SFTP 환경 구축

구축 목적

: SSH의 파일전송 버전으로 같은 22 포트를 사용하며, 실무에서 많이 사용하는 파일전송 방법으로, 보안상으로 안전하게 파일전송을 하기 위하여

SFTP 환경 구축

```
# rpm -qa | grep ssh
libssh2-1.4.3-10.el7_2.1.x86_64
openssh-server-7.4p1-21.el7.x86_64
openssh-clients-7.4p1-21.el7.x86_64
openssh-7.4p1-21.el7.x86_64
```

< 1. SSH / SFTP Port 분리 >

- ssh : 22
- sftp : 2222

```
# vi /etc/ssh/sshd_config
---------------------------------------
17 Port 22
18 Port 2222
( Port 주석부분 제거하고 2222 포트 추가 )

162 Match LocalPort 2222
163         AllowTCPForwarding no
164         X11Forwarding no
165         ForceCommand internal-sftp
( 2222번 포트를 sftp 로 사용 )
---------------------------------------

# systemctl restart sshd

# netstat -plunt
-------------------------------------------------------------------------------
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
PID/Program name
tcp        0      0 0.0.0.0:2222            0.0.0.0:*               LISTEN
26108/sshd
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN
26108/sshd
tcp        0      0 127.0.0.1:25            0.0.0.0:*               LISTEN
1727/master
```

```
tcp6       0      0 :::2222                 :::*                    LISTEN
26108/sshd
tcp6       0      0 :::22                   :::*                    LISTEN
26108/sshd
tcp6       0      0 ::1:25                  :::*                    LISTEN
1727/master
udp        0      0 0.0.0.0:5353            0.0.0.0:*
586/avahi-daemon: r
udp        0      0 127.0.0.1:323           0.0.0.0:*
594/chronyd
udp        0      0 0.0.0.0:37212           0.0.0.0:*
586/avahi-daemon: r
udp        0      0 0.0.0.0:17411           0.0.0.0:*
1160/dhclient
udp        0      0 0.0.0.0:68              0.0.0.0:*
1160/dhclient
udp6       0      0 :::48334                :::*
1160/dhclient
udp6       0      0 ::1:323                 :::*
594/chronyd

( 정상적으로 22번포트와 2222포트 나뉘어서 적용되었는지 확인 )
--------------------------------------------------------------------------------
```

< 2. 관리자 계정 - Xeno 계정 생성 >

- 22번 port로 접근 가능한 계정
- root 권한 부여

```
# useradd xeno
# passwd

# sudo -i
# visudo
---------------------------------------
76 ##
77 ## User privilege specification
78 ##
79 root ALL=(ALL) ALL
80 xeno ALL=(ALL) ALL
---------------------------------------
( root 밑에 새로운 사용자 xeno 추가해서 ALL 권한 부여 )
```

< 3. root 직접 접근 불가 >

- ssh , sftp

```
# vi /etc/ssh/sshd_config

49 PermitRootLogin no
```

< 4. sftp 전용 그룹 생성 및 chroot 적용 >

- 그룹명 : sftpUsers
- 사용자 2명
- 그룹 사용자들의 쉘 로그인 불가 설정 (/sbin/nologin)
- 해당 그룹 사용자들만 sftp (2222) 포트로 접속 가능
- ssh (22) 포트는 사용불가
- 각 home 디렉토리는 /data/[username]

```
# groupadd sftpUsers
# vi /etc/ssh/sshd_config
--------------------------------------------------------------------------------
149 #Subsystem sftp /usr/libexec/openssh/sftp-server
150 Subsystem sftp internal-sftp

169 Match Group sftpUsers
170         ChrootDirectory /data/%u
171         ForceCommand internal-sftp
172         X11Forwarding no
173         AllowTCPForwarding no
--------------------------------------------------------------------------------
( sftpUsers 그룹에 chroot 설정으로 /data/%u(유저 홈 디렉토리) 를 루트 디렉토리로 설정
하여 상위폴더 접근 제한 )
( chroot 설정으로 인하여 SSH 사용 불가 )


# useradd -s /sbin/nologin -G sftpUsers sftpxeno1
# useradd -s /sbin/nologin -G sftpUsers sftpxeno2
( 쉘을 /sbin/nologin 으로 추가하여 sftp전용 그룹에 계정 2개 생성 )
# passwd sftpxeno1
# passwd sftpxeno2

# usermod -d /data/sftpxeno1 sftpxeno1
# usermod -d /data/sftpxeno2 sftpxeno2
( sftp 전용계정들의 홈 디렉토리 변경 )
# cat /etc/passwd

# cp -r /home/sftpxeno1 /data/sftpxeno1
# cp -r /home/sftpxeno2 /data/sftpxeno2
( 변경한 홈 디렉토리로 원래 디렉토리 내용들 복사해서 가져오기 )

# cd /data
# chmod 755 sftpxeno1
# chmod 755 sftpxeno2
# chown root.sftpxeno1 sftpxeno1
```

```
# chown root.sftpxeno2 sftpxeno2
( SFTP 보안을 위해 디렉토리에 권한과 소유자 설정 )

# mkdir -p /data/sftpxeno1/www
# mkdir -p /data/sftpxeno2/www
( 위에서 쓰기작업을 제거하여 디렉토리 생성이 불가하기 때문에, 디렉토리 생성용으로 추가
디렉토리 생성 )

# cd sftpxeno1
# chmod 775 www
# chown root.sftpUsers www
# cd..
# cd sftpxeno1
# chmod 775 www
# chown root.sftpUsers www
( 쓰기작업을 추가한 권한과 소유자 설정 )
```

- TEST : SecureFX나 FileZilla 등으로 Chroot 설정 잘 되어있는지 확인 !!

< 5. sftp 접근 시 패스워드가 아닌 KEY로 접속 >

- sftp 그룹 사용자들만 패스워드로 접속 불가 설정
- KEY로만 접속 가능하게 설정

- sftpxeno1 계정 -

```
# mkdir ~/.ssh
# chmod 700 .ssh
( 키파일 전용 디렉토리 생성 , *꼭 유저의 홈디렉토리 밑에 생성 ! )

# cd .ssh
# ssh-keygen -t rsa -b 2048 -f my-key
enter enter
( my-key (개인키) , my-key.pub (공개키) 2개의 키가 만들어짐 )

# mv my-key.pub authorized_keys
# chmod 600 authorized_keys
```

- sftpxeno2 계정 -

```
# mkdir ~/.ssh
# chmod 700 .ssh

# cd .ssh
# ssh-keygen -t rsa -b 2048 -f my-key2
enter enter
( my-key2 (개인키) , my-key2.pub (공개키) 2개의 키가 만들어짐 )
```

```
# mv my-key2.pub authorized_keys
# chmod 600 authorized_keys
```

- xeno 계정 -

```
# mkdir ~/.ssh
# chmod 700 .ssh

# cd .ssh
# ssh-keygen -t rsa -b 2048 -f my-key-admin
enter enter
( my-key-admin (개인키) , my-key-admin.pub (공개키) 2개의 키가 만들어짐 )

# mv my-key-admin.pub authorized_keys
# chmod 600 authorized_keys

# vi /etc/ssh/sshd_config
--------------------------------------------------------------------------------
    162 Match LocalPort 2222
    163         AllowTCPForwarding no
    164         X11Forwarding no
    165         ForceCommand internal-sftp
    166         PasswordAuthentication no
    167         PubkeyAuthentication yes
    168
    169 Match Group sftpUsers
    170         ChrootDirectory /data/%u
    171         ForceCommand internal-sftp
    172         X11Forwarding no
    173         AllowTCPForwarding no
    174         PasswordAuthentication no
    175         PubkeyAuthentication yes
--------------------------------------------------------------------------------
( 2222번 포트와 sftpUsers 그룹의 접속에 대해서 패스워드 접속 불가 설정과 공개키 인증 방
식을 허용하는 설정을 추가해줌 )
```

TEST

: FileZilla 실행 후 Client로 my-key(개인키) 다운로드 -> 사이트 설정에서 각 계정별로 정리 -> 일반 - 로그온 유형 키 파일로 변경 -> 개인키 등록 후 연결

- 연결 잘되고 업로드 다운로드 잘되는지 확인!!
- 오류 발생시 /var/log/secure 파일 참고해서 수정!!
- 사용자 연결 중 bash-4.2$로 이상하게 접속될때 /etc/skel 내용 복사해서 홈디렉토리에 추가!!

★ 정상적으로 작동된다면 SFTP 환경 구축 완료 ! ★

참조

- https://studyforus.tistory.com/243
- http://www.iwav.co.kr/527