Create SSH Key

Contents [hide]

1 SSH Key for Access to Yale HPC Clusters
1.1 What is a SSH key ?
1.2 Why Use an SSH Key?
2 Creating your SSH Key
2.1 Required Software for your desktop or laptop
2.2 Choosing a passphrase
3 Send your public key to HPC
4 Creating SSH Key in Windows
4.1 Download PuTTY Software
4.2 PuTTYgen
5 Using your SSH Key with Windows PuTTY
6 Creating SSH Key in Linux
6.1 Generating SSH keys for RedHat Linux
6.1.1 RHEL 5 Instructions
6.1.2 RHEL 4 Instructions
6.2 Using ssh-keygen Linux
6.3 Linux Implementation Notes
6.3.1 file ownership and permissions
7 FAQ
7.1 Should I create a separate keys for my Mac/PC/Linux systems, or is there a way to use to same key across the different systems?
7.1.1 Step 1: Generation of the key Linux
7.1.2 Step 2: Copy the .ssh/id_rsa file to Windows & Import the key then Save it as a .ppk file for putty to use
7.1.3 Importing a Putty key to Linux

SSH Key for Access to Yale HPC Clusters [edit]

Starting May 2011 all users must use a SSH cryptographic key to access Yale HPC clusters.

All users will need to generate their own personal ssh key and send the public part of the key to hpc@yale.edu.

Users are recommend to send the file to hpc@yale.edu.

- Please include your netid and the cluster name your wish to access when sending your ssh public key.

What is a SSH key ? [edit]

SSH uses concept called "asymmetric public key encryption", a private key (secret code) and a related public key (different secret code) are created. Messages encrypted with the private key can only be un-encrypted with the related public key.

This is "one-way" encryption; you can give the public key to people you trust to decode your encrypted messages. The public key does not allow these people to "impersonate" your coded messages (they need the private key to encrypt the messages).

The private/public key method allows you to choose people (or computers) you trust to have your public key. These people (or computers) can verify you are who you claim to be by decrypting your messages with the public key you provided. If they can decrypt your message they know it was made with your private key.

- Do not share your private key. Do not copy your private key to computers you do not trust.

Why Use an SSH Key? [edit]

The public key encryption provides an extra level of security passwords do not.

A password challenge/response only verifies you are authorized for access. It does not authenticate you are who you claim to be. Just because you know the air-speed of an unladen swallow does not mean you are a really from Camelot (even castle guards know about swallows).

When sharing your public key, the other person or computer can authenicate you who you claim to be. Then any future messages unencrypted with that shared public key will be guarateed to come from the paired private key only you have. This assumes your private key is really private. If your private key is stolen or shared, this extra authentication is compromised.

Creating your SSH Key [edit]

Required Software for your desktop or laptop [edit]

You will need to install SSH software on your laptop or desktop computer. You will use this software to generate your private & public ssh key.

- Windows users are recommended to download & install PuTTY software
  - PuTTY can be downloaded from Yale Software website
- Macintosh & Linux systems will already have openssh software

Choosing a passphrase [edit]

You will need to enter a passphrase as part of generating your key. This passphrase should be different than your NetID or email password.

- Do not use your NetID password for your SSH key. Choose a different password.
- If you forget your password, you will have to start over and create a new SSH key. HPC staff cannot recover your SSH key passphrase.

Send your public key to HPC [edit]

Users are recommend to send the public key file to hpc@yale.edu.

- Please include your netid and the HPC cluster name when sending your ssh public key.
- Disclaimer: Only keys transferred from a valid yale email address will be accepted.

Creating SSH Key in Windows [edit]

Download PuTTY Software [edit]

- Windows users are recommended to download & install PuTTY software

- Install PuTTY software

PuTTYgen [edit]

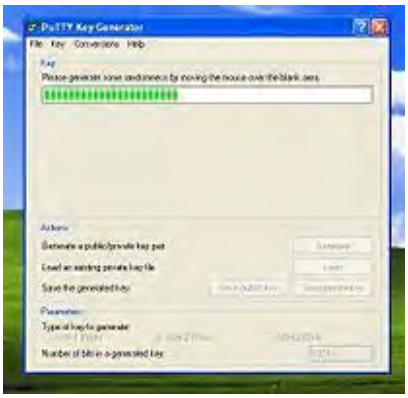
Instructions below cover:

- Use PuTTYgen to generate a SSH key
- Save PuTTY private key file with .ppk extension
- Copy-and-paste the generated OpenSSH key from PuTTYgen to notepad

- After installing PuTTY, select "PuTTYgen" from the windows start menu

- In PuTTY Key Generator Screen, click the "Generate" Button

- The Generate function requires you to move your mouse cursor around the screen...



- After the Key is generated you should enter a passhprase.
  - **Important** Do not use your NetID or email password. Choose a different password.

- After entering your passphrase, choose the "Save Private Key" button. This will save the private key to a file with a ".ppk" extension.
  - **Note** Remember the folder/directory where you save the private key. You will need this file to establish a connection to HPC clusters.

- After saving the private key, select (highlight) the text in the box "Public Key for pasting into OpenSSH authorized_keys file:"
- Copy-and-paste the highlighted text to a Notepad or other text editor. Save the Notepad file.

- Send saved notepad file to *hpc@yale.edu*
- Please include your netid and the HPC cluster name ywhen sending your ssh public key.

Outdated instructions for windows with PuTTY software:

- http://kb.siteground.com/article/How_to_generate_an_SSH_key_on_Windows_using_PuTTY.html
- http://siteadmin.gforge.inria.fr/ssh_windows.html
- https://www.racf.bnl.gov/docs/authentication/ssh/sshkeygenwin

Using your SSH Key with Windows PuTTY [edit]

After you have created your PuTTY SSH Key and received confirmation from HPC Staff. You can connect to your hpc cluster.

- **Note:** you will need the "private key file" you created to connect to HPC.
- From the windows start menu choose the "PuTTY" application. This will start the "PuTTY Configuration" screen

- Expand the "SSH" menu item in the left menu list. Choose the "Auth" sub-menu item.

- In the right part of the PuTTY screen, use the "Browse" button to select your private key file. The private key file should have a ".ppk" file extension.

- Choose the "Session" menu item at top of left menu list. In the box under "Host Name (or IP address)

enter the HPC cluster login hostname (eg. bulldogk.wss.yale.edu). Click "Open" button to make the connection.

- **Note:** the first time you connect to a HPC cluster with PuTTY it will popup a "Security Alert" screen. The alert prompts you to save the host key on the remote HPC machine. Click "Yes" to continue.

- You should be prompted to enter your username. Use your Yale NetID as username.

Creating SSH Key in Linux [edit]

OpenSSH includes command-line tool "ssh-keygen". This will generate the (private) key $HOME/.ssh/id_rsa and public key $HOME/.ssh/id_rsa.pub. The file id_rsa.pub is the one you want to send to Yale HPC.

- Note: Some SSH versions may create the files id_dsa & id_dsa.pub instead.

Generating SSH keys for RedHat Linux [edit]

If you are using Redhat with GNOME Desktop manager, these instructions outline how to create your ssh key. CentOS and Fedora linux will have similar steps.

RHEL 5 Instructions [edit]

- http://docs.redhat.com/docs/en-US/Red_Hat_Enterprise_Linux/5/html/Deployment_Guide/s2-openssh-generate-keypairs.html

RHEL 4 Instructions [edit]

- http://docs.redhat.com/docs/en-US/Red_Hat_Enterprise_Linux/4/html/System_Administration_Guide/Configuring_an_OpenSSH_Client-Generating_Key_Pairs.html

Using ssh-keygen Linux [edit]

Macintosh OS X users will have similar instructions

- Open a terminal (console) window.
- At the command-line enter the command "ssh-keygen"
  - full path for ssh-keygen: /usr/bin/ssh-keygen
- You will be prompted for the path to save the (private) key. The default is $HOME/.ssh/id_rsa
- You will be prompted for a passphrase
  - **Note:** Do not use your NetID or email password for your SSH passphrase. Choose a different password.
- The program should print the path to your public key, Ex)

```
Your identification has been saved in /home/testuser/.ssh/id_rsa.
Your public key has been saved in /home/testuser/.ssh/id_rsa.pub.
```

- Send the file $HOME/.ssh/id_rsa.pub to HPC at hpc@yale.edu.
- **Note:** The "ssh" command by default uses the private key named $HOME/.ssh/id_rsa or $HOME/.ssh/id_dsa. If you save your private key in a different location, use the command-line flag "ssh -i <keyfile>" See the ssh manpage for details.
- **Note:** OpenSSH check the permissions and ownership of the $HOME/.ssh directory and the key files. *ssh will simply ignore a private key file if it is accessible by others.* If you are having problems connecting to HPC clusters, check the permissions & ownerships. See the ssh manpage for proper settings.

Older instructions for linux with openssh software (ssh-keygen)

- http://kb.siteground.com/article/How_to_generate_an_SSH_key_in_Linux.html
- http://pkeck.myweb.uga.edu/ssh/
- http://oreilly.com/pub/h/66

Linux Implementation Notes [edit]

file ownership and permissions [edit]

Linux and OS X ssh are very strict about file ownership and permissions.

Permissions for should be as follows:

- your $HOME/.ssh directory should not be group- or world- readable

```
chmod 700 $HOME/.ssh
```

- your private key file $HOME/.ssh/id_rsa file should not be group- or world- readable

```
chmod 600 $HOME/.ssh/id_rsa
chmod 600 $HOME.ssh/id_dsa
```

- your public key file $HOME/.ssh/id_rsa.pub should not be group- or world- writeabke

```
chmod 644 $HOME/.ssh/id_rsa.pub
chmod 644 $HOME/.ssh/id_rsa.pub
```

FAQ [edit]

Should I create a separate keys for my Mac/PC/Linux systems, or is there a way to use to same key across the different systems? [edit]

We recommend just using one ssh and converting it to different formats. Below is an example of starting with a key from Linux and importing it to work under Windows with Putty.

Step 1: Generation of the key Linux [edit]

```
ssh-keygen -t rsa -b 2048 -C "My 2048 bit rsa key"
```

Step 2: Copy the .ssh/id_rsa file to Windows & Import the key then Save it as a .ppk file for putty to use [edit]

PuTTY: PUTTYGEN.EXE can import and convert some key file formats to the proper type. Follow these steps to do so:

Run PUTTYGEN.EXE Select the 'Import key' option from the 'Conversion' menu Select the private key that is to be imported, then click the 'Open' button At this point, you can save the key to the PuTTY .ppk format and the public key can either be copied and pasted from the interface or saved to a file as needed

Importing a Putty key to Linux [edit]

Similar to above, one could start out with a putty key and then import that key to linux

```
ssh-keygen -i -f putty-key.ppk > .ssh/id_rsa
```

Category: HOWTO

This page was last modified on 9 December 2012, at 11:08. This page has been accessed 1,886 times. Privacy policy About Yale HPC Wiki Disclaimers
Powered by MediaWiki