168.1.6)' can't be established.  
RSA key fingerprint is b8:36:c1:38:01:db:cc:89:b1:a9:b8:f7:f7:a8:17:ef.  
Are you sure you want to continue connecting (yes/no)? yes  
Warning: Permanently added 'server1,192.168.1.6' (RSA) to the list of known hosts.  
user1@server1's password: [Give password for user1]  
Now try logging into the machine, with "ssh 'user1@server1'", and check in:  
  
  .ssh/authorized\_keys  
  
to make sure we haven't added extra keys that you weren't expecting.  
[**user1@server3**~]$ ssh-copy-id user1@server2  
The authenticity of host 'server2 (192.168.1.11)' can't be established.  
RSA key fingerprint is de:75:8a:ff:26:1b:b5:82:61:36:9c:44:d2:57:3c:9e.  
Are you sure you want to continue connecting (yes/no)? yes  
Warning: Permanently added 'server2,192.168.1.11' (RSA) to the list of known hosts.  
user1@server2's password: [Give password for user1]  
Now try logging into the machine, with "ssh 'user1@server2'", and check in:  
  
  .ssh/authorized\_keys  
  
to make sure we haven't added extra keys that you weren't expecting.Using the above steps we have successfully created a password less authentication from  
server 3 ------> server 1  
server 3 ------> server 2

|  |
| --- |
| **IMPORTANT NOTE:** |
| For creating password less ssh authentication between multiple Linux machine using normal users make sure the two permissions are implemented or else the password less ssh authentication won't work  Permission 600 on **authorized\_keys**file and  Permission 700 on **.ssh** directory |

**What are the types of authentication which can be used for ssh connection to any host?**

You can create a password less connection between two Linux box using RSA authentication.  **RSA** and **DSA** are used as an algorithm for public-key encryption

RSA and DSA keys are used for password authentication and providing much higher security for data transfer or connectivity between two remote machines.

* RSA keys have minimum key length of 768 bits and the default length is 2048 bit.The key length of DSA is limited to 1024 bit so one can generate stronger RSA keys than DSA keys.
* DSA encryption is faster as compared to RSA.
* RSA can be used for both encryption and signing whereas DSA can only be used for signing.
* RSA can be used with ssh v1 and v2 whereas DSA can only be used with v2

**What is the difference between A record and CNAME record in DNS?**  
**A record**

* It is the Address records also known as host records
* Points to the IP address reflecting the domain
* Used for forward lookup of any [domain name](javascript:void(0);)

**For example:**  
Our website is configured on 50.63.202.15 IP so the A record of my domain name will point towards that IP.  
  
Every time a query for golinuxhub.com is made the internet will lookup for contents stored on the machine with 50.63.202.15 this IP.

**CNAME Record**

* It is short abbreviation for Canonical Name
* Provides an alias name for same hostname
* Helps create subdomains

**NOTE:** You can not create a CNAME record for the domain name itself (it should be done with A record)  
  
**For example:**  
*golinuxhub.com* is a domain name whereas *www.golinuxhub.com* is a sub domain name

**How will you restrict anonymous users from accessing your ftp server?**  
Change this value inside vsftpd.conf  
anonymous\_enable=NO  
**How does a dns lookup query works when you type a url on browser?**

* When you type a URL on the browser below are the course of actions performed
* [Browser cache](javascript:void(0);) is checked
* Local hosts file is looked up for any records placed inside etc folder
* URL query works right to left i.e for www.golinuxhub.com, .com is queried first and then the query moves from right to left.
* The request then goes to ISP, if any earlier request for the same website was made then they will bring up the page from the stored cache
* Next the query goes to root servers which will provide you the address of the [Top Level Domain](javascript:void(0);)
* The TLD will provide the location of nameserver, so next the ISP contacts nameserver for proper record
* Once the ISP gets the record information it locally stores the information for further queries and throws the output on your browser.
* Next time the query is made for the same page the ISP won't go through all these steps and bring out the page as per the cache stored from last query till the TTL value for that record is expired.

**For more detailed information follow the below link**  
[What happens in the backend when you type a url on the browser?](http://www.golinuxhub.com/2014/01/how-does-dns-query-works-when-you-type.html)  
  
**What is the command to check quota values for any user?**  
# repquota /partion/path | grep username  
**How many types of virtual hosting are their in apache?**  
There are 3 types of virtual hosting in Apache

* Port based
* Hostname based
* IP based

**What are the port nos for DNS, DHCP, SMTP, POP3 and**[**IMAP**](javascript:void(0);)**(with and without**[**SSL**](javascript:void(0);)**)**  
DNS 53  
DHCP 67  
SMTP with ssl 465, 567  
SMTP without SSL 25  
POP3 with SSL 995  
POP3 without ssl 110  
IMAP with SSL 943  
IMAP without SSL 143  
  
**What is the default port for ssh? How will you change it to some other random port no.?**  
SSH port no. by default is 22  
  
To change the default port no. we need make required changes inside sshd\_conf file in the below mentioned line  
#Port 22(Uncomment the above line and define the new port no.)  
  
Restart the services for changes to take affect  
  
**Which command do you use to download a file from ftp or http website using CLI?**  
# wget path\_to\_the\_file  
**How to disable root login via ssh?**  
Uncomment the below line inside sshd\_config to "**NO**"  
#PermitRootLogin yes  
**What if I have made a host entry in hosts.allow as well as hosts.deny file of my localhost. So will that remote host will be allowed to connect with my localhost machine? Explain**

* Yes, The host will be allowed to connect because their is a specific order which is followed before allowing or blocking any host/service.
* Access will be granted when a (daemon,client) pair matches an entry in the /etc/hosts.allow file.
* Otherwise, access will be denied when a (daemon,client) pair matches an entry in the /etc/hosts.deny file. Otherwise, access will be granted.

**How do you limit maximum connections in your apache server?**  
Change the below parameter value inside httpd.conf  
MaxClients 256