리눅스 원격 접속

SSH(Secure Shell) 란

- 원격지로 연결을 가능하도록 하는 네트워크 접속 도구이다.
- 리눅스 시스템 자체에 있는 터미널 클라이언트는 원격 접속이 아니기 때문에 SSH 프로토콜을 사용하지 않는다.
- SSH 는 보안을 중요시한 프로토콜이다.

Telnet 과 SSH

- Telnet 은 보안이 취약함
- SSH 프로토콜을 사용했을 때 일반 문자열이 출력되면 식별할 수 없는 내용으로 패킷이 보내진다. 따라서 암호화된 통신을 가능하게 하여 누군가 정보를 탈취하여도 쉽게 해석하지 못하도록 보안성을 향상 시킨다.
- Telnet 프로토콜을 사용했을 때는 일반 문자열이 출력되었을 때 별도의 암호화가 되지 않는다. 이로 인해 패스워드 등의 보안 문자열이 입력 또는 출력될 때 탈취자가 파악할 수 있다.

원격 서버에서 SSH 프로토콜을 사용하여 터미널에 접속하기 위한 조건

- 22 번 tcp 포트 사용 가능
- SSH 서버 프로그램의 설치 및 구동
- SSH 프로토콜로 접속할 수 있는 SSH 클라이언트 필요

ssh 설치

- 설치된 내역 확인

```
# rpm -qa | grep openssh-server
openssh-server-6.6.1p1-31.el7.x86_64
```

- 설치가 되어있지 않으면 yum 또는 rpm 으로 설치

```
# yum install openssh*
```

- 방화벽 확인

```
# firewall-cmd --get-active-zone
public
  interfaces: ens33
# firewall-cmd --list-all --zone public
public (active)
  target: default
  icmp-block-inversion: no
  interfaces: ens33
  sources:
  services: dhcpv6-client ssh
  ports:
  protocols:
  masquerade: no
  forward-ports:
  sourceports:
  icmp-blocks:
  rich rules:
```

방화벽에서 ssh 서비스 또는 22 번포트가 열려있지 않은 경우 다음과 같이 허용

```
# firewall-cmd --zone=drop --add-port=22/tcp --permanent
```

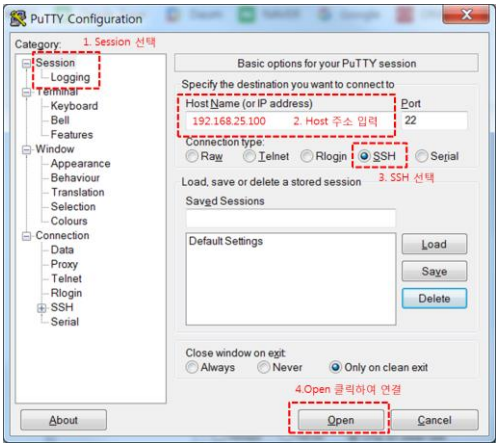
- ssh 서비스 구동

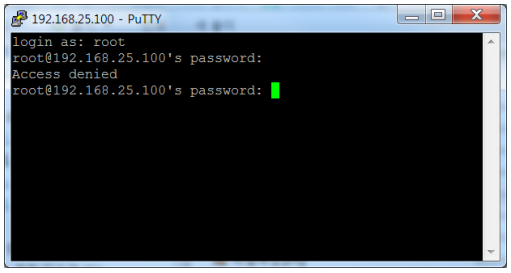
```
# systemctl start sshd.service
```

- ssh 명령을 사용하여 원격지 서버에서 접속

```
# ssh   192.168.25.100
The authenticity of host '192.168.25.100 (192.168.25.100)' can't be established.
ECDSA key fingerprint is 81:0c:2e:f6:78:d3:84:9a:41:59:8a:53:84:c0:3a:af.
Are you sure you want to continue connecting (yes/no)? yes      -- 최초 접속 시 호스트 키 검증
Warning: Permanently added '192.168.25.100' (ECDSA) to the list of known hosts.
root@192.168.25.100's password:
...
[root@RHEL7-SVR ~]#
```

- putty(외부 터미널 클라이언트 중 하나) 로 접속





SSH 서버 설정 파일 : /etc/ssh/sshd_config

- SSH 프로토콜 접속 시의 규칙을 지정하거나 서버의 연결 설정을 정의한다.
- SSH 포트 변경
- 접속 허용 클라이언트 및 패스워드 입력 시도 횟수 제한 설정
- 패스워드, 공개 키 사용자 인증 설정
- 접속 로그, 배너 메세지

/etc/ssh/sshd_config 파일을 수정하여 root 계정에 대한 직접적인 로그인 차단

1. 다음과 같이 /etc/ssh/sshd_config 파일의 PermitRootLogin 값 수정

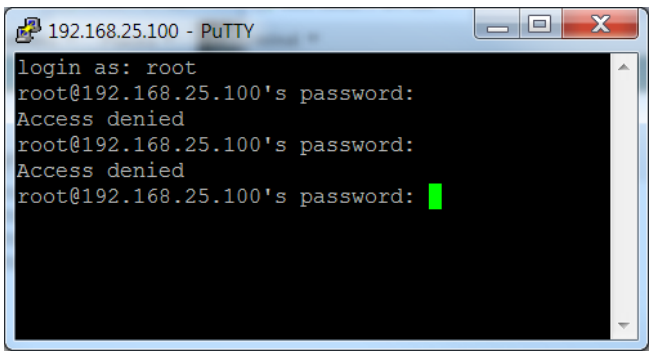
```
PermitRootLogin no
```

- yes : root 로그인 허용. 보안상 권장하지 않음
- no : root 로그인 차단

2. sshd service restart

```
# systemctl   restart   sshd.service
```

3. SSH 로 접속 시도



→ Access denied.

로그인 시 보안을 강화할 수 있는 값

- LoginGraceTime 2m

  로그인 시도 시 사용자 인증을 요청 받을 수 있는 최대 시간이며 인증 도중 이 시간이 초과되면 연결이 끊긴다. 기본 2m(2 분)

- MaxAuthTries 6

  개정 당 최대 연결 시도 횟수

- MaxSessions 10

  SSH 연결을 허용할 최대 클라이언트 수

방화벽(firewalld) 문제 해결하기

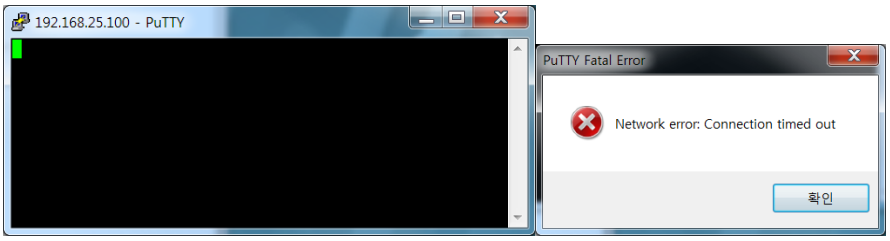
현재 설정되어 있는 default zone 에 ssh service 또는 22 번 포트가 추가 되지 않은 경우

- default zone 인 public 에 설정되어 있던 ssh 서비스 삭제 후 접속 시도

```
# firewall-cmd --get-active-zone
public
  interfaces: ens33
# firewall-cmd --zone=public --remove-service=ssh        → 원래 있던 ssh service 삭제
success
# firewall-cmd --list-all --zone public
public (active)
  target: default
  icmp-block-inversion: no
  interfaces: ens33
  sources:
  services: dhcpv6-client ftp
  ports:
  protocols:
  masquerade: no
  forward-ports:
  sourceports:
  icmp-blocks:
```

rich rules:

Putty 로 접속 시도



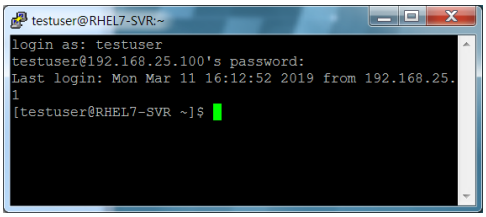
→ 연결 안됨

- 해결 방법 : ssh 서비스 추가 또는 22 번 포트 추가

```
# firewall-cmd --zone=public --add-service=ssh
success

또는

# firewall-cmd --zone=public --add-port=22/tcp
success
```



→ 접속 됨

telnet 을 이용한 원격접속

- telnet 은 ssh 와 달리 암호화되지 않은 원격 통신 방법이다.

telnet-server rpm 설치

 # rpm -qa | grep telnet-server

 # yum install telnet-server

Loaded plugins: langpacks, product-id, search-disabled-repos, subscription-
: manager

This system is not registered to Red Hat Subscription Management. You can use subscription-manager to register.

Resolving Dependencies

--> Running transaction check

---> Package telnet-server.x86_64 1:0.17-60.el7 will be installed

--> Finished Dependency Resolution

```
Dependencies Resolved

================================================================================
 Package                Arch           Version                 Repository          Size
================================================================================
Installing:
 telnet-server          x86_64         1:0.17-60.el7           InstallMedia        40 k

Transaction Summary
================================================================================
Install  1 Package

Total download size: 40 k
Installed size: 55 k
Is this ok [y/d/N]: y
Downloading packages:
Running transaction check
Running transaction test
Transaction test succeeded
Running transaction
  Installing : 1:telnet-server-0.17-60.el7.x86_64                           1/1
  Verifying  : 1:telnet-server-0.17-60.el7.x86_64                           1/1

Installed:
  telnet-server.x86_64 1:0.17-60.el7

Complete!
```

telnet 서비스 등록 및 시작

```
# systemctl status telnet
Unit telnet.service could not be found.
# systemctl status telnet.socket
* telnet.socket - Telnet Server Activation Socket
   Loaded: loaded (/usr/lib/systemd/system/telnet.socket; disabled; vendor preset: disabled)
   Active: inactive (dead)
     Docs: man:telnetd(8)
   Listen: [::]:23 (Stream)
 Accepted: 0; Connected: 0
# systemctl start telnet.socket
# systemctl enable telnet.socket
Created symlink from /etc/systemd/system/sockets.target.wants/telnet.socket to
/usr/lib/systemd/system/telnet.socket.
```

```
# systemctl status telnet.socket
* telnet.socket - Telnet Server Activation Socket
    Loaded: loaded (/usr/lib/systemd/system/telnet.socket; enabled; vendor preset: disabled)
    Active: active (listening) since Mon 2019-03-11 20:25:31 KST; 34s ago
      Docs: man:telnetd(8)
    Listen: [::]:23 (Stream)
 Accepted: 0; Connected: 0

Mar 11 20:25:31 RHEL7-SVR systemd[1]: Listening on Telnet Server Activation...t.
Mar 11 20:25:31 RHEL7-SVR systemd[1]: Starting Telnet Server Activation Socket.
Hint: Some lines were ellipsized, use -l to show in full.
```

telnet 을 이용하여 원격 접속

- Putty 접속 시도 – 연결 안됨
- 방화벽 확인 및 Telnet 접속이 가능하도록 설정

```
# firewall-cmd --list-all --zone public
public (active)
  target: default
  icmp-block-inversion: no
  interfaces: ens33
  sources:
  services: dhcpv6-client ftp          -- telnet 서비스 또는 telnet port(23) 이 없음
  ports: 21/tcp 22/tcp
  protocols:
  masquerade: no
  forward-ports:
  sourceports:
  icmp-blocks:
  rich rules:

# firewall-cmd --zone=public --add-service=telnet
success
또는
# firewall-cmd --zone=public --add-port=23/tcp
```

```
# firewall-cmd --list-all --zone public
public (active)
  target: default
  icmp-block-inversion: no
  interfaces: ens33
  sources:
  services: dhcpv6-client ftp telnet
  ports: 21/tcp 22/tcp
  protocols:
  masquerade: no
  forward-ports:
  sourceports:
  icmp-blocks:
  rich rules:
```

- putty 접속 시도 - 성공