2014/07/29

SSH Keys Authentication

Configure SSH server to login with Keys Authentication. Create a private key for client and a public key for server to do it.

[1] Create key pair for each user, so login with a common user and work it like follows.

```
# create key pair
[cent@dlp ~]$ ssh-keygen -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (/home/cent/.ssh/id_rsa):   # Enter
Created directory '/home/cent/.ssh'.
Enter passphrase (empty for no passphrase):   # set passphrase (set no
passphrase to Enter with empty)
Enter same passphrase again:
Your identification has been saved in /home/cent/.ssh/id_rsa.
Your public key has been saved in /home/cent/.ssh/id_rsa.pub.
The key fingerprint is:
38:f1:b4:6d:d3:0e:59:c8:fa:1d:1d:48:86:f0:fe:74 cent@dlp.srv.world
The key's randomart image is:

[cent@dlp ~]$ mv ~/.ssh/id_rsa.pub ~/.ssh/authorized_keys
[cent@dlp ~]$ chmod 600 ~/.ssh/authorized_keys
```

[2] Transfer the secret key created on the Server to a Client, then it's possbile to login with keys authentication.

```
[cent@www ~]$ mkdir ~/.ssh
[cent@www ~]$ chmod 700 ~/.ssh

# copy the secret key to local ssh directory
[cent@www ~]$ scp cent@10.0.0.30:/home/cent/.ssh/id_rsa ~/.ssh/
cent@10.0.0.30's password:
id_rsa

[cent@www ~]$ ssh -i ~/.ssh/id_rsa cent@10.0.0.30
Enter passphrase for key '/home/cent/.ssh/id_rsa':   # passphrase
Last login: Wed Jul 30 21:37:19 2014 from www.srv.world
[cent@dlp ~]$   # just logined
```

[3] If you set "PasswordAuthentication" no, it's more secure.

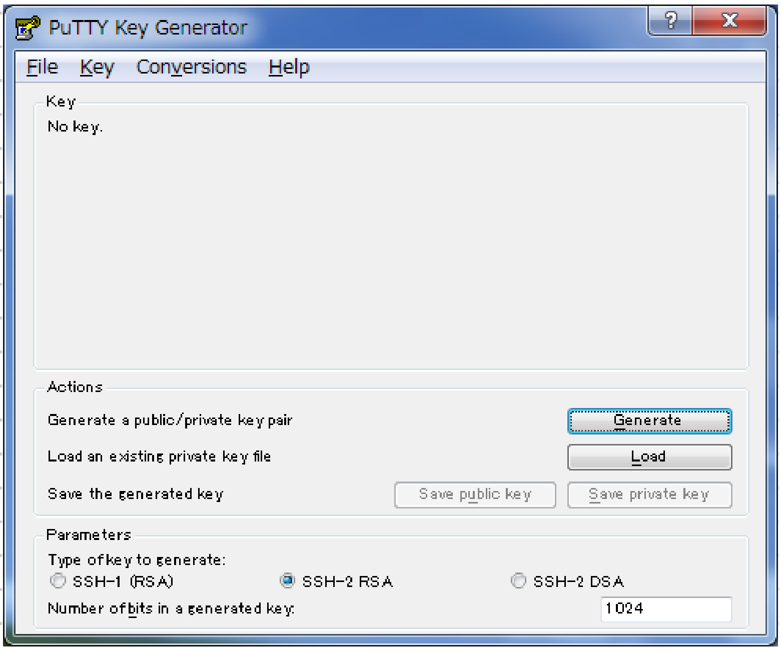
```
[root@dlp ~]# vi /etc/ssh/sshd_config

# line 78: turn to "no"
PasswordAuthentication no

# line 83: make sure the value is "no"
ChallengeResponseAuthentication no

# line 110: make sure the value is "yes"
UsePAM yes

[root@dlp ~]# systemctl restart sshd
```

SSH Keys Auth from Windows Client

It's the example to login to SSH server from Windows Client. It uses Putty on here.
Transfer a secret key to Windows Client first.

[4] Download "Puttygen.exe" from Putty Site and save it under the Putty

directory. Next execute it and click "Load" button.

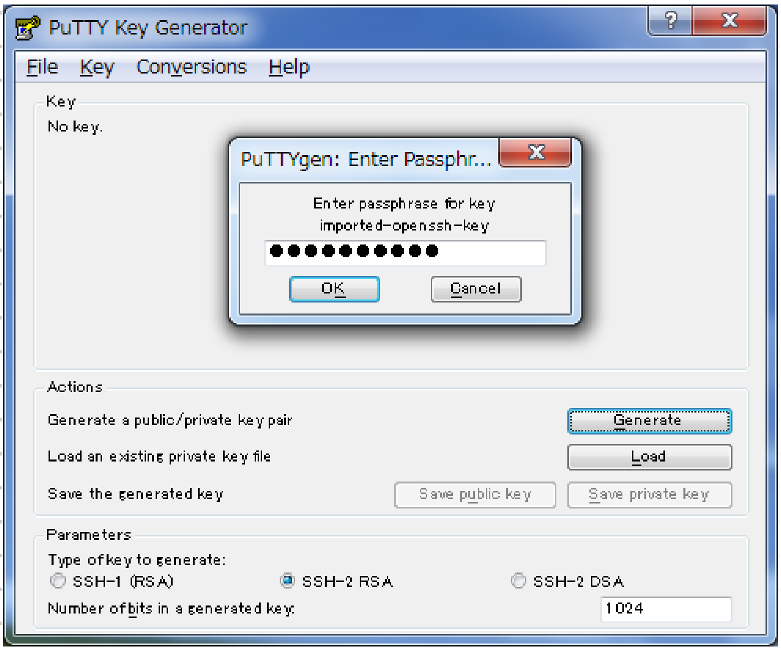


No key.

Type of key to generate:
○ SSH-1 (RSA) ● SSH-2 RSA ○ SSH-2 DSA

Number of bits in a generated key: 1024

[5] Specify the secret key which you downloaded, then passphrase is required like follows, answer it.


PuTTY Key Generator
File Key Conversions Help
Key
PuTTYgen: Enter Passphr...
OK
Cancel
Actions
Generate a public/private key pair
Generate
Load an existing private key file
Load
Save the generated key
Save public key
Save private key
Parameters

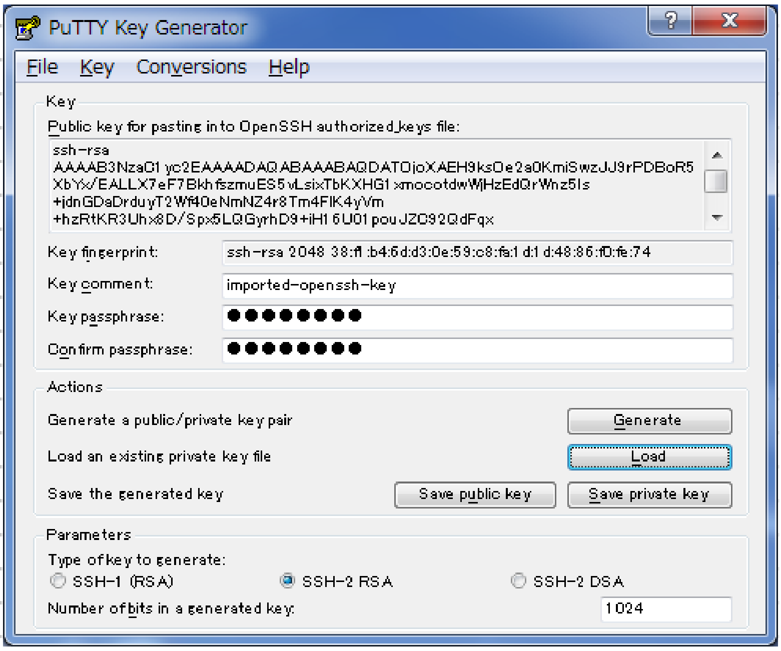
No key.

Enter passphrase for key imported-openssh-key
●●●●●●●●●●

Type of key to generate:
○ SSH-1 (RSA) ● SSH-2 RSA ○ SSH-2 DSA

Number of bits in a generated key: 1024

[6] Click "Save private key" button to save it under a folder you like with any file name you like.



Key

Public key for pasting into OpenSSH authorized_keys file:

```
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQDATOjoXAEH9ksOe2a0KmiSwzJJ9rPDBoR5
XbYx/EALLX7eF7BkhfszmuES5vLsixTbKXHG1xmocotdwWjHzEdQrWnz5ls
+jdnGDaDrduyT2Wf40eNmNZ4r8Tm4FlK4yVm
+hzRtKR3Uhx8D/Spx5LQGyrhD9+iH16U01pouJZC92QdFqx
```

Key fingerprint: ssh-rsa 2048 38:f1:b4:6d:d3:0e:59:c8:fa:1d:1d:48:86:f0:fe:74

Key comment: imported-openssh-key

Key passphrase: ●●●●●●●●

Confirm passphrase: ●●●●●●●●

Actions

Generate a public/private key pair

Load an existing private key file

Save the generated key

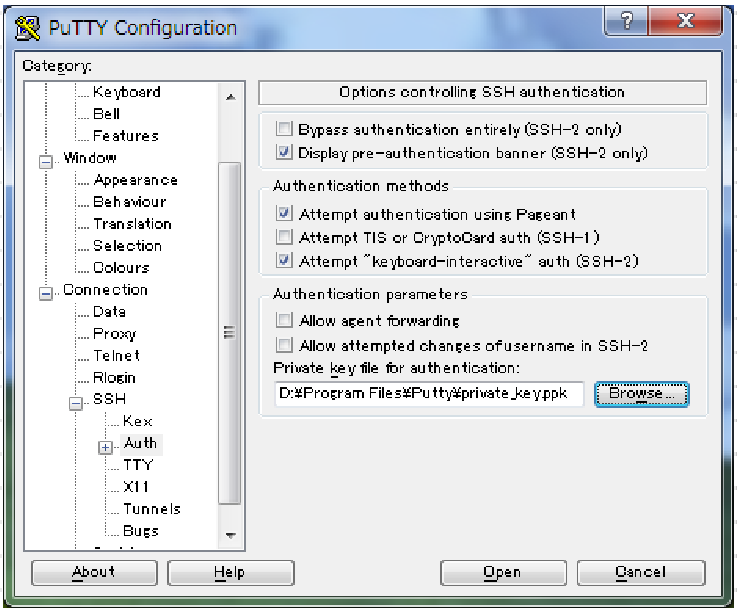
Parameters

Type of key to generate:

○ SSH-1 (RSA) ● SSH-2 RSA ○ SSH-2 DSA

Number of bits in a generated key: 1024

[7] Start Putty and open [Connection]-[SSH]-[Auth] on the left menu, then select the "private_key" which was just saved above.



Options controlling SSH authentication

□ Bypass authentication entirely (SSH-2 only)

☑ Display pre-authentication banner (SSH-2 only)

Authentication methods

☑ Attempt authentication using Pageant

□ Attempt TIS or CryptoCard auth (SSH-1)

☑ Attempt "keyboard-interactive" auth (SSH-2)

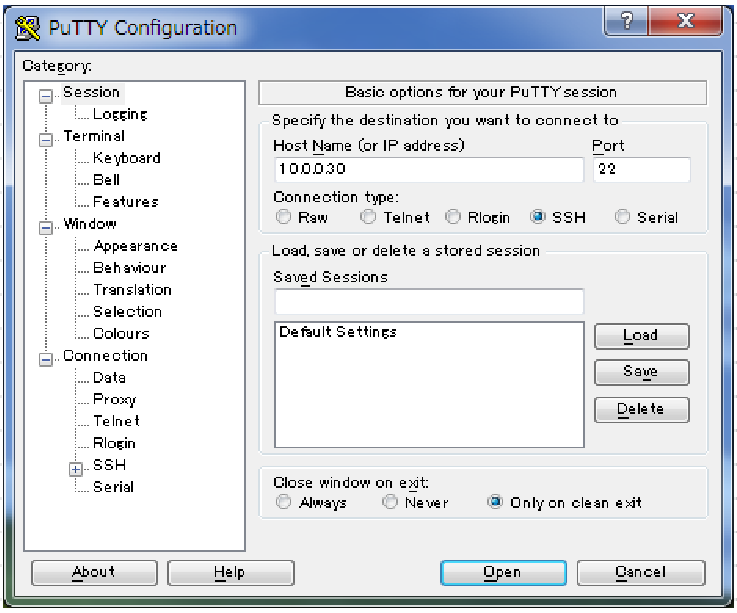
Authentication parameters

□ Allow agent forwarding

□ Allow attempted changes of username in SSH-2

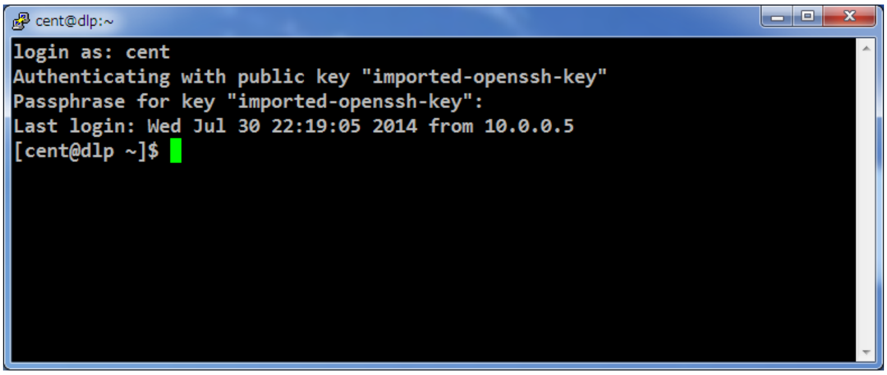
Private key file for authentication: D:¥Program Files¥Putty¥private_key.ppk

[8] Back to the [Session] on the left menu and connect to the SSH server.



Host Name (or IP address): 10.0.0.30
Port: 22
Connection type: ○ Raw ○ Telnet ○ Rlogin ● SSH ○ Serial
Close window on exit: ○ Always ○ Never ● Only on clean exit

[9] The passphrase is required to input, then answer it. If it's correct passphrase, it's possible to login normally like follows.



```
login as: cent
Authenticating with public key "imported-openssh-key"
Passphrase for key "imported-openssh-key":
Last login: Wed Jul 30 22:19:05 2014 from 10.0.0.5
[cent@dlp ~]$ 
```