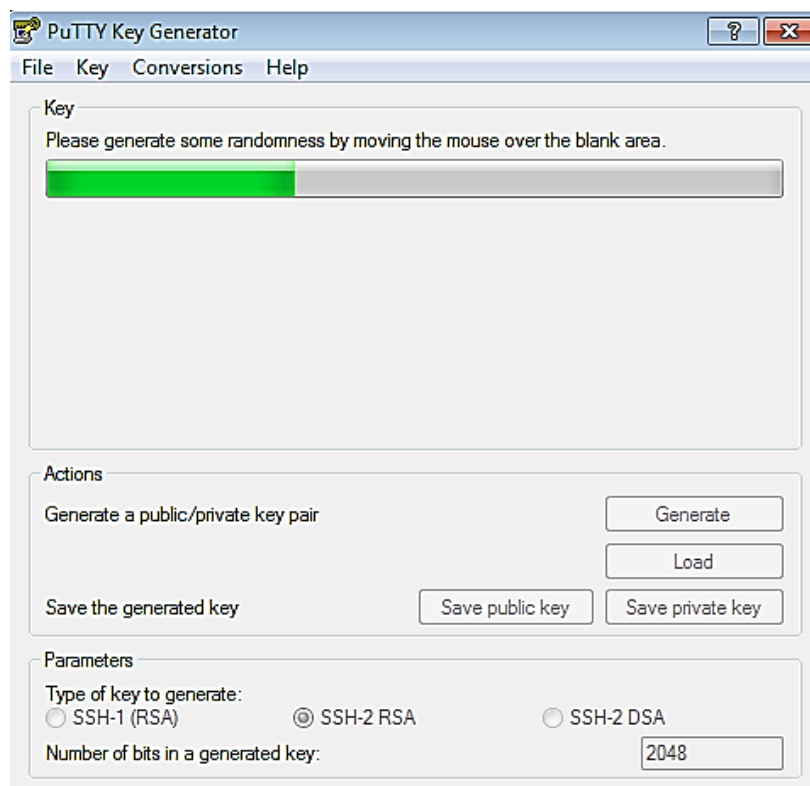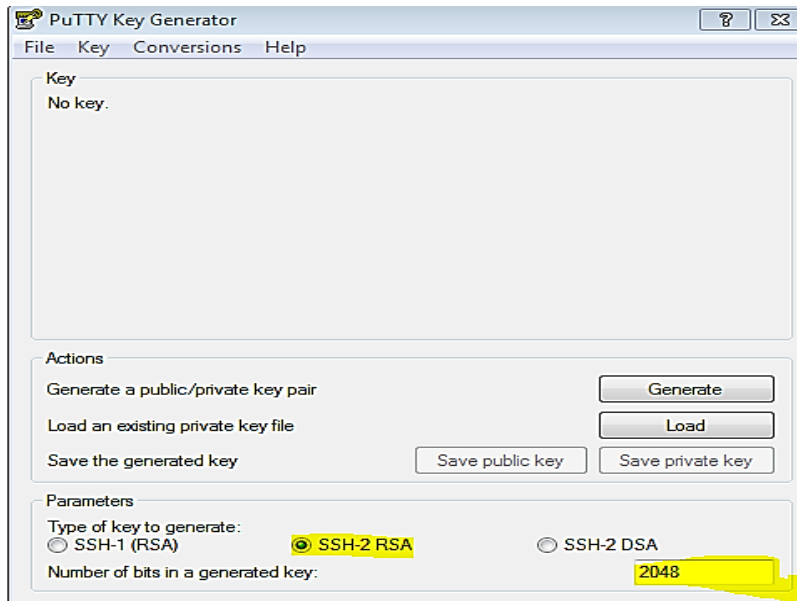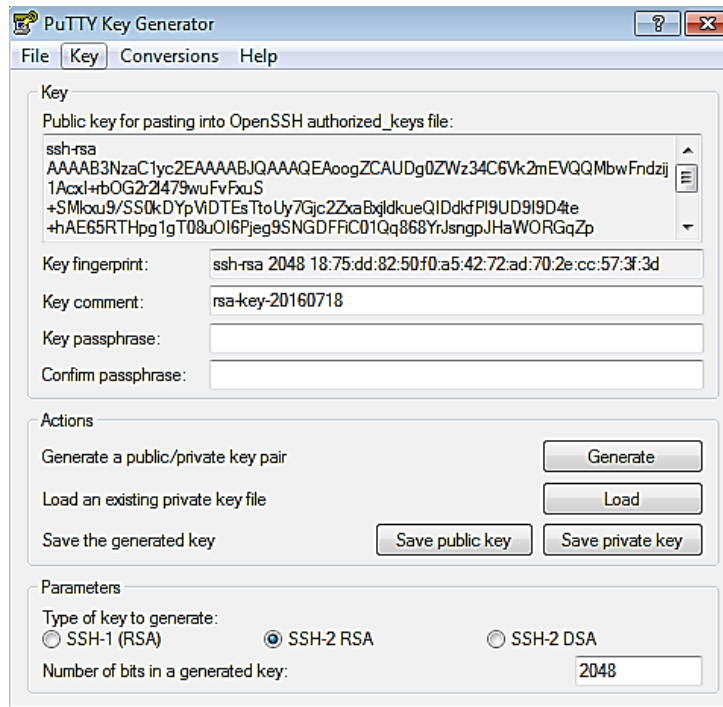Author: Sampath Kunapareddy
          sampath.a926@gmail.com

SSH keys setup for password less login to Linux servers and ability to SSH from JUMP

1. **Generate SSH key pair:**
   - Select SSH2-RSA and a minimum 2048 or 4096 bit key and click **Generate**

- Copy private key to a secure location on your local machine. **DO NOT share private key with any person or application.** If private key is shared by mistake, please generate a new key pair and delete old key pair.
- Click on "**Save private key**" without passphrase. If saved with a passphrase for more security, you will need to use this passphrase whenever key is used.
- **Save to your local laptop location. For example as below:**
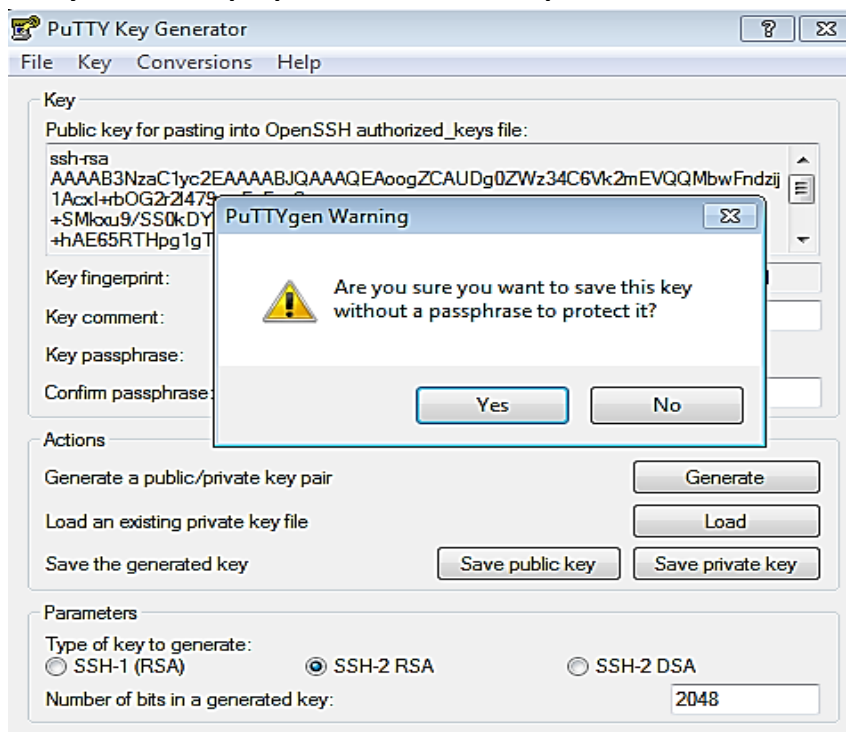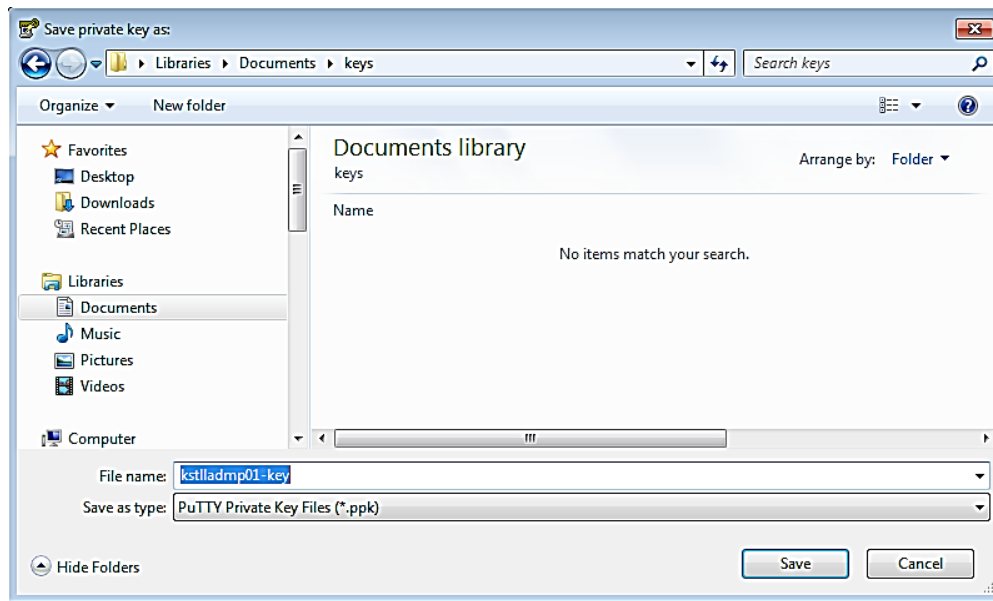
- **Copy public key and paste into your home: ~/.ssh/authorized_keys as below**

For example, copy public key:
ssh-rsa AAAAB3NzaC1yc2EAAAABJQAAAQEAoogZCAUDg0ZWz34C6Vk2mEuS+*******something will be here************ZA 8jbL0T9Ax0aokXf6HnYFWytPs0L3KzLnXQ+zm7M9QvYa+wHiF3ae9q62JYw== **rsa-key**-20160718
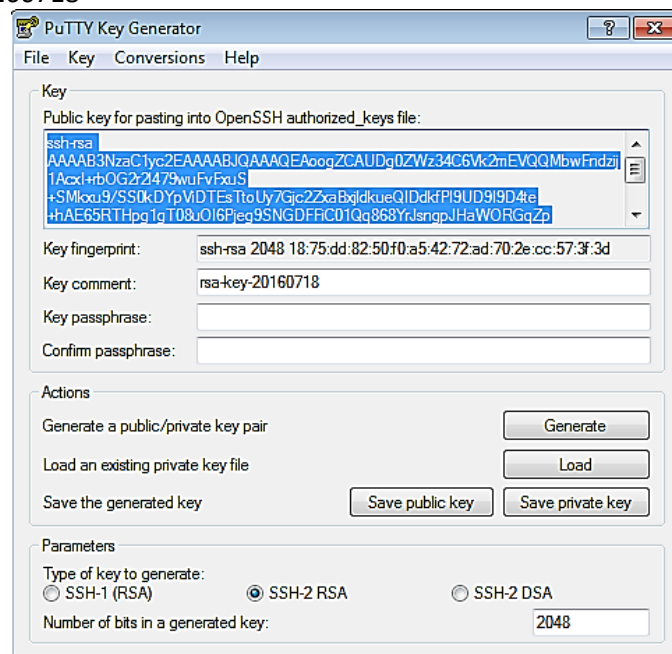
Login into host **(JUMP HOST** - where you want the password less login and password less SSH**)** to be setup and paste public key to below file:

➔ **vi ~/.ssh/authorized_keys:**

2. **Login using ssh keys from PUTTY:**
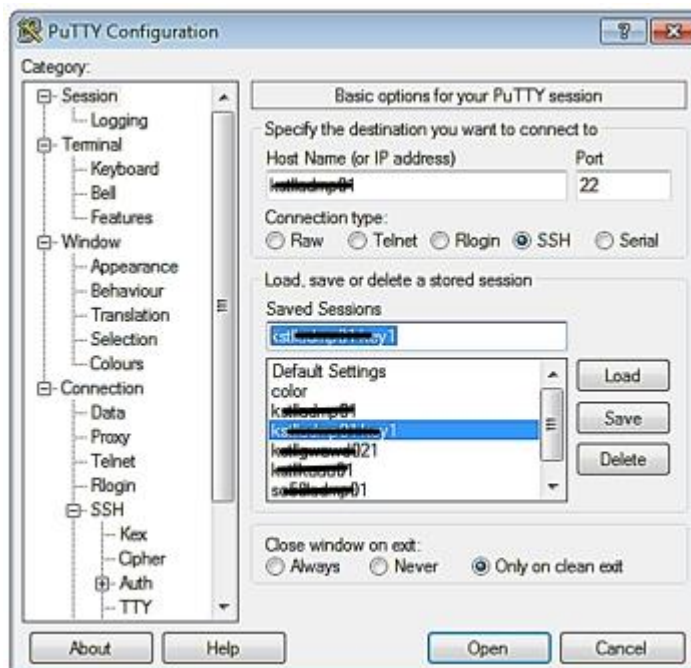   Open putty session. Expand -> **SSH** -> **Auth** -> click Browse and provide private key location
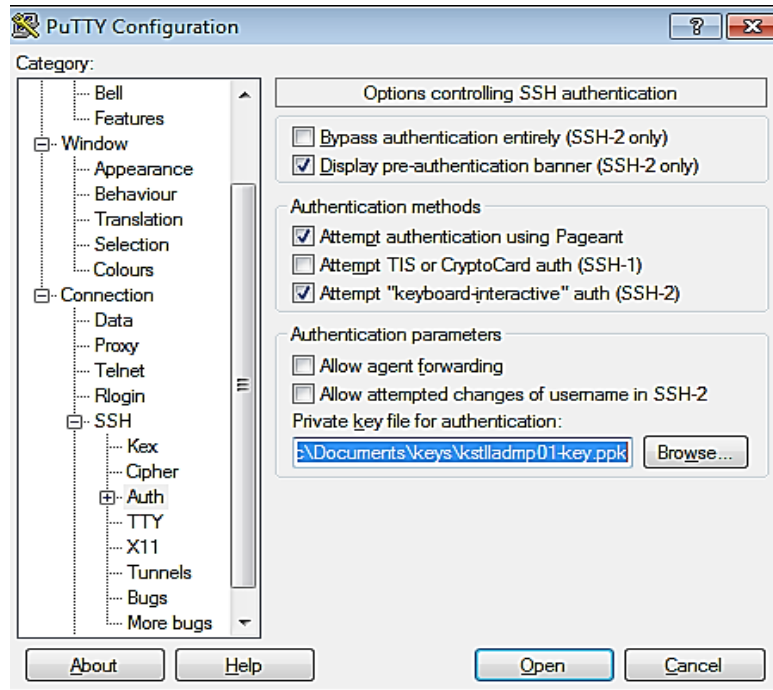
Enter host details ((JUMP HOST - where you want the password less login and password less SSH) - (also select Default Settings and save for better results)

Successful login without password will be successful now for that particular host where you did

vi ~/.ssh/authorized_keys and copied the keys..

For ALL/set of hosts this can be done by using below script...

Keys setup for password-less login for servers in DMZ – password-less login from jump/bastion servers to app servers:

Generate ssh key pair on jump server/bastion host, example below:

```
[usernameadm@JUMPHOST ~]$ ssh-keygen -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (/home/usernameADM/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):                 - PRESS ENTER
Enter same passphrase again:                 - PRESS ENTER
Your identification has been saved in /home/usernameADM/.ssh/id_rsa.
Your public key has been saved in /home/usernameadm/.ssh/id_rsa.pub.
The key fingerprint is:
ae:da:f8:0b:b3:78:f1:2b:70:c9:3b:47:a9:01:45:fd
The key's randomart image is:
+--[ RSA 2048]----+
|    ...          |
|    . .          |
|    . .          |
|    .  E         |
|   o . .S        |
|   . * o.        |
|   ooB .         |
|   .**o.         |
|   ..+**o        |
+-----------------+
[usernameadm@JUMPHOST ~]$
```

- Copy public key generated above – **id_rsa.pub** to destination server in DMZ @ .ssh/authorized_keys. This will enable password-less authentication between jump server/bastion host to servers in DMZ. Example below:

```
[usernameadm@JUMPHOST ~]$ cat .ssh/id_rsa.pub | ssh usernameadm@hostname1 "mkdir .ssh && cat >>.ssh/authorized_keys"
or if .ssh directory is already existing on destination server in your home directory, just copy the public key using:
[usernameadm@ JUMPHOST ~]$ cat .ssh/id_rsa.pub | ssh usernameadm@hostname1 "cat >>.ssh/authorized_keys"
```

Skip above manual steps by running below scripts:

Login to appropriate Bastion/Jump host and following below:

➢ Change to **~/.ssh** dir

- ➢ Please run above steps in the document to create **authorized_keys** and **id_rsa.pub** files.
- ➢ cd ~/.ssh/
- ➢ "ls –lrt" must show below files:
  - ○ id_rsa
  - ○ id_rsa.pub
  - ○ authorized_keys

- ➢ create a file **"vi ssh_keys_copy.sh"** and copy contents from URL:
- ➢ chmod 755 **./ssh_keys_copy.sh**
- ➢ **./ssh_keys_copy.sh**

 Note:
>Provide the password when prompted
>list of servers are present under "**servers_list**" dir., pick a list based on requirement **or** create a new file

Example:
./ssh_keys_copy.sh "./servers_list/ servers_list_nextgen" "Pxxxxxxxadm   or   Vxxxxxx"

- ➢ Now we can able to login without password and able SSH from bastion/jump servers without asking for password…

Note: **In order to copy keys to all servers we should have "home dir." on servers, in case you are missing it please raise a request for UNIX team to create one…**

To check servers missing home dir., please run the following script as below **–** this doesn't require a home dir. in bastion host.

- ➢ **./homecheck.sh** "**server_list**(or) **server**"   "**uid**"

Above script will prints and also create a file under **/tmp_stage/"uid"/** with list of servers, which you can use for creating a request for UNIX team.