

인스턴스 연결을 ID/PW 방식으로 변경하고 싶어요

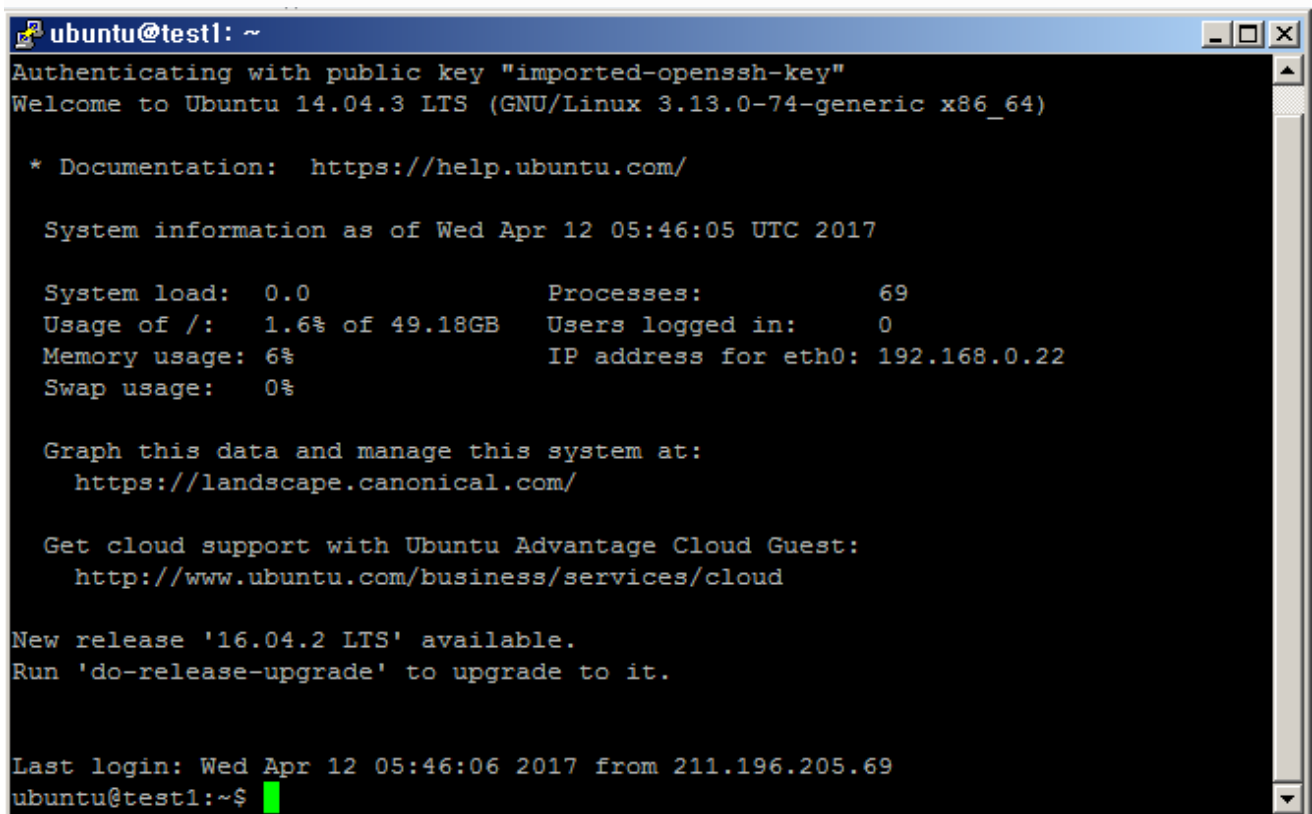
SSH 접속이나 싱글모드를 통해 인스턴스 접속 방식을 키 페어 인증 방식 대신에 ID/PW 방식으로 변경할 수 있습니다. 아래 내용을 참고하여 Ubuntu와 CentOS의 접속 방식을 ID/PW 방식으로 변경하세요.

- ▶ Ubuntu 키 페어가 있는 경우(SSH)
- ▶ Ubuntu 키 페어가 없는 경우(싱글모드)
- ▶ CentOS 키 페어가 있는 경우(SSH)
- ▶ CentOS 키 페어가 없는 경우(싱글모드)

Ubuntu 키 페어가 있는 경우(SSH)

키 페어가 있는 경우, SSH 접속을 통해 ID/PW 방식으로 접속 방식을 변경할 수 있습니다.

Step 1. PuTTY로 Linux 인스턴스 접속 및 편집창 진입



```
ubuntu@test1: ~
Authenticating with public key "imported-openssh-key"
Welcome to Ubuntu 14.04.3 LTS (GNU/Linux 3.13.0-74-generic x86_64)

* Documentation:  https://help.ubuntu.com/

System information as of Wed Apr 12 05:46:05 UTC 2017

System load:  0.0          Processes:      69
Usage of /:   1.6% of 49.18GB  Users logged in:  0
Memory usage: 6%          IP address for eth0: 192.168.0.22
Swap usage:   0%

Graph this data and manage this system at:
  https://landscape.canonical.com/

Get cloud support with Ubuntu Advantage Cloud Guest:
  http://www.ubuntu.com/business/services/cloud

New release '16.04.2 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Last login: Wed Apr 12 05:46:06 2017 from 211.196.205.69
ubuntu@test1:~$
```

· Linux 인스턴스 연결 후에 아래의 내용을 입력하여 편집창에 진입합니다.

```
$ sudo vi /etc/ssh/sshd_config
```

Step 2. 내용 수정

```
ubuntu@test1: ~
# similar for protocol version 2
HostbasedAuthentication no
# Uncomment if you don't trust ~/.ssh/known_hosts for RhostsRSAAuthentication
#IgnoreUserKnownHosts yes

# To enable empty passwords, change to yes (NOT RECOMMENDED)
PermitEmptyPasswords no

# Change to yes to enable challenge-response passwords (beware issues with
# some PAM modules and threads)
ChallengeResponseAuthentication no

# Change to no to disable tunnelled clear text passwords
PasswordAuthentication yes

# Kerberos options
#KerberosAuthentication no
#KerberosGetAFSToken no
#KerberosOrLocalPasswd yes
#KerberosTicketCleanup yes

# GSSAPI options
#GSSAPIAuthentication no
```

52, 26 58%

· 내용 수정

```
PasswordAuthentication : yes (yes로 수정하면 패스워드 방식의 인증을 허용합니다.)
```

· 변경 내용 저장

```
:$ :wq!
```

· SSH 재시작

```
$/etc/init.d/sshd restart
```

Ubuntu 키 페어가 없는 경우(싱글모드)

키 페어가 없는 경우, 싱글모드를 통해 ID/PW 방식으로 접속 방식을 변경할 수 있습니다. 매뉴얼의'Q. Root 비밀번호를 분실했어요 (Linux)'에서 '싱글모드 부팅' 을 참고하여 싱글 모드 접속 후에 아래의 작업을 진행하세요.

※ 싱글모드 부팅은 원격으로 작업할 수 없으며 인스턴스 콘솔에서만 작업할 수 있습니다.

Step 1. 싱글모드 편집창 진입

```
Connected (encrypted) to: QEMU (instance-00001da1) Send CtrlAltDel
c00000)
Loading, please wait...
[ 0.601811] systemd-udevd[120]: starting version 204
[ 0.652494] FDC 0 is a S82078B
[ 0.852151] usb 1-1: new full-speed USB device number 2 using uhci_hcd
[ 1.012671] usb 1-1: New USB device found, idVendor=0627, idProduct=0001
[ 1.012994] usb 1-1: New USB device strings: Mfr=1, Product=3, SerialNumber=5
[ 1.013320] usb 1-1: Product: QEMU USB Tablet
[ 1.013581] usb 1-1: Manufacturer: QEMU
[ 1.013867] usb 1-1: SerialNumber: 42
[ 1.320105] tsc: Refined TSC clocksource calibration: 2600.061 MHz
[ 1.653721] input: ImExPS/2 Generic Explorer Mouse as /devices/platform/i8042
/serio1/input/input3
Begin: Loading essential drivers ... done.
Begin: Running /scripts/init-premount ... done.
Begin: Mounting root file system ... Begin: Running /scripts/local-top ... done.
Begin: Running /scripts/local-premount ... done.
[ 2.012712] EXT4-fs (vda1): mounted filesystem with ordered data mode. Opts:
(null)
Begin: Running /scripts/local-bottom ... done.
done.
Begin: Running /scripts/init-bottom ... done.
bash: cannot set terminal process group (-1): Inappropriate ioctl for device
bash: no job control in this shell
root@(none):/# _
```

· 편집창 진입 명령어

```
$ vi /etc/ssh/sshd_config
```

Step 2. 내용 수정

```
#IgnoreUserKnownHosts yes
# To enable empty passwords, change to yes (NOT RECOMMENDED)
PermitEmptyPasswords no
# Change to yes to enable challenge-response passwords (beware issues with
# some PAM modules and threads)
ChallengeResponseAuthentication no
# Change to no to disable tunnelled clear text passwords
PasswordAuthentication yes
# Kerberos options
#KerberosAuthentication no
#KerberosGetAFSToken no
#KerberosOrLocalPasswd yes
#KerberosTicketCleanup yes
# GSSAPI options
#GSSAPIAuthentication no
#GSSAPICleanupCredentials yes
X11Forwarding yes
X11DisplayOffset 10
-- INSERT --
```

52,27

64%

· 내용 수정

```
PasswordAuthentication : yes (yes로 수정하면 패스워드 방식의 인증을 허용합니다.)
```

· 변경 내용 저장

```
:$ :wq!
```

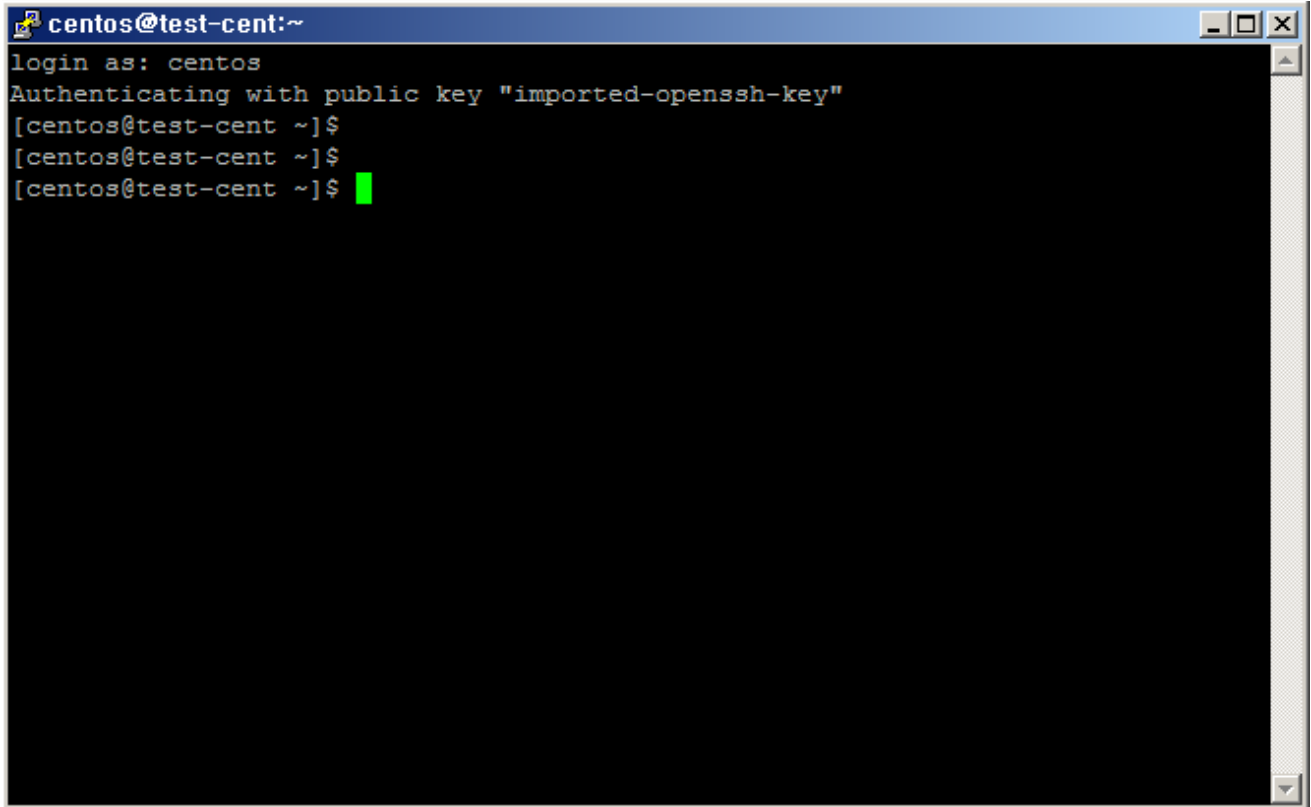
· SSH 재시작

```
$/etc/init.d/sshd restart
```

CentOS 키 페어가 있는 경우(SSH)

키 페어가 있는 경우, SSH 접속을 통해 ID/PW 방식으로 접속 방식을 변경합니다. 'Linux 인스턴스 연결 (PuTTY)' 를 참고하여 Linux 인스턴스에 연결하세요.

Step 1. PuTTY로 CentOS 인스턴스 접속 및 편집창 진입

A terminal window titled 'centos@test-cent:~' showing the SSH login process. The text in the terminal is: 'login as: centos', 'Authenticating with public key "imported-openssh-key"', and three lines of '[centos@test-cent ~]\$' with a green cursor at the end of the last line.

```
centos@test-cent:~
login as: centos
Authenticating with public key "imported-openssh-key"
[centos@test-cent ~]$
[centos@test-cent ~]$
[centos@test-cent ~]$
```

· 편집창 진입 명령어

```
$ sudo vi /etc/ssh/sshd_config
```

Step 2. 내용 수정

```
centos@test-cent:~
# but this is overridden so installations will only check .ssh/authorized_keys
AuthorizedKeysFile .ssh/authorized_keys

#AuthorizedPrincipalsFile none

#AuthorizedKeysCommand none
#AuthorizedKeysCommandUser nobody

# For this to work you will also need host keys in /etc/ssh/ssh_known_hosts
#RhostsRSAAuthentication no
# similar for protocol version 2
#HostbasedAuthentication no
# Change to yes if you don't trust ~/.ssh/known_hosts for
# RhostsRSAAuthentication and HostbasedAuthentication
#IgnoreUserKnownHosts no
# Don't read the user's ~/.rhosts and ~/.shosts files
#IgnoreRhosts yes

# To disable tunneled clear text passwords, change to no here!
#PasswordAuthentication yes
#PermitEmptyPasswords no
PasswordAuthentication yes
```

· 내용 수정

```
PasswordAuthentication : yes (yes로 수정하면 패스워드 방식의 인증을 허용합니다.)
```

· 변경 내용 저장

```
:$ :wq!
```

· SSH 재시작

```
$/etc/init.d/sshd restart
```

CentOS 키 페어가 없는 경우(싱글모드)

키 페어가 없는 경우, 싱글모드를 통해 ID/PW 방식으로 접속 방식을 변경할 수 있습니다. 매뉴얼의'Q. Root 비밀번호를 분실했어요 (Linux)'에서 '싱글모드 부팅' 을 참고하여 싱글 모드 접속 후에 아래의 작업을 진행하세요.

※ 싱글모드 부팅은 원격으로 작업할 수 없으며 인스턴스 콘솔에서만 작업할 수 있습니다.

Step 1. 싱글모드 편집창 진입

```
Connected (encrypted) to: QEMU (instance-00001fff) Send CtrlAltDel
udev: starting version 147
piix4_smbus 0000:00:01.3: SMBus Host Controller at 0xb100, revision 0
[ OK ]
Setting hostname test-5.novalocal: [ OK ]
Checking filesystems
/dev/vda1: clean, 21805/3276800 files, 446112/13106775 blocks
[ OK ]
Remounting root filesystem in read-write mode: [ OK ]
Mounting local filesystems: [ OK ]
Enabling /etc/fstab swaps: [ OK ]
growroot: NOCHANGE: partition 1 is size 104854207. it cannot be grown
Welcome to CentOS
Starting udev: udevd[369]: can not read '/etc/udev/rules.d/75-persistent-net-generator.rules'
udev[369]: can not read '/etc/udev/rules.d/75-persistent-net-generator.rules'
[ OK ]
Setting hostname test-5.novalocal: [ OK ]
Checking filesystems
/dev/vda1: clean, 21805/3276800 files, 446112/13106775 blocks
[ OK ]
Remounting root filesystem in read-write mode: [ OK ]
Mounting local filesystems: [ OK ]
Enabling /etc/fstab swaps: [ OK ]
[root@test-5 /]#
```

· 편집창 진입 명령어

```
$ vi /etc/ssh/sshd_config
```

Step 2. 내용 수정

```
#RhostsRSAAuthentication no
# similar for protocol version 2
#HostbasedAuthentication no
# Change to yes if you don't trust ~/.ssh/known_hosts for
# RhostsRSAAuthentication and HostbasedAuthentication
#IgnoreUserKnownHosts no
# Don't read the user's ~/.rhosts and ~/.shosts files
#IgnoreRhosts yes

# To disable tunneled clear text passwords, change to no here!
#PasswordAuthentication no
#PermitEmptyPasswords no
PasswordAuthentication yes

# Change to no to disable s/key passwords
#ChallengeResponseAuthentication yes
ChallengeResponseAuthentication no

# Kerberos options
#KerberosAuthentication no
#KerberosOrLocalPasswd yes
#KerberosTicketCleanup yes
#KerberosGetAFSToken no
#KerberosUseKuserok yes
-- INSERT --
```

· 내용 수정

PasswordAuthentication : yes (yes로 수정하면 패스워드 방식의 인증을 허용합니다.)

· 변경 내용 저장

\$:wq!

· SSH 재시작

\$ /etc/init.d/sshd restart